Topics in metric geometry, combinatorial geometry, extremal combinatorics and additive combinatorics

Luka Milićević

Trinity College
and
Department of Pure Mathematics and Mathematical Statistics
University of Cambridge

This dissertation is submitted for the degree of
Doctor of Philosophy

June, 2017

Topics in metric geometry, combinatorial geometry, extremal combinatorics and additive combinatorics

Luka Milićević

Abstract

In this thesis, we consider several combinatorial topics, belonging to the areas appearing in the thesis title.

Given a non-empty complete metric space (X, d), a family of n continuous maps $f_1, f_2, \dots, f_n \colon X \to X$ is a *contractive family* if there exists $\lambda < 1$ such that for any $x, y \in X$ we have $d(f_i(x), f_i(y)) \leq \lambda d(x, y)$ for some i. In the first part of the thesis, we

(i) construct a compact metric space (X, d) with a contractive family $\{f, g\}$, such that no word in f, g has a fixed point, and

(ii) show that if $\{f, g, h\}$ is a contractive family such that f, g, h commute and $\lambda < 10^{-23}$, then they have a common fixed point.

The proofs of these two statements are combinatorial in nature. For **(i)**, we introduce a new concept of a *diameter space*, leading us naturally to a combinatorial problem about constructing certain sets of words. The result **(ii)** has a Ramsey-theoretic flavour, and is based on studying the local and global structure of a related metric space on $\mathbb{N}^3$. These answer questions of Austin and Stein.

In the second part, we prove that given any 4-colouring of the edges of K_n, we can find sets X, Y, Z and colours x, y, z (not necessarily distinct) such that $X \cup Y \cup Z = V(K_n)$, and each of $K_n[X, x], K_n[Y, y]$ and $K_n[Z, z]$ has diameter bounded by 160 (where $K_N[X, x]$ denotes the edges in X that have colour x). This theorem is motivated by the work on commuting contractive families, where the analogous statement for 3 colours played a crucial role, and by the Lovász-Ryser conjecture. The proof is in the spirit of structural graph theory. The key point is the fact that the diameters are bounded. This strengthens a result of Gyárfás, who proved the same but with no diameter bounds (i.e. just with the sets being connected).

Recall that a set of points in $\mathbb{R}^d$ is in *general position* if no $d+1$ lie on a common hyperplane. Similarly, we say that a set of points in $\mathbb{R}^d$ is in *almost general position* if no $d+2$ lie on a common hyperplane. In the third part, we answer a question of Füredi, by showing that, for each d, there are sets of n points in almost general position in $\mathbb{R}^d$, whose subsets in general position have size at most $o(n)$. The proof is based on algebraically studying to what extent polynomial maps preserve cohyperplanarity, and an application of the density version of the Hales–Jewett theorem.

In the fourth part, we answer a question of Nathanson in additive combinatorics about sums, differences and products of sets in $\mathbb{Z}_N$ (the integers modulo N). For all $\epsilon > 0$ and $k \in \mathbb{N}$, we construct a subset $A \subset \mathbb{Z}_N$ for some N, such that $|A^2 + kA| \leq \epsilon N$, while $A - A = \mathbb{Z}_N$. (Here $A - A = \{a_1 - a_2 : a_1, a_2 \in A\}$ and $A^2 + kA = \{a_1 a_2 + a_1' + a_2' + \cdots + a_k' : a_1, a_2, a_1', a_2', \ldots, a_k' \in A\}$.) We also prove some extensions of this result. Among other ingredients, the proof also includes an application of a quantitative equidistribution result for polynomials.

In the final part, we consider the Graham-Pollak problem for hypergraphs. Let $f_r(n)$ be the minimum number of complete r-partite r-graphs needed to partition the edge set of the complete r-uniform hypergraph on n vertices. We disprove a conjecture that $f_4(n) \geq (1 + o(1))\binom{n}{2}$, by showing that $f_4(n) \leq \frac{14}{15}(1 + o(1))\binom{n}{2}$. The proof is based on the relationship between this problem and a problem about decomposing products of complete graphs, and understanding how the Graham-Pollak theorem (for graphs) affects what can happen here.

Declaration

This dissertation is the result of my own work and includes nothing which is the outcome of work done in collaboration except for Chapter 5, which represents joint work with Imre Leader and Ta Sheng Tan. It is not substantially the same as any that I have submitted, or, is being concurrently submitted for a degree or diploma or other qualification at the University of Cambridge or any other University or similar institution. I further state that no substantial part of my dissertation has already been submitted, or, is being concurrently submitted for any such degree, diploma or other qualification at the University of Cambridge or any other University or similar institution. It does not exceed the prescribed word limit for the relevant Degree Committee.

Acknowledgements

I am very grateful to my supervisor, Prof Imre Leader, for all the stimulating mathematical discussions and for the helpful advice. He was a truly excellent and wise supervisor, and most importantly, he has always had understanding for me and encouraged me to pursue my own intuition.

I would like to thank Vytautas Gruslys, for all the brilliant mini-seminars he prepared. Some of the most exciting mathematics that I know, I learned from him.

I am grateful to Dr Ta Sheng Tan, for collaborating with me and for helping me with preparing some of the text for this thesis.

I would also like to thank Prof Timothy Gowers, for the work we did together in the last stage of my PhD (these results do not appear in the thesis). Working with him has been a very rewarding experience.

My thanks also go to Trinity College and Department of Pure Mathematics and Mathematical Statistics for their generous financial support and hospitality.

Finally, I am indebted to my wife Teodora, for all her love, support, encouragement and patience. Over the past few years, she helped me realize that I should not be obsessed with the results, but that I should remember instead to enjoy the work as much as possible, and that the beauty will emerge in mathematics, once the mathematical results become a labour of love. She has always inspired me to pose questions and to stay curious. The things that I learned from her are the things that I treasure the most in my PhD studies. I dedicate this thesis to her.

Contents

1 Introduction

This dissertation is divided into three parts, the first comprising Chapters 2 and 3, the second consisiting of Chapers 4 and 5 and the third having Chapters 6 and 7. Chapters 2 and 3 are devoted to a problem in metric geometry. Chapter 4 deals with a problem in graph theory that naturally arises in Chapter 3, while Chapter 5 we study a problem in extremal combinatorics. Chapter 6 of this thesis is about a result in combinatorial geometry. In Chapter 7, we consider some topics in additive combinatorics. The results in this thesis are my own work, except for Chapter 5, which was done in collaboration with Imre Leader and Ta Sheng Tan. The remainder of this introductory chapter is a brief discussion of the problems and results presented in this thesis.

1.1 Metric Geometry

In the first part of the thesis we consider a couple of problems in metric geometry.

Let (X, d) be a (non-empty) complete metric space. Given n functions f_1, $f_2, \ldots,$ f_n: $X \to X$, and a real number $\lambda \in (0, 1)$, we call $\{f_1, f_2, \ldots, f_n\}$ a λ-*contractive* family if for every pair of points x, y in X there is i such that $d(f_i(x), f_i(y)) \leq \lambda d(x, y)$. Further, we say that $\{f_1, f_2, \ldots, f_n\}$ is a *contractive* family if it is a λ-contractive family for some $\lambda \in (0, 1)$. In particular, when f is a function on X and $\{f\}$ is a contractive family we say that f is a *contraction*. Recall the well-known theorem of Banach [8] which says that any contraction on a complete metric space has a unique fixed point.

An *operator* on X is a continuous map from space to itself. In [51], Stein conjectured the following generalisation of the theorem of Banach:

Let $\{f_1, f_2, \ldots, f_n\}$ be a λ-contractive family of operators on a complete metric space. Then some composition of $f_1, f_2, \ldots, f_n$ (i.e. some word in $f_1, \ldots, f_n$) has a fixed point.

In [7], Austin constructed a counterexample to this statement.

Theorem I.1 (Austin [7])**.** *There is a complete metric space (X, d) with a contractive family of operators $\{f, g\}$, such that no word in f, g has a fixed point.*

Furthermore, Austin asked if this is possible in a compact space.

Question I.2 (Austin [7])**.** *Does every contractive family of operators on a compact space have a composition with a fixed point?*

Our first result is that even with the additional assumption of compactness, there still need not be a fixed point.

Theorem. *There is a compact metric space (X, d) with a contractive family of operators $\{f, g\}$, such that no word in f, g has a fixed point.*

We remark that our construction provides the counterexample for any given $\lambda \in (0, 1)$.

This work appears in [36].

In [7], Austin additionally showed that if $n = 2$ and f_1 and f_2 commute the conjecture of Stein will hold.

With this in mind, we say that $\{f_1, f_2, \ldots, f_n\}$ is *commuting* if every f_i and f_j commute.

Theorem I.3 (Austin [7])**.** *Suppose that $\{f, g\}$ is a commuting contractive family of operators on a complete metric space. Then f and g have a common fixed point.*

Let us mention another result in this direction, which was proved by Arvanitakis in [6] and by Merryfield and Stein in [35].

Theorem I.4 (Arvanitakis [6], Merryfield, Stein [35], Generalized Banach Contraction Theorem)**.** *Let f be a function from a complete metric space to itself, such that $\{f, f^2, \ldots, f^n\}$ is a contractive family. Then f has a fixed point.*

Note that there is no assumption of continuity in the statement of Theorem I.4. We also remark that Merryfield, Rothschild and Stein proved this theorem for the case of operators in [34]. Furthermore, Austin raised a question which is a version of Stein's conjecture, and generalizes these two theorems in the context of operators.

Conjecture I.5 (Austin [7])**.** *Suppose that $\{f_1, f_2, \dots, f_n\}$ is a commuting contractive family of operators on a complete metric space. Then $f_1, f_2, \dots, f_n$ have a common fixed point.*

Our second result proves the case $n = 3$, provided λ is sufficiently small.

Theorem I.6. *Let (X, d) be a complete metric space and let $\{f_1, f_2, f_3\}$ be a commuting λ-contractive family of operators on X, for a given $\lambda \in (0, 10^{-23})$. Then f_1, f_2, f_3 have a common fixed point.*

This work appears in [37].

1.2 Graph Theory

The second part of the thesis is about problems in graph theory.

1.2.1 Covering Complete Graphs by Monochromatically Bounded Sets

Given a graph G, whose edges are coloured with a colouring $\chi\colon E(G) \to C$ (where adjacent edges are allowed to use the same colour), given a set of vertices A, and a colour $c \in C$, we write $G[A, c]$ for the subgraph induced by A and the colour c, namely the graph on the vertex set A and the edges $\{xy\colon x, y \in A, \chi(xy) = c\}$. In particular, when $A = V(G)$, we write $G[c]$ instead of $G[V(G), c]$. Finally, we also use the usual notion of the induced subgraph $G[A]$ which is the graph on the vertex set A with edges $\{xy\colon x, y \in A, xy \in E(G)\}$. We usually write $[n] = \{1, 2, \dots, n\}$ for the vertex set of K_n.

Our starting point is the following conjecture of Gyárfás.

Conjecture I.7 (Gyárfás [23], [25])**.** *Let k be fixed. Given any colouring of the edges of K_n in k colours, we can find sets $A_1, A_2, \dots, A_{k-1}$ whose union is $[n]$, and colours $c_1, c_2, \dots, c_{k-1}$ such that $K_n[A_i, c_i]$ is connected for each $i \in [k-1]$.*

This is an important special case of the well-known Lovász-Ryser conjecture, which we now state.

Conjecture I.8 (Lovász-Ryser conjecture [33], [27])**.** *Let G be a graph, whose maximum independent set has size $\alpha(G)$. Then, whenever $E(G)$ is k-coloured, we can cover G by at most $(k-1)\alpha(G)$ monochromatic components.*

Conjectures I.7 and I.8 have attracted a great deal of attention. When it comes to the Lovász-Ryser conjecture, we should note the result of Aharoni ([1]), who proved the case of $k = 3$. For $k \geq 4$, the conjecture is still open. The special case of complete graphs was proved by Gyárfás ([24]) for $k \leq 4$, and by Tuza ([52]) for $k = 5$. For $k > 5$, the conjecture is open.

Let us also mention some results similar in the spirit to Conjecture I.7. In [46], inspired by questions of Gyárfás ([23]), Ruszinkó showed that every k-colouring of edges of K_n has a monochromatic component of order at least $n/(k-1)$ and of diameter at most 5. This was improved by Letzter ([32]), who showed that in fact there are monochromatic triple stars of order at least $n/(k-1)$. For more results and questions along these lines, we refer the reader to surveys of Gyárfás ([23], [25]).

In a completely different direction, recall Theorem I.6 about contraction mappings on metric spaces. Some of the ingredients in the proof of Theorem I.6 were the following simple lemmas. Note that next lemma is in fact a classical observation due to Erdős and Rado.

Lemma. *Suppose that the edges of K_n are coloured in two colours. Then we may find a colour c such that $K_n[c]$ is connected and of diameter at most 3.*

Lemma. *Suppose that the edges of K_n are coloured in three colours. Then we may find colours c_1, c_2, (not necessarily distinct), and sets A_1, A_2 such that $A_1 \cup A_2 = [n]$, with $K_n[A_1, c_1], K_n[A_2, c_2]$ are each connected and of diameter at most 8.*

A common generalization of these statements and a strengthening of Conjecture I.7 is conjectured in Section 3.9.

Conjecture I.9. *For every k, there is an absolute constant C_k such that the following holds. Given any colouring of the edges of K_n in k colours, we can* *find sets $A_1, A_2, \ldots, A_{k-1}$ whose union is $[n]$, and colours $c_1, c_2, \ldots, c_{k-1}$ such that $K_n[A_i, c_i]$ is connected and of diameter at most C_k, for each $i \in [k-1]$.*

The main result in this chapter of thesis is

Theorem. *Conjecture I.9 holds for 4 colours, and one may take $C_4 = 160$.*

The work of this chapter appears in [38].

1.2.2 Decomposing the Complete r-Graph

The work we now describe is the content of Chapter 5 and is done in collaboration with Imre Leader and Ta Sheng Tan.

The edge set of K_n, the complete graph on n vertices, can be partitioned into $n-1$ complete bipartite subgraphs: this may be done in many ways, for example by taking $n-1$ stars centred at different vertices. Graham and Pollak [21, 22] proved that the number $n-1$ cannot be decreased. Several other proofs of this result have been found, by Tverberg [53], Peck [42], and Vishwanathan [55, 56].

Generalising this to hypergraphs, for $n \geq r \geq 1$, let $f_r(n)$ be the minimum number of complete r-partite r-graphs needed to partition the edge set of $K_n^{(r)}$, the complete r-uniform hypergraph on n vertices (i.e., the collection of all r-sets from an n-set). Thus the Graham-Pollak theorem asserts that $f_2(n) = n-1$. For $r \geq 3$, an easy upper bound of $\binom{n-\lceil r/2 \rceil}{\lfloor r/2 \rfloor}$ may be obtained by generalising the star example above. Indeed, having ordered the vertices, consider the collection of r-sets whose 2^{nd}, 4^{th}, $\ldots$, $(2\lfloor r/2 \rfloor)^{\text{th}}$ vertices are fixed. This forms a complete r-partite r-graph, and the collection of all $\binom{n-\lceil r/2 \rceil}{\lfloor r/2 \rfloor}$ such is a partition of $K_n^{(r)}$. (There are many other constructions achieving the exact same value; see, for example Alon's recursive construction in [4].)

Alon [4] showed that $f_3(n) = n-2$. More generally, for each fixed $r \geq 1$, he showed that

$$\frac{2}{\binom{2\lfloor r/2 \rfloor}{\lfloor r/2 \rfloor}}(1+o(1))\binom{n}{\lfloor r/2 \rfloor} \leq f_r(n) \leq (1-o(1))\binom{n}{\lfloor r/2 \rfloor},$$

where the upper bound is from the construction above.

The best known lower bound for $f_r(n)$ was obtained by Cioabă, Küngden and Verstraëte [12], who showed that $f_{2k}(n) \geq \frac{2\binom{n-1}{k}}{\binom{2k}{k}}$. For upper bounds for $f_r(n)$, the above construction is not sharp in general. Cioabă and Tait [13] showed that $f_6(8) = 9 < \binom{8-3}{3}$, and used this to give an improvement in a lower-order term, showing that $f_{2k}(n) \leq \binom{n-k}{k} - 2\left\lfloor \frac{n}{16} \right\rfloor \binom{\lfloor \frac{n}{2} \rfloor - k + 3}{k-3}$ for any $k \geq 3$. (We mention briefly that any improvement of $f_4(n)$ for any n will further improve the above upper bound. Indeed, one can check that $f_4(7) = 9 < \binom{7-2}{2}$, and this will imply that $f_r(n) \leq \binom{n - \lfloor r/2 \rfloor}{\lfloor r/2 \rfloor} - cn^{\lfloor r/2 \rfloor - 1}$ for some positive constant c. But note that, again, this is only an improvement to a lower-order term.)

Despite these improvements, the asymptotic bounds of Alon have not been improved. Perhaps the most interesting question was whether the asymptotic upper bound is the correct estimate.

The main result of the last part of thesis is that the asymptotic upper bound is not correct for each even $r \geq 4$. In particular, we will show that

$$f_4(n) \leq \frac{14}{15}(1 + o(1))\binom{n}{2},$$

and obtain the same improvement of $\frac{14}{15}$ for each even $r \geq 4$.

The work of this chapter appears in [31].

1.3 Combinatorics on Algebraic Structures

In the final part of the thesis we consider a problem in combinatorial geometry and a problem in additive combinatorics.

1.3.1 Combinatorial Geometry

A set of points in the plane is said to be *in general position* if it has no 3 collinear points, and *in almost general position* if there are no 4 collinear points. Let $\alpha(n)$ be the maximum k such that any set of n points in the plane in almost general position has k points in general position. In [15], Erdős asked for an improvement of the (easy) bounds $\sqrt{2n-1} \leq \alpha(n) \leq n$ (see equation (13) in the paper). This was done by Füredi [17], who proved $\Omega(\sqrt{n \log n}) \leq \alpha(n) \leq o(n)$.

In [11] Cardinal, Tóth and Wood considered the problem in $\mathbb{R}^3$. Firstly, let us generalize the notion of general position. A set of points in $\mathbb{R}^d$ is said to be in *general position* if there are no $d+1$ points on the same hyperplane, and in *almost general position* if there are no $d+2$ points on the same hyperplane. Let $\alpha(n,d)$ stand for the maximum integer k such that all sets of n points in $\mathbb{R}^d$ in almost general position contain a subset of k points in general position. Cardinal, Tóth and Wood proved that $\alpha(n,3) = o(n)$ holds. They noted that for a fixed $d \geq 4$, only $\alpha(n,d) \leq Cn$ is known, for a constant $C \in (0,1)$, and they asked whether $\alpha(n,d) = o(n)$. The goal of the fourth part of thesis is to answer their question in all dimensions. In particular, we prove the following.

Theorem. *For a fixed integer $d \geq 2$, we have $\alpha(n,d) = o(n)$.*

In fact, we are able to get better bounds for certain dimensions. This is the content of the next theorem.

Theorem. *Suppose that $d, m \in \mathbb{N}$ satisfy $2^{m+1} - 1 \leq d \leq 3 \cdot 2^m - 3$. Let $N \geq 1$. Then*

$$\alpha(2^N, d) \leq \left(\frac{25}{N}\right)^{1/2^{m+1}} 2^N.$$

It is worth noting the lower bound $\alpha(n,d) = \Omega_d((n \log n)^{1/d})$ due to Cardinal, Tóth and Wood ([11]), but we do not try to improve their bound here.

In [17] Füredi used the density Hales-Jewett theorem ([18], [14]) to establish $\alpha(n) = \alpha(n,2) = o(n)$. Here we reproduce his argument. By the density Hales-Jewett theorem, for a given $\epsilon > 0$, there is a positive integer N such that all subsets of $[3]^N$ of density ϵ contain a combinatorial line. Map the set $[3]^N$ to $\mathbb{R}^2$ using a generic linear map f to obtain a set $X = f([3]^N) \subseteq \mathbb{R}^2$. By the choice of f, collinear points in X correspond to collinear points in $[3]^N$, and f restricted to $[3]^N$ is injective. Therefore, X has no 4 points on a line, and so is in almost general position, but if $S \subseteq X$ has size at least $\epsilon|X|$, the set $f^{-1}(S) \subseteq [3]^N$ has density at least ϵ in $[3]^N$. Therefore, $f^{-1}(S)$ has a line, hence $S = f(f^{-1}(S))$ has 3 collinear points. Since $\epsilon > 0$ was arbitrary, this proves that $\alpha(n,2) = o(n)$.

If one tries to generalize this argument to higher dimensions, by mapping $[m]^N$ to $\mathbb{R}^d$, then there will be m^{d-1} cohyperplanar points, and we must have $m^{d-1} = d+1$ to get almost general position. But the only positive integers that have this property are $(m,d) \in \{(3,2),(2,3)\}$. Taking $m = 2, d = 3$ gives $\alpha(n,3) = o(n)$, as observed by Cardinal, Tóth and Wood ([11]). For other choices of (m,d) we have too many cohyperplanar points as $m^{d-1} > d+1$. Overcoming this obstacle is the main goal of our work.

The work of this chapter appears in [39].

1.3.2 Additive Combinatorics

The problem of comparing different expressions involving the same subset A of an abelian group G (e.g. $A+A$ and $A-A$) is one of the central topics in additive combinatorics. For example, one of the starting points in the study of this field is the Plünnecke-Ruzsa inequality that bounds $|kA - lA|$ in terms of $|A|$ and $|A+A|$.

Theorem I.10 (Plünnecke-Ruzsa inequality [43], [47]). *Let A be a subset of an abelian group. Then, for any $k, l \geq 1$ we have*

$$|kA - lA||A|^{k+l-1} \leq |A+A|^{k+l}.$$

To illustrate the difficulties in determining the right bounds for such inequalities, we note that even for the comparison of $|A+A|$ and $|A-A|$ the right exponents are not known. In fact, the best known lower bounds for $|A+A|$ in terms of $|A-A|$ have not changed for more than 40 years.

Theorem I.11 (Freiman, Pigaev [16], Ruzsa [49]). *Let A be a subset of an abelian group. Then $|A-A|^{3/4} \leq |A+A|$.*

In the opposite direction, the best known lower bound is given by the following result.

Theorem I.12 (Hennecart, Robert, Yudin, [28]). *There exist arbitrarily large sets $A \subset \mathbb{Z}$ such that $|A+A| \leq |A-A|^{\alpha+o(1)}$, where $\alpha := \log(2)/\log(1+\sqrt{2}) \approx 0.7864$.*

In 1973, Haight [26] found for each k and $\epsilon > 0$, an integer q and a set $A \subset \mathbb{Z}_q$ such that $A - A = \mathbb{Z}_q$ and $|kA| \leq \epsilon q$. Recently, Ruzsa [48] gave a similar construction, and observed that Haight's work even gives a constant $\alpha_k > 0$ for each k with the property that there are arbitrarily large q with sets $A \subset \mathbb{Z}_q$ such that $A - A = \mathbb{Z}_q$ and $|kA| \leq q^{1-\alpha_k}$. The ideas in both constructions are relatively similar, but Ruzsa's argument is considerably more concise.

In [41], Nathanson applied Ruzsa's method to construct sets $A \subset R$ with $A - A = R$, but kA small, for rings R that are more general than $\mathbb{Z}_q$. In the same paper, he posed the following more general question. Given a polynomial $F(x_1, x_2, \dots, x_n)$ with coefficients in $\mathbb{Z}$, and a set $A \subset \mathbb{Z}_N$, write $F(A) = \{F(a_1, a_2, \dots, a_n) : a_1, \dots, a_n \in A\}$. His question can be stated as: given two polynomials F, G over $\mathbb{Z}$ and $\epsilon > 0$, does there exist arbitrarily large N and a set $A \subset \mathbb{Z}_N$ such that $F(A) = \mathbb{Z}_N$, but $|G(A)| < \epsilon N$?[1]

Let us now state the main result of the fourth part of the thesis, which answers the first interesting cases of Nathanson's question. Once again we recall the notation

$$A^2 + kA = \{a_1 a_2 + a_1' + a_2' + \cdots + a_k' : a_1, a_2, a_1', \dots, a_k' \in A\},$$

and more generally,

$$lA^2 + kA = \{a_1 a_2 + \cdots + a_{2l-1} a_{2l} + a_1' + a_2' + \cdots + a_k' : a_1, a_2, \dots, a_{2l}, a_1', \dots, a_k' \in A\}.$$

Theorem. *Given $k \in \mathbb{N}_0$ and any $\epsilon > 0$, there is a natural number q and a set $A \subset \mathbb{Z}_q$ such that*

$$A - A = \mathbb{Z}_q, \ \textit{but } |A^2 + kA| \leq \epsilon q.$$

In fact we prove rather more.

Theorem. *For $l \in \{1, 2, 3\}$, any $k \in \mathbb{N}_0$ and any $\epsilon > 0$, there is a natural number q and a set $A \subset \mathbb{Z}_q$ such that*

$$A - A = \mathbb{Z}_q, \ \textit{but } |lA^2 + kA| < \epsilon q.$$

Moreover, we can take q to be a product of distinct primes, and we can take the smallest prime dividing q to be arbitrarily large.

We shall discuss each of the cases $l = 1, 2, 3$ separately. Note also an interesting phenomenon in the opposite direction. Namely, if we are not allowed freedom in the choice of the modulus, a statement like the theorem above cannot hold. The reason is that, by the result of Glibichuk and Rudnev (Lemma 1 in

[1] Actually, Nathanson poses this question for more general rings R, but for $R = \mathbb{Z}$, the formulation we give here is a natural one.

[19]) whenever $A \subset \mathbb{F}_p$ for a prime p, is a set of size at least $|A| > \sqrt{p}$, then $10A^2 = \mathbb{F}_p$ (and $A - A = \mathbb{F}_p$ certainly implies $|A| > \sqrt{p}$). Hence, unlike the linear case, already for quadratic expressions we have strong obstructions.

The work of this chapter appears in [40].

Part I

Contractive Families

1.1 Introduction

Let (X, d) be a (non-empty) complete metric space. Given n functions f_1, $f_2, \ldots, f_n : X \to X$, and a real number $\lambda \in (0,1)$, we call $\{f_1, f_2, \ldots, f_n\}$ a λ-*contractive* family if for every pair of points x, y in X there is i such that $d(f_i(x), f_i(y)) \leq \lambda d(x, y)$. Further, we say that $\{f_1, f_2, \ldots, f_n\}$ is a *contractive family* if it is a λ-contractive family for some $\lambda \in (0,1)$. In particular, when f is a function on X and $\{f\}$ is a contractive family we say that f is a *contraction.* Recall the well-known theorem of Banach [8] which says that any contraction on a complete metric space has a unique fixed point.

An *operator* on X is a continuous map from space to itself. In [51], Stein conjectured the following generalisation of the theorem of Banach:

Let $\{f_1, f_2, \ldots, f_n\}$ be a λ-contractive family on a complete metric space. Then some composition of $f_1, f_2, \ldots, f_n$ (i.e. some word in $f_1, \ldots, f_n$) has a fixed point.

In [7], Austin constructed a very nice counterexample to this statement.

Theorem 1.1 (Austin [7])**.** *There is a complete metric space (X, d) with a contractive family of operators $\{f, g\}$, such that no word in f, g has a fixed point.*

Furthermore, Austin asked if this is possible in a compact space.

Question 1.2 (Austin [7])**.** *Does every contractive family of operators on a compact space have a composition with a fixed point?*

Our first result in this part of the thesis is that even with the additional assumption of compactness, there still need not be a fixed point.

Theorem 1.3. *There is a compact metric space (X, d) with a contractive family of operators $\{f, g\}$, such that no word in f, g has a fixed point.*

We remark that our construction provides the counterexample for any given $\lambda \in (0,1)$.

Remarkably, Austin also showed that if $n = 2$ and f_1 and f_2 commute, the conjecture of Stein will hold.

With this in mind, we say that $\{f_1, f_2, \ldots, f_n\}$ is *commuting* if every f_i and f_j commute.

Theorem 1.4 (Austin [7]). *Suppose that $\{f, g\}$ is a commuting contractive family of operators on a complete metric space. Then f and g have a common fixed point.*

Let us mention another very elegant result in this direction, which was proved by Arvanitakis in [6] and by Merryfield and Stein in [35].

Theorem 1.5 (Arvanitakis [6], Merryfield, Stein [35], Generalized Banach Contraction Theorem). *Let f be a function from a complete metric space to itself, such that $\{f, f^2, \ldots, f^n\}$ is a contractive family. Then f has a fixed point.*

Note that there is no assumption of continuity in the statement of Theorem 1.5. We also remark that Merryfield, Rothschild and Stein proved this theorem for the case of operators in [34]. Furthermore, Austin raised the following fascinating question which is a version of Stein's conjecture, and generalizes these two theorems in the context of operators.

Conjecture 1.6 (Austin [7]). *Suppose that $\{f_1, f_2, \ldots, f_n\}$ is a commuting contractive family of operators on a complete metric space. Then $f_1, f_2, \ldots, f_n$ have a common fixed point.*

Let us now state the second result that we establish in this part of the thesis, which proves the case $n = 3$ and λ sufficiently small:

Theorem 1.7. *Let (X, d) be a complete metric space and let $\{f_1, f_2, f_3\}$ be a commuting λ-contractive family of operators on X, for a given $\lambda \in (0, 10^{-23})$. Then f_1, f_2, f_3 have a common fixed point.*

We remark that such a fixed point is necessarily unique.

2 Contractive Families on Compact Spaces

This chapter is devoted to the proof of Theorem 1.3, where we construct a compact metric space (X, d) with a contractive family of operators $\{f, g\}$, such that no word in f, g has a fixed point.

2.1 Outline of the construction of the counterexample

We begin by providing some motivation for our steps. Suppose that $(X, d), f, g$ satisfy the conclusion of Theorem 1.3. Given any set S of points in our space, since X is compact, we know that S is bounded. Let D be its diameter. Then, it is not hard to show that the diameter of one of $f(S)$ or $g(S)$ is at most $4\lambda D$. To see this, pick any point x in S and consider set $S_f = \{y \in S : \lambda d(x, y) \geq d(f(x), f(y))\}$ and let $S_g = S \setminus S_f$. If $S_f = S$, we are done, so suppose that $S_g \neq \emptyset$. If we can find $y \in S_f$ such that $\lambda d(y, z) \geq d(f(y), f(z))$ for all $z \in S_g$, then, by looking at distance from $f(y)$, the diameter of $f(S)$ does not exceed $4\lambda D$. On the other hand, if there is no such y, then each point of $g(S_f)$ is on distance at most λD from some point in $g(S_g)$ which is on distance at most λD from $g(x)$, so $g(S)$ has diameter at most $4\lambda D$.

This simple observation leads us to the idea that instead of considering distances between each pair of points in the wanted space, thinking about diameters of sets should be much more convenient in our problem. With this in mind, we develop the notion of 'diameter spaces', which will play a key role throughout our construction. Due to their importance in our work, we include a proper definition.

Definition. Let X be a non-empty set. Given a collection $\mathcal{D}$ of subsets of X, we call $(X, \mathcal{D})$ a *diametrisable space* provided the following conditions are met.

(i) Given $x, y \in X$, there is $U \in \mathcal{D}$ with $x, y \in U$.

(ii) If $U, V \in \mathcal{D}$ and $U \cap V \neq \emptyset$, then $U \cup V \in \mathcal{D}$.

We refer to elements of X as *points* and elements of $\mathcal{D}$ as *diametrisable sets*. Further, if a function $\mathrm{diam}\colon \mathcal{D} \to \mathbb{R}_{\geq 0}$ is such that whenever $U, V \in \mathcal{D}$ intersect, the inequality

$$\mathrm{diam}(U) + \mathrm{diam}(V) \geq \mathrm{diam}(U \cup V)$$

holds, we call diam the *diameter* and $(X, \mathcal{D}, \mathrm{diam})$ a *diameter space*. We refer to this inequality as the *triangle inequality for the diameter spaces*.

In a very natural way, one can use a diameter space to induce a pseudometric on the underlying space, by simply finding the infimum of diameters of all the diametrisable sets containing any two given (distinct) points. Furthermore, by imposing suitable conditions on the diametrisable sets, one can get nice properties to hold for the pseudometric space.

In order to proceed further, we must first specify the underlying set. Hence, let us look for the space that should, in some vague sense, be the minimal counterexample. One of the possible ways to approach this issue is to fix a point x_0, and then examine what other points we can obtain. It is not hard to see that completion of the set of all images that one can get by applying f and g to x_0 is itself a compact metric space, and that f, g form a λ-contractive map on this subspace of X as well. Now, starting from x_0 we must include all the points described, and we can actually map all these points that are obtained using f, g from x_0 to finite words over a two-letter alphabet (this is a bijection if no two results of distinct compositions of f, g applied to x_0 coincide). Therefore, our construction will start from an underlying set X of all finite words over $\{a, b\}$, with the obvious functions f and g, each of which adds one of the characters a and b to the beginning of the word that is given as input. Then, provided we have a metric on X, we will take its completion, and hope that the metric space that we get, along with f and g, satisfies all the properties of Theorem 1.3. This is where diameter spaces come in play. We will introduce properties of a collection $\mathcal{D}$ of diametrisable sets on X, that will guarantee that the completion of the induced pseudometric space, along with f and g, (which are the concatenation functions described), is the desired counterexample. Being a relatively long list, we refer the reader to Corollary 2.9 to get an idea of what conditions we impose on $\mathcal{D}$. The collection $\mathcal{D}$ will in fact be a sequence of subsets of X, denoted by $S_0, S_1, S_2, \ldots$.

2.2 Inducing a counterexample from a diameter space

2.2.1 Diameter spaces and their connection with metric spaces

In this subsection we show how one can obtain a pseudometric space from diameter spaces. The following proposition tells us how to induce pseudometric on the underlying set.

Proposition 2.1. *Let $(X, \mathcal{D}, \operatorname{diam})$ be a diameter space. Define a function $d\colon X^2 \to \mathbb{R}$ by $d(x, y) = \inf \operatorname{diam}(U)$ when x and y are distinct, where infimum is taken over all diametrisable sets that contain points x and y, and $d(x, y) = 0$ otherwise. Then d is well-defined and (X, d) is a pseudometric space.*

Proof. Firstly, suppose we are given two distinct points x and y. Then the set S of all values that diameter of a diametrisable set containing x, y can take, is non-empty and bounded from below by 0, so $\inf S$ exists, and d is well-defined.

To prove that d is a pseudometric, we just need to show that the triangle inequality holds, since $d(x, x) = 0$ holds for all points x and d is symmetric by construction. Let $x, y, z \in X$. If any of these points are equal, we are done. Otherwise, given $\epsilon > 0$ we can find sets $U, V \in \mathcal{D}$ such that $x, y \in U$, $y, z \in V$, $d(x, y) \leq \operatorname{diam} U \leq d(x, y) + \epsilon/2, d(y, z) \leq \operatorname{diam} V \leq d(y, z) + \epsilon/2$. But U and V intersect, hence $U \cup V$ is also a diametrisable set, and further $\operatorname{diam}(U \cup V) \leq \operatorname{diam}(U) + \operatorname{diam}(V) \leq d(x, y) + d(y, z) + \epsilon$, so $d(x, z) \leq d(x, y) + d(y, z) + \epsilon$. But this holds for any positive ϵ, proving the triangle inequality, and therefore the proposition follows. $\square$

The pseudometric that we constructed from a given diameter space will be referred to as the *induced pseudometric* by diam.

Note that given any metric space (X, d) we can construct a diameter space $(X, \mathcal{D}, \operatorname{diam})$ by taking diametrisable sets to be the finite subsets of X, and the diameter function diam to have the usual meaning, that is for any $U \in \mathcal{D}$, we set $\operatorname{diam}(U)$ to be $\max d(x,y)$ where maximum is taken over all pairs of points in U. Then, the metric d coincides with the pseudometric induced by diam. In this way, we can view any metric space as a diameter space at the same time.

2.2.2 Required properties of the diameter space

In the previous subsection we saw how to obtain a pseudometric space from a diameter space. To construct a counterexample to the conjecture, we will use that procedure, but as the proposition only guaranties that we get a pseudometric space, we need to add additional properties of a diameter space to ensure that we reach our goal. First of all, we work with specific underlying set X and the diameter function which are consistent with the nature (or more precisely the geometry) of the problem. As noted before, we are essentially considering compositions of functions applied to an element of the given metric space satisfying the assumptions of the conjecture, and therefore we will work with points of X being finite words over the alphabet consisting of two letters $\Sigma = \{a, b\}$, including the empty word. Before we proceed further, let us introduce some notation.

Notation. If u, v are two words of X, we write uv for the word obtained by writing first u then v. Say that u is a *prefix* or an *initial segment* of v, if there is another word w with $v = uw$, and if this holds write $u \leq v$. The *length* of a word u, denoted by $l(u)$, is the number of letters in u. Characters are considered to be words of length one simultaneously as being characters. When S is a subset of X and $u \in X$, we write $uS = \{us : s \in S\}$ and $Su = \{su : s \in S\}$. Given a positive integer n and word u, write u^n for $uu \dots u$, where u appears n times. The empty word is denoted by $\emptyset$. Finally, we occasionally allow infinite words in our arguments (although these are not elements of X), and write u^∞ to stand for the infinite word obtained by writing consecutive copies of u infinitely many times.

We will take our functions $f, g \colon X \to X$ to be given by $f(u) = au$ and $g(u) = bu$ for all words $u \in X$. Then every word is actually equal to the result of applying the corresponding composition of functions to the empty word. On the other hand, having in mind the contraction property of the family of the functions that we want to hold, we take $\mathcal{D}$ to be a sequence of subsets of X, namely $\mathcal{D} = \{S_0, S_1, S_2, \dots\}$ and set $\operatorname{diam}(S_k) = \lambda^k$ for some fixed $\lambda \in (0,1)$. Now, we just need to specify what needs to hold for $\mathcal{D}$ so that we get a counterexample.

Let us start with ensuring that $(X, \mathcal{D}, \operatorname{diam})$ is a diameter space. We accomplish this by requiring the following property.

A1 For any non-negative integers $i < j$, if $S_i \cap S_j \neq \emptyset$, then $S_j \subset S_i$. Also, $S_0 = X$.

If this property holds, then we see that given any two intersecting diametrisable sets S_i and S_j, we have $S_i \cup S_j = S_i$ or $S_i \cup S_j = S_j$. Therefore, $(X, \mathcal{D})$ is a diametrisable space and the triangle inequality holds for diam, thus this is indeed a diameter space.

Consider now (X, d), where d is the pseudometric induced by diam. To make d non-degenerate, we introduce another property.

A2 Each point belongs to only finitely many diametrisable sets.

If **A2** holds, since diam is always positive, and the infimum defining $d(x, y)$ for $x \neq y$ is actually minimum taken over finitely many positive values, we get that d is non-degenerate, and thus a metric.[1]

As far as the compactness is concerned, the fact that we can obtain a compact space from a totally bounded one by taking its completion is what motivates our following step. Hence, another condition is introduced.

A3 For any positive integer N, there are integers $i_1, i_2, \dots, i_n$, greater than N, such that $X \setminus (S_{i_1} \cup S_{i_2} \cup \dots \cup S_{i_n})$ is finite.

Proposition 2.2. *Provided $\mathcal{D}$ satisfies **A1-A3**, the completion $(\overline{X}, d)$ of the metric space induced by $(X, \mathcal{D}, \operatorname{diam})$ is compact.*

Proof. By the comments above, we just need to show that (X, d) is totally bounded. Let $\epsilon > 0$ be given, and choose N for which $\lambda^N < \epsilon/2$ holds. By

[1] It is easy to see that this is in fact an ultra metric.

A3, there are $i_1, i_2, \ldots, i_n > N$ for which the union of $S_{i_1}, S_{i_2}, \ldots, S_{i_n}$ covers all but finitely many points, denoted by $y_1, y_2, \ldots, y_m$. Then, each S_{i_k} is contained in $B_{x_k}(\epsilon)$ for some $x_k \in S_{i_k}$, and $y_k \in B_{y_k}(\epsilon)$, so X is covered by finitely many open balls of radius ϵ, and so the metric space is totally-bounded. □

Say that a Cauchy sequence $(x_n)_{n\geq 1}$ is *proper* if there is no N with $x_N = x_{N+1} = \ldots$. The three conditions described so far give us a nice characterisation of the proper Cauchy sequences in $(\overline{X}, d)$, whose elements lie in X.

Proposition 2.3. *Suppose that $\mathcal{D}$ satisfies properties **A1**-**A3**. Then a sequence of points in X is proper Cauchy with respect to the induced metric if and only if for any given positive integer M there is $m > M$ such that S_m contains all but finitely many points of the sequence.*

Proof. Only if direction. Let $(x_n)_{n\geq 1}$ be a proper Cauchy sequence in X and let a positive integer M be given. Take a positive $\epsilon < \lambda^M$. Then, as the given sequence is Cauchy, we have N such that $m, n > N$ implies $d(x_n, x_m) < \epsilon$.

Now fix any $m > N$ and let $I = \{i > M : \exists n > N, x_n, x_m \in S_i\}$. By the definition of d, we know that this set is nonempty, therefore has a minimal element i_0. If $n > N$ then $d(x_n, x_m) < \epsilon < \lambda^M$, so there is $j > M$ with x_n, x_m both belonging to S_j. But $x_m \in S_{i_0}$ so S_{i_0}, S_j intersect and by the choice of i_0 and property **A1** we have $x_n \in S_j \subset S_{i_0}$, so almost all points of the sequence are contained in S_{i_0}.

If direction. Given $\epsilon > 0$ take M such that $\lambda^M < \epsilon$. Then there is $m > M$ with S_m containing almost all points in the sequence, and the distance between two points in S_m is at most $\lambda^{M+1} < \epsilon$, so the sequence is Cauchy. If it was not a proper one, the point which is equal to almost all of its members would belong to infinitely many of the sets S_i which is impossible by **A2**. □

Proposition 2.4. *Under the same assumptions as in the previous proposition, no proper Cauchy sequence in $(\overline{X}, d)$ converges to a point in X.*

Proof. Suppose that a point $x \in X$ is a limit of a proper Cauchy sequence (x_n) in $\overline{X}$. First of all, if $x_n \in \overline{X} \setminus X$, substitute x_n by a point $y \in X$ such that $d(x_n, y) < \frac{1}{2} d(x_n, x)$. The newly obtained sequence now lies in X, and is still proper Cauchy, with unchanged limit. As $x \in X$ belongs to S_i for only finitely many i, we have $B_x(\lambda^n) \cap X = \{x\}$, for sufficiently large n, which is a contradiction. □

Lemma 2.5. *Let $(\overline{X}, d)$ be the metric space considered so far. Suppose F is a function on X that preserves Cauchy sequences, that is given Cauchy sequence $(x_n)_{n\geq 1}$, the sequence of images $(F(x_n))_{n\geq 1}$ is Cauchy as well. Then, extension of F to the completion of the space given by $F(x) = \lim_{n\to\infty} F(x_n)$, where (x_n) is any Cauchy sequence in X tending to x in $\overline{X} \setminus X$, is continuous.*

Proof. Firstly, we should prove that such an extension of F is well-defined. Take arbitrary $x \in \overline{X} \setminus X$, and thus since $\overline{X}$ is completion of x, there must be Cauchy sequence in X whose limit is x. But the image of this sequence under F is Cauchy as well, so it has limit in $\overline{X}$, so we just need to show its uniqueness. Therefore, suppose that $(x_n)_{n\geq 1}$ and $(y_n)_{n\geq 1}$ are two sequences in X tending to x. Merging these two sequence into $(t_n)_{n\geq 1}$, where $t_{2n-1} = x_n, t_{2n} = y_n$, implies that $(t_n)_{n\geq 1}$ is Cauchy, hence $(F(t_n))_{n\geq 1}$ is also Cauchy, so $(F(x_n))_{n\geq 1}$ and $(F(y_n))_{n\geq 1}$ have the same limit, as required.

Secondly, we should prove that F is continuous in $\overline{X}$. Let $(x_n)_{n\geq 1}$ be sequence tending to some $x \in \overline{X}$. If $x \in X$, then sequence is eventually constant and equal to x, hence $(F(x_n))_{n\geq 1}$ trivially tends to $F(x)$. Otherwise, $x \notin X$, so consider new sequence $(t_n)_{n\geq 1}$ given as follows. If $x_n \in X$, set $t_n = x_n$, and if this does not hold, there is Cauchy sequence $(y_m)_{m\geq 1}$ in X whose limit is x_n. By assumption, $(F(y_m))_{m\geq 1}$ is Cauchy in X, and as we have shown previously, it tends to $F(x_n)$. Hence, for sufficiently large m, we have that $d(x_n, y_m), d(F(x_n), F(y_m)) < 1/n$, so set $t_n = y_m$. Thus, as for all n we have $d(x_n, t_n) < 1/n$, we have that $(t_n)_{n\geq 1}$ is Cauchy in X and tends to x, so its image under F is Cauchy sequence with limit $F(x)$, but $d(F(x_n), F(t_n)) < 1/n$ holds for all n, thus $\lim_{n\to\infty} F(x_n) = F(x)$, as required, implying continuity of F. □

This lemma suggests the fourth property of the diametrisable sets.

A4 If $i_1 < i_2 < \dots$ are indices such that $S_{i_1} \supset S_{i_2} \supset \dots$, then, given any N, we can find $n_a, n_b > N$ for which S_{n_a} contains all but finitely many elements of aS_{i_m} for some m, and S_{n_b} contains all but finitely many elements of bS_{i_p} for some p.

Proposition 2.6. *If $\mathcal{D}$ satisfies **A1**-**A4**, then $f, g : \overline{X} \to \overline{X}$, defined before and then extended as in the previous lemma are continuous with respect to the induced metric.*

Proof. We will show the claim for f, proof for g follows the same lines. We only need to show that f preserves Cauchy sequences in X, in fact, it is sufficient to prove that if $(x_n)_{n\geq 1}$ is proper Cauchy, then $(f(x_n))_{n\geq 1}$ is Cauchy. Thus, suppose we are given a proper Cauchy sequence $(x_n)_{n\geq 1}$ in X, so there are indices $i_1 > 1, i_2 > 2, \dots$ (without loss of generality $i_1 < i_2 < \dots$) such that S_{i_k} covers all but finitely many elements of the sequence for every k. Due to intersections and **A1** we have $S_{i_1} \supset S_{i_2} \supset \dots$. Let $\epsilon > 0$ be given and take N which satisfies $\lambda^N < \epsilon$. Further, by **A4** there is $n > N$ and some m for which S_n contains all but finitely many elements of aS_{i_m}. Exploiting the fact that almost all elements of $(f(x_n))_{n\geq 1}$ are contained in aS_{i_m} yields that there is M such that $k, l > M$ implies $f(x_k), f(x_l) \in S_n$. Hence $d(x_k, x_l) \leq \lambda^N < \epsilon$ holds when $k, l > M$, as required. $\square$

Next property is defined in order to make $\{f, g\}$ a contractive family.

A5 For any $i \in \{0, 1, 2, \dots\}$, there are $j > i$ and a character $c \in \{a, b\}$, such that $cS_i \subset S_j$.

Proposition 2.7. *If $\mathcal{D}$ satisfies **A1**-**A5**, then f, g form a λ-contractive family in $(\overline{X}, d)$.*

Proof. Let us consider first $x, y \in X$. Taking the largest possible n for which $x, y \in S_n$, by **A5** we have $m > n$ such that without loss of generality $aS_n \subset S_m$, thus $d(f(x), f(y)) = d(ax, ay) \leq \lambda^m \leq \lambda \cdot \lambda^n = \lambda d(x, y)$, as wanted. (If we had character b instead, we would get contraction when applying g.)

In the general case, when $x, y \in \overline{X}$, we can find two sequences in X, $(x_n)_{n\geq 1}$ tending to x, and $(y_n)_{n\geq 1}$ tending to y (if one of these is already in X, then take trivial sequence). Then, by the previous case, one of f, g contracts infinitely many pairs (x_n, y_n), f say. Let indices of those pairs be $i_1 < i_2 < \dots$. Then, $\lambda d(x, y) = \lambda \lim_{n\to\infty} d(x_{i_n}, y_{i_n}) \geq \lim_{n\to\infty} d(f(x_{i_n}), f(y_{i_n})) = d(f(x), f(y))$, since f is continuous, as required. $\square$

Proposition 2.8. *Suppose that a function F, which is a word in f and g, has a fixed point. Let w be the nonempty word which corresponds to F, i.e. $F(x) = wx$ for all x. Then there are infinitely many i such that there is u_i in S_i with wu_i also being a member of S_i.*

Proof. Suppose F fixes u. Then $u \notin X$, so take $(x_n)_{n\geq 1}$ in X converging to u. Hence $(wx_n)_{n\geq 1}$ converges to $u = F(u)$ as well, so merging these two sequences together, we get a Cauchy sequence, and the result follows from Proposition 2.3. □

Based on this proposition, we now introduce the final property of the diametrisable sets that we want to hold. The following corollary does this and sums up our work so far.

Corollary 2.9. *Let $\lambda \in (0, 1)$. Consider a collection $\mathcal{D}$ of diametrisable subsets of X that obeys:*

- ***A1*** *The set S_0 is the whole of X and given any nonnegative integers $i < j$, $S_i \cap S_j \neq \emptyset$ implies $S_j \subset S_i$.*
- ***A2*** *Any point in X belongs to only finitely many diametrisable sets.*
- ***A3*** *For any positive integer N, there are integers $i_1, i_2, \ldots, i_n$ greater than N such that $X \setminus (S_{i_1} \cup S_{i_2} \cup \ldots \cup S_{i_n})$ is finite.*
- ***A4*** *If $i_1 < i_2 < \ldots$ are indices such that $S_{i_1} \supset S_{i_2} \supset \ldots$ then, given any N, we can find $n_a, n_b > N$ for which S_{n_a} contains all but finitely many elements of aS_{i_m} for some m, and S_{n_b} contains all but finitely many elements of bS_{i_p} for some p.*
- ***A5*** *For any $i \in \{0, 1, 2, \ldots\}$, there is $j > i$ such that $cS_i \subset S_j$ for some character $c \in \{a, b\}$.*
- ***A6*** *Given a nonempty word w in X there are only finitely many diametrisable sets S_i with $u_i \in S_i$ for which $wu_i \in S_i$.*

Then, with constructions described above, $(\overline{X}, d)$ is a compact metric space with continuous functions $f, g : \overline{X} \to \overline{X}$ that form a λ-contractive family, but no word in f and g has a fixed point.

2.3 Choosing the diametrisable sets

Our main task now is to find a collection of diametrisable sets $\mathcal{D}$ which has the properties **A1**-**A6**. The obvious candidates for the subsets in the desired collection are $W_w = wX$, where w is any word in X. Immediately, we observe that these, ordered by length of w, then by alphabetical order (so that $S_0 = W_\emptyset, S_1 = W_a, \dots$) satisfy all the properties we demand except for **A6**. Hence, we will use these as the pillar of our construction, however, to make **A6** hold, we need to modify these slightly. The issue with the sets described is that given any nonempty word $w \in X$, we allow W_w to contain all the initial segments of w^∞. With this in mind, we say that a nonempty word w in X is *forbidden* if there is another finite word u such that w is a prefix of u^∞ and $l(w) > l(u)^2$. Otherwise, say that w is *available*. For example, $\emptyset, a, abab$ are available, while $ababa$ is forbidden.

Proposition 2.10. *Given a word $w \in X$, either aw or bw is available.*

Proof. If $w = \emptyset$, aw is available. Suppose $l(w) \geq 1$ and that the claim is false, so aw is an initial segment of w_1^∞ for some non-empty w_1, bw is an initial segment of w_2^∞ for some non-empty w_2 and $l(w) \geq l(w_1)^2, l(w_2)^2$. We can permute w_1 cyclically to v_1 so that $av_1^\infty = w_1^\infty$ holds, and we can correspondingly transform w_2 to v_2. Observe that the last character of v_1 is a and of v_2 is b. This way, w becomes a prefix of v_i^∞ for $i = 1, 2$. But $l(w) \geq l(v_1)^2, l(v_2)^2$, hence $l(w) \geq l(v_1)l(v_2)$ and so $v_1^{l(v_2)} = v_2^{l(v_1)}$, by comparing them as initial segments of w. However, this implies equality of the last characters of v_1 and v_2, which is impossible. The claim now follows. □

In the same spirit, we prove the following statement.

Proposition 2.11. *Given a word $w \in X$, either wa or wb is available.*

Proof. Suppose, on the contrary contrary, both are forbidden. Let t_1, t_2 be words such that $wa \leq t_1^\infty$, $wb \leq t_2^\infty$, $l(wa) > l(t_1)^2, l(wb) > l(t_2)^2$. Observe that both $t_1^{l(t_2)}$ and $t_2^{l(t_1)}$ are prefixes of w, so being of the same length, they coincide. But, then $t_1^\infty = t_2^\infty$, which is a contradiction, as otherwise $wa \neq wb$ would be two prefixes of the same length of this infinite word. □

Corollary 2.12. *Let w be a non-empty word. Let u be an initial segment of w^∞, and suppose $l(u) \geq l(w)^2$. Take character s such that $v = us$ is not a prefix of w^∞. Then v is available.*

Say that a word w is *minimal* if it is non-empty and given non-empty u for which $u^\infty = w^\infty$ we have $l(w) \leq l(u)$.

Proposition 2.13. *A non-empty word w is not minimal if and only if there is word u such that $w = u^k$, for some $k \geq 2$.*

Proof. If $w = u^k$ with $k > 1$ then $l(w) > l(u)$ and $w^\infty = u^\infty$, therefore w is not minimal. Suppose now that we have non-empty w, for which there exists u such that $u^\infty = w^\infty$, but $l(u) < l(w)$. Write $d = \gcd(l(u), l(w))$, so $l(u) = qd, l(w) = pd$, for some positive integers p, q, in particular $p \geq 2$. Further $u^p = w^q = v_1 v_2 \dots v_{pq}$, where $v_1, v_2, \dots, v_{pq}$ are of length d. Considering successive copies of u we have that $v_{i+q} = v_i$, when $i \leq pq - q$ and similarly by looking at copies of w we have $v_{i+p} = v_i$ when $i \leq pq - p$. So $v_i = v_{p+i} = \cdots = v_{p(q-1)+i}$ for $i \in [p]$, (where for a positive integer N, $[N]$ denotes the set $\{1, 2, \dots, N\}$). Observe that $v_q = v_{2q} = \cdots = v_{pq}$ and as p and q are coprime $q, 2q, \dots, pq$ take all possible values modulo p hence $v_1 = v_2 = \cdots = v_{pq}$, allowing us to conclude $w = v_1^p$, $p > 1$. □

Having established these results about the words, we are ready to choose the diametrisable subsets $\mathcal{D}$ of X. Consider the following subsets.

For all available words w, including $\emptyset$, we include W_w in $\mathcal{D}$. We refer to these as the *W-type sets*, i.e say that S_i is of W-type if $S_i = W_w$, for some available w.

For all minimal words w, all integers p, r such that $p \in \{2^i : i \in \mathbb{N}_0\}$ and $0 \leq r \leq p - 1$, we set $A_{w,p,r} = \{u \in X : u \text{ initial segment of } w^\infty, l(u) \in \{r + ip : i \in \mathbb{N}\}, l(u) > l(w)^2\}$. Call these sets the *$A$-type* sets.

Finally, for each minimal word w and $k \in \mathbb{N}$, we define $B_{w,k}$, which we refer to as the *B-type* sets. For these, we need additional notation.

First of all, for each $k \in \mathbb{N}$ we define an infinite arithmetic progression I_k. We set $I_1 = \mathbb{N}$, $I_2 = I_1 \setminus \{\min I_1\} = \mathbb{N} \setminus \{1\}$. For each integer $m \geq 2$, if k is an integer such that $2^m - 1 \leq k \leq 2^m + 2^{m-1} - 2$, we set $I_k = \{s + i \cdot 2^{m-1} \colon i \in \mathbb{N}_0\}$ where

$s = \min I_{\frac{k-1}{2}+2^{m-2}}$, when k is odd; if k is even, then put $I_k = \{s+i\cdot 2^{m-1}\colon i \in \mathbb{N}_0\}$ where $s = \min I_{\frac{k-2}{2}+2^{m-2}} + 2^{m-2}$. On the other hand, if k is an integer such that $2^m + 2^{m-1} - 1 \leq k \leq 2^{m+1} - 2$, then we set $I_k = I_{k-2^{m-1}} \setminus \{\min I_{k-2^{m-1}}\}$.

Note that, given a minimal word w and $n \in \mathbb{N}$, by Corollary 2.12 we get a unique word w_n such that: w_n is of the form $v_n s_n$ where $v_n \leq w^\infty$ and s_n is a character, w_n is available, and $l(w_n) = l(w)^2 + n$. At last, we define $B_{w,k} = \cup_{i\in I_k} W_{w_i}$.

Thus, we set

$$
\begin{aligned}
\mathcal{D} =&\{W_w : w \in X, w \text{ is available}\}\\
&\cup\{A_{w,p,r}\colon w \in X, p, r \in \mathbb{Z}, w \text{ is minimal}, p \in \{2^i\colon i \in \mathbb{N}_0\}, 0 \leq r \leq p-1\}\\
&\cup\{B_{w,k} : w \in X, k \in \mathbb{N}, w \text{ is minimal}\}.
\end{aligned}
$$

To illustrate the definition of B-type sets, we list a couple of examples.

$$
\begin{aligned}
I_7 &= \{4, 8, 12, 16, \ldots\},\\
B_{a,7} &= W_{aaaab} \cup W_{aaaaaaaab} \cup W_{aaaaaaaaaaaab} \cup \ldots,\\
I_{13} &= \{9, 13, 17, 21, \ldots\},\\
B_{ba,13} &= W_{bababababaa} \cup W_{bababababababaa} \cup W_{bababababababababaa} \cup \ldots.
\end{aligned}
$$

Let us make a few easy remarks about $\mathcal{D}$. Fix a minimal word w. Then we have $B_{w,1} = W_{w^{l(w)}} \setminus (A_{w,1,0} \cup \{w^{l(w)}\})$. Also, if $m \geq 2$ is an integer, and k is an odd integer that satisfies $2^m - 1 \leq k \leq 2^m + 2^{m-1} - 2$, then $I_{\frac{k-1}{2}+2^{m-2}} = I_k \cup I_{k+1}$. Furthermore, if $I_{k_1} \cap I_{k_2} \neq \emptyset$ then $I_{k_1} \subset I_{k_2}$ or vice-versa.

For any $U \in \mathcal{D}$, observe that there is a unique word in U of the shortest length, which we will denote by $\sigma(U)$.

Let us now establish a few claims about the structure of $\mathcal{D}$, which will be exploited in the rest of the proof.

Proposition 2.14. *If $U \neq V$ are two diametrisable sets and they intersect, then one is contained in the other. Furthermore, if they are not identical, then $U \triangle V$ is infinite.*

Proof. We are going through possible types of U and V.

Case 1. U and V are W-type sets.

Suppose $U = W_{w_1}, V = W_{w_2}$, without loss of generality $l(w_1) \leq l(w_2)$.

If w_1 is not initial segment of w_2, then U and V do not intersect, so we must have $W_{w_1} \supset W_{w_2}$, that is $U \supset V$. If $U \neq V$, then $w_1 \neq w_2$, and hence $W_{w_1 s} \subset (U \setminus V)$, where s is character for which $w_1 s$ is not prefix of w_2. We will use this case for showing the other ones.

Case 2. U and V are A-type sets.

Suppose $U = A_{w_1,p_1,r_1}, V = A_{w_2,p_2,r_2}$, where w_1, w_2 are some minimal words, and p_1, p_2, r_1, r_2 are suitable integers. There is word $w \in U \cap V$, so w is initial segment of w_1^∞ and w_2^∞, while $l(w) \geq l(w_1)^2, l(w_2)^2$, from which we deduce that $w_1^{l(w_2)} = w_2^{l(w_1)}$, being the initial segment of w of length $l(w_1)l(w_2)$. Therefore $w_1^\infty = w_2^\infty$ and due to minimality $w_1 = w_2$. Now, due to definition of A-type sets for fixed minimal word, we get $U \subset V$ or vice versa and infinite symmetric difference.

Case 3. U is a A-type set, V is a B-type set.

Let $w \in U \cap V$. This makes w a prefix of some t^∞, where t is minimal and $l(t)^2 < l(w)$, as $U = A_{t,p,r}$, p, r being suitable integers. Also $w \in W_v \subset V$, some available v, so as v is an initial segment of w, hence t^∞, we have $l(v) \leq l(t)^2$, since v is available. But then $U \subset A_{t,1,0} \subset W_{t^{l(t)}} \subset W_v \subset V$, which proves the first claim.

On the other hand U has no available words, but V has infinitely many of these, which gives the second part.

Case 4. U is a A-type set, V is a W-type.

Same proof as in the **Case 3**.

Case 5. U and V are B-type sets.

Suppose $U = B_{w_1,k_1}, V = B_{w_2,k_2}$, for some minimal words w_1, w_2 and positive integers k_1, k_2. Let $w \in U \cap V$, thus $w \in W_{v_1} \subset B_{w_1,k_1}$ and $w \in W_{v_2} \subset B_{w_2,k_2}$. By **Case 1**, without loss of generality, $W_{v_1} \subset W_{v_2}$ holds.

If $v_1 = v_2$, letting u_i be v_i without the last character, gives us prefix of w_i^∞, $i \in [2]$, and $l(w_1)^2, l(w_2)^2 \leq l(u_1)$, so as before $w_1^\infty = w_2^\infty$ and due to minimality $w_1 = w_2$. So $U \subset V$ or $V \subset U$, due to construction of B-type sets for a fixed minimal word, and also the second part of the claim follows.

On the other hand, if $v_1 \neq v_2$, then $v_2 \leq u_1$, u_1 being v_1 after omitting the last character, as before. Further we have that u_1 is a prefix of w_1^∞, so v_2 is too, but v_2 is available, hence $l(v_2) \leq l(w_1)^2$, hence $U \subset W_{v_2} \subset V$.

For the second part of the claim, consider any other W-type set contained in V, distinct form W_{v_2}.

Case 6. U is a B-type set, V is a W-type set.

Let $V = W_v$, some available word v, and $w \in U \cap V$, so $w \in W_u \subset U$. If $W_v \subset W_u$, then $V \subset U$, so we are done, and second part follows as in previous case. Otherwise, by **Case 1**, $W_u \subsetneq W_v$, so $v \neq u$ and $v \leq u$. We have $U = B_{t,k}$, some minimal t and integer k, so $v \leq t^\infty$ and available so $l(v) \leq l(t)^2$, hence $U \subset W_v = V$. Also, $(W_v \setminus U) \supset W_{t^{l(t)}} \setminus B_{t,1} = A_{t,1} \cup \{t^{l(t)}\}$, which is infinite. $\square$

Proposition 2.15. *If U is any of the diametrisable sets, then there are unique V_1, V_2 (up to ordering) which are proper subsets of U in $\mathcal{D}$, such that $V_1 \cup V_2$ has almost all elements of U.*

Proof. Firstly, let us show the existence of such sets. Of course, we go through the possible types of set U. The only non-trivial case, that is the one that does not directly follow from construction of $\mathcal{D}$ is the third one.

Case 1. U is of A-type.

Say $U = A_{w,p,r}$, some minimal w and integers p, r. Then, we can take $V_1 = A_{w,2p,r}, V_2 = A_{w,2p,p+r}$.

Case 2. U is of B-type.

Say $U = B_{w,k}$, some minimal w and integer k. Then, by construction, we have either $B_{w,k} = B_{w,k_1} \cup B_{w,k_2}$, some two integers k_1, k_2, or $B_{w,k} = B_{w,k+1} \cup W_v$, some available v, giving us the needed sets V_1, V_2.

Case 3. U is of W-type.

Suppose $U = W_w$, for some available w. If both wa and wb are available, we can take $V_1 = W_{wa}$ and $V_2 = W_{wb}$.

Otherwise, ws is not available for some character s. Therefore, there is a word t such that ws is prefix of t^∞, and $l(t)^2 < l(ws) = l(w) + 1$. But

w is also a prefix of t^∞ and available so $l(t)^2 \geq l(w)$ so $l(w) = l(t)^2$, i. e. $w = t^{l(t)}$.

The next thing to do is to establish the minimality of t. Let u be any word such that $l(u) \leq l(t)$ and $t^\infty = u^\infty$. Then, as before ws is an initial segment of u^∞ and $l(u)^2 < l(ws) = l(w) + 1$, so by the same arguments we get $l(w) = l(u)^2$, thus $l(u) = l(t)$, as wanted. But then $W_w = A_{t,1,0} \cup B_{t,1} \cup \{w\}$, proving the existence part of the claim.

Suppose now that U' is any set strictly contained in U. Then, by Proposition 2.14, $U \setminus U'$ is infinite, so U' cannot contain both V_1, V_2. Also, from the same proposition we get that V_1 and V_2 are disjoint, as otherwise, one must contain the other and thus be equal to U. So, U' intersects at precisely one of V_1, V_2, since all diametrisable sets are infinite. W.l.o.g. U' intersects V_1. If $V_1 \subsetneq U'$, then $U' \setminus V_1$ is infinite, and thus intersects V_2, which is impossible. Hence, by Proposition 2.14, $U' \subset V_1$. So, if we had any other V_1', V_2' with the property in assumption, we would have $V_1' \subset V_1$ and $V_2' \subset V_2$, reordering if necessary, (we cannot have both sets included in the same V_i), so unless these are both equalities $V_1 \cup V_2 \setminus (V_1' \cup V_2')$ would be infinite, yielding a contradiction, and concluding the proof. □

Corollary 2.16. *If U is a diametrisable set with proper diametrisable subsets V_1, V_2, U', such that $U \setminus (V_1 \cup V_2)$ is finite, then V_1, V_2 are disjoint and one of them contains U'.*

Proposition 2.17. *Given word w, there are only finitely many diametrisable sets containing it.*

Proof. If $w \in W_u$, for some u, then u is prefix of w, hence there are only finitely many such sets containing w.

If $w \in A_{t,p,r}$, then, $l(w) \geq p, l(t)$, so there are only finitely many choices for t, p, r.

Finally, suppose $w \in B_{t,k}$. Length of w must be greater than $l(t)^2$, which gives us finitely many choices for minimal word t. Fix t. Recalling the definition of B-type sets, we have $B_{t,k} = \cup_{i \in I_k} W_{w_i}$, where $l(w_i) = l(t)^2 + i$. But if m is a nonnegative integer, then $\min I_k \geq m$ for $k \geq 2^m - 1$. Thus, for such k, we get $l(\sigma(B_{t,k})) \geq l(t)^2 + m$, so $w \in B_{t,k}$ for only finitely many k, as desired. □

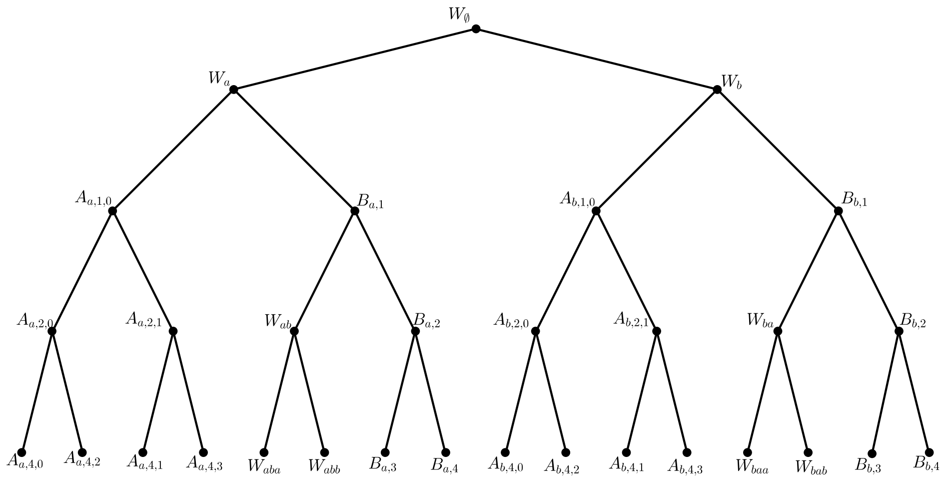


Figure 2.1: Structure of the collection of diametrisable sets

These claims serve us to better understand the structure of $\mathcal{D}$. In particular, we can view $\mathcal{D}$ as a binary tree whose nodes are the diametrisable sets, the root is $W_\emptyset$ and given a set $U \in \mathcal{D}$, its children V_1, V_2 are given by Corollary 2.16. What is not clear, however, is that the tree so defined actually contains all the diametrisable sets. But, given any such a set $U \in \mathcal{D}$, we have either $U = W_\emptyset$ or U is contained in one of the children of the root, by Corollary 2.16. Proceeding further in this fashion, either we reach U, or we get an infinite collection of diametrisable sets all containing U. But, that implies that if we do not reach U, its elements belong to infinitely many members of $\mathcal{D}$, which contradicts Proposition 2.17. Hence this binary tree has precisely $\mathcal{D}$ for its set of nodes. Moreover, to say that a diametrisable set U_1 is a subset of another such set U_2 is equivalent to having U_2 as an ancestor of U_1 in this binary tree. To depict what has just been discussed, we include Figure 2.1 which shows the first few layers of tree. We refer to this tree as $\mathcal{T}$.

2.4 Ordering $\mathcal{D}$

In order to finish constructing the counterexample, we must make $\mathcal{D}$ well-ordered, so that then we know which diametrisable set is which S_n. Defining such an order, and proving that it is in fact what we need, is the purpose of this section.

Consider the relation $<$ on $\mathcal{D}$, given as follows: if $U \neq V$, we say $U < V$ if any of these holds:

O1 $l(\sigma(U)) < l(\sigma(V))$,

O2 $l(\sigma(U)) = l(\sigma(V))$ and $U \supset V$,

O3 $l(\sigma(U)) = l(\sigma(V))$, none is contained in the other and we have that either U is of A-type, but V is not, or U is of B-type and V is of W-type,

O4 $l(\sigma(U)) = l(\sigma(V))$, none is contained in the other, they are of the same type and $\sigma(U)$ is alphabetically before than $\sigma(V)$.

Proposition 2.18. *If $U < V$ by **O2**, then either:*

(i) *both U and V are A-type, or,*

(ii) *both U and V are B-type, or,*

(iii) *U is B-type, V is W-type.*

Proof. Regard $\mathcal{D}$ as a binary tree $\mathcal{T}$ that was described in the final remarks of the previous section. Then, $U \supset V$ tells us that U is an ancestor of V, and as $U < V$ by **O2**, we have $\sigma(U) = \sigma(V)$. Thus, the shortest word must be the same for all sets on the path from U to V in $\mathcal{T}$. Now, we analyze the splits, i.e. given a node, what its children are. Returning back to the choice of the diametrisable sets, we see that A-type sets always split into two A-type sets, and B-type sets split into B and W-type sets. We conclude that the claim is true if, when W-type set splits into an A-type and a B-type set, the shortest word of the parent is not in any of the children. But, suppose that we have such a situation, a set $T = W_w$, whose children are $A_{t,1,0}$ and $B_{t,1}$. From the proof of **Case 6** of Proposition 2.14, recall that $w = t^{l(t)}$. But then $w \notin A_{t,1,0}$ and $w \notin B_{t,1}$, as desired. □

Proposition 2.19. *Relation $<$ on the chosen sets is a total order. Furthermore, the collection of chosen sets is well ordered under $<$.*

Proof. If U, V are two distinct sets among the chosen ones, we want that precisely one of $U < V$, $V < U$ is true.

Suppose neither of these holds. Hence $\sigma(U) = \sigma(V)$. But then their intersection is non-empty, hence one is contained in the other, so $U < V$ or vice versa by **O2**.

Now, assume that both hold. Therefore, $l(\sigma(U)) = l(\sigma(V))$, none is contained in the other (otherwise we have $U \subset V$ and $V \subset U$, thus $U = V$), they are of the same type, and further $\sigma(U) = \sigma(V)$. But as before, these must intersect, leading us to a contradiction.

Having proved the trichotomy, we now move to establishing transitivity of the relation. Suppose we have three chosen sets U, V, T such that $U < V < T$, from which $U \neq V$, $V \neq T$ follows. Further, we cannot have $T = U$ as this would imply $U < V < U$. Hence, we can assume that all three sets are distinct. If **O1** holds for $U < V$ or $V < T$, then it also holds for U, T. So, assume this is not true. Then we have the following cases:

Case 1. $U < V$ by **O2**, $V < T$ by **O2**.

Then $U \supsetneq V \supsetneq T$, so $U < T$ by **O2** as well.

Case 2. $U < V$ by **O2**, $V < T$ by **O3**.

By Proposition 2.18, we see that (as V cannot be of W-type), U and V are of same type. As $V \subset U$ and $V \not\subset T$, then $U \not\subset T$, so either $T \subset U$ and $U < T$ by **O2**, or $U < T$ by **O3**.

Case 3. $U < V$ by **O2**, $V < T$ by **O4**.

As above, we get $U \not\subset T$. If $T \subset U$ then $T > U$. Hence, assume that $T \not\subset U$. Suppose that U is B-type and V is W-type, thus $U < T$ by **O3**. Otherwise, by Proposition 2.18 U and V have the same type, hence so does T, and $\sigma(U) = \sigma(V)$ (because of inclusion) so $U < T$ by **O4**.

Case 4. $U < V$ by **O3**, $V < T$ by **O2**.

If $T \supset U$, then $U \subset V$, which is impossible, so $U \not\subset T$. If $T \subset U$, we are done, otherwise from Proposition 2.18 we obtain $U < T$ by **O3**.

Case 5. $U < V$ by **O3**, $V < T$ by **O3**.

Thus U is of A-type, V is of B-type, T is of W-type. By Proposition 2.18, we conclude that $U \not\subset T$, $T \not\subset U$, so $U < T$ by **O3**.

Case 6. $U < V$ by **O3**, $V < T$ by **O4**.

By Proposition 2.18, $U \not\subset T$, so either $T \subset U$ giving $U < T$ by **O2**, or none is contained in the other and $U < T$ by **O3**.

Case 7. $U < V$ by **O4**, $V < T$ by **O2**.

Having U as a subset of T implies $U \subset V$ which is impossible. So $U \not\subset T$ and if $T \subset U$, then $U < T$ by **O2**. Otherwise, unless U and T are of the same type, we have $U < T$ by **O3**, due to Proposition 2.18. Finally, from inclusion we deduce $\sigma(T) = \sigma(U)$ and thus $U < T$ by **O4**.

Case 8. $U < V$ by **O4**, $V < T$ by **O3**.

If $U \subset T$, by Proposition 2.18, we reach a contradiction. Hence $U \supset T$, so $U < T$ by **O2**, or $U < T$ by **O3** otherwise.

Case 9. $U < V$ by **O4**, $V < T$ by **O4**.

If $T \supset U$ or vice versa, we have $\sigma(T) = \sigma(U)$ which is impossible. As all three sets are of same type, we get $U < T$ by **O4**.

Finally, given a subset P of $\mathcal{D}$, consider its subset P' of those sets $U \in P$ such that $l(\sigma(U)) = \min\{l(\sigma(V)) : V \in P\}$. This is finite by Proposition 2.17, hence we can find the minimal element of P' with respect to $<$, which is smaller than any member of $P \setminus P'$ by **O1**, making $\mathcal{D}$ well-ordered under $<$. $\square$

Hence, as $\mathcal{D}$ is countable, we can take $S_0 = \min \mathcal{D}$ and for $k \geq 1$, $S_{k+1} = \min(\mathcal{D} \setminus \{S_0, S_1, \dots, S_k\})$. Observe that for any given $U \in \mathcal{D}$ there are only finitely many words of length at most $l(\sigma(U))$. Proposition 2.17 then tells us that there are only finitely many $V \in \mathcal{D}$ such that $l(\sigma(V)) \leq l(\sigma(U))$. Hence, there are only finitely many $V \in \mathcal{D}$ such that $V < U$, so $U = S_k$ for some $k \in \mathbb{N}$. Therefore, $\{S_0, S_1, S_2, \dots\} = \mathcal{D}$. Note also that $S_0 = X = W_\emptyset$ because $W_\emptyset$ is the only set whose shortest word has zero length.

2.4.1 Proof that $\mathcal{D}$ satisfies the required properties

All that is left is to show that $S_0, S_1, \dots$ satisfy **A1** - **A6**. Having done the most of the work already, the proofs of the following claims will either be rather short or the obvious case-examination.

Proposition 2.20. $(S_n)_{n\geq 0}$ *satisfy* ***A1***.

Proof. Let S_i, S_j be such that $i < j$ and they intersect. Thus, $S_i < S_j$, $l(\sigma(S_i)) \leq l(\sigma(S_j))$ and also $S_i \subset S_j$ or $S_i \supset S_j$, by Proposition 2.14. But if $S_i \subset S_j$, then we must have $l(\sigma(S_i)) = l(\sigma(S_j))$ and hence $S_j < S_i$ by **O2**, which is a contradiction. Also $S_0 = X$. $\square$

Proposition 2.21. $(S_n)_{n\geq 0}$ *satisfy* ***A2***.

Note that this is Proposition 2.17, but we include it here for completeness.

Proposition 2.22. $(S_n)_{n\geq 0}$ *satisfy* ***A3***.

Proof. Let N be given. By Corollary 2.16, given S_i, we can find S_j, S_k, disjoint subsets of S_i, which cover all but finitely many elements of S_i, therefore $i < j, k$ by **O1** or **O2**. So, we can start with S_0, and perform such splits until we are left with sets $S_{m_1}, S_{m_2}, \ldots, S_{m_k}$, with $m_1, m_2, \ldots, m_k > N$, which cover almost all elements of X, as in each split we lose only finitely many elements. $\square$

Proposition 2.23. $(S_n)_{n\geq 0}$ *satisfy* ***A4***.

Proof. Suppose that $S_{i_1} \supset S_{i_2} \supset \ldots$ for some $i_1 < i_2 < \ldots$. As usual, we consider different cases.

Case 1. There is set of A-type among these.

Let S_{i_k} be such a set. As A-type set splits into A-type sets, we have that when $n \geq k$, $S_{i_n} = A_{w,p_n,r_n}$, some minimal word w, and integers p_n, r_n, and $p_{n+1} > p_n$, so in fact $p_{n+1} \geq 2p_n$, as these are powers of 2. In particular, we deduce that for sufficiently large n, $p_n > nl(w)$ and thus w^n is prefix of all words in S_{i_n} implying $S_{i_n} \subset W_{w^n}$. By Proposition 2.10, one of aw^n, bw^n is available, w.l.o.g. the former is true, hence $aS_{i_n} \subset W_{aw^n} = S_{j_n}$, some j_n.

Consider the cyclic permutation u of w such that $sw = us$, s being the last character of w. Let v be a word such that $v^\infty = u^\infty$ and $l(u) \geq l(v)$. But then for the cyclic permutation t of v such that for character s' we have $s't = vs'$, we have $s't^\infty = v^\infty = sw^\infty$, so $l(u) = l(t) \geq l(w) = l(v)$, proving the minimality of v. If $s = a$, we would have that aw^n is not available as it would be initial segment of u^∞, but $l(u) = l(w)$. Hence $s = b$, and $bS_{i_n} \subset A_{v,p_n,r} = S_{j_n}$, where $r = r_n + 1$, unless $r_n = p_n - 1$ and then $r = 0$, j_n suitable index. As j_n tends to infinity as n does, **A4** holds in this case.

Case 2. There are no A-type sets, but there are infinitely many of W-type.

Denote W-type sets among these by $W_{w_1} \supsetneq W_{w_2} \supsetneq \dots$. As w_i is prefix of w_{i+1}, for all i, these define an infinite word w whose initial segments the words w_i are. By Proposition 2.10, w.l.o.g. aw_i is available infinitely often, so we can take $W_{aw_{i_1}}$ for suitable $i_1 < i_2 < \dots$, to establish a part of the claim.

Similarly, if there are infinitely many initial segments of bw available, choosing these and their corresponding W-type sets establishes the claim. Suppose contrary, i. e. there is m such that prefixes of bw of length greater or equal to m are all forbidden. Denote by u_n initial segment of bw of length n, and let t_n be the shortest word such that $l(t_n)^2 < l(u_n)$ and u_n is initial segment of t_n^∞. Now, suppose there is no $n \geq m$ such that $l(t_{n+1}) > l(t_n)$, hence $l(t_m) \geq l(t_{m+1}) \geq \dots$, so $bw = t_n^\infty$, some n. But this means that w_i are forbidden from some point, resulting in a contradiction. So, there must be such an $n \geq m$, pick the smallest possible. Hence u_{n+1} is not the initial segment of t_n^∞, but u_n is both initial segment of t_n^∞ and t_{n+1}^∞. Further, $l(u_n) \geq l(t_n)^2, l(t_{n+1})^2$ so as before, $t_n^\infty = t_{n+1}^\infty$, but u_{n+1} is prefix of the latter, but not former, giving us a contradiction.

Case 3. Almost all sets are of B-type.

Given $S_{i_n} = B_{w,k}$, let s be the last character of w, so $sw^{l(w)}$ is forbidden. Let u be the cyclic permutation of w such that $sw = us$, and so u is minimal as well, by arguments in **Case 1** of this proof. Then, $sB_{w,k} = B_{u,l}$ or $sB_{w,k} = B_{u,l} \setminus W_v$ for suitable index l and word v, so take $S_{j_n} = B_{u,l}$. Let s' be the character not equal to s and u be $\sigma(B_{w,k})$ without the last character. Then as su is forbidden, so $s'u$ is available and $s'B_{w,k} \subset W_{s'u} = S_{j_n}$. As j_n tends to infinity as n does, we are done. □

Proposition 2.24. *$(S_n)_{n\geq 0}$ satisfy **A5**.*

Proof. Let S_n be given. If it is of A or W-type, $S_n \subset W_{\sigma(S_n)}$, so choose a character s such that $s\sigma(S_n)$ is available and hence $sS_n \subset W_{s\sigma(S_n)}$ and $S_n < W_{s\sigma(S_n)}$, since $l(\sigma(S_n)) < l(\sigma(W_{s\sigma(S_n)}))$. If S_n is of B-type, then let u be the shortest word in S_n after erasing the last character, so $S_n \subset W_u$ and once again choose $s \in \{a, b\}$ for which su is available, hence $sS_n \subset W_{su}$. If W_{su} intersects

W_u, it must be its subset and u prefix of su, but then $u = s^{l(u)}$, so su is forbidden, as $l(u) \geq 1$. So W_{su} and W_u are disjoint, hence W_{su} and S_n are also. Combining this with $l(\sigma(S_n)) = l(\sigma(W_{su})$ and comparing the types gives $S_n < W_{su}$, by **O3**. □

Proposition 2.25. *$(S_n)_{n \geq 0}$ satisfy **A6**.*

Proof. Let $w \neq \emptyset$ be given. We will divide the proof into three cases, each showing the claim for particular set type.

Case 1. Suppose for some word u we have $u, wu \in S_n = A_{t,p,r}$, where t is minimal. Hence $l(u) > l(t)^2$. Suppose further $l(w) < l(t)$. So w is an initial segment of u, as u is an initial segment of wu. But then, w^2 is also an initial segment of u, etc. up to $w^{l(t)}$ as $l(u) > l(t)^2 > l(w)l(t)$. Hence $t^{l(w)} = w^{l(t)}$, but t is minimal so $l(w) \geq l(t)$. Hence we have only finitely many choices for A-type S_n, as $l(w) \geq l(t)$ and $p \leq l(w)$ must hold.

Case 2. If S_n is of W-type, say W_v, we have $u, wu \in W_v$, v available. As there are only finitely many v such that $l(v) \leq l(w)$, w.l.o.g. $l(v) > l(w)$. We have $u = vr_1$, some word r_1. Hence $wvr_1 \in W_v$ so $wv \in W_v$. But then $wv = vr_2$, some r_2, so $v = wv_1$, for some v_1, as $l(w) < l(v)$, and $wwv_1 = wv_1r_2$ implies $wv_1 = v_1r_2$. We can iterate this until $v = w^k v_k, l(v_k) < l(w)$. But $wv_k = v_k r_{k+1}$, some r_{k+1}, making v an initial segment of w^∞, but it is available hence $l(v) \leq l(w)^2$, therefore we have finitely many choices for S_n of W-type.

Case 3. Finally, suppose S_n is B-type, and $u, wu \in S_n$. Then we have two available words w_1s_1, w_2s_2, where s_1, s_2 are characters, w_1, w_2 prefixes of t^∞, some minimal word t, $u \in W_{w_1s_1}, wu \in W_{w_2s_2}, l(w_1), l(w_2) \geq l(t)^2$. So $u = w_1s_1r_1$, $wu = w_2s_2r_2$ holds for some words r_1, r_2.

Suppose $l(w) \leq l(t)$. Let wu' be the initial segment of wu of length $l(t)^2$ thus it is a prefix of w_2, and hence of t^∞. Thus $wt^{l(t)-1}$ is a prefix of $t^{l(t)}$. Hence, $w^k t^{l(t)-k}$ is a prefix of $t^{l(t)}$ for all $k \in [l(t)]$. In particular, $w^{l(t)}$ is prefix of $t^{l(t)}$, thus $w^{l(t)} = t^{l(w)}$, implying $w^\infty = t^\infty$, but t is minimal, so $w = t^\alpha$, some $\alpha \geq 1$, so $w = t$ as $l(w) \leq l(t)$. Now we have $wu = w_2s_2r_2 = ww_1s_1r_1 = tw_1s_1r_1$, which differ from t^∞ for the first time at s_1

and s_2, hence $w_2 = tw_1$. However, due to construction of B-type sets and the fact that the common difference of arithmetic progression I_k is at least $k/4$, there are only finitely many k for which $B_{w,k}$ have such $W_{w_1s_1}, W_{w_2s_2}$ as subsets.

Now, suppose $l(w) > l(t)$. If the claim is to be false, we can assume without loss of generality, that for infinitely many k we have some $u \in B_{t,k}$ and $wu \in B_{t,k}$ too. Hence we can assume that there are w_1, w_2 prefixes of t^∞, with some characters s_1, s_2, such that w_1s_1, w_2s_2 are available, $u \in W_{w_1s_1}, wu \in W_{w_2s_2}$, w_1, w_2 arbitrarily long, thus say $l(w_1), l(w_2) > l(w)^2$. So $u = w_1s_1r_1$, $wu = w_2s_2r_2$ for some words r_1, r_2, thus $wu = ww_1s_1r_1 = w_2s_2r_2$. Hence $t^{l(w)}$ is a prefix of w_2 as $l(w_1) > l(w)^2 > l(t)^2$, and similarly $wt^{l(w)-1}$ is initial segment of ww_1 so both are prefixes of wu hence $t^{l(w)}$ is a prefix of $wt^{l(w)-1}$, which is then prefix of $w^2t^{l(2)-2}$, etc. and a prefix of $w^{l(w)}$, so $w^\infty = t^\infty$ and due to minimality $w = t^k$, some $k \geq 2$. Hence $w_2s_2r_2 = wu = t^kw_1s_1r_1$ so the character where wu first differs from t^∞ is at the same time at s_1 and s_2, hence $w_2 = t^kw_1 = ww_1$, implying $l(w_2) = l(w_1) + l(w)$, but as previously explained, this can occur just for finitely many $B_{t,k}$, which proves the claim. $\square$

Having proved the desired properties of our collection of sets, we are ready to conclude:

Theorem 2.26. *Given $\lambda \in (0,1)$, there is a compact (pseudo-)metric space (X,d) on which we have continuous functions $f, g : X \to X$ such that given $x, y \in X$ either $d(f(x), f(y)) \leq \lambda d(x,y)$ or $d(g(x), g(y)) \leq \lambda d(x,y)$ holds, but no word in f, g has a fixed point.*

3 Commuting Contractive Families

This chapter contains the proof of Theorem 1.7, which we recall here.

Theorem. *Let (X, d) be a complete metric space and let $\{f_1, f_2, f_3\}$ be a commuting λ-contractive family of operators on X, for a given $\lambda \in (0, 10^{-23})$. Then f_1, f_2, f_3 have a common fixed point.*

3.1 Main goal, notation and definitions

In this section, we provide the notation and definitions that will be used extensively throughout the proof of Theorem 1.7. We write $\mathbb{N}_0$ for the set of nonnegative integers and recall that for a positive integer N, $[N]$ stands for the set $\{1, 2, \ldots, N\}$.

When a is an ordered triple of nonnegative integers and $x \in X$, we define $a(x) = f_1^{a_1} \circ f_2^{a_2} \circ f_3^{a_3}(x)$. Since our functions commute, we have $a(b(x)) = (a + b)(x)$, for $a, b \in \mathbb{N}_0^3$.

Pick an arbitrary point p_0 of our space X, and define a new pseudometric space (abusing the notation slightly) $G(p_0) = (\mathbb{N}_0^3, d)$, where $d(a, b) = d(a(p_0), b(p_0))$, when a, b, are ordered triples of non-negative integers. Therefore, we will actually work on an integer grid instead. Define e_i to be triple with 1 at position i, and zeros elsewhere. We now derive a few basic observations culminating in a proposition that implies Theorem 1.7 and whose proof will therefore occupy most of this chapter.

Proposition 3.1. *Let (X, d) be a complete metric space and $\lambda \in (0, 10^{-23})$ given, with $f_1, f_2, f_3 : X \to X$ which form a commuting λ-contractive family. Then for some i, f_i has a fixed point.*

Proposition 3.2. *Proposition 3.1 implies Theorem 1.7.*

Proof. Without loss of generality, we have a fixed point x of f_1. Thus, define X_1 to be the set of all fixed points of f_1. It is a closed subspace of X, hence complete. Further, $s \in S_1$ implies $f_1(f_i(s)) = f_i(f_1(s)) = f_i(s)$, so $f_i(s) \in S_1$, hence the other two functions preserve S_1, and form a λ-contractive family themselves, so f_2 has a fixed point in S_1, and repeat the same argument once more to obtain a common fixed point. $\square$

Proposition 3.3. *Let $(\mathbb{N}_0^3, d)$ be a pseudometric space and $\lambda \in (0, 10^{-23})$. Suppose that given any $a, b \in \mathbb{N}_0^3$, there is $i \in [3]$ such that $\lambda d(a, b) \geq d(a+e_i, b+e_i)$. Then there is a Cauchy sequence $(x_n)_{n\geq 1}$ in this space, such that $x_{n+1} - x_n$ is always an element of $\{e_1, e_2, e_3\}$.*

Proposition 3.4. *Proposition 3.3 implies Theorem 1.7.*

Proof. It suffices to show that Proposition 3.3 implies Proposition 3.1. Let (X, d) be a metric space as in Proposition 3.1, along with three functions acting on it. Pick an arbitrary point $p_0 \in X$, and consider pseudometric space $G(p_0)$ defined before. By Proposition 3.3, we have a Cauchy sequence $(x_n)_{n\geq 1}$, with the property above. So, $(x_n(p_0))$ is Cauchy in X. Without loss of generality, we have that x_n and x_{n+1} differ by e_1 infinitely often, say for $(x_{n_i})_{i\geq 1}$, $x_{n_i+1} = x_{n_i}+e_1$ holds. As X is complete, $x_n(p_0)$ converges to some x. Hence $x_{n_i}(p_0)$ converges to x, and so does $f_1(x_{n_i}(p_0))$, but f_1 is continuous, thus, $f_1(x) = x$. $\square$

Therefore, it suffices to prove Proposition 3.3. The following definitions aim to capture some of the structure of the integer grid relevant to our proof.

Let x be a point in the grid. Define $\rho(x)$ to be the maximum of the distances $d(x, x+e_1), d(x, x+e_2), d(x, x+e_3)$. As we shall see in the following section, ρ will be of fundamental importance. Given x in the grid, we define $N(x) = \{x+e_1, x+e_2, x+e_3\}$ and refer to this set as the *neighbourhood* of x.

Let S be a subset of the grid. Given $k \in [3]$, we say that S is a *k-way* set, if for all $s \in S$, precisely k elements of $N(s)$ are in S. We denote the unique 3-way set starting from x by $\langle x\rangle_3 = \{x+k : k \in \mathbb{N}_0^3\}$.

3.2 Overview of the proof of Proposition 3.3

The proof of Proposition 3.3 will occupy the most of the remaining part of this chapter. To elucidate the proof, we will structure it in a few parts. The short first section will explain our strategy in the proof along with some of the basic ideas. The second part will be about k-way sets and how they interact with each other. Afterwards, we shall be dealing with local structure, namely we shall show existence or non-existence of certain finite sets of points, and our main means to this end will be the k-way sets. Finally, after we have clarified the local structure sufficiently well, we will be able to obtain the final contradiction. Let us now be more precise and elaborate on these parts of the proof.

First of all, we shall establish a few basic facts about ρ, most importantly $\mu = \inf \rho(x) > 0$, where x ranges over all points. The proof of this statement is based on a lemma that says $d(x, y) \leq (\rho(x) + \rho(y))/(1 - \lambda)$. The fact that $\mu > 0$ will be the pillar of the proof, and the mentioned lemma will be used quite frequently. The basic idea which is introduced in this part of the proof is to create sets of points by contracting with some previously chosen ones (by contracting a pair x, y we mean choosing suitable function f in our family such that $d(f(x), f(y)) \leq \lambda d(x, y)$). By doing so, we will be able to construct k-ways sets of bounded diameter.

After that, we shall prove a few propositions about the k-way sets. For example, if we have 3-way set of bounded diameter then it contains 2-way subset of much smaller diameter, in a precise sense discussed afterwards. At first glance, it seems that we have lost a dimension by doing this, however, we shall also show that if we have 2-way set of sufficiently small diameter, we can obtain 3-way set of small diameter as well. So, for example, given K and provided λ is small enough, we cannot have 3-way sets of diameter $K\mu$, and we cannot have 2-way sets of diameter $\lambda K\mu$ inside every 3-set. From that point on, we shall combine the results and approaches of these two parts in the proof. Most of the claims that we establish later will either show that certain finite configuration (by which we mean finite set of points with suitable distances between) exists or do not exist, and we do so by supposing contrary, contracting the new points with the given ones and finding suitable k-way sets, which give us a contradiction.

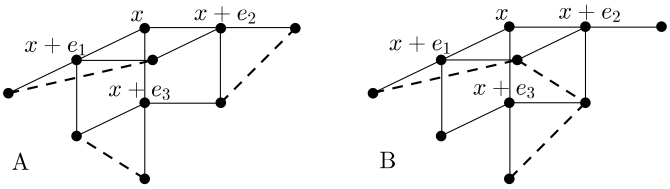


Figure 3.1: Examples of diagrams

As a basic example of this method, we note that each point x induces a 1-way set of diameter at most $2\rho(x)/(1-\lambda)$, and importantly, such a set exists in every 3-way set. With a greater number of suitable points we are able to induce bounded k-way sets for larger k. Using the facts established, we prove the existence or non-existence of specific finite sets. Gradually, we learn more about the local structure of the grid. For example, for some constant C (independent of λ) we have y with $\rho(y) \leq C\mu, d(y+e_1, y+e_2) \leq \lambda C\mu$, provided λ is small enough. Similarly, we shall establish that there is no point y with $\rho(y) \leq C\mu, \operatorname{diam} N(y) \leq \lambda C\mu$, for suitable λ, C. Such points will be used at a few places in the later part of the proof and in the final argument to reach the contradiction.

Let us now introduce the (somewhat vague) notion of a *diagram* of a point x. A diagram for x contains the information about the contractions in $\{x\} \cup N(x)$. Diagrams will be shown as figures, and usually the dashed lines will imply that the corresponding edge is a result of a contraction. In the Figure 3.1 we give examples of two diagrams[1], the left one, denoted by A, tells us among others that $x+e_1, x+e_2$ are contracted by 1 (i.e. $d(x+2e_1, x+e_1+e_2) \leq \lambda d(x+e_1, x+e_2)$). The claims established so far allow us to have a very restricted number of possibilities for diagrams, and one of the possible strategies will then be to classify the diagrams, see how they fit together and establish the existence of a 1-way Cauchy sequence. The most important claim that we use for rejecting diagrams is the following proposition. (Here $C_1 = 49158$.) Let us now introduce the (somewhat vague) notion of a *diagram* of a point x. A diagram for x contains

[1]In other figures we shall not explicitly name the points on the diagram itself, however, the coordinate axes will always be the same.

the information about the contractions in $\{x\} \cup N(x)$. Diagrams will be shown as figures, and usually the dashed lines will imply that the corresponding edge is result of a contraction. In the Figure 3.1 we give an example of two diagrams[2], the left one, denoted by A, tells us among others that $x+e_1, x+e_2$ are contracted by 1 (i.e. $d(x+2e_1, x+e_1+e_2) \leq \lambda d(x+e_1, x+e_2)$). The claims established so far allow us to have a very restricted number of possibilities for diagrams, and one of the possible strategies will then be to classify the diagrams, see how they fit together and establish the existence of a 1-way Cauchy sequence. The most important claim that we use for rejecting diagrams is the following proposition. (Here $C_1 = 49158$.)

Proposition 3.5. *Given $K \geq 1$, suppose we have x_0, x_1, x_2, x_3 such that* $\operatorname{diam}\{x_i + e_j : i, j \in [3], i \neq j\} \leq \lambda K\mu$. *Furthermore, suppose $\rho(x_0) \leq K\mu$ and that $d(x_0, x_i) \leq K\mu$ for $i \in [3]$. Let $\{a, b, c\} = [3]$.*

Provided $\lambda < 1/(820 C_1 K)$, whenever there is a point x which satisfies $d(x+e_a, x+e_b) \leq \lambda K\mu$ and $d(x, x_0) \leq K\mu$, then we have $d(x+e_c, x_c+e_c) \leq 16\lambda K\mu$.

The final part of the proof is based on the following proposition.

Proposition 3.6. *Fix arbitrary x_0 with $\rho(x_0) < 2\mu$. Given $K \geq 1$, when $i \in [3]$, define $S_i(K, x_0) = \{y : d(x_0, y) \leq K\mu, d(y, y+e_i) \leq K\mu\}$. Provided $1 > 10\lambda K C_1$, in every $\langle z \rangle_3$ there is t such that $d(t, x_0) \leq 3K\mu$, but for some i we have $s \overset{i}{\not\nearrow} t$ when $s \in S_i(K, x_0)$.*

Using the point t, whose existence is provided, we shall discuss the cases on $d(t+e_1, t+e_2)$ being large or small. Both cases help us to reject many diagrams and then to establish the contradiction in a straightforward manner.

To sum up, the basic principle here is that contractions ensure that we get specific finite sets. On the other hand, certain finite sets empower contractions further, allowing us to construct k-way sets of small diameter. Therefore, if we are to establish a contradiction, we can expect a dichotomy; either we get finite sets that imply global structure that is easy to work with, or we do not have such sets, and we impose strong restrictions on the local structure of the grid.

[2] In other figures we shall not denote the points on the diagram itself, however, the coordinate axes will always be the same.

We are now ready to start the proof of Proposition 3.3. The proof will run for the most of the chapter, ending in Section 3.7.

Proof of Proposition 3.3. Suppose contrary, there is no 1-way Cauchy sequence in the given pseudometric space on $\mathbb{N}_0^3$. This condition will, as we shall see, imply a lot about the structure of the space, and we will start by getting more familiar with the function ρ, which will, as it was already remarked, play a fundamental role.

3.3 Basic finite contractive configurations arguments and properties of ρ

In this section we establish some properties of ρ, together with some claims which will come in handy at several places throughout the proof.

Lemma 3.7 ((Furthest neighbour inequality - FNI))**.** *Given x, y in the grid we have $d(x,y) \leq (\rho(x) + \rho(y))/(1-\lambda)$.*

Proof. Let i be such that $\lambda d(x,y) \geq d(x+e_i, y+e_i)$, which we denote from now on by $x \overset{i}{\frown} y$, and say that i *contracts*[3] x, y. Using the triangle inequality a few times yields $d(x,y) \leq d(x, x+e_i) + d(x+e_i, y+e_i) + d(y+e_i, y) \leq \lambda d(x,y) + \rho(x) + \rho(y)$, which implies the result. □

Similarly to $x \overset{i}{\frown} y$, we write $x \overset{i}{\not\frown} y$ to mean that $d(x+e_i, y+e_i) > \lambda d(x,y)$.

Lemma 3.8. *Let x, y be any two points in the grid. Then we can find a 1-way subset S, such that $y \in S$ and given $\epsilon > 0$ we have $d(s,x) \leq \frac{1}{1-\lambda}\rho(x) + \epsilon$ for all but finitely many $s \in S$.*

Proof. Consider the sequence $(x_n)_{n\geq 0}$ defined inductively by $x_0 = y$ and for any $k \geq 0$, we set $x_{k+1} = x_k + e_i$ when i contracts x and x_k. By induction on k, we prove that $d(x, x_k) \leq \lambda^k d(x,y) + \rho(x)/(1-\lambda)$.

Case $k = 0$ is clear as $\rho(x_0) \geq 0$. If the claim holds for some k and $x_k \overset{i}{\frown} x$, then by the triangle inequality we have $d(x_{k+1}, x) \leq d(x_{k+1}, x+e_i) + d(x+e_i, x) \leq \lambda d(x_k, x) + \rho(x_0) \leq \lambda^{k+1} d(x,y) + \lambda\rho(x_0)/(1-\lambda) + \rho(x_0) \leq \lambda^{k+1} d(x,y) + \rho(x_0)/(1-$

[3] We also say x, y is *contracted* by i, or x, y is *contracted in the direction* e_i.

$\lambda)$, as desired.

Now, take n sufficiently large so that $\rho(x_0)/(1-\lambda)+\lambda^n d(x,y) \leq \frac{1}{1-\lambda}\rho(x_0)+\epsilon$. Hence $d(x_k,x) \leq \frac{1}{1-\lambda}\rho(x_0)+\epsilon$ for all $k \geq n$, so choose $(x_k)_{k\geq 0}$ as the desired set. $\square$

Proposition 3.9. *Given any x in the grid, we have $\rho(x) > 0$.*

Proof. Suppose contrary, $\rho(x) = 0$ for some x. Then Lemma 3.8 immediately gives a 1-way Cauchy sequence, which is a contradiction. $\square$

Proposition 3.10. *The infimum* $\inf\{\rho(x) : x \in \mathbb{N}_0^3\}$ *is positive.*

This result is one the of crucial structural properties for the rest of the proof, and having it in mind, we will try either to find small ρ, or use the structure implied to get a Cauchy sequence, which will yield a contradiction. To prove this statement, we use Lemma 3.8, the difference being that we now contract with many different points of small ρ instead of just one.

Proof. Suppose contrary, hence we get $(y_n)_{n\geq 1}$ such that $\rho(y_n) < 1/n$. As ρ is always positive, we can assume that all elements of the sequence are distinct.

We define a 1-way sequence $(x_k)_{k\geq 0}$ as follows: start from arbitrary x_0 and contract with y_1 as in the proof of Lemma 3.8 until we get a point x_{k_1} with $d(x_{k_1}, y_1) \leq 2\rho(y_1)/(1-\lambda)$ (such a point exists by Lemma 3.8). Now, start from x_{k_1} and contract with y_2 until we reach x_{k_2} with $d(x_{k_2}, y_2) \leq 2\rho(y_2)/(1-\lambda)$. We insist that $k_{i+1} > k_i$ for all possible i, so that, proceeding in this way, one defines the whole sequence. Recalling the estimates in the proof of Lemma 3.8, we see that for $k_i \leq j \leq k_{i+1}$ we have $d(x_j, y_{i+1}) \leq d(x_{k_i}, y_{i+1}) + \rho(y_{i+1})/(1-\lambda) \leq d(x_{k_i}, y_i) + d(y_i, y_{i+1}) + \rho(y_{i+1})/(1-\lambda)$. So by FNI, we see that $d(x_j, y_{i+1}) \leq (3\rho(y_i) + 2\rho(y_{i+1}))/(1-\lambda) \leq \frac{5}{i(1-\lambda)}$. Hence, if we are given any other $x_{j'}$ with $k_{i'} \leq j' \leq k_{i'+1}$, by the triangle inequality and FNI we see that $d(x_j, x_{j'}) \leq \frac{6}{1-\lambda}(1/i + 1/i')$, which is enough to show that the constructed sequence is 1-way Cauchy. $\square$

We will denote $\inf \rho$, where the infimum is taken over the whole grid, by μ. The proposition we have just proved gives $\mu > 0$.

3.4 Properties of and relationship between k-way sets

The following propositions are about the nature of k-way sets. These both confirm their importance for the problem and are useful at various places throughout the proof.

Proposition 3.11. *If $\langle\alpha\rangle_3$ is a 3-way set of diameter D, then it contains a 2-way subset of diameter not greater than $\lambda C_1 D$, where $C_1 = 49158$.*

Proof. The proof will be a consequence of Proposition 3.12 and Lemma 3.14, each requiring its own auxiliary lemma. Let us start by establishing

Proposition 3.12. *If the conclusion of Proposition 3.11 does not hold, then given $x, y \in \langle\alpha\rangle_3$ and distinct $i, j \in [3]$, there is $z \in \langle\alpha\rangle_3$ with $d(x, z+e_i) > 2\lambda D$ and $d(y, z+e_j) > 2\lambda D$.*

The purpose of this proposition is to provide us with a finite set of points which will then be used to induce a 2-way set of the wanted diameter, by contractions. To prove this claim, we examine two cases on the distance between x and y, one being $d(x, y) > 5\lambda D$ and the other being $d(x, y) \leq 5\lambda D$.

Proof of Proposition 3.12. As noted above, we look at the two cases on $d(x, y)$.

Case 1. Suppose $d(x, y) > 5\lambda D$. We actually obtain a slightly more general conclusion in this case; if $d(x, y) > 5\lambda D$ and we cannot find a desired point z, then we get a 3-way subset T of $\langle\alpha\rangle_3$ of diameter not greater than $4\lambda D$.

Suppose there is no such z, hence for all $z \in \langle\alpha\rangle_3$ either $d(x, z+e_1) \leq 2\lambda D$ or $d(y, z+e_2) \leq 2\lambda D$ is true. We can colour all points t in this 3-way set by $c(t) = 1$ if $d(t, x) \leq 2\lambda D$, by $c(t) = 2$ if $d(t, y) \leq 2\lambda D$, and $c(t) = 3$ otherwise. This is well-defined as the triangle inequality prevents the first two conditions from holding simultaneously. Thus, for any z either $c(z+e_1) = 1$ or $c(z+e_2) = 2$. Also given any two points z, t in the grid such that $t \overset{j}{\frown} z$, and whose neighbours take only colours 1 and 2, it cannot be that $c(z+e_j) \neq c(t+e_j)$, as otherwise, w.l.o.g. $c(t+e_j) = 1, c(z+e_j) = 2$. Then we get $d(x, y) \leq d(x, t+e_j) + d(t+e_j, z+e_j) + d(z+e_j, y) \leq 5\lambda D$, which is a contradiction. Thus for any such z and t, there is an i such that $c(t+e_i) = c(z+e_i)$.

The following auxiliary lemma tells us that all such colourings are essentially trivial. (Note that we are still in the **Case 1** of the proof of Proposition 3.12.)

Lemma 3.13. *Let* $c : \langle \beta \rangle_3 \to [3]$ *be a colouring such that*

(i) *given* $z \in \langle \beta \rangle_3$ *either* $c(z + e_1) = 1$ *or* $c(z + e_2) = 2$,

(ii) *given* $z, t \in \langle \beta \rangle_3$ *such that neighbours of* z, t *take only colours 1 and 2, then* $c(z + e_i) = c(t + e_i)$ *for some* i.

Then there is a 3-way subset of $\langle \beta \rangle_3$ *which is either entirely coloured by 1 or entirely coloured by 2.*

Proof of Lemma 3.13. We denote the coordinates by superscripts. Given non-negative integers $a \geq \beta^{(3)}, b \geq \beta^{(1)} + \beta^{(2)}$ denote $\mathcal{L}(a, b) = \{z \in \mathbb{N}_0^3 : z^{(3)} = a, z^{(1)} + z^{(2)} = b\}$. Hence such a line must be coloured as $c(b - \beta_2, \beta_2, a) = 1, c(b - \beta_2 - 1, \beta_2 + 1, a) = 1, \dots c(t + e_1 - e_2) = 1, c(t)$ arbitrary, $c(t + e_2 - e_1) = 2, \dots, c(\beta_1, b - \beta_1, a) = 2$, for some point t. If all z in $\mathcal{L}(a, b)$, with $z^{(1)} \geq \beta^{(1)} + 3, z^{(2)} \geq \beta^{(2)} + 3$ are coloured by 1, say that $\mathcal{L}(a, b)$ is *1-line*. Similarly, if these are coloured by 2, call it a *2-line*, and otherwise *1,2-line*.

Observe that if $\mathcal{L}(a, b)$ is 1,2-line for $a \geq \beta^{(3)}$ and $b > \beta^{(1)} + \beta^{(2)} + 10$, then $\mathcal{L}(a + 1, b - 1)$ is not 1,2-line, for otherwise we have

- $(\beta^{(1)}, b - \beta^{(1)}, a), (\beta^{(1)} + 1, b - \beta^{(1)} - 1, a), (\beta^{(1)}, b - \beta^{(1)} - 1, a + 1)$ are coloured by 1,
- $(b - \beta^{(2)}, \beta^{(2)}, a), (b - \beta^{(2)} - 1, \beta^{(2)} + 1, a), (b - \beta^{(2)} - 1, \beta^{(2)}, a + 1)$ are coloured by 2,

which is impossible by the second property of the colouring.

Suppose we have a 1,2-line $\mathcal{L}(a, b)$ for $a > \beta^{(3)}, b > \beta^{(1)} + \beta^{(2)} + 20$. Then $\mathcal{L}(a + 1, b - 1)$ and $\mathcal{L}(a - 1, b + 1)$ are either 1- or 2-lines. But as above we can exhibit x', y' such that $x' + e_1, x' + e_2, y' + e_3$ are of colour 1 while $y' + e_1, y' + e_2, x' + e_3$ are of 2, or we can find x', y' for which $x' + e_1, x' + e_2, x' + e_3$ have $c = 1$, and $y' + e_1, y' + e_2, y' + e_3$ are coloured by 2. So, there can be no such 1,2-lines. Further, by the same arguments we see that $\mathcal{L}(a, s - a)$ for fixed s must all be 1-lines or all 2-lines, for $a > \beta_3 + 1$, and that in fact only one of these possibilities can occur, hence we are done. $\square$

Applying Lemma 3.13 immediately yields the **Case 1** of the proof.

Case 2. Assume that $d(x, y) \leq 5\lambda D$, and suppose contrary. Then, in particular, for any z, we have $d(x, z+e_1) \leq 7\lambda D$ or $d(x, z+e_2) \leq 7\lambda D$. Further, we must have z such that $d(x, z+e_{i_1}), d(x, z+e_{i_2}) > 10\lambda D$ holds for some distinct $i_1, i_2 \in [3]$. Take such a z, and without loss of generality $i_1 = 2, i_2 = 3$. So $d(z+e_1, x) \leq 7\lambda D$. Hence $d(z+(-1,1,1), x) \leq 7\lambda D$ and contracting $z, z+(-1,0,1)$ gives $d(z+(-1,0,2), x) > 9\lambda D$. Now contract $z, z+(-1,1,0)$ to get $d(z, z+(-1,2,0)) > 9\lambda D$. However, this is a contradiction, as both $z+(-1,1,0)+e_1$ and $z+(-1,1,0)+e_2$ are too far from x.

Having settled both cases on the distance $d(x, y)$, the proposition is proved. $\square$

If there is $x \in \langle\alpha\rangle_3$ such that for some $x' \in \langle\alpha\rangle_3$ and for all points $y \in \langle x'\rangle_3$ we have $d(x, y) \leq 5\lambda D$, we are done. Hence, we can assume that for all $x, x' \in \langle\alpha\rangle_3$ there is $y \in \langle x'\rangle_3$ which violates the above distance condition.

Take now an arbitrary $x_0 \in \langle\alpha\rangle_3$. Due to the observation we have just made, we know that for any $i \in [3]$ there is an $x_i \neq x_0$ such that $d(x_i+e_i, x_0+e_i) > 5\lambda D$. To be on the safe side, assume that the neighbourhoods of x_0, x_1, x_2, x_3 are all disjoint. Now, by Proposition 3.12, given $i \neq j$ in [3], we can find $x_{i,j} \in \langle\alpha\rangle_3$ such that $d(x_{i,j}+e_i, x_0+e_i) > 2\lambda D, d(x_{i,j}+e_j, x_i+e_j) > 2\lambda D$. Now, let y be any element of the 3-way set generated by α. Take i which contracts x_0, y, implying $d(x_0+e_i, y+e_i) \leq \lambda D$. Hence, by triangle inequality $d(x_i+e_i, y+e_i) > \lambda D$, so x_i, y must be contracted by some $j \neq i$. Using the triangle inequality once more, we get $d(x_{i,j}+e_j, y+e_j) > \lambda D$ and by construction $d(x_{i,j}+e_i, y+e_i) \geq d(x_{i,j}+e_i, x_0+e_i) - d(x_0+e_i, y+e_i) > \lambda D$, therefore for $k \neq i, j$, $d(y+e_k, x_{i,j}+e_k) \leq \lambda D$. We are now ready to conclude that there is finite set of points P such that whenever $y \in \langle\alpha\rangle_3$ is given, for each $i \in [3]$ there is a point $p \in P$ with $d(p, y+e_i) \leq \lambda D$. Here P consists of $N(x_0), x_i+e_j$ and $x_{i,j}+e_k$ for suitable induces $i \neq j \neq k \neq i$. In particular, $|P| = 15$.

Lemma 3.14. *Suppose we are given a 3-way set $\langle\beta\rangle_3 = \cup_{i=1}^k A_i$ of diameter C, where diameters of sets A_i are not greater than $\lambda r C$. Then there is constant $K_{k,r}$ (i.e. does not depend on λ or C) such that $\langle\beta\rangle_3$ has a two-way subset of diameter at most $K_{k,r}\lambda C$. Further, we can take $K_{1,r} = r, K_{2,r} = 2r+8, K_{k+1,r} = K_{k,2r+1}$*

for all r and $k \geq 2$.

Proof of Lemma 3.14. We prove the lemma by induction on k. When $k = 1$, there is nothing to prove, and $K_{1,r} = r$. Suppose $k = 2$.

Before we proceed, we need to establish

Lemma 3.15. *Consider a 3-colouring of edges of complete graph G whose vertex set consists of positive integers, namely $c : \{\{a, b\} : a \neq b, a, b \in \mathbb{N}\} \to [3]$. Then we can find sets A, B whose union is $\mathbb{N}$, while for some colours c_A, c_B, we have $\operatorname{diam}_{c_A} G[A], \operatorname{diam}_{c_B} G[B] \leq 8$. (Here $\operatorname{diam}_{c_0}$ means diameter of the subgraph induced by the colour c_0.) Furthermore, we can assume that A and B intersect when $c_a \neq c_b$.*

Proof of Lemma 3.15. Let x be any vertex. Define $A_i = \{a : c(a, x) = i\}$, for $i \in [3]$, the monochromatic neighbourhood of colour i of x. We shall start by looking at sets A_i. If these are not sufficient to complete the proof, we shall look at similar candidates for A, B until we find the right pair of sets. The following simple fact will play a key role: if X, Y intersect and $\operatorname{diam}_c G[X], \operatorname{diam}_c G[Y]$ are both finite, then $\operatorname{diam}_c G[X \cup Y] \leq \operatorname{diam}_c G[X] + \operatorname{diam}_c G[Y]$.

Firstly, if any of the sets A_i is empty, then taking $A_j \cup \{x\}$ and $A_k \cup \{x\}$ for the other two indices j, k proves the lemma. Otherwise, we may assume that all A_i are non-empty. The next idea is to try to 'absorb' all the vertices into two of the sets A_i. To be more precise, let $B_{i,j} = \{a_i \in A_i : \forall a_j \in A_j, c(a_i, a_j) \neq j\}$ for distinct $i, j \in [3]$. Then,

$$\operatorname{diam}_i \{x\} \cup A_i \cup (A_j \setminus B_{j,i}) \leq 4$$

for all distinct i, j (which is what we meant by 'absorbing vertices' above). Observe that if $\{i, j, k\} = [3]$ and $B_{j,i}$ and $B_{j,k}$ are disjoint, then $A_j \setminus B_{j,i}$ and $A_j \setminus B_{j,k}$ cover the whole A_j so we can take $c_A = i, c_B = k$ and $A = \{x\} \cup A_i \cup (A_j \setminus B_{j,i}), B = \{x\} \cup A_k \cup (A_j \setminus B_{j,k})$. Hence, we may assume that $B_{j,i}$ and $B_{j,k}$ intersect, and that in particular these are non-empty.

Observe also that for $\{i, j, k\} = [3]$, if we are given $a_i \in B_{i,j}, a_j \in B_{j,i}$ then $c(a_i, a_j) \neq i, j$ so $c(a_i, a_j) = k$. This implies $\operatorname{diam}_k G[B_{i,j} \cup B_{j,i}] \leq 2$. We shall exploit this fact to finish the proof.

Now pick arbitrary $a_3 \in B_{3,1} \cap B_{3,2}$. If $c(a_1, a_3) = 3$ for some $a_1 \in B_{1,2}$, then $\mathrm{diam}_3(B_{1,2} \cup B_{2,1} \cup A_3 \cup \{x\}) \le 5$ and $\mathrm{diam}_1(A_1 \cup (A_2 \setminus B_{2,1}) \cup \{x\}) \le 4$, so we are done. The same arguments works for a_3 and $B_{2,1}$, allowing us to assume that no edge between $B_{1,2} \cup B_{2,1}$ and a_3 is coloured by 3. Therefore, since $a_3 \in B_{3,1} \cap B_{3,2}$, we have $c(B_{1,2}, a_3) = 2$ and $c(B_{2,1}, a_3) = 1$.

Recall that previously we tried to absorb the vertices of A_1 to A_2 to have a set of bounded diameter in colour 2, but this failed for the set $B_{1,2}$. Now, we have $c(B_{1,2}, a_3) = 2$, so we can once again try the same idea, by looking for an edge of colour 2 between a_3 and $A_1 \setminus B_{1,2}$ (vertices of which are joined by an edge of colour 2 to a vertex in A_2).

Suppose that $c(a_1, a_3) = 2$ for some $a_1 \in A_1 \setminus B_{1,2}$. Then $\mathrm{diam}_2(A_1 \cup A_2 \cup \{x\} \cup \{a_3\}) \le 8$, and taking $A_3 \cup \{x\}$ for the other set, proves the lemma. Analogously, the lemma is proved if $c(a_2, a_3) = 1$ for some $a_2 \in A_2 \setminus B_{2,1}$.

Finally, since $a_3 \in B_{3,1} \cap B_{3,2}$, we may assume that $c(A_1 \setminus B_{1,2}, a_3) = 3$ and $c(A_2 \setminus B_{2,1}, a_3) = 3$. Observing that $\mathrm{diam}_3(B_{1,2} \cup B_{2,1}) \le 2$ and $\mathrm{diam}_3(\mathbb{N} \setminus B_{1,2} \setminus B_{2,1}) \le 4$, completes the proof. $\square$

We refer to diam_c as the *monochromatic diameter* for c.

Consider the complete graph on $\langle \beta \rangle_3$ along with a edge 3-colouring c, such that $x \overset{c(xy)}{\frown} y$. Due to Lemma 3.15, we have sets B_1, B_2 whose union is $\langle \beta \rangle_3$, and their monochromatic diameters for some colours are at most 8, that is, by the triangle inequality $\mathrm{diam}(B_1 + e_{i_1}) \le 8\lambda C, \mathrm{diam}(B_2 + e_{i_2}) \le 8\lambda C$ for some i_1, i_2. If $i_1 = i_2$ we are done, hence we can assume these are different, and in fact without loss of generality $i_1 = 1, i_2 = 2$. If A_1, A_2 intersect, then diameter of union is not greater than $2r\lambda C$, proving the claim. Therefore, we shall consider only the situation when these are disjoint. Similarly, if $B_1 + e_1$ intersects both A_1, A_2, by triangle inequality, $\mathrm{diam}\,\langle \beta \rangle_3 \le (2r+8)\lambda C$, so without loss of generality $B_1 + e_1 \subset A_1$. Depending on which of the two sets contains $B_2 + e_2$, we distinguish the following cases.

Case 1. $A_1 \supset B_2 + e_2$.

We now claim that A_1 has a 2-way subset, whose diameter is then bounded by the diameter of A_1, which suffices to prove the claim. Suppose $a \in A_1$. Then $a \in B_i$ for some i, hence $a + e_1$ or $a + e_2$ is in A_1. If both are, there is nothing left to prove. Otherwise, the other point must be in A_2, say $a+e_1 \in A_1, a+e_2 \in A_2$. Suppose $a+e_3 \in A_2$ as well. Then $a+e_2-e_1, a+e_3-e_1 \in B_2$, thus $a+(-1,2,0), a+(-1,1,1) \in A_1$, hence contracting $a, a-e_1+e_2$ gives that $d(A_1, A_2) \leq \lambda C$. Otherwise $a+e_3 \in A_1$, hence we are done.

Case 2. $A_2 \supset B_2 + e_2$.

Colour point by i if it belongs to A_i. Such a colouring satisfies the hypothesis of Lemma 3.13 since given a point y, either $y+e_1$ is coloured by 1, or $y+e_2$ is coloured by 2, and the second condition is also satisfied, (or after contraction we get $d(A_1, A_2) \leq \lambda C$ so done). Hence, we have a colouring that is essentially trivial, proving the claim.

Suppose the claim holds for some $k \geq 2$, and we have $k+1$ sets. As before, we can assume that these are disjoint and thus define colouring c, such that $y \in A_{c(y)}$. Further, we can assume that $d(A_i, A_j) > \lambda C$ for distinct i, j. Moreover, we have $A_i \cap \langle \beta + (1,1,1) \rangle_3 \neq \emptyset$, as otherwise we are done by considering $\beta + (1,1,1)$ instead of β.

Let $z \in \langle \beta \rangle_3$. Define *signature* of z as $\sigma(z) = (c(z+e_1), c(z+e_2), c(z+e_3))$. By the discussion above, given $i \in [k+1], l \in [3]$ we have a point z such that $\sigma(z)^{(l)} = i$. Also, whenever z, z' are two points in our 3-way set, we must have $\sigma(z)^{(i)} = \sigma(z')^{(i)}$ for some i, for otherwise we violate the condition on the distance between the sets A_j.

Let (a, b, c) be a signature. Suppose there was another signature (p, d, e), where $b \neq d, c \neq e$, which implies $p = a$. Since $k+1 \geq 3$, there are signatures $(g_1, h_1, j_1), (g_2, h_2, j_2)$, where g_1, g_2, a are distinct. Then $(h_1, j_1) = (h_2, j_2) \in \{(b, e), (d, c)\}$, without loss of generality these are (b, e). Hence, for any z we have $\sigma(z)^{(2)} = b$ or $\sigma(z)^{(3)} = e$. Now, define a new colouring c' of $\langle \beta \rangle_3$, if a point p was coloured by b set $c'(p) = 1$, if it was coloured by e set $c'(p) = 2$ otherwise $c'(p) = 3$. Recalling the previous observations, we see that c' satisfies the necessary assumptions in Lemma 3.13, and apply it (formally change the coordinates first) to finish the proof.

Otherwise, any two signatures must coincide at at least two coordinates. In particular, the only possible ones are $(\cdot, b, c), (a, \cdot, c), (a, b, \cdot)$, where instead of a dot we can have any member of $[k+1]$. If $a \neq b, c$, we have that $\sigma(z+$

$(1,0,-1)) = (a,b,a)$ and $\sigma(z+(1,-1,0)) = (a,a,c)$. Thus $\sigma(z+(2,-1,-1))^{(2)} = \sigma(z+(2,-1,-1))^{(3)} = a$, which is impossible. Similarly $b \in \{a,c\}, c \in \{a,b\}$ hence $a = b = c$, and so A_a is a two-way set with the wanted diameter. $\square$

By Lemma 3.14, there is a 2-way set T with $\operatorname{diam} T \leq K_{15,2}\lambda D$. Setting $s = 3$, we have $K_{15,s-1} = K_{14,2s-1} = K_{13,2^2 s-1} = \cdots = K_{2,2^{13}s-1} = 2^{14} \cdot 3 + 6 = 49158$, as wanted. $\square$

We say that a set of points of the grid Q is a *quarter-plane* if there are distinct $i_1, i_2 \in [3]$ such that $Q = \{t + ae_{i_1} + be_{i_2} : a, b \in \mathbb{N}_0\}$, for some point t.

Proposition 3.16. *Suppose $\lambda < 1/4$ and there is a 2-way set S of diameter D. Provided $m_1 = \inf_{s\in S} \rho(s) > (2+\lambda)D$, S contains a quarter-plane subset Q.*

Proof. Without loss of generality, we can assume that S has a point p such that $S \subset \langle p \rangle_3$, and all points s of S except p have a unique point s' such that $s \in N(s')$. This is because we can always pick such subset of S, and it suffices to prove the statement in such a situation. We say that such a k-way set is *spreading* (from p).

Case 1. For all $i \in [3]$, there is x with $x + e_i$ not in S.

Let $x, y \in S$ be points such that $x + e_i, y + e_j \notin S$, for i, j distinct. Take k so that $\{i, j, k\} = [3]$. Then if $x \overset{i}{\frown} y$, by the triangle inequality we have $m_1 \leq d(x, x+e_i) \leq d(x,y) + d(y, y+e_i) + d(y+e_i, x+e_i) \leq (2+\lambda)D$, which is a contradiction. Similarly we drop the possibility of $x \overset{j}{\frown} y$ happening, hence $x \overset{k}{\frown} y$. Hence, if we define $A_l = \{s \in S : s = t + e_l \text{ for some } t \in S\}$, these are all of diameter $\leq 2\lambda D$.

Suppose A_1 and A_2 are disjoint. Consider x such that $x + e_3 \notin S$. If $x + e_1 + e_2 \in S$, it is both in A_1, A_2, which is impossible. Hence, we have that $x + e_1 + e_3, x + e_2 + e_3 \in S$, thus $x + e_3 + e_1 + e_2$ is not in S, so we can repeat the argument, to get all the $x + (1,0,n)$ and $x + (0,1,n)$ in S. Now, by triangle inequality, we must have $x + (1,0,n) \overset{3}{\frown} x + (0,1,n), x + (1,0,n) \overset{3}{\frown} x + (0,1,n+1)$, for all non-negative n, so $(x + (1,0,n))_{n\geq 1}$ is Cauchy, which is contradiction. Thus A_1, A_2 intersect, and similarly A_1 and A_2 intersect A_3, therefore, take T to be union of these, which is thus

2-way (as every point of S belongs to some A_i, except the starting one), and has $\operatorname{diam} T \leq 4\lambda D$.

Case 2. Suppose that there is i such that for any $x \in S$, $x + e_i$ is in S.

Without loss of generality, we assume $i = 3$. Pick any x_0 in S and set $a = (x_0)^{(3)}$. Thus, starting at x_0 we can form the sequence $(x_n)_{n \geq 0}$ such that $\{x_{n+1}\} = S \cap \{x_n + e_1, x_n + e_2\}$. Suppose we have x, y among these such that $x+e_1, y+e_2 \in S$. Hence, $x+(1,0,n), x+(0,0,n), y+(0,1,n), y+(0,0,n)$ belong to S for all nonnegative n, thus $x+(0,1,n), y+(1,0,n)$ are never elements of S. Now, contracting pairs $x+(0,0,n), y+(0,0,n)$ and $x+(0,0,n+1), y+(0,0,n)$ gives 1-way Cauchy sequence as in the Case 1. If there are no such x, y then we have that S contains a quarter-plane.

Therefore, if we ever get into **Case 2**, we are done. Hence, let $S_1 = S$, then by **Case 1**, we have a 2-way S_2 subset of S_1, which we can assume to be spreading, by the same arguments as those for the set S. It also satisfies the necessary hypothesis of this claim, so we can apply the **Case 1** once more to obtain 2-way set $S_3 \subset S_2$. Proceeding in the same manner, we obtain a sequence of spreading 2-way sets $S_1 \supset S_2 \supset \dots$, whose diameters tend to zero, so just pick a point in each of them, and then find a 1-way Cauchy sequence containing these to reach a contradiction. $\square$

Proposition 3.17. *Let $\{i_1, i_2, i_3\} = [3]$. Suppose we have a quarter-plane $S = \{\alpha + me_{i_1} + ne_{i_2} : m, n \in \mathbb{N}_0\}$, of diameter D, and let $R = \inf_S \rho$. Provided $\lambda < 1/3$ and $D(1-\lambda^2) < (1-4\lambda)R$, there is a 3-way set of diameter at most $2\lambda(\frac{2}{1-\lambda}D + \frac{1+2\lambda}{1-\lambda}R)$.*

Proof. Without loss of generality $i_3 = 1$. Observe that for any point $s \in S$ we must have $\rho(s) = d(s, s+e_1)$. The reason for this is that both $s+e_2, s+e_3 \in S$ and so $d(s, s+e_2), d(s, s+e_3) \leq \operatorname{diam} S = D$, but $\max\{d(s, s+e_1), d(s, s+e_2), d(s, s+e_3)\} = \rho(s) \geq R > D$.

Let $x_n \in S$ be a point with $\rho(x_n) < (1+1/n)R \leq 2R$. As $\lambda < 1/2$, we must have $x_n \overset{1}{\frown} x_n + e_1$. Furthermore, suppose $i \neq 1$ contracts $y, x_n + e_1$, for some point y in S. Thus $x_n + e_i \in S$ and so $\rho(x_n + e_i) = d(x_n + e_i, x_n + e_1 + e_i)$. Then, by triangle inequality, we have $\rho(x_n + e_i) = d(x_n + e_i, x_n + e_1 + e_i) \leq$

$d(x_n+e_i, y+e_i)+d(y+e_i, x_n+e_1+e_i) \leq \lambda d(y, x_n+e_1)+D \leq \lambda 2R+(1+\lambda)D < R$, therefore it must be $y \overset{1}{\frown} x_n+e_1$. Hence $\rho(y) \leq d(y, x_n)+d(x_n, x_n+2e_1)+d(x_n+2e_1, y+e_1) \leq D + R(1+1/n)(1+\lambda) + \lambda(D + R(1+1/n))$, for all n, hence $\rho(y) \leq D(1+\lambda) + R(1+2\lambda) < 2R$.

Now we claim that for all $y \in S$, and all $k \geq 1$, we have $y \overset{1}{\frown} y + ke_1$, which we prove by induction on k. For $k = 1$, we are done as otherwise there is y with $\rho(y) < 2\lambda R < R$.

Suppose the claim holds for some $k \geq 1$. Then for any y and $l \leq k+1$ we have $d(y, y+le_1) \leq d(y, y+e_1) + d(y+e_1, y+le_1) \leq \rho(y) + \lambda d(y, y+(l-1)e_1) \leq \ldots \leq \rho(y)(1+\lambda+\cdots+\lambda^{l-1}) < \rho(y)/(1-\lambda)$. Also, $d(y, y+le_1) \geq d(y, y+e_1) - d(y+e_1, y+le_1) \geq \rho(y) - \lambda d(y, y+(l-1)e_1) > \rho(y)\frac{1-2\lambda}{1-\lambda}$. As $\lambda < 1-2\lambda$, we have that 1 always contracts $y, y+(k+1)e_1$. In particular $\rho(y)\frac{1-2\lambda}{1-\lambda} < d(y, y+ke_1) < \rho(y)/(1-\lambda)$.

Fix any $x \in S$. Now, suppose $x \overset{i}{\frown} y + ke_1$ for some $i \neq 1$. Then $R\frac{1-2\lambda}{1-\lambda} \leq \rho(y+e_i)\frac{1-2\lambda}{1-\lambda} < d(y+e_i, y+e_i+ke_1) \leq d(y+e_i, x+e_i)+\lambda(d(x,y)+d(y, y+ke_1)) \leq D(1+\lambda) + \lambda\rho(y)/(1-\lambda) < (1+\lambda)D + \frac{2\lambda}{1-\lambda}R$, which is a contradiction. Hence, by looking at distance from $x+e_1$, we see that $\operatorname{diam}\{\alpha + (a,b,c) : a \geq 2, b, c \geq 0\} \leq 2\lambda(D + D(1+\lambda)/(1-\lambda) + R(1+2\lambda)/(1-\lambda))$, as required. □

In order to make the calculations throughout the proof easier, we use the following corollary instead.

Corollary 3.18. *Suppose we have a 2-way set S of diameter D, and $R = \inf_{s\in S} \rho(s)$. Provided $\lambda < 1/9$ and $R > (2+\lambda)D$, there is a 3-way set of diameter at most $6\lambda R$.*

Proof. Firstly, apply Proposition 3.16 to find a quarter-plane inside the given 2-way set. Since $R(1-4\lambda) > R/(2+\lambda) > D > (1-\lambda^2)D$ and $\lambda < 1/3$, we can apply Proposition 3.17, to obtain a 3-way set of diameter at most $2\lambda(\frac{2}{1-\lambda}D + \frac{1+2\lambda}{1-\lambda}R)$. An easy calculation shows that this expression is smaller than $\lambda(5D+3R) < 6\lambda R$. □

Recall that we defined $\mu = \inf_x \rho(x)$, where x ranges over the whole grid. Recall also that $\mu > 0$ by Proposition 3.10.

Proposition 3.19. *Given K, provided $1 > (2+\lambda)\lambda K C_1$, all 3-way sets of have diameter greater than $K\mu$.*

Proof. The proposition is trivial when $K < 1$, so assume $K \geq 1$ and in particular $\lambda < 1/9$. Suppose contrary, let T be a 3-way set of diameter $D \leq K\mu$. By Proposition 3.11, we know that there is a 2-way set $S \subset T$, with $\operatorname{diam} S \leq \lambda C_1 K\mu$. Therefore by Corollary 3.18, as $\lambda C_1 K\mu < \mu/(2+\lambda)$, we have a 3-way set of diameter not greater than $6\lambda K\mu < \mu$, resulting in a contradiction. $\square$

Proposition 3.20. *Given K, provided $\lambda < 1/9, 1/(3K)$, all 2-way sets have diameter greater than $\lambda K\mu$.*

Proof. Suppose contrary, pick a 2-way set S_0 of diameter at most $\lambda K\mu$. Since $K\lambda\mu(2+\lambda) < \mu$, we have a 3-way set T_1 with $r_1 = \operatorname{diam} T_1$ by Corollary 3.18. Now take a 2-way subset $S_1 \subset T_1$ with $\operatorname{diam} S_1 \leq K\lambda\mu$, so we have 3-way set T_2 of diameter not greater than $r_2 = 6\lambda r_1$. Repeating this argument, for all $k \geq 1$ we find 3-way set T_k, with diameter bounded by r_k, where $r_{k+1} = 6\lambda r_k$. But, then we must have $r_k < \mu$ for some k, resulting in a contradiction. $\square$

Note that the only way for a 2-way subset not to have elements in every $\langle (n,n,n) \rangle_3$ is to be contained in a union of finitely many quarter-planes.

3.5 Finite contractive structures

Recall the proofs of Proposition 3.11 and Lemma 3.8. There we fixed a finite set S of points, and then contracted various points with points in S to obtain k-way sets. We pursue this approach further in the following few claims. In this section, we also show that we cannot have certain configurations of points.

Proposition 3.21. *Suppose we have $K \geq 1$ and that $\lambda < 1/(24K)$ holds. Then we cannot have a point x_0 in the grid with $\rho(x_0) \leq K\mu$ such that $N(x_0) = \{x_1, x_2, x_3\}$, where x_1, x_2, x_3 satisfy $\operatorname{diam}(N(x_0) \cup \{x_i + e_j : i, j \in [3], i \neq j\}) \leq \lambda K\mu$.*

When using this proposition (in order to obtain a contradiction in the proofs to follow), we say that we are applying Proposition 3.21 to $(x_0; x_1, x_2, x_3)$ with constant K.

Proof. Suppose we do have points described in the assumptions. By Lemma 3.8, in each 3-way set we have a point t such that $d(t, x_0) \leq 2K\mu$. Consider the contractions of t with x_0, x_1, x_2, x_3; our main aim is to obtain a 2-way set of a small diameter and then use Proposition 3.20 to yield a contradiction.

Observe that from the assumptions of the proposition, for any $\{i, j, k\} = [3]$, we have $\max\{d(x_i, x_i + e_i), d(x_i, x_i + e_j), d(x_i, x_i + e_k))\} = \rho(x_i) \geq \mu > \lambda K\mu \geq \max\{d(x_i, x_i + e_j), d(x_i, x_i + e_k)\}$. Thus for all $i \in [3]$, $\rho(x_i) = d(x_i, x_i + e_i)$ holds. Suppose first that $t \overset{i}{\frown} x_i$ for all $i \in [3]$. Take i so that $t \overset{i}{\frown} x_0$. Then $\rho(x_i) = d(x_i, x_i + e_i) \leq d(x_i, x_0 + e_i) + d(x_0 + e_i, t + e_i) + d(t + e_i, x_i + e_i) \leq \lambda K\mu + \lambda d(x_0, t) + \lambda d(x_i, t) \leq 6\lambda K\mu < \mu$, which is impossible.

Thus, there are distinct $i, j \in [3]$ with $t \overset{j}{\frown} x_i$. If j was to contract t, x_j, we get $\rho(x_j) = d(x_j, x_j + e_j) \leq d(x_j, x_i + e_j) + d(x_i + e_j, t + e_j) + d(t + e_j, x_j + e_j) \leq \lambda K\mu + \lambda d(x_i, t) + \lambda d(t, x_j) \leq 7\lambda K\mu < \mu$, which is impossible. Therefore, for some $k \neq j$, we have $t \overset{k}{\frown} x_j$. In particular, $d(t + e_j, x_1 + e_2) \leq d(t + e_j, x_i + e_j) + d(x_i + e_j, x_1 + e_2) \leq \lambda d(t, x_i) + \lambda K\mu \leq 4\lambda K\mu$, and in a similar fashion $d(t + e_k, x_1 + e_2) \leq 4\lambda K\mu$. Furthermore by the triangle inequality, both $t + e_j$ and $t + e_k$ are on the distance at most $K\mu + 4\lambda K\mu \leq 2K\mu$ from x_0, so the same arguments we used for t can be applied to these points as well. Hence, we obtain a bounded 2-way set of diameter at most $4K\mu$. But, considering all the points of the 2-way set except t and their distance from $x_1 + e_2$, this is actually a 2-way set of diameter at most $8\lambda K\mu$, and we have such a set in every 3-way subset of the grid. Now, apply Proposition 3.20 to obtain a contradiction, since $\lambda < 1/(24K)$ and $K \geq 1$. $\square$

Proposition 3.22. *Given $K \geq 1$, provided $\lambda < 1/(78K), 1/(13C_1)$, there is no x such that $\rho(x) \leq K\mu$, but $\rho(x + e_i) > 7K\mu$ for all $i \in [3]$.*

Sometimes we refer to a pair of points a, b in the grid as the *edge* a, b, and by the *length* of the edge a, b we mean $d(a, b)$. The points a and b are the *endpoints* of the edge a, b.

Proof. Suppose there was such an x. Consider the contractions of $x + e_i, x + e_j$ for $i \neq j$ and suppose that two such pairs are contracted by the same k. Thus $\operatorname{diam}\{x + e_k + e_1, x + e_k + e_2, x + e_k + e_3\} \leq 4\lambda K\mu$. Now, contract $x, x + e_k$ to get $\rho(x + e_k) \leq (2 + 5\lambda)K\mu < 3K\mu$, giving us contradiction. So, the pairs de-

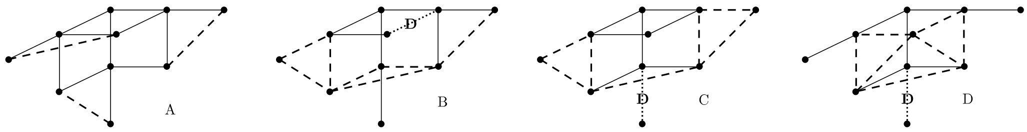


Figure 3.2: Case 1

scribed above must be contracted in different directions. Further, we can make a distinction between the *short* edges of the form $a, a+e_i$ and the *long* edges[4] $a+e_i, a+e_j$, where a is any point of the grid and i, j are distinct integers in [3]. For every such long edge we have a unique short *orthogonal* edge $a, a+e_k$ where $\{i, j, k\} = [3]$. We can observe that if we have a short edge and a long edge in $\{x\} \cup N(x)$ which are not orthogonal, but both contracted by some i, we must have another such pair, contracted by some $j \neq i$. One can show this by looking at the short edge e which is orthogonal to the long one in a given pair of edges contracted by i.

If we write $[3] = \{i, j, k\}$, then j contracts one long edge, and so does k. But now consider the described orthogonal short edge e. It cannot be contracted by i, for otherwise $\rho(x+e_i)$ is too small. Thus, it gives us another desired pair. Having shown this, we have two cases, the first where there are at least two such pairs (i.e. non-orthogonal short and long edge contracted in the same direction), and the second without such pairs.

Case 1. There are at least two such pairs.

In Figure 3.2, we show the possibilities for contractions. The edges shown as dashed lines have length at most $3K\lambda\mu$. Here we actually consider possible contractions and then apply triangle inequalities. This way, we obtain very few possible diagrams. We only list the possible configurations up to rotation or reflection, as the same arguments still carry through. In the diagram A, by short edge contractions we see that we get $\rho(x+e_i) \leq 3K\mu$ for some i, which gives the claim. Dotted lines with letter **D** will be called the *D-lines*. On the other hand,

[4]Note, words 'short' and 'long' have nothing to do with the length of an edge previously defined. Instead, they simply describe how these edges look like in the figures used in the proofs.

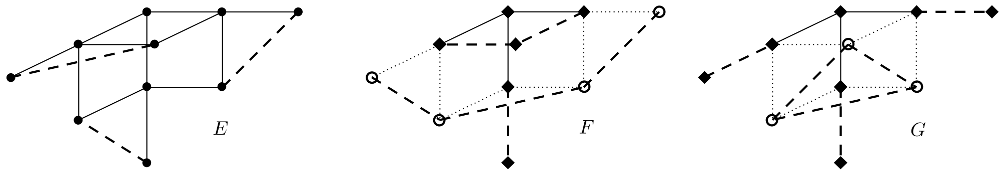


Figure 3.3: Case 2

in the diagrams B, C and D, we claim that we are either done or the dotted lines with letter **D** are of length at most $9\lambda K\mu$. Once this is established, we have $\rho(x + e_i) \le 3K\mu$ for some i, resulting in a contradiction.

For each $i \in [3]$, let $x_i \in N(x)$ be such that $x_i + e_i$ is not an endpoint of long edge shown as dashed line. By Lemma 3.8, in each 3-way set we have a point t with $d(x, t) \le 2\rho(x)/(1 - \lambda) \le 3K\mu$. Observe that from the diagrams we have $d(x_i, x_i + e_j) \le (2 + 6\lambda)K\mu$ whenever $i \ne j$. Further, we cannot have $x_i \overset{i}{\frown} t$ for all i, otherwise we get a contradiction by considering contraction $x \overset{j}{\frown} t$. If $x + e_j$ is an endpoint of a edge shown as a D-line, and $x + e_j + e_l$ is the other endpoint, we have $x + e_l = x_k$, hence $d(x + e_l + e_j, x + e_j) \le \lambda(d(x + e_j, t) + d(t, x)) \le 7\lambda K\mu$, which is impossible. Thus, $x + e_j$ is not on a D-line edge, which gives $\rho(x_j) = d(x_j, x_j + e_j) \le d(x_j, x) + d(x, x + e_j) + d(x + e_j, t + e_j) + d(t + e_j, x_j + e_j) \le (2 + 7\lambda)K\mu$.

Previous arguments imply that we must have $i \ne j$ with $x_i \overset{j}{\frown} t$, and hence $x_j \overset{j}{\not\frown} t$ (otherwise $\rho(x_j) \le (2 + 14\lambda)K\mu$), so, given such a t, we get $t + e_a, t + e_b$, $a \ne b$ on distance at most $13\lambda K\mu$ from $x_1 + e_2$ and on distance not greater than $3K\mu$ from x, by the triangle inequality. Hence, in every $\langle z \rangle_3$ we get a 2-way subset of diameter not greater than $\lambda 26K\mu$, yielding a contradiction, due to $\lambda < \frac{1}{78K}$ and Proposition 3.20. Hence, edges shown as D-lines satisfy the wanted length condition.

Case 2. There are no such pairs.

The possible cases up to rotation or reflection are shown in Figure 3.3, where the short edges shown as dashed lines are of length at most $\lambda K\mu$, while the long ones shown as dashed lines are of the length at most $2\lambda K\mu$. As above, the diagram E gives $\rho(x + e_i) \le 3K\mu$ immediately. On the other hand, if we get diagram F or G, we can consider points shown as black squares and empty circles. We call a point *black* if it is a black square and *white* if it is shown as an empty circle. In the course of the proof, we shall colour more points in black and white. Let r be the minimal length of dotted edges in Figure 3.3, and r' the maximal. Then we have $r' \leq r + 2K\mu + 6\lambda K\mu$. Furthermore, given $i \in [3]$ we have $7K\mu < \rho(x + e_i) \leq r' < r + 3K\mu$, so $r > 4K\mu$.

Consider t such that $d(x, t) \leq 2r$. Let j contract $x + e_i, t$, so we have $d(t+e_j, x) \leq d(t+e_j, x+e_i+e_j)+d(x+e_i+e_j, x+e_i)+d(x+e_i, x) \leq \lambda d(t, x+e_i)+\rho(x+e_i)+\rho(x) \leq \lambda(d(t, x)+d(x, x+e_i))+r'+K\mu \leq 2\lambda r+\lambda K\mu+r+2K\mu+6\lambda K\mu+K\mu \leq (1+2\lambda)r+(3+8\lambda)K\mu < (1+2\lambda+\frac{3+8\lambda}{4})r \leq 2r$, since $\lambda < 1/16$. Similarly if j contracts x, t we have $d(t+e_j, x) \leq d(t+e_j, x+e_j)+d(x+e_j, x) \leq 2\lambda r+K\mu \leq 2r$, as well. Further, observe that if $t+e_j$ is the result of a scontraction as before, then we have a point $a \in N(x) \cup \{x+e_i+e_j : i, j \in [3]\}$ with $d(t+e_j, a) \leq \lambda(2r+K\mu)$. Restrict our attention to the black (shown as black squares) and white (shown as empty circles) points shown in Figure 3.3. We have $\operatorname{diam}\{\text{white points}\} \leq 6\lambda K\mu, \operatorname{diam}\{\text{black points}\} \leq (2 + 2\lambda)K\mu$ and distance from any white to any black point is at least $r - K\mu - 4\lambda K\mu$. Take a point t on distance at most $2r$ from x (note that by Lemma 3.8 such a point exists in every 3-way set). Consider contractions with $\{x\} \cup N(x)$ and suppose that $t+e_i, w$ and $t+e_i, b$ are results of these operations, where w is a white and g is a black point. Then, using the triangle inequality, we establish $r - K\mu - 4\lambda K\mu \leq d(w, b) \leq d(w, t+e_i)+d(t+e_i, b) \leq 2\lambda(2r + K\mu)$, which is a contradiction. For any given $i \in [3]$ let x_i stand for the point of $N(x)$ such that $d(x_i, x_i + e_i) \leq \lambda K\mu$, thus $N(x) = \{x_1, x_2, x_3\}$. Let $t \overset{i}{\frown} x$. Then take $j \in [3]$ distinct from i. We see that $x_j + e_i$ is white, while $x + e_i$ is black, hence i does not contract t, x_j. Let $k \neq i$ contract t, x_j and let l be such that $\{i, j, l\} = [3]$. If $k = j$ then similarly we see that $x_l \overset{l}{\frown} t$, while in the other case $k = l$ and $x_l \overset{j}{\frown} t$. Hence, in conjunction with the previous arguments, we obtain a 3-way set of diameter at most $4r$.

Furthermore, recall that given pairs $t + e_i, p$ and $t + e_i, q$, which are results of contracting t with x or a point in $N(x)$, we must have p and q of the same colour. As each of $t + e_1, t + e_2$ and $t + e_3$ is a result of such a contraction, we can extend the 2-colouring of the points in the diagrams F and G to all points of $\langle x \rangle_3$, namely $c : \langle x \rangle_3 \to \{\text{black, white}\}$, with point $t+e_i$ being coloured by black, if p described above is black in the original colouring, and white otherwise.

Now, the distance between any black point and any white point in the extended colouring is at least $r-K\mu-4\lambda K\mu-2\lambda(2r+K\mu) = (1-4\lambda)r-(1+6\lambda)K\mu$. Recall Proposition 3.11, which guarantees the existence of a 2-way set $S \subset \langle x\rangle_3$ of diameter at most $4\lambda C_1 r$ from which we infer that S is monochromatic, since $4\lambda C_1 r < (1-4\lambda)r-(1+6\lambda)K\mu$.

Case 2.1. *S is black.*

Consider any $t \in \langle x\rangle_3$ which has two black neighbours $t+e_{i_1}, t+e_{i_2}$, where $i_1 \neq i_2$. Then, letting i_3 be the third direction, that is $[3] = \{i_1, i_2, i_3\}$, we have $t \overset{i_3}{\frown} x_{i_3}$, since the points of $N(x_{i_3}) \setminus \{x_{i_3}+e_{i_3}\}$ are white. Hence, for any $t \in S$, we have that $N(t)$ is black. Furthermore, from the same arguments we see that $t \overset{i}{\frown} x_i$ for all $i \in [3]$. Now, if t is in S, and without loss of generality so are $t+e_1, t+e_2$, then $N(t+e_1), N(t+e_2)$ are black, so at least two elements of $N(t+e_3)$ are black too, implying that $N(t+e_3)$ is black. But, now looking at t gives $t \overset{3}{\frown} x_3$ and similarly, looking at $t+e_1, t+e_2, t+e_3$ tells us that 3 contracts points $t+e_1, t+e_2, t+e_3$ with x_3.

Let s be the distance from such a t to x. Then, for all $i \in [3]$, we have a black point p in $\{x\} \cup N(x)$, which is contracted with t by i, so that $p+e_i$ is black as well. Now, by the triangle inequality, we get $d(x, t+e_i) \leq d(x,p)+d(p,p+e_i)+d(p+e_i, t+e_i) \leq d(x,p)+d(p,p+e_i)+\lambda d(p,t) \leq \lambda d(t,x)+(1+\lambda)d(x,p)+d(p,p+e_i) \leq \lambda s+(2+\lambda)(K\mu)$. As in the proof of Lemma 3.8, we see that there is $t \in S$, such that $d(t,x) < 3K\mu$. From the estimates we have just made, we can see that $d(t+e_i, x) < 3K\mu$ for all $i \in [3]$. Without loss of generality $t, t+e_1, t+e_2 \in S$. Recalling that this implies $d(t+e_3, x_3), d(t+e_3+e_i, x_3) < 3\lambda K\mu$ where i takes all the values in $[3]$, shows that $\rho(t+e_3) < 6\lambda K\mu$, which is a contradiction.

Case 2.2. *S is white.*

If $t \in S$, after contracting t, x, we see that the single point in $N(t) \setminus S$ must be black. Hence, by Proposition 3.18, we must have a 3-way set inside $\langle x\rangle_3$ of diameter at most $6\lambda r$, since $(1-4\lambda)r-(1+6\lambda)K\mu > (1-4\lambda)r-(1+6\lambda)r/4 > 2r/3 > (2+\lambda)\lambda 4C_1 r$, since $\lambda < 1/(13C_1)$. But, such a set has at least one black point, so it must have black points only, and we have a contradiction as in **Case 2.1**. □

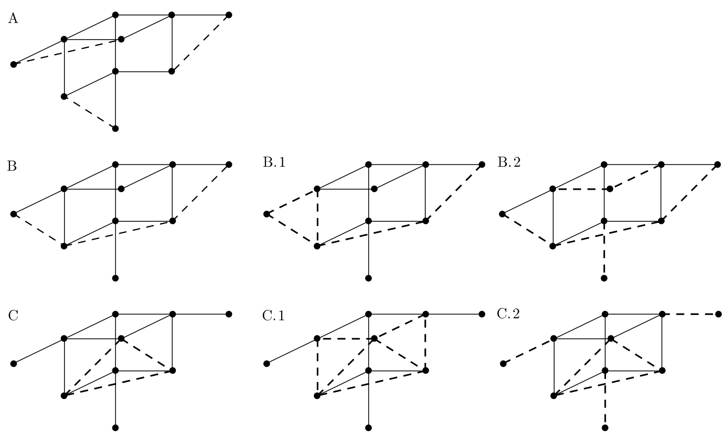


Figure 3.4: Possible distances in the proof of Proposition 3.23

Proposition 3.23. *Given $K \geq 1$, provided $\lambda < 1/(41KC_1)$, there is no x with $\rho(x) \leq K\mu$ and $\operatorname{diam} N(x) \leq \lambda K\mu$.*

Proof. Suppose we have such an x. We start by observing that two pairs of the form $x + e_i, x + e_j$ cannot be contracted by the same k. Otherwise, since $\operatorname{diam} N(x) \leq \lambda K\mu$, after an application of the triangle inequality, we also have $N(x + e_k) \leq 2\lambda^2 K\mu$. Let t be such that $x \overset{t}{\frown} x + e_k$. Then $d(x + e_k, x + 2e_k) \leq d(x+e_k, x+e_t)+d(x+e_t, x+e_k+e_t)+d(x+e_k+e_t, x+2e_k) \leq \operatorname{diam} N(x)+\lambda d(x, x+e_k)+\operatorname{diam} N(x+e_k) \leq \lambda K\mu+\lambda K\mu+2\lambda^2 K\mu < 4\lambda K\mu$. But then, for any $s \in [3]$, we have $d(x+e_k, x+e_k+e_s) \leq d(x+e_k, x+e_k+e_k)+\operatorname{diam} N(x+e_k) < 6\lambda K\mu < \mu$, implying that $\rho(x + e_k) < \mu$, which is impossible.

Thus, all three pairs of the form $x + e_i, x + e_j$ are contracted in different directions, hence we can distinguish the following cases (up to symmetry).

Case 1. The results of contractions are shown as dashed lines in the Figure 3.4, diagram marked by A. It is not hard to see that after contracting pairs $x, x + e_i$, we get $\rho(x + e_j) < \mu$ for some j, giving us contradiction.

Case 2. The results of contractions are shown as dashed lines in Figure 3.4, diagram marked by B. By considering the contractions of pairs $x, x + e_i$, we either get $\rho(x + e_j) < \mu$ for some j, or diagrams B.1, B.2 in figure 3.4, where dashed lines edges now indicate lengths at most $3\lambda K\mu$.

Case 3. The results of contractions are shown as dashed lines in Figure 3.4, diagram marked by C. By considering the contractions of pairs $x, x + e_i$, we either get $\rho(x + e_j) < \mu$ for some j, or diagrams C.1, C.2 in Figure 3.4, where now dashed line implies length at most $3\lambda K\mu$.

We now examine more closely diagrams B.1, B.2, C.1 and C.2. Firstly, we will use Proposition 3.21 to reject B.1 and C.1. In these two diagrams, for each $i \in [3]$, we can find a unique $x_i \in N(x)$ such that $\rho(x_i) = d(x_i, x_i + e_i)$. Then we have $\mathrm{diam}(N(x) \cup \{x_i + e_j : i, j \in [3], i \neq j\}) \leq 15\lambda K\mu$. Also $\rho(x) \leq K\mu$, hence we can apply Proposition 3.21 to $(x; x_1, x_2, x_3)$ with constant $15K$ to obtain a contradiction, since $\lambda < 1/(360K)$.

Observe that in diagrams B.2 and C.2 we can denote $N(x) = \{x_1, x_2, x_3\}$ so that $d(x_i, x_i + e_i) \leq 3\lambda K\mu$. By Proposition 3.22, we have that $\rho(x_i) \leq (7+7\lambda)K\mu$ holds for all $i \in [3]$, as $\lambda < 1/(78K), 1/(13C_1)$. Now, start from a point t with $d(t, x) \leq 2\rho(x)/(1 - \lambda) \leq 2K\mu/(1 - \lambda) \leq 10K\mu$, which exists by Lemma 3.8. Take any $p \in \{x\} \cup N(x)$ and contract with t. If $t \overset{i}{\frown} p$, then $d(t + e_i, x) \leq d(t+e_i, p+e_i)+d(p+e_i, p)+d(p, x) \leq \lambda d(t, p)+d(p+e_i, p)+d(p, x) \leq \lambda(d(t, x)+ d(x, p)) + d(p + e_i, p) + d(p, x) \leq \lambda 10K\mu + (7 + 7\lambda)K\mu + (1 + \lambda)K\mu \leq 10K\mu$.

Contract such a point t with x by some i. Write $[3] = \{i, j, k\}$ and consider the contraction of t, x_j. It is not i that contracts this couple of points, as otherwise $\rho(x_j) < \mu$. If it is j, then we can see that $x_k \overset{k}{\frown} t$, and if it is k, then $x_k \overset{j}{\frown} t$. Hence, all the points of $N(t)$ are on distance at most $10K\mu$ from x, so we can repeat the argument to obtain a bounded 3-way set of diameter at most $20K\mu$. However, we get a contradiction by Proposition 3.19, since $1 > 41KC_1\lambda$. $\square$

Proposition 3.24. *Given $K \geq 1$, suppose we have x_0, x_1, x_2, x_3 such that $\mathrm{diam}\{x_i + e_j : i, j \in [3], i \neq j\} \leq \lambda K\mu$. Furthermore, suppose $\rho(x_0) \leq K\mu$ and that $d(x_0, x_i) \leq K\mu$ for $i \in [3]$. Let $\{a, b, c\} = [3]$.*

Provided $\lambda < 1/(820C_1K)$, whenever there is a point x which satisfies $d(x + e_a, x + e_b) \leq \lambda K\mu$ and $d(x, x_0) \leq K\mu$, then we have $d(x + e_c, x_c + e_c) \leq 16\lambda K\mu$.

Note that this is Proposition 3.5 in the overview of the proof. When using this proposition, we say that we are applying Proposition 3.24 to $(x_0; x_1, x_2, x_3; x)$ with constant K.

Proof. Suppose contrary. Without loss of generality, we may assume $a = 1, b =$

$2, c = 3$. Let us first establish $d(x, x+e_1), d(x, x+e_2) \leq 3K\mu$. As $d(x+e_3, x_3+e_3) > 16\lambda K\mu$, we must have 1 or 2 contracting x, x_3. Similarly, we cannot have $x \overset{3}{\frown} x_0$ and $x_0 \overset{3}{\frown} x_3$ simultaneously. If $x \overset{3}{\frown} x_0$ then we have $x_0 \overset{i}{\frown} x_3$ for some $i \in [2]$, and recall that $x \overset{j}{\frown} x_3$ some $j \in [2]$, so $d(x, x+e_1) \leq d(x, x_0) + d(x_0, x_0+e_i) + d(x_0+e_i, x_3+e_i) + d(x_3+e_i, x_3+e_j) + d(x_3+e_j, x+e_j) + d(x+e_j, x+e_1) \leq K\mu + K\mu + \lambda K\mu + \lambda K\mu + 2\lambda K\mu + \lambda K\mu < 3K\mu$ and in the same way we get $d(x, x+e_2) < 3K\mu$. On the other hand if $x \overset{i}{\frown} x_0$ for $i \in [2]$ we get $d(x, x+e_j) \leq d(x, x_0) + d(x_0, x_0+e_i) + d(x_0+e_i, x+e_i) + d(x+e_i, x+e_j) \leq K\mu + K\mu + \lambda K\mu + \lambda K\mu < 3K\mu$ for any $j \in [2]$.

Similarly, let us observe that $\operatorname{diam}\{x_1, x_2, x_3\} \cup \{x_i + e_j : i, j \in [3], i \neq j\} \leq 5K\mu$. We see that this certainly holds in the case that there are distinct $i, j \in [3]$ with $x_0 \overset{j}{\frown} x_i$, as then $d(x_i, x_i+e_j) \leq d(x_i, x_0) + d(x_0, x_0+e_j) + d(x_0+e_j, x_i+e_j) \leq (2+\lambda)K\mu$, and the claim about the given diameter follows. Hence, suppose that for all $i \in [3]$ the contractions are $x_0 \overset{i}{\frown} x_i$. Then we cannot have $x_0 \overset{3}{\frown} x$, so suppose that $x_0 \overset{j}{\frown} x$ and also that $x \overset{k}{\frown} x_3$, where $j, k \in [2]$. Now, we can apply the triangle inequality to see $d(x_3+e_k, x_3) \leq d(x_3+e_k, x+e_k) + d(x+e_k, x+e_j) + d(x+e_j, x_0+e_j) + d(x_0+e_j, x_0) + d(x_0, x_3) \leq 2\lambda K\mu + \lambda K\mu + \lambda K\mu + K\mu + K\mu = (2+4\lambda)K\mu$, so once again we have the desired bound on the given diameter.

Now, by Lemma 3.8, in every 3-way set we have a point t with $d(t, x_0) \leq 7K\mu$. Suppose that for some distinct $i, j \in [3]$ we have $t \overset{i}{\frown} x_i$ and $t \overset{i}{\frown} x_j$. Then $d(x_i+e_i, x_i+e_k) \leq d(x_i+e_i, t+e_i) + d(t+e_i, x_j+e_i) + d(x_j+e_i, x_i+e_k) \leq 17\lambda K\mu$ for any $k \neq i$. Hence $\operatorname{diam} N(x_i) \leq 17\lambda K\mu$. However, contract x_0, x_i to see that $\rho(x_i) \leq (2+18\lambda)K\mu < 17K\mu$. But we can apply Proposition 3.23, as $\lambda < (17 \cdot 41KC_1)$, to obtain a contradiction. Hence, we cannot have $x_i \overset{i}{\frown} t$ and $x_j \overset{i}{\frown} t$.

Suppose that for every such t we have distinct $i, j \in [3]$ with $t \overset{i}{\frown} x_j$. Then, by the previous observation, we see that $t \overset{k}{\frown} x_i$, for some $k \neq i$. Hence $d(t+e_i, x_0) \leq d(t+e_i, x_j+e_i) + d(x_j+e_i, x_j) + d(x_j, x_0) \leq 8\lambda K\mu + 6K\mu \leq 7K\mu$ and similarly for $t + e_k$. So, we can apply the same arguments to the newly obtained points and proceeding in this manner we construct a bounded 2-way set. However, the points that we construct after t are on distance at most $9\lambda K\mu$ from x_1+e_2, hence, we get a 2-way set of diameter at most $18\lambda K\mu$. This is a contradiction with Proposition 3.20, as we have such a point t in every 3-way set and $\lambda < 1/(54K)$.

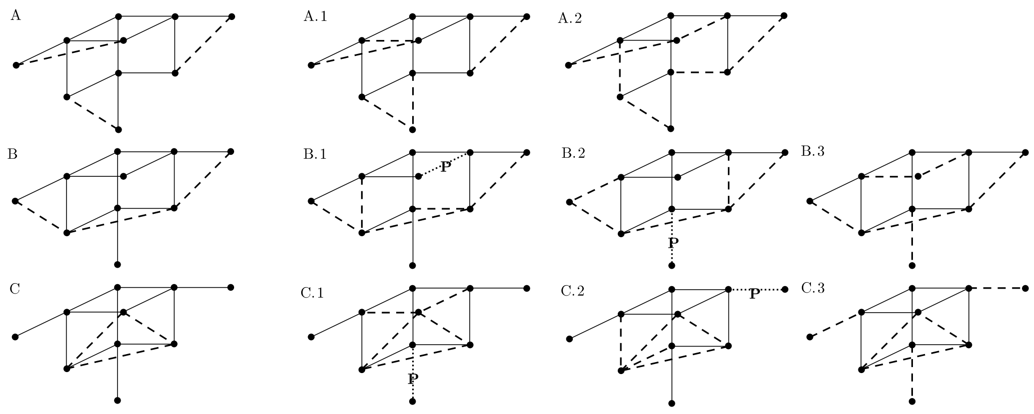


Figure 3.5: Possible contractions in the proof of existence of auxiliary point

With this in mind, we see that in every 3-way set, there is a point t with $d(x_0, t) \leq 7K\mu$ but for all $i \in [3]$ we have $t \overset{i}{\frown} x_i$. Contract such a t with x. It cannot be by 3, as then $d(x + e_3, x_3 + e_3) \leq 16\lambda K\mu$, so without loss of generality we have $x \overset{1}{\frown} t$. But then for any $j \in \{2, 3\}$ and $k \in [2]$ that contracts x and x_3 we obtain $d(x_1 + e_1, x_1 + e_j) \leq d(x_1 + e_1, t + e_1) + d(t + e_1, x + e_1) + d(x + e_1, x + e_k) + d(x + e_k, x_3 + e_k) + d(x_3 + e_k, x_1 + e_j) \leq 8\lambda K\mu + 8\lambda K\mu + \lambda K\mu + 2\lambda K\mu + \lambda K\mu = 20\lambda K\mu$, giving $\operatorname{diam} N(x_1) \leq 20\lambda K\mu$ and as before $\rho(x_1) \leq 20K\mu$. Applying Proposition 3.23 establishes the final contradiction, as $\lambda < 1/(820C_1K)$. $\square$

3.6 Existence of certain finite configurations

Our next aim is to show that, provided λ is sufficiently small, certain finite configurations must exist. Recalling Proposition 3.23, which is a non-existence result, we see that we are approaching the final contradiction in the proof of Proposition 3.3.

Proposition 3.25. *Provided $\lambda < 1/(5 \cdot 10^{12})$, there is a point x such that $\rho(x) \leq C_2\mu$ and $\operatorname{diam}\{x, x + e_i, x + e_j\} \leq \lambda C_2\mu$ for some distinct $i, j \in [3]$. Here $C_2 = 100000$.*

Proof. Suppose contrary. The first part of the proof will be to establish the existence of an auxiliary point y with $\rho(y) \leq 15\mu$ and $d(y, y + e_i) \leq 192\lambda\mu$, $d(y +$

$e_j, y + e_k) \leq 4\lambda\mu$ for some $\{i, j, k\} = [3]$. Pick any t with $\rho(t) \leq 2\mu$ and consider contractions $\{t\} \cup N(t)$. As before, up to symmetry, we have diagrams A, B and C in Figure 3.5 as the possibilities for contractions of pairs of the form $t+e_a, t+e_b$, since no two such long edges can be contracted by the same i. If an edge is a dashed line in Figure 3.5, then it is the result of a contraction of some pair of points in $\{t\} \cup N(x)$. Dotted lines with letter **P** indicate that bounds on the lengths of those edges are results of applying Proposition 3.24.

Case 1. Suppose that we have diagram A. We see that we have diagrams A.1 and A.2 up to symmetry or otherwise some $\rho(z)$ is too small. However, diagram A.1 is impossible since $\rho(t+e_1) \leq C_2\mu$ and $\operatorname{diam}\{t+e_1, t+e_1+e_1, t+e_1+e_2\} \leq \lambda C_2\mu$, which does not exist by the assumption. Hence, it is diagram A.2 that must occur, so we have y with $\rho(y) \leq (4+6\lambda)\mu$, $d(y, y+e_3) \leq 2\lambda\mu$, $d(y+e_1, y+e_2) \leq 4\lambda\mu$.

Case 2. Suppose that we have diagram B. As above, we can distinguish diagrams B.1, B.2, B.3, up to symmetry. First of all, if we have diagram B.3, we can apply Proposition 3.22 to t, as $\lambda < 1/(13 \cdot C_1), 1/(78 \cdot 2)$, to obtain $\rho(t + e_i) \leq 14\mu$ for some i. Using this, we see that we have $\rho(y+e_3) \leq 15\mu$, $d(y+e_3+e_1, y+e_3+e_2) \leq 4\lambda\mu$, $d(y + e_3, y + 2e_3) \leq 2\lambda\mu$, as desired.

Consider now diagrams B.1 and B.2. We can denote $N(t) = \{t_1, t_2, t_3\}$ so that $t_1 + e_2, t_1 + e_3$ is a result of a contraction in $N(t)$ and so on. Observe that $\operatorname{diam}\{t_i + e_j : i, j \in [3], i \neq j\} \leq 12\lambda\mu$ and that $\rho(t) \leq 2\mu$, and in diagram B.1 $d(t+e_1, t+e_3) \leq 8\lambda\mu$, while in diagram B.2 $d(t+e_1, t+e_2) \leq 10\lambda\mu$, we can apply Proposition 3.24, as $\lambda < (9840C_1)$, to $(t; t_1, t_2, t_3; t)$ with constant 12 to see that $d(t+e_2, t_2+e_2) \leq 12 \cdot 16\lambda\mu = 192\lambda\mu$ in diagram B.1 and $d(t+e_3, t_3+e_3) \leq 192\lambda\mu$. Hence, $t+e_2$ in diagram B.1 and $t+e_3$ in the diagram B.2 are the desired points.

Case 3. As in the previous case, we are able to reach the same conclusion using the similar arguments.

To sum up, without loss of generality, we can assume that there is y_0, with $\rho(y_0) \leq 15\mu$, $d(y_0 + e_1, y_0 + e_2) \leq 4\lambda\mu$ and $d(y_0, y_0 + e_3) \leq 192\lambda\mu$. We shall now use this point to obtain a contradiction.

Let $K = 20000$, and consider now those points which satisfy $\rho(y) \leq K\mu$, $d(y+e_i, y+e_j) \leq \lambda K\mu$ and $d(y, y+e_k) \leq \lambda K\mu$ for some $\{i, j, k\} = [3]$. We know that y_0 is one such point. Contract first the pairs inside $N(y)$, that is, the long edges.

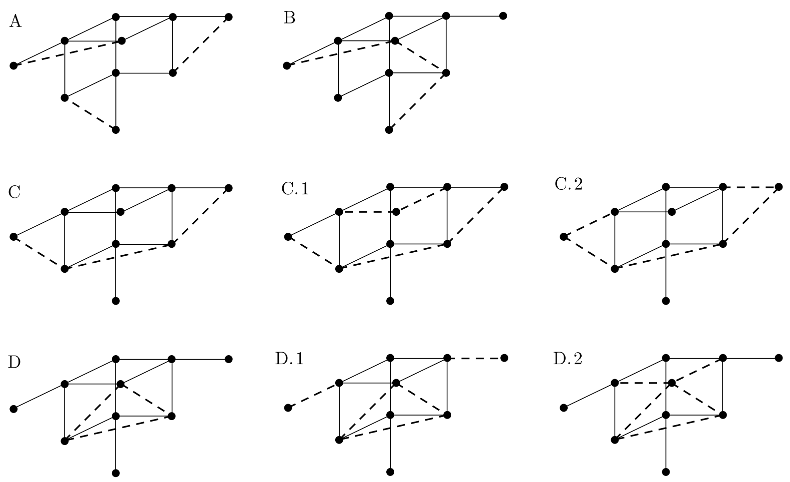


Figure 3.6: Possible contractions in the neighbourhood of an auxiliary point

As a few times before, it is not hard to see that for $i = 1, j = 2, k = 3$ we can only have diagrams A, B, C and D in Figure 3.6 (if an edge is shown as dashed line, that implies that it is a result of a contraction) and diagrams symmetric to these for different values of i, j, k. However, we can immediately reject diagram A, for if a point y has diagram A, by contracting the short edges, we either obtain a point $t \in N(y)$ with $\rho(t) \leq 3K\mu$ and $\text{diam}\{t, t+e_i, t+e_j\} \leq 3\lambda K\mu$, or we get a point $t \in N(y)$ with $\rho(y) \leq 4\lambda K\mu < \mu$, both resulting in a contradiction. Furthermore, if we are given a diagram B, then we can immediately apply Proposition 3.24 to $(y; y+e_3, y+e_2, y+e_1; y)$ with constant $6K$, as $\lambda < 1/(4920C_1K)$, which gives $d(y+e_3, y+e_1+e_3) \leq 96\lambda K\mu$. Then we must have $y \overset{2}{\frown} y+e_3$, hence $\rho(y+e_1) \leq (1+97\lambda)K\mu < (K+1)\mu, \text{diam}\{y+e_1, y+e_1+e_1, y+e_1+e_2\} \leq 5\lambda K\mu$ giving a contradiction once more.

Therefore, we must end up with either diagram C or D. Also observe that $y + e_i \overset{k}{\frown} y + e_j$ must then hold for any y that satisfies the properties stated above. Furthermore we must have $d(y + e_k, y + 2e_k) \leq 96\lambda K\mu$, as we can apply Proposition 3.24 to $(y; y_1, y_2, y_3; y)$, where $\{y_1, y_2, y_3\} = N(y)$ with constant $6K$. From this, we can conclude that neither $y \overset{k}{\frown} y+e_i$ nor $y \overset{k}{\frown} y+e_j$ can occur. Also we cannot have $y \overset{i}{\frown} y + e_i$ and $y \overset{i}{\frown} y + e_j$ simultaneously, as then $\rho(y + e_i) < \mu$, and similarly cannot have both $y \overset{j}{\frown} y + e_i$ and $y \overset{j}{\frown} y + e_j$. Hence, contracting the short edges implies that in fact we can only have diagrams C.1, C.2, D.1 or

D.2.

Observe that we can actually only have either C.1 and D.1, or C.2 and D.2 appearing. This is because if we had y_1 with its diagram among C.1 and D.1, and a point y_2 with a diagram among C.2 and D.2, we could first find the unique e_i, e_j such that $d(y_1+e_i, y_1+e_i+e_1) \leq \lambda K\mu$ and $d(y_2+e_j, y_2+e_j+e_1) = \rho(y_2+e_j)$. Now, apply Proposition 3.24 to $(y_1; y_1+e_i, y_1+e_k, y_1+e_3; y_2+e_j)$ with constant $6K$, where $k \in [2]$ distinct from i, to obtain $\rho(y_2+e_j) = d(y_2+e_j, y_2+e_j+e_1) \leq d(y_2+e_j, y_2) + d(y_2, y_1) + d(y_1, y_1+e_i) + d(y_1+e_i, y_1+e_i+e_1) + d(y_1+e_i+e_1, y_2+e_j+e_1) \leq K\mu + 2K\mu/(1-\lambda) + K\mu + \lambda K\mu + 96\lambda K\mu \leq 5K\mu$, while $\operatorname{diam}\{y_2+e_j, y_2+e_j+e_2, y_2+e_j+e_3\} \leq 3\lambda K\mu$, which is a contradiction. Thus, we shall consider the cases depending on the allowed pair of diagrams among these four.

Case 1. We can only have diagrams C.1 and D.1.

Suppose that we had y with $\rho(y) \leq K\mu/10, d(y+e_i, y+e_j) \leq \lambda K\mu/10, d(y, y+e_k) \leq \lambda K\mu/10$, for some $\{i,j,k\} = [3]$ that gave us diagram C.1 after contractions in $\{y\} \cup N(y)$. Without loss of generality, take $i=1, j=2$ and $k=3$. Then, by Proposition 3.22 and the triangle inequality, we get $\rho(y+e_1), \rho(y+e_2) \leq K\mu$. In conjunction with $d(y+e_1+e_1, y+e_1+e_3), d(y+e_2+e_2, y+e_2+e_3) \leq \lambda K\mu/5$ and $d(y+e_1, y+e_1+e_2), d(y+e_2, y+e_2+e_1) \leq \lambda K\mu/10$, we see that $y+e_1, y+e_2$ are points whose neighbourhoods contracting gives one of the diagrams considered, in particular $y+e_1+e_1 \overset{2}{\frown} y+e_1+e_3$ and $y+e_2+e_2 \overset{1}{\frown} y+e_2+e_3$. But contract $y+e_1+e_2$ with y, this gives $\rho(y+e_1+e_2) \leq K\mu/5 < K\mu$ and $\operatorname{diam} N(y+e_1+e_2) \leq \lambda^2 K\mu < \lambda K\mu$ which is a contradiction with Proposition 3.23, since $\lambda < 1/(41C_1K)$.

Hence, as long as y satisfies $\rho(y) \leq K\mu/10, d(y+e_i, y+e_j) \leq \lambda K\mu/10, d(y, y+e_k) \leq \lambda K\mu/10$, for some $\{i,j,k\} = [3]$ it must have diagram D.1. Start from y_0. Then we have $d(y_0+e_3+e_1, y_0+e_3+e_2) \leq \lambda^2 K\mu, d(y_0+e_3, y_0+2e_3) \leq \lambda^2 K\mu$. Now, apply Proposition 3.22 to y_0 see that $\rho(y_0+e_3) \leq 8\rho(y_0)$. Therefore, contractions around y_0+e_3 give us diagram D.1. But, contract $y_0+e_1, y_0+e_1+e_3$ to obtain $\rho(y_0+e_1+e_3) < \mu$ or $\rho(y_0+e_1) < \mu$.

Case 2. We can only have diagrams C.2 and D.2.

Start from y_0 and define $y_n = y_0 + ne_3$ for all $n \geq 1$. By induction on n we claim that $\rho(y_n) \leq 16\mu, d(y_n+e_1, y_n+e_2) \leq 4\lambda^{n+1}\mu, d(y_n+e_1, y_{n+1}+e_1) \leq$

$(45+8n)\lambda^{n+1}\mu, d(y_n+e_2, y_{n+1}+e_2) \leq (45+8n)\lambda^{n+1}\mu, d(y_n, y_n+e_3) \leq 2000\lambda\mu$.

For $n = 0$ the claim holds, since y_0 has diagram C.2 or D.2. Suppose the claim holds for some $n \geq 0$. Then it must have diagram C.2 or D.2, so $y_n + e_1 \overset{3}{\frown} y_n + e_2$, giving $d(y_{n+1}+e_1, y_{n+1}+e_2) \leq \lambda d(y_n+e_1, y_n+e_2) \leq 4\lambda^{n+1}\mu$. We can apply Proposition 3.24 to $(y_0; y_0+e_2, y_0+e_1, y_0+e_3; y_n)$ or $(y_0; y_0+e_1, y_0+e_2, y_0+e_3; y_n)$ (depending on the diagram of y_0) and to $(y_0; y_0+e_2, y_0+e_1, y_0+e_3; y_{n+1})$ or $(y_0; y_0+e_1, y_0+e_2, y_0+e_3; y_{n+1})$ with constant 60, so we get $d(y_0+e_3, y_n+e_3), d(y_0+e_3, y_{n+1}+e_3) \leq 960\lambda\mu$, thus $d(y_{n+1}, y_{n+1}+e_3) \leq 2000\lambda\mu$. So $\rho(y_{n+1}) \leq (1+3\lambda)\rho(y_n) \leq 17\mu$, so y_{n+1} has diagram C.2 or D.2.

If the diagrams of y_n and y_{n+1} are distinct, then $y_n + e_1 \overset{3}{\frown} y_{n+1} + e_1$ and $y_n + e_2 \overset{3}{\frown} y_{n+1} + e_2$, so the inequalities for $d(y_{n+1}+e_1, y_{n+2}+e_1)$ and $d(y_{n+1}+e_2, y_{n+2}+e_2)$ follow. Otherwise, $y_n + e_1 \overset{3}{\frown} y_{n+1} + e_2$ and $y_n + e_2 \overset{3}{\frown} y_{n+1} + e_1$, so $d(y_{n+1}+e_1, y_{n+2}+e_1) \leq d(y_{n+1}+e_1, y_{n+1}+e_2) + d(y_{n+1}+e_2, y_{n+2}+e_1) \leq 4\lambda^{n+2}\mu + \lambda(d(y_n+e_2, y_n+e_1) + d(y_n+e_1, y_{n+1}+e_1)) \leq 8\lambda^{n+2}\mu + \lambda(45+8n)\lambda^{n+1} = (45+8(n+1))\lambda^{n+2}\mu$. The inequality for $d(y_{n+1}+e_2, y_{n+2}+e_2)$ is proved in the same spirit.

Finally, by the triangle inequality we get $d(y_0+e_1, y_{n+1}+e_1) \leq d(y_0+e_1, y_1+e_2) + d(y_1+e_2, y_1+e_1) + d(y_1+e_1, y_2+e_2) + \cdots + d(y_n+e_1, y_{n+1}+e_1) < 50\lambda\mu$. Also $d(y_0, y_{n+1}) \leq d(y_0, y_0+e_3) + d(y_0+e_3, y_n+e_3) \leq 192\lambda\mu + 960\lambda\mu = 1152\lambda\mu$. Combining these conclusions further implies $\rho(y_{n+1}) \leq 16\mu$, as desired. Having established this claim, we can see that $(y_n+e_1)_{n\geq 0}$ is a 1-way Cauchy sequence, which is the final contradiction in this proof. □

Proposition 3.26. *Set $C_3 = 24\cdot 10^{10}, C_{3,1} = 19\cdot 10^9$ and let $i, j \in [3]$ be distinct. If $\lambda < 1/(7380 C_1 C_{3,1})$, there is x such that $\rho(x) \leq C_3\mu; d(x+e_i, x+e_j) \leq \lambda C_3\mu$.*

Proof. The proof will be a consequence of a few lemmas, the last one being Lemma 3.32. It suffices to prove the claim for $i = 1, j = 2$. Suppose contrary, there is no such a point. Consider those y which satisfy $\rho(y) \leq C_{3,1}\mu$ and $d(y+e_3, y+e_i) \leq \lambda C_{3,1}\mu$. For such a point y say that it is $C_{3,1}$-*good*, and more generally use this definition for arbitrary constant instead of $C_{3,1}$. We already know that such a y exists by Proposition 3.25. We list the possible diagrams of contractions in $\{y\} \cup N(y)$ for such a point, these are given in Figure 3.6 for

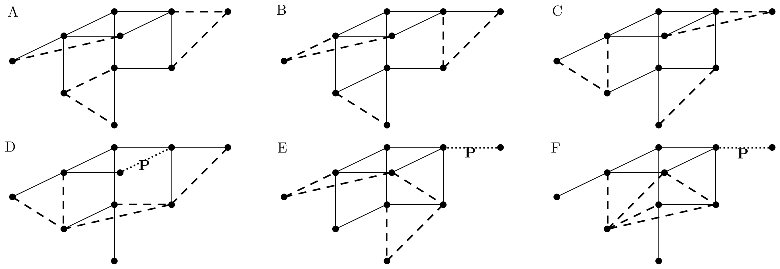


Figure 3.7: Possible diagrams in the proof of Proposition 3.26

$i = 1$. If an edge is shown as a dashed line, then it is a result of a contraction. Furthermore, with dotted lines with letter **P** we mark edges whose bound on length will be the result of applying Proposition 3.24. It is not hard to show that these are the only possible diagrams, but for the sake of completeness we include the full proof in Section 3.8 devoted to the contraction diagrams, which in particular provides an explanation for Figure 3.6. The symmetric diagrams to these for the case $i = 2$ are denoted by A', B', etc.

Our aim is to reject diagrams one by one. We shall start by discarding diagram A, and this method will then be used for the others. As we shall see, we can first apply the propositions proved so far to discard many diagrams in the presence of the given one, and then the remaining ones can be fitted together so that we obtain a 1-way Cauchy sequence.

Lemma 3.27. *Set $C_{3,2} = 31 \cdot 10^8$. There is no $C_{3,2}$-good y such that contractions give diagram A or A' for y.*

Proof of Lemma 3.27. Suppose contrary, we do have such a point y, and without loss of generality $d(y + e_1, y + e_3) \leq \lambda C_{3,2}\mu$. Firstly, suppose that there was another point z that is $C_{3,1}$-good, but whose diagram is among D, D', E, E', F, F'. By FNI we have $d(y, z) \leq (C_{3,2}+C_{3,1})\mu/(1-\lambda) < 2C_{3,1}\mu$. Then, for a suitable choice $\{z_1, z_2, z_3\} = N(z)$, we can apply Proposition 3.24 to $(z; z_1, z_2, z_3; y + e_1)$ with constant $6C_{3,1}$ to get $d(z_3, z_3 + e_3) \leq d(z_3, z) + d(z, y) + d(y, y + e_1 + e_3) + d(y + e_1 + e_3, z_3 + e_3) \leq C_{3,1}\mu + 2C_{3,1}\mu + (1 + \lambda)C_{3,2}\mu + 96\lambda C_{3,1}\mu < 4C_{3,1}\mu$. Hence, $\rho(z_3) \leq 4C_{3,1}\mu$, except when the diagram is D or D', so we must apply Proposition 3.22 to z first, so obtain $\rho(z_3) \leq 10C_{3,1}\mu$. Also, $d(z_3 + e_1, z_3 + e_2) \leq$

$2\lambda C_{3,1}\mu$, but such a point z cannot exist by the assumptions.

Now, take an arbitrary $(C_{3,1}/3)$-good point z with diagram A. Consider the point $z+e_3$. We have $\rho(z+e_3) \leq (2+3\lambda)\rho(z), d(z+e_3+e_1, z+e_3+e_3) \leq 2\lambda\rho(z)$ so $z+e_3$ is $C_{3,1}$-good, so its diagram is one of A, B or C (it cannot be among the symmetric to these ones as then $\rho(z+e_3) < \mu$). If it was B, then contracting the pair $z+e_1, z+e_3+e_2$ would give immediate contradiction, for we would obtain one of $\rho(z+e_1) < C_{3,1}\mu$, $\rho(z+e_2) < \mu$ or $\rho(z+e_2+e_3) < \mu$. Similarly, it cannot be C, since contracting the same pair of points would give the contradiction once again as it would yield $\rho(z+e_2) < \mu$ or $\rho(z+2e_3) < \mu$. Therefore, whenever we have a $(C_{3,1}/3)$-good point z with diagram A, then $z+e_3$ is $C_{3,1}$-good and has the same diagram.

Now, start from the y given, and define $y_n = y+ne_3$, for $n \geq 0$. We shall now show that $(y_n)_{n\geq 0}$ is a Cauchy sequence and hence obtain a contradiction. By induction on n we claim $d(y_n, y_n+e_1) \leq \lambda^n C_{3,2}\mu, d(y_n+e_1, y_{n+1}) \leq \lambda^{n+1}C_{3,2}\mu$, $\rho(y_n) < (2+10\lambda)C_{3,2}\mu$ and diagram of y_n is A. This is clearly true for $n=0$.

Suppose that the claim holds for $n \geq 0$. Note $d(y_0, y_{n+1}) \leq d(y_0, y_1) + d(y_1, y_2) + \cdots + d(y_n + y_{n+1}) \leq C_{3,2}\mu + 2\lambda C_{3,2}\mu + 2\lambda^2 C_{3,2}\mu + \cdots < (1+3\lambda)C_{3,2}\mu$. The fact that y_n has the diagram A and is in fact $C_{3,1}/3$-good implies that y_{n+1} is $C_{3,1}$-good and itself has diagram A. Further, $y_n \overset{3}{\frown} y_n + e_1$ and $y_n + e_1 \overset{3}{\frown} y_n + e_3$. This is then sufficient to obtain the next two inequalities. Also $d(y_0 + e_2, y_{n+1}) < C_{3,2}\mu + 3C_{3,2}\mu/(1-\lambda) < 5C_{3,2}\mu$. Hence, we must have $y_0 + e_2 \overset{2}{\frown} y_{n+1}$, for otherwise $\rho(y_0+e_1) < \mu$ or $\rho(y_1) < \mu$. So $d(y_0, y_{n+1}+e_2) \leq d(y_0, y_0+2e_2) + \lambda d(y_0+e_2, y_{n+1}) \leq C_{3,2}\mu + \lambda C_{3,2}\mu + 5\lambda C_{3,2}\mu$, from which we can infer $\rho(y_{n+1}) = d(y_{n+1}, y_{n+1}+e_2) \leq d(y_{n+1}, y_0) + d(y_0, y_0+e_2) + d(y_0+e_2, y_0+2e_3) + d(y_0+2e_2, y_{n+1}+e_2) < (2+10\lambda)C_{3,2}\mu$, as claimed.

From this we immediately get that $(y_n)_{n\geq 0}$ is a Cauchy sequence. $\square$

Lemma 3.28. *Set $C_{3,3} = 1029 \cdot 10^6$. There is no $C_{3,3}$-good point y with diagram E or E'.*

Proof of Lemma 3.28. Suppose contrary, without loss of generality $d(y+e_1, y+e_3) \leq \lambda C_{3,3}\mu$. Firstly, suppose there was a $C_{3,2}$-good point z with $d(z+e_1, z+e_3) \leq \lambda C_{3,2}\mu$ and diagram among B, C, D. Take $p = z+e_2$ for diagrams B, D, $p = z+e_3$ for C, and apply Proposition 3.24 with constant $3C_{3,2}$ (for $d(p,y) \leq$

$3C_{3,2}\mu$ and for such a constant the other necessary assumptions also hold) to $(y; y+e_3, y+e_2, y+e_1; p)$ to obtain a contradiction at $y+e_1$, as it has $d(y+e_1+e_1, y+e_1+e_2) \leq 2C_{3,3}\lambda\mu$ and $\rho(y+e_1) = d(y+e_1, y+e_1+e_3) \leq d(y+e_1, y) + d(y, z) + d(z, p+e_1) + d(p+e_1, y+e_3+e_1) \leq C_{3,3}\mu + (C_{3,3}+C_{3,2})\mu/(1-\lambda) + 2C_{3,2}\mu + 48\lambda C_{3,2} < C_{3,1}\mu$. Hence, any such a $C_{3,2}$-good point z can only have diagram E or F.

Now, return to the point y and define $y_n = y + ne_2$, for all $n \geq 0$. We show that $(y_n)_{n\geq 0}$ is a Cauchy sequence. By induction on n we show that $d(y_n+e_1, y_n+e_3) \leq \lambda^{n+1}C_{3,3}\mu, d(y_n+e_3, y_{n+1}+e_3) \leq (3+2n)\lambda^{n+1}C_{3,3}\mu$ and $\rho(y_n) < 3C_{3,3}\mu$. Case $n = 0$ is clear.

Suppose the claim holds for some $n \geq 0$. Firstly, y_n is $C_{3,2}$-good, so it has diagram E or F, so in particular $d(y_{n+1}+e_1, y_{n+1}+e_3) \leq \lambda d(y_n+e_1, y_n+e_3) \leq \lambda^{n+1}C_{3,3}\mu$. Applying the triangle inequality gives $d(y_{n+1}+e_3, y_0+e_3) \leq d(y_{n+1}+e_3, y_n+e_3) + \cdots + d(y_1+e_3, y_0+e_3) \leq (5+2n)\lambda^{n+1}C_{3,3}\mu + \ldots 3\lambda C_{3,3}\mu < 3\lambda C_{3,3}\mu/(1-2\lambda)$. Further, since $d(y_0, y_{n+1}) \leq d(y_0, y_n) + d(y_n, y_{n+1}) \leq (\rho(y_0) + \rho(y_n))/(1-\lambda) + \rho(y_n) \leq 8C_{3,3}\mu$ apply Proposition 3.24 to $(y; y+e_3, y+e_2, y+e_1; y_{n+1})$ with constant $8C_{3,3}$ which gives $d(y_1, y_{n+2}) \leq 128\lambda C_{3,3}\mu$. Therefore, $\rho(y_{n+1}) < 3C_{3,3}\mu$, in particular is $C_{3,2}$-good, hence its diagram can also only be E or F. If y_n and y_{n+1} have the same diagram, then contract $y_n+e_1, y_{n+1}+e_3$, otherwise $y_n+e_3, y_{n+1}+e_3$. These must be contracted by 2, so using the triangle inequality gives in the former case $d(y_{n+1}+e_3, y_{n+2}+e_3) \leq d(y_{n+1}+e_3, y_{n+1}+e_1) + d(y_{n+1}+e_1, y_{n+2}+e_3) \leq \lambda^{n+2}C_{3,3}\mu + \lambda d(y_n+e_1, y_{n+1}+e_3) \leq \lambda^{n+2}C_{3,3}\mu + \lambda(d(y_n+e_1, y_n+e_3) + d(y_n+e_3, y_{n+1}+e_3)) \leq 2\lambda^{n+2}C_{3,3}\mu + \lambda d(y_n+e_3, y_{n+1}+e_3) \leq (5+2n)\lambda^{n+2}C_{3,3}\mu$ as desired. In the latter case we are immediately done.

Furthermore this claim implies that $(y_n+e_1)_{n\geq 0}$ is a Cauchy sequence, so we obtain a contradiction. □

Lemma 3.29. *Set $C_{3,4} = 147 \cdot 10^6$. There is no $C_{3,4}$-good point y with diagram F or F'.*

Proof of Lemma 3.29. Suppose contrary, there is such a point y and without loss of generality we may assume $d(y+e_1, y+e_3) \leq \lambda C_{3,4}\mu$.

Suppose that we have a point z that is $3C_{3,4}$-good with diagram F and that $d(z+e_1, z+e_3) \leq 3\lambda C_{3,4}\mu$, and that $z+e_2$ being $C_{3,3}$-good has diagram B, C or D. If it was B, we would immediately obtain a contradiction by contracting $z+e_1, z+2e_2$, and if it was C, contracting $z+e_1, z+e_2+e_3$, would once again end the proof, both giving a point p with $\rho(p) < \mu$, so suppose that it was D. Apply Proposition 3.24 to $(z; z+e_1, z+e_2, z+e_3; z+e_2+e_3)$ and to $(z; z+e_1, z+e_2, z+e_3; z+2e_2)$ with constant $12C_{3,4}$. Now $z+e_1$ is $7C_{3,4}$-good, so it has diagram among B', C', D', F'. However $\operatorname{diam}\{z+e_1+e_2, z+2e_1+e_2, z+e_1+e_2+e_3\} \leq 4\lambda C_{3,4}\mu$, so it must in fact be F'. Apply Proposition 3.24 to $(z; z+e_1, z+e_2, z+e_3; z+e_1+e_3)$ with constant $12C_{3,4}$. Thus $z+e_3 \overset{3}{\frown} z+2e_3$. Write $r = d(z+e_3, z+2e_3)$, so we see that FNI implies $r - \rho(z) \leq d(z, z+2e_3) \leq \lambda(r+\rho(z))/(1-\lambda)$, but $r \geq C_3\mu$ and $\rho(z) \leq 3C_{3,4}\mu$ give contradiction.

Hence, whenever z is a $3C_{3,4}$-good point with diagram F, $z+e_2$ is $C_{3,3}$-good and has the same diagram. Now $(y+ne_2)_{n\geq 0}$ is Cauchy by the arguments from the proof of Lemma 3.28, since there we allow both E and F as diagrams. $\square$

Lemma 3.30. *Set $C_{3,5} = 21 \cdot 10^6$. There is no $C_{3,5}$-good point y with diagram D or D'.*

Proof of Lemma 3.30. Suppose contrary, there is such a point y and without loss of generality we may assume $d(y+e_1, y+e_3) \leq \lambda C_{3,5}\mu$.

Consider a point $3C_{3,5}$-good point z with the diagram D and $d(z+e_1, z+e_3) \leq \lambda 3C_{3,5}\mu$. Since $z+e_1$ is $C_{3,4}$-good, it can only have diagram B, C or D. If it was not D, contract $z+e_2, z+e_1+e_3$ for the sake of contradiction, namely, if it was B we would get $\rho(z+e_2) < \mu$ or $\rho(z+2e_1) \leq C_3\mu$, but $d(z+2e_1+e_1, z+2e_1+e_2) \leq 2\lambda C_{3,5}\mu$ and if it was C, we would obtain $\rho(z+e_1+e_3) < \mu$ or $\rho(z+2e_1) < \mu$. Hence, whenever z has the given properties, $z+e_1$ has diagram D.

Return to y, and consider the sequence $y_n = y+ne_1$, for $n \geq 0$. By induction on n, we show that $\rho(y_n) \leq 3C_{3,5}\mu$, $d(y_n, y_n+e_3) \leq \lambda^n C_{3,5}\mu$ and $d(y_n+e_3, y_{n+1}) \leq \lambda^{n+1}C_{3,5}\mu$. The claim is clearly true for $n=0$.

Suppose that the claim holds for some $n \geq 0$. Then y_n is $3C_{3,5}$-good so it has diagram D. Hence, $y_n \overset{1}{\frown} y_n+e_3$ and $y_{n+1} \overset{1}{\frown} y_n+e_3$, which establishes two of the necessary inequalities. Also, by the triangle inequality $d(y_{n+1}, y_0) \leq C_{3,5}\mu + 2\lambda C_{3,5}\mu/(1-\lambda)$, so we can apply Proposition 3.24 to $(y_0; y_0+e_2, y_0+e_1, y_0+e_3; y_{n+1})$ with constant $6C_{3,5}$ to get $d(y_{n+1}+e_2, y_0+e_1+e_2) \leq 96C_{3,5}\mu$, in particular $\rho(y_{n+1}) \leq 3C_{3,5}\mu$, as desired.

It follows that $(y_n)_{n\geq 0}$ is a Cauchy sequence. $\square$

Lemma 3.31. *Set $C_{3,6} = 3 \cdot 10^6$. There is no $C_{3,6}$-good point y with diagram C or C'.*

Proof of Lemma 3.31. Suppose contrary, there is such a point y and without loss of generality we may assume $d(y+e_1, y+e_3) \leq \lambda C_{3,6}\mu$.

Firstly, suppose that we have a $3C_{3,6}$-good point z such that $d(z+e_1, z+e_3) \leq 3\lambda C_{3,6}\mu$, and $z+e_1$ has diagram B. We shall obtain a contradiction by considering contractions in such a situation. First of all we can observe that $z+e_3 \overset{3}{\frown} z+e_1+e_3$. Note that $d(z+2e_1, z+2e_1+e_3) > C_3\mu$, so $d(z+e_3, z+2e_3) \geq d(z+2e_1, z+2e_1+e_3) - d(z+e_3, z+2e_1) - d(z+2e_3, z+2e_1+e_3) > C_3\mu - 24\lambda C_{3,6}\mu$.

Case 1. Suppose that $z+e_3 \overset{2}{\frown} z+2e_3$.

We see that $z+e_2+e_3, z+2e_3$ is not contracted by 1, and from FNI, we must have $\rho(z+2e_3) \geq (1-\lambda)d(z, z+2e_3) - \rho(z) \geq (1-\lambda)d(z+e_3, z+2e_3) - (2-\lambda)\rho(z)$, thus $z+e_2+e_3, z+2e_3$ is neither contracted by 3, hence $z+e_2+e_3 \overset{2}{\frown} z+2e_3$. Now suppose that $z+2e_2 \overset{3}{\frown} z+e_1+e_2$. Then $d(z+e_3, z+2e_3) \leq d(z+e_3, z+e_2+2e_3) + d(z+e_2+2e_3, z+e_2+e_3) + d(z+e_2+e_3, z+2e_3)$ so $d(z+e_3, z+2e_3)(1-\lambda) \leq 3\rho(z)$ which is impossible.

Therefore we must have $z+2e_2 \overset{2}{\frown} z+e_1+e_2$ and $z+2e_1 \overset{3}{\frown} z+2e_2$, otherwise $\rho(z+e_1+e_2) < \mu$. Finally, contract $z+2e_1$with $z+2e_3$ to get $\rho(z+2e_1) < \mu$ or $\rho(z+2e_3) < \mu$.

Case 2. Suppose that $z+e_3 \overset{3}{\frown} z+2e_3$.

By FNI applied to $z, z+2e_3$ we see that $\rho(z+2e_3) \geq (1-\lambda)d(z+e_3, z+2e_3) - (2-\lambda)\rho(z)$, hence $\rho(z+2e_3) = d(z+2e_3, z+e_2+2e_3) \geq (1-\lambda)d(z+e_3, z+2e_3) - (2-\lambda)\rho(z)$. So we have $z+2e_3 \overset{2}{\frown} z+e_2+e_3$. Also $z+2e_2 \overset{2}{\frown} z+e_3$, from which we see that $z+2e_2 \overset{2}{\frown} z+2e_1$, giving a contradiction.

Thus, whenever we have a point z as described, we must have $z+e_1$ with diagram C as well. Now, set $y_n = y+ne_1$ for $n \geq 0$. By induction on n we prove that $d(y_n, y_n+e_3) \leq \lambda^n C_{3,6}\mu, d(y_n+e_3, y_{n+1}) \leq \lambda^{n+1}C_{3,6}\mu, \rho(y_n) \leq 3C_{3,6}\mu$ and y_n has diagram C. This is clear for $n=0$.

Suppose the claim holds for some $n \geq 0$, so y_n must have diagram C, from which the first two inequalities follow. Observe that $d(y_{n+1}, y_0) < \rho(y_0) + 2\lambda\rho(y_0)/(1-\lambda)$ and $d(y_0+e_2, y_0+e_2+e_3) > C_3\mu$, so $y_{n+1} \overset{2}{\frown} y_0+e_2$. Therefore

$\rho(y_{n+1}) < 3\rho(y_0) \le 3C_{3,6}\mu$, which gives the rest of the claim, as $y_{n+1} = y_n + e_1$ must have diagram C, by the previous conclusions.

Hence $(y_n)_{n\ge 0}$ is a 1-way Cauchy sequence, which is a contradiction. $\square$

Lemma 3.32. *Set $C_{3,7} = 10^5$. There is no $C_{3,7}$-good point y with diagram B or B'.*

Proof of Lemma 3.32. Suppose contrary, there is such a point y and without loss of generality we may assume $d(y + e_1, y + e_3) \le \lambda C_{3,7}\mu$.

Consider a $6C_{3,7}$-good point z, which has $d(z + e_1, z + e_3) \le 6\lambda C_{3,7}\mu$, which therefore must have diagram B. We have $\rho(z + e_2) \le (2 + 3\lambda)\rho(z), d(z + e_2 + e_2, z + e_2 + e_3) \le 2\lambda\rho(z)$, so $z + e_2$ is $C_{3,6}$-good so has diagram B'. Observe that $z + e_3 \overset{3}{\frown} z + e_2 + e_3$ as $d(z + (1, 0, 1), z + (1, 1, 1)) \ge R - 4\lambda\rho(z)$ and $d(z+(0, 1, 1), z+(0, 2, 1)) > C_3\mu-2\lambda\rho(z)$, where $R = d(z+e_1, z+e_1+e_3) > C_3\mu$. Also $z+e_1 \overset{3}{\frown} z+e_3$ since z has diagram B. Similarly, since $z+e_2$ has diagram B', we must have $z+2e_2 \overset{3}{\frown} z+e_2+e_3$. Furthermore $\rho(z+e_1+e_2) \le (2+3\lambda)\rho(z+e_2) \le (2 + 3\lambda)^2\rho(z), d(z + e_1 + e_2 + e_1, z + e_1 + e_2 + e_3) \le 2\lambda\rho(z + e_2) \le 5\lambda\rho(z)$, so $z + e_1 + e_2$ is $C_{3,6}$-good, hence itself has diagram B, from which we infer $z + (0, 1, 1) \overset{3}{\frown} z + (1, 1, 1)$.

Suppose that $z + e_1 + e_3 \overset{3}{\frown} z + e_2 + e_3$, so have $d(z + (1, 0, 2), z + (0, 1, 2)) \le \lambda(R+3\rho(z))$ and $d(z+(1, 0, 2), z+(0, 0, 2)) \le \lambda(R+6\rho(z))$. Thus $d(z+(1, 0, 1), z+(1, 0, 2)) \le \lambda(R + 8\rho(z))$, hence $z \overset{3}{\frown} z + 2e_3$, which implies $d(z + 2e_3, z + 3e_3) \ge R(1 - \lambda) - 3\rho(z)$, so $z + e_1 + e_3 \overset{1}{\frown} z + 2e_3$ (if $z + e_1 + e_3 \overset{2}{\frown} z + 2e_3$, then $\rho(z + 2e_1 + e_2) < \mu$) giving $d(z + (2, 0, 1), z + (1, 0, 1)) \le \lambda(R + 10\rho(z))$. Also $z+(1, 1, 0) \overset{1}{\frown} z+(2, 0, 0)$ and $z+2e_1 \overset{3}{\frown} z+2e_2$, but then contracting $z+2e_1, z+2e_3$, results in contradiction.

Thus $z + (1, 0, 1) \overset{1}{\frown} z + (0, 1, 1)$, as otherwise $R(1-\lambda) \le 2C_{3,7}\mu$, which is not possible. From the fact that z has the diagram B, we have $z \overset{1}{\frown} z + e_1$. Also, we must have $z+e_1 \overset{1}{\frown} z+e_1+e_2$. As $d(z+e_1+e_3, z+2e_1+e_3) \ge (1-\lambda)R-7\lambda\rho(z)$, we cannot have $z + e_1 \overset{3}{\frown} z + 2e_1$. Suppose that $z + e_1 \overset{1}{\frown} z + 2e_1$, then contracting $z + 2e_2, z + e_1$ and $z + 2e_2, z + 2e_1$ (both must be in the direction e_3) gives $d(z + e_1 + e_3, z + 2e_1 + e_3) \le 6\lambda\rho(z)$, which is a contradiction.

We conclude that $z \overset{1}{\frown} z + e_1$, $z + e_1 \overset{1}{\frown} z + e_1 + e_2$ and $z + e_1 \overset{2}{\frown} z + 2e_1$, for such a z. By symmetry, when $d(z + e_2, z + e_3) \le 6\lambda C_{3,7}\mu$ holds instead of

$d(z+e_1, z+e_3) \leq 6\lambda C_{3,7}\mu$, then we must have $z \overset{2}{\frown} z+e_2$, $z+e_2 \overset{2}{\frown} z+e_1+e_2$ and $z+e_2 \overset{1}{\frown} z+2e_2$.

Return now to the point y and consider the sequence given as $y_0 = y$, when k is even set $y_{k+1} = y+e_2$, otherwise $y_{k+1} = y+e_1$. By induction on k we obtain $\rho(y_k) \leq 3C_{3,7}\mu, d(y_k, y_{k+2}) \leq 3\lambda^k \frac{1+\lambda^2}{1-\lambda} C_{3,7}\mu, d(y_k, y_k+e_3) \leq \lambda^k C_{3,7}\mu$; and for even k we have $d(y_k, y_k+e_1) \leq 3\lambda^k C_{3,7}\mu$, and for odd k we have $d(y_k, y_k+e_2) \leq 3\lambda^k C_{3,7}\mu$.

When $k=0$, the claim clearly holds. Suppose that the claim is true for all values less than or equal to some even $k \geq 0$. We shall argue when k is even, the same argument works in the opposite situation. By the triangle inequality, we have $d(y_0, y_i) \leq 3\frac{1+\lambda^2}{(1-\lambda)(1-\lambda^2)} C_{3,7}\mu$ for even $i \leq k+2$ and $d(y_1, y_i) \leq 3\lambda\frac{1+\lambda^2}{(1-\lambda)(1-\lambda^2)} C_{3,7}\mu$ for the odd $i \leq k+2$. In particular, as y_k is $C_{3,6}$-good, it has diagram B, so $\rho(y_{k+1}) = d(y_{k+1}, y_{k+2}) \leq d(y_{k+1}, y_1) + \rho(y_0) + d(y_0, y_{k+2}) \leq 3(1+\lambda)\frac{1+\lambda^2}{(1-\lambda)(1-\lambda^2)} C_{3,7}\mu + C_{3,7}\mu \leq 5C_{3,7}\mu$ and $d(y_{k+1}+e_2, y_{k+1}+e_3) \leq 2\lambda\rho(y_k) \leq 10\lambda C_{3,7}\mu$. Then y_{k+1} is $10C_{3,7}$-good, so it must have diagram B'. From the contractions implied by this diagram described previously, we get that $d(y_{k+1}, y_{k+1}+e_3) \leq \lambda^{k+1} C_{3,7}\mu$. Moreover, $y_{k+1} \overset{2}{\frown} y_{k+1}+e_2$, $y_{k+1}+e_2 \overset{2}{\frown} y_{k+1}+e_1+e_2$ and $y_{k+1}+e_2 \overset{1}{\frown} y_{k+1}+2e_2$. Therefore $d(y_{k+1}+e_2, y_{k+3}) \leq d(y_{k+1}+e_2, y_{k+1}+2e_2) + d(y_{k+1}+2e_2, y_{k+1}+2e_2+e_1) + d(y_{k+1}+2e_2+e_1, y_{k+3}) \leq \lambda d(y_{k+1}+e_2, y_{k+3}) + (1+\lambda) d(y_{k+1}+e_2, y_{k+1}+2e_2) \leq \lambda d(y_{k+1}+e_2, y_{k+3}) + \lambda(1+\lambda) d(y_{k+1}, y_{k+1}+e_2)$. Hence $d(y_{k+1}, y_{k+3}) \leq \frac{1+\lambda^2}{1-\lambda} d(y_{k+1}, y_{k+1}+e_2)$, proving the claim.

We infer that $y_0, y_0+e_1, y_1, y_1+e_1, y_2, \ldots$ is a 1-way Cauchy sequence, which is a contradiction. □

But Proposition 3.25 provides us with a $C_{3,7}$-good point, which however cannot exist because of the lemmas we have shown in the course of this proof. □

3.7 Final contradiction

In the rest of the proof of Proposition 3.3, an important role will be played by the sets $S_i(K, x_0) = \{y : d(x_0, y) \leq K\mu, d(y, y+e_i) \leq K\mu\}$, defined for any point x_0, constant K and $i \in [3]$. Given any point t, the set $S_i(K, x_0)$ serves to give approximate versions of contractions of x_0 and t in the direction i, in the following sense. If $t \overset{i}{\frown} y$ for some $y \in S_i(K, x_0)$, then we have

$$\begin{aligned} d(x_0, t+e_i) &\le d(x_0, y) + d(y, y+e_i) + d(y+e_i, t+e_i) \le K\mu + K\mu + \lambda d(y,t) \\ &\le 2K\mu + \lambda(d(y, x_0) + d(x_0, t)) \le (2+\lambda)K\mu + \lambda d(x_0, t). \end{aligned}$$

Using this idea, unless t never contracts with $S_i(K, x_0)$ in the direction i for some i, we can get 3-way sets of small diameter, as we shall see in the proof of the next proposition.

An additional benefit of using these sets is that they usually do not consist of x_0 only (note $x_0 \in S_i(K, x_0)$ if $\rho(x_0) \le K\mu$), and that for example, under certain circumstances, we can find a point y with the property that $y, y+e_3 \in S_3(K, x_0)$. Such points will play an important role in the proofs of Propositions 3.35 and 3.36, which, when combined with the following proposition, are used to deduce the key result in this chapter.

Recall that $x \overset{i}{\not\frown} y$ means that $d(x+e_i, y+e_i) > \lambda d(x, y)$.

Proposition 3.33. *Fix arbitrary x_0 with $\rho(x_0) < 2\mu$. Given $K \ge 2$, when $i \in [3]$, define $S_i(K, x_0) = \{y : d(x_0, y) \le K\mu, d(y, y+e_i) \le K\mu\}$. Provided $1 > 2\lambda K C_1 (2+\lambda)^2/(1-\lambda)$, in every $\langle z \rangle_3$ there is t such that $d(t, x_0) \le \frac{2+\lambda}{1-\lambda} K\mu$, but for some $i \in [3]$, we have $t \overset{i}{\not\frown} s$ for all $s \in S_i(K, x_0)$.*

Proof. First of all, we have $x_0 \in S_1(K, x_0), S_2(K, x_0), S_3(K, x_0)$, making these non-empty, as $K\mu \ge \rho(x_0) \ge d(x_0, x_0+e_i)$ for all $i \in [3]$. Suppose contrary to our statement, there is z without any t described above. Since $\frac{2+\lambda}{1-\lambda} K\mu > \rho(x_0)/(1-\lambda)$, we know that there is $y \in \langle z \rangle_3$ such that $d(x_0, y) \le \frac{2+\lambda}{1-\lambda} K\mu$, by Lemma 3.8. Then we have $s_1 \in S_1(K, x_0)$ such that $s_1 \overset{1}{\frown} y$. Hence $d(y+e_1, x_0) \le d(y+e_1, s_1+e_1) + d(s_1+e_1, s_1) + d(s_1, x_0) \le \lambda(d(y, x_0) + d(x_0, s_1)) + 2K\mu \le \lambda(\frac{2+\lambda}{1-\lambda} K\mu + K\mu) + 2K\mu = \frac{2+\lambda}{1-\lambda} K\mu$. Similarly, we get the same result for $y+e_2, y+e_3$, and so we have constructed a 3-way set of diameter not greater $2\frac{2+\lambda}{1-\lambda} K\mu$, but there are no such sets since $1 > 2\lambda K C_1 (2+\lambda)^2/(1-\lambda)$ by Proposition 3.19, giving a contradiction. $\square$

Similarly as before, we use tighter constraints on λ. Here we use $\lambda < 1/10$ implies $\frac{2+\lambda}{1-\lambda} < 3$ and $(2+\lambda)^2/(1-\lambda) < 5$. Note that the following statement is Proposition 3.6 described in the overview of the proof.

Corollary 3.34. *Fix arbitrary x_0 with $\rho(x_0) < 2\mu$. Given $K \geq 2$, when $i \in [3]$, define $S_i(K, x_0) = \{y : d(x_0, y) \leq K\mu, d(y, y + e_i) \leq K\mu\}$. Provided $1 > 10\lambda KC_1$, in every $\langle z\rangle_3$ there is t such that $d(t, x_0) \leq 3K\mu$, but for some i we have $s \overset{i}{\not\frown} t$ when $s \in S_i(K, x_0)$.*

Based on this, we shall reach the final contradiction in the proof of Proposition 3.3. To do this, we consider the possible cases on the $d(t+e_j, t+e_k)$ where $\{i, j, k\} = [3]$ and t is a point given by Corollary 3.34. Namely, suppose that $d(t + e_j, t + e_k)$ is small enough, and in fact $j = 1, k = 2, i = 3$. Then whenever we have a point y with $y \in S_3(K, x_0)$ and if $d(y+e_1, y+e_2)$ is small we also have $\operatorname{diam}\{y+e_1, y+e_2, t+e_1, t+e_2\}$ small as well. On the other hand, if $d(t+e_1, t+e_2)$ is large, and $y_1, y_2 \in S_3(K, x_0)$ with $d(y_1 + e_1, y_1 + e_2), d(y_2 + e_1, y_2 + e_2)$ small, but $d(y_1 + e_1, y_2 + e_1)$ large, we also have pairs t, y_1 and t, y_2 contracted by the different values in $\{1, 2\}$. Of course, we need to specify what we mean by small and large in this context, and this is done in the following two propositions.

Proposition 3.35. *Let $C_4 = 16C_3$. Fix x_0 with $\rho(x_0) < 2\mu$. Let $\{i, j, k\} = [3]$. Given K, provided $\lambda < 1/(44C_3+6C_4+K), 1/(34440C_1C_3)$, we have $d(t+e_j, t+e_k) > K\lambda\mu$, when t is such that $d(t, x_0) \leq 3C_4\mu$ and $s \overset{i}{\not\frown} t$ when $s \in S_i(C_4, x_0)$.*

Proposition 3.36. *Let $C_5 = 1000C_3$. Fix x_0 with $\rho(x_0) < 2\mu$. Let $\{i, j, k\} = [3]$. Provided $\lambda < 1/(8200000C_1C_3)$, we have $d(t + e_j, t + e_k) \leq 10C_5\lambda\mu$, when t is such that $d(t, x_0) \leq 3C_5\mu$ and $s \overset{i}{\not\frown} t$ when $s \in S_i(C_5, x_0)$.*

Once we have shown these propositions, we just need to take λ small enough so that they both hold.

Let us now prove a lemma that classifies the relevant possible diagrams we will need in the incoming arguments.

Lemma 3.37. *Let $K \geq 1$ and $\lambda < 1/(4920KC_1)$. Suppose that we have a point y with $\rho(y) \leq K\mu$ and $d(y + e_1, y + e_2) \leq \lambda K\mu$. Then y must have one of the diagrams shown in Figure 3.7 (up to symmetry).*

Proof of Lemma 3.37. Contracting the long edges in $N(y) \cup \{y\}$ can only, up to symmetry, give us diagrams A, B, C and D, as described in the first part of Section 3.8, with the requirement $1/(164KC_1) > \lambda$. Observe that in diagrams B, C and D, we can apply Proposition 3.24 to $(y; y+e_3, y+e_2, y+e_1; y+e_1), (y; y+$

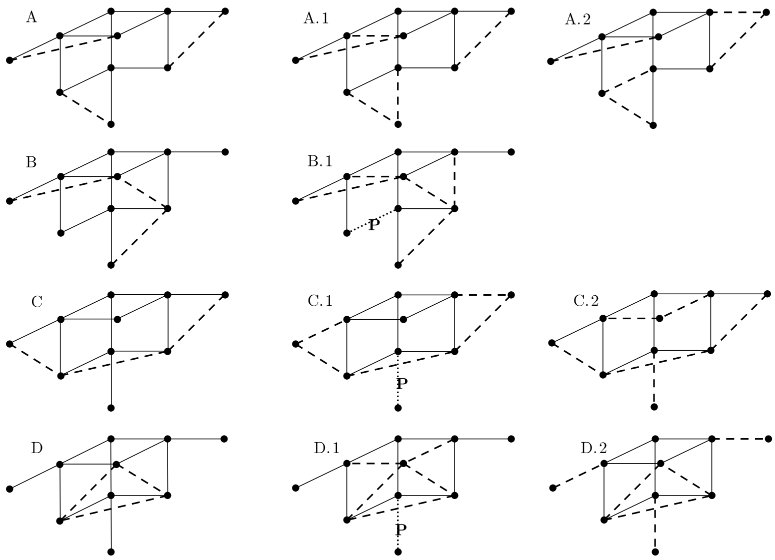


Figure 3.8: Possible diagrams for $\rho(y) \leq K\mu, d(y+e_1, y+e_2) \leq \lambda K\mu$.

$e_2, y+e_1, y+e_3; y+e_3)$ and $(y; y+e_1, y+e_2, y+e_3; y+e_3)$ respectively with constant $6K$, as long as $\lambda < 1/(4920KC_1)$. Further, by contracting the short edges, we can only obtain diagrams A.1, A.2, B.1, etc. shown in Figure 3.7, up to symmetry, as otherwise we obtain a point $p \in \{y\} \cup N(y)$ with $\rho(p) < \mu$. $\square$

Proof of Proposition 3.35. We prove the claim for $i = 3, j = 2, k = 1$, the other cases follow from symmetry. Suppose contrary, for some K and $\lambda < 1/(44C_3 + 6C_4 + K), 1/(34440C_1C_3)$, we have t_0 such that $d(t_0+e_1, t_0+e_2) \leq K\lambda\mu, d(t_0, x_0) \leq 3C_4\mu$ and $s \overset{3}{\not\frown} t_0$ whenever $s \in S_3(C_4, x_0)$, where x_0 is a point with $\rho(x_0) < 2\mu$.

Consider points y with $\rho(y) \leq 7C_3\mu, d(y+e_1, y+e_2) \leq 7\lambda C_3\mu$. Existence of such points is granted by Proposition 3.26. Apply Lemma 3.37 to y. We shall now discard some of the diagrams by contractions with t_0.

Suppose that y had the diagram A.1. By FNI $d(y, x_0) \leq (7C_3+2)\mu/(1-\lambda) \leq 8C_3\mu$, and so $y, y+e_3 \in S_3(C_4, x_0)$. Hence y, t_0 and $y+e_3, t_0$ would be contracted by 1 or 2. However, from this we see that if $y+e_3 \overset{1}{\frown} t_0$ we would get $\rho(y+e_1) = d(y+e_1, y+e_3+e_1) \leq d(y+e_1, t_0+e_1) + d(t_0+e_1, y+e_3+e_1) \leq d(y+e_1, y+e_2) + \lambda d(t_0, y) + d(t_0+e_1, t_0+e_2) + \lambda(d(t_0, y) + d(y, y+e_3)) \leq 7\lambda C_3\mu + 3\lambda C_4\mu + \lambda d(x_0, y) + \lambda K\mu + 3\lambda C_4\mu + \lambda d(x_0, y) + 7\lambda C_3\mu \leq \lambda(30C_3 + 6C_4 + K)\mu < \mu$.

On the other hand if $y+e_3 \overset{2}{\frown} t_0$, we would get $\rho(y+e_2) \leq d(y+e_3+e_2, y+e_2)+ d(y+e_2+e_3, y+e_2+e_2) \leq d(y+e_3+e_2, t_0+e_2)+d(t_0+e_2, y+e_2)+14\lambda C_3\mu \leq \lambda(d(t_0,x_0)+d(x_0,y)+d(y,y+e_3))+d(y+e_1,y+e_2)+d(t_0+e_1,t_0+e_2)+\lambda d(y,t_0)+ 14\lambda C_3 \leq 3\lambda C_4\mu+8\lambda C_3\mu+7\lambda C_3\mu+7\lambda C_3\mu+\lambda K\mu+3\lambda C_4\mu+8\lambda C_3\mu+14\lambda C_3\mu \leq \lambda(44C_3+6C_4+K)\mu < \mu$.

Similarly, if it was A.2 instead of A.1, we would have $y, y+e_1 \in S_3(C_4, x_0)$ and so contracting these two points with t_0, would give $\rho(y+e_2) = d(y+e_2+e_1, y+ e_2) \leq d(y+e_1+e_2, y+2e_1)+\lambda d(y+e_1, t_0)+d(y+e_1, y+e_2)+\lambda d(y,t_0)+\lambda K\mu \leq \lambda(14C_3+15C_3+3C_4+8C_3+3C_4+K)\mu < \mu$.

Now consider diagrams C.2 and D.2. We have $y, y+e_3 \in S_3(C_4, x_0)$ so contracting these points with t_0 must be by 1 or 2, so we immediately get $\rho(y+e_1) \leq \lambda(44C_3+6C_4+K)\mu < \mu$.

Therefore, we can only have diagrams B.1, C.1, D.1 and the diagram symmetric to B.1, which we shall refer to as B.2. Suppose now that y with $\rho(y) \leq 7C_3\mu, d(y+e_1,y+e_2) \leq 7\lambda C_3\mu$ had diagram C.1 or D.1. Also, assume $\rho(y+e_3) \leq 7C_3\mu, d(y+e_3+e_1, y+e_3+e_2) \leq \lambda C_3\mu$, thus $y+e_3$ itself has one of the mentioned diagrams. Suppose that it had diagram B.1 or B.2. Without loss of generality, it was B.1, the other case is symmetric to this one.

Suppose y has diagram C.1. Then given any point z with $d(z,y) \leq 2\rho(y)$, suppose $d(y+e_1, z+e_1), d(y+e_2, z+e_2) > 5\lambda\rho(y)$. Then $z \overset{3}{\frown} y$ and so $y+e_1 \overset{2}{\frown} z$, $y+e_2 \overset{1}{\frown} z$. However, we can apply Proposition 3.24 to $(y; y+e_2, y+e_1, y+e_3; y+ 2e_3)$ with constant $42C_3$, to see that $\operatorname{diam} N(z) \leq 800\lambda C_3\mu$, so after contracting y, z we obtain $\rho(z) < 12C_3\mu$ and applying Proposition 3.23 gives the contradiction, provided $\lambda < 1/(32800C_1C_3)$. So whenever $d(z,y) \leq 2\rho(y)$, we must have $d(y+e_1, z+e_1) \leq 5\lambda\rho(y)$ or $d(y+e_2, z+e_2) \leq 5\lambda\rho(y)$. But contract z with $y+e_2$ in the former case and with $y+e_1$ in the latter to see that for some choice of distinct $i,j \in [3]$ we must have $d(z+e_i, y+e_1), d(z+e_j, y+e_1) \leq 20\lambda\rho(y)$, so $d(z+e_i, y), d(z+e_j, y) \leq 2\rho(y)$, thus we can repeat these arguments to points $z+e_i, z+e_j$. Doing so, we obtain a 2-way set of diameter at most $280\lambda C_3\mu$ by considering the distance from $y+e_1$, if the point z is dropped out. But, by Lemma 3.8, we get such a 2-way set in every 3-way set, which is a contradiction by Proposition 3.20, since $\lambda < 1/(840C_3)$. We argue similarly, if y has diagram D.1.

We conclude that if y is as described and has diagram C.1 or D.1, then $y+e_3$ also has diagram among these two. Now, start from a point y_0 with $d(y_0+e_1, y_0+e_2) \leq 3\lambda C_3\mu, \rho(y_0) \leq 3C_3\mu$ and diagram C.1 or D.1, provided such a point exists. Define the sequence $y_n = y_0 + ne_3$, for all $n \geq 0$. Our aim is to show that this is Cauchy. By induction on n we show that $\rho(y_n) \leq 7C_3\mu, d(y_n + e_1, y_{n+1}+e_1), d(y_n+e_2, y_{n+1}+e_2) \leq (n+3)\lambda^{n+1}C_3\mu, d(y_n+e_1, y_n+e_2) \leq 3C_3\lambda^{n+1}\mu$ and y_n has either diagram C.1 or diagram D.1, which is true for $n=0$.

Suppose the claim holds for all m not greater than some $n \geq 0$. By Proposition 3.24 applied to $(y_0; p_1, p_2, p_3; y_n)$ with constant $18C_3$ with suitable $\{p_1, p_2, p_3\} = N(y_0)$ we get $d(y_1, y_{n+1}) \leq 288\lambda C_3\mu$, so we infer that $\rho(y_{n+1}) \leq d(y_{n+1}, y_{n+1} + e_1) + d(y_{n+1}+e_1, y_{n+1}+e_2) \leq d(y_{n+1}, y_1) + d(y_1, y_0+e_2) + d(y_0+e_2, y_1+e_2) + d(y_1+e_2, y_2+e_2) + \cdots + d(y_n+e_2, y_{n+1}+e_2) \leq 7C_3\mu$ and $y_n + e_1 \overset{3}{\frown} y_n + e_2$ so $d(y_{n+1}+e_1, y_{n+1}+e_2) \leq 3\lambda^{n+2}C_3$ therefore, y_{n+1} must itself have diagram C.1 or D.1. If y_n and y_{n+1} have the same diagram, then we can see that $y_n+e_1 \overset{3}{\frown} y_{n+1}+e_2$ and $y_{n+1}+e_1 \overset{3}{\frown} y_n+e_2$, which is sufficient to establish the claim, as we obtain $d(y_{n+1}+e_1, y_{n+2}+e_1) \leq d(y_{n+1}+e_1, y_{n+2}+e_2) + d(y_{n+2}+e_2, y_{n+2}+e_1) \leq \lambda(d(y_n+e_1, y_{n+1}+e_1) + d(y_{n+1}+e_1, y_{n+1}+e_2)) + \lambda d(y_{n+1}+e_1, y_{n+1}+e_2) \leq \lambda d(y_n+e_1, y_{n+1}+e_2) + 6\lambda^{n+3}C_3\mu \leq (n+3)\lambda^{n+2}C_3\mu + \lambda^{n+2}C_3\mu \leq (n+4)\lambda^{n+2}C_3\mu$. Likewise, we get the bound on $d(y_{n+1}+e_2, y_{n+2}+e_2)$. If the diagrams are different, it must be the case that $y_n + e_1 \overset{3}{\frown} y_{n+1} + e_1$ and $y_n + e_2 \overset{3}{\frown} y_{n+1} + e_2$, once again proving the claim.

Hence, if y is a point such that $\rho(y) \leq 3C_3\mu, d(y+e_1, y+e_2) \leq 3\lambda C_3\mu$, then it can only have diagram B.1 or B.2. In the light of this, pick y_0 with $\rho(y_0) \leq C_3\mu, d(y_0+e_1, y_0+e_2) \leq \lambda C_3\mu$, whose existence is provided by Proposition 3.26, so it has diagram B.1, without loss of generality. Set $y_1 = y_0 + e_1$ and so have $\operatorname{diam}\{y_1, y_1+e_1, y_1+e_2\} \leq 3\lambda\rho(y_0)$ for the diagram for y_0. Also, by Proposition 3.24 applied to $(y_0; y_0+e_3, y_0+e_2, y_0+e_1; y_1)$ with constant $6C_3$ we get $\rho(y_1) \leq 3C_3\mu$, so y_1 has diagram B.1 or B.2. If it is B.1 define y_2 to be y_1+e_1, otherwise y_1+e_2. We similarly proceed to define a sequence $(y_k)_{k\geq 0}$. As long as y_k is defined and has one of these diagrams, define $y_{k+1} = y_k+e_1$ when y_k has diagram B.1, and set $y_{k+1} = y_k+e_2$ if it has diagram B.2. We now claim by induction on k that y_k is defined, $\rho(y_k) \leq 3C_3\mu$ and $\operatorname{diam}\{y_k, y_k+e_1, y_k+e_2\} \leq 3(3\lambda)^kC_3\mu$. This is clear for $k=0$.

Suppose the claim holds for some $k \geq 0$. Then we have that y_k has B.1 or B.2 for its diagram. Suppose it is the former, we argue in the same way for the other option. Firstly, y_{k+1} is defined. Then, from contractions implied by the diagram B.1, we get $\operatorname{diam}\{y_{k+1}, y_{k+1}+e_1, y_{k+1}+e_2\} \leq 3\lambda \operatorname{diam}\{y_k, y_k+e_1, y_k+e_2\}$. Finally, as $d(y_0, y_k) \leq (\rho(y_0) + \rho(y_k))/(1-\lambda) < 5C_3\mu$, we may apply Proposition 3.24 to $(y_0; y_0 + e_3, y_0 + e_2, y_0 + e_1; y_{k+1})$ with constant $6C_3$ to obtain $\rho(y_{k+1}) = d(y_{k+1}, y_{k+1}+e_3) \leq d(y_{k+1}, y_0) + d(y_0, y_0+e_3) + d(y_0+e_3, y_{k+1}+e_3) \leq d(y_{k+1}, y_k) + d(y_k, y_{k-1}) + \cdots + d(y_1, y_0) + \rho(y_0) + 96\lambda C_3\mu \leq 9\lambda C_3\mu/(1-3\lambda) + 2C_3\mu + 96\lambda C_3\mu \leq 3C_3\mu$, which proves the claim.

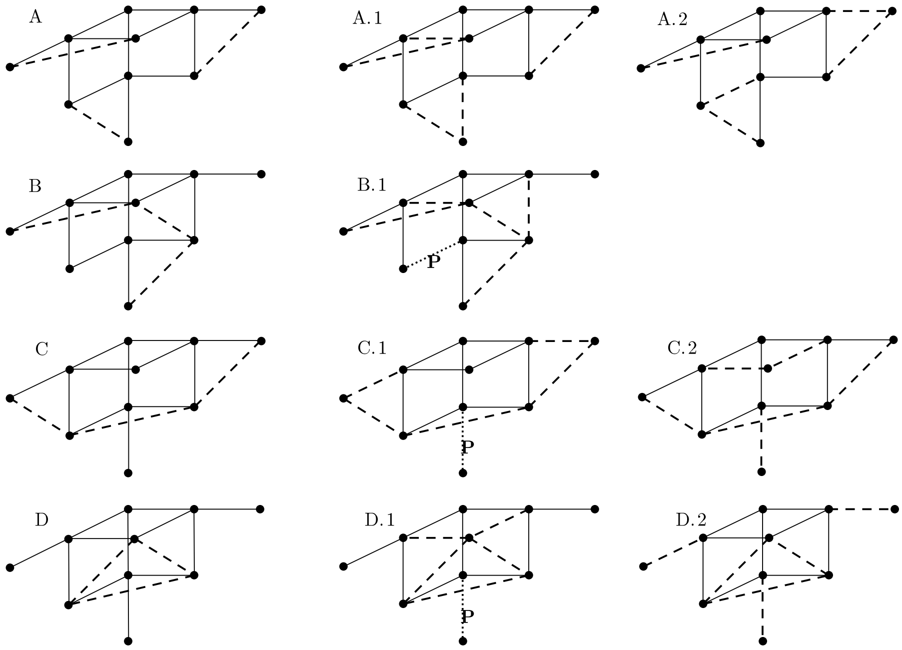
This brings us to the conclusion that $(y_k)_{k\geq 0}$ is a 1-way Cauchy sequence, providing us with a contradiction. □

Proof of Proposition 3.36. During the course of our argument, we shall prove a few auxiliary lemmas, the last one being Lemma 3.41, allowing us to conclude the proof. It suffices to prove the claim for $i = 3, j = 2, k = 1$. Suppose contrary, there is t_0 with $d(t_0 + e_1, t_0 + e_2) > 10\lambda C_5\mu$, $d(t_0, x_0) \leq 3C_5\mu$ and whenever $s \in C_3(C_5, x_0)$, we must have either $s \overset{1}{\frown} t_0$ or $s \overset{2}{\frown} t_0$.

Set $C_{5,1} = 100C_3$ and consider the points y with $\rho(y) \leq C_{5,1}\mu, d(y + e_1, y + e_2) \leq \lambda C_{5,1}\mu$. Note that such a point exists by Proposition 3.26. The possible diagrams of contractions are shown in Figure 3.9, and the arguments to justify these are provided in Section 3.8. These are precisely the same diagrams as in the previous proposition. Using $d(t_0 + e_1, t_0 + e_2) > 10\lambda C_5\mu$, we reject most of these.

B.1 Suppose that y as above has diagram B.1. First of all, as $\lambda < 1/(4920 C_1 C_{5,1})$, apply Proposition 3.24 to $(y; y + e_3, y + e_2, y + e_1; y)$ with constant $6C_{5,1}$ to see that in particular $y, y + e_1, y + e_2, y + e_3$ are all in $C_3(x_0, C_5)$, as $d(y, x_0) \leq (C_{5,1} + 2)\mu/(1-\lambda)$, $\rho(y) \leq C_{5,1}\mu$, $d(y, y + e_3) \leq C_{5,1}\mu, d(y + e_1, y + e_1 + e_3) \leq (2 + 96\lambda)C_{5,1}\mu, d(y + e_2, y + e_2 + e_3) \leq \lambda C_{5,1}\mu$ and $d(y + e_3, y + 2e_3) \leq (2 + 3\lambda)C_{5,1}\mu$.
If $t_0 \overset{1}{\frown} y$, then contract $t_0, y+e_3$ to get $\rho(y+e_1) < 6\lambda(C_{5,1}+C_5)\mu < \mu$ when $t_0 \overset{1}{\frown} y + e_3$ or $d(t_0+e_1, t_0+e_2) \leq d(t_0+e_1, y+e_1) + d(y+e_1, y+e_3+e_2) + d(y+e_3+e_2, t_0+e_2) \leq \lambda(3C_{5,1}+3C_5)\mu + 3\lambda C_{5,1}\mu + (3C_{5,1}+3C_5)\mu < 10\lambda C_5\mu$ otherwise, both of which are not allowed.

Figure 3.9: Possible diagrams of points p with $d(p+e_1, p+e_2) \leq \lambda C_{5,1}\mu$, $\rho(p) \leq C_{5,1}\mu$



C.1 Suppose that y as above has diagram C.1. Then $d(y, y+e_3) \leq C_{5,1}\mu, d(y+e_1, y+e_1+e_3), d(y+e_2, y+e_2+e_3) \leq 3\lambda C_{5,1}\mu, d(y+e_3, y+2e_3) \leq 96\lambda C_{5,1}\mu$. Also $d(y, x_0) \leq (C_{5,1}+2)\mu/(1-\lambda), \rho(y) \leq C_{5,1}\mu$, so $y, y+e_1, y+e_2, y+e_3 \in S_3(x_0, C_5)$. Without loss of generality $y \overset{1}{\frown} t_0$. But if $y + e_2 \overset{1}{\frown} t_0$, then $\rho(y+e_1) = d(y+e_1, y+e_1+e_2) \leq \lambda d(y, t_0) + \lambda d(y+e_2, t_0) \leq 6\lambda(C_{5,1} + C_5)\mu < \mu$. However, $y + e_2 \overset{2}{\frown} t_0$ is impossible as well, for that implies $d(t_0+e_1, t_0+e_2) \leq d(t_0+e_1, y+e_1) + d(y+e_1, y+2e_2) + d(y+2e_2, t_0+e_2) \leq 6\lambda(C_{5,1} + C_5)\mu + 7\lambda C_{5,1} < 10\lambda C_5\mu$.

C.2 Assume that y as above has diagram C.2. First of all apply Proposition 3.22 to y (we have $\lambda < 1/(78C_{5,1})$) to see that $d(y+e_1, y+e_1+e_3), d(y+e_2, y+e_2+e_3) \leq 9C_{5,1}\mu$. Also $d(y+e_3, y+2e_3) \leq \lambda C_{5,1}\mu, \rho(y) \leq C_{5,1}\mu, d(y, x_0) \leq (C_{5,1}+2)\mu/(1-\lambda)$, so $y, y+e_1, y+e_2, y+e_3 \in S_3(x_0, C_5)$. Without loss of generality $y \overset{1}{\frown} t_0$. If $y+e_1 \overset{1}{\frown} t_0$ then $\rho(y+e_1) \leq d(y+e_1, y+2e_1) + d(y+2e_1, y+e_1+e_2) \leq \lambda(d(y, t_0) + d(y+e_1, t_0)) + 2\lambda C_{5,1}\mu \leq 6\lambda(C_{5,1} + C_5)\mu + 2\lambda C_{5,1} < \mu$. So, we must have $y+e_1 \overset{2}{\frown} t_0$, but this also yields contradiction as $d(t_0+e_1,t_0+e_2) \leq d(t_0+e_1,y+e_1)+d(y+e_1,y+y_1+e_2)+d(y+e_1+e_2,t_0+e_2) \leq \lambda d(y,t_0)+\lambda C_{5,1}\mu+\lambda d(y+e_1,t_0) \leq 6\lambda(C_5+C_{5,1})\mu+\lambda C_{5,1}\mu < 10\lambda C_5\mu$.

D.1 Let y have diagram D.1. Then $d(y,y+e_3) \leq C_{5,1}\mu, d(y+e_1,y+e_1+e_3), d(y+e_2,y+e_2+e_3) \leq 3\lambda C_{5,1}\mu, d(y+e_3,y+2e_3) \leq 96\lambda C_{5,1}\mu$. Also $d(y,x_0) \leq (C_{5,1}+2)\mu/(1-\lambda), \rho(y) \leq C_{5,1}\mu$, so $y, y+e_1, y+e_2, y+e_3 \in S_3(x_0,C_5)$. Without loss of generality $y \overset{1}{\frown} t_0$. If $t_0 \overset{1}{\frown} y+e_1$, then $\rho(y+e_1) = d(y+e_1,y+2e_1) \leq d(y+e_1,t_0+e_1)+d(t_0+e_1,y+2e_1) \leq \lambda(d(y,t_0)+d(t_0,y+e_1)) \leq 6\lambda(C_5+C_{5,1}) < \mu$. On the other hand $t_0 \overset{2}{\frown} y+e_1$ implies $d(t_0+e_1,t_0+e_2) \leq d(t_0+e_1,y+e_1)+d(y+e_1,y+e_1+e_2)+d(y+e_1+e_2,t_0+e_2) \leq \lambda(6C_5+7C_{5,1})\mu < 10\lambda C_5\mu$. Thus, y cannot have diagram D.1.

D.2 Suppose that y as above has diagram D.2. First of all apply Proposition 3.22 to y to see that $d(y+e_1,y+e_1+e_3), d(y+e_2,y+e_2+e_3) \leq 9C_{5,1}\mu$. Also $d(y+e_3,y+2e_3) \leq \lambda C_{5,1}\mu, \rho(y) \leq C_{5,1}\mu, d(y,x_0) \leq (C_{5,1}+2)\mu/(1-\lambda)$, so $y, y+e_1, y+e_2, y+e_3 \in S_3(x_0,C_5)$. Without loss of generality $y \overset{1}{\frown} t_0$. Now contract $y+e_2, t_0$. If these are contracted by 1, then $\rho(y+e_1) \leq d(y+e_1,y+e_1+e_2)+d(y+e_1+e_2,y+e_1+e_3) \leq \lambda(6C_5+8C_{5,1})\mu < \mu$, which is a contradiction. Therefore $t_0 \overset{2}{\frown} y+e_2$, which gives $d(t_0+e_1,t_0+e_2) \leq d(t_0+e_1,y+e_1)+d(y+e_1,y+2e_2)+d(y+2e_2,t_0+e_2) \leq \lambda(6C_5+8C_{5,1})\mu < 10\lambda C_5\mu$.

Thus, we are only left with diagrams A.1 and A.2. Let A.1' and A.2' be the diagrams symmetric to these, obtained by swapping the roles of e_1 and e_2. Let y once again be the same point as before. We distinguish the possibilities for contractions with t_0.

A.1 If y has diagram A.1, then $y, y+e_1, y+e_3 \in S_3(x_0,C_5)$, and it is easy to see that t_0, y and $t_0, y+e_1$ are contracted in the same direction, while $t_0, y+e_3$ is contracted in the other. Similarly, we obtain the possible contractions with t_0 for diagram A.1'.

A.2 If y has diagram A.2, we have all the points in $\{y\} \cup N(y)$ being members of $S_3(x_0,C_5)$, and pairs t_0, y and $t_0, y+e_1$ must be contracted in the different directions (otherwise $\rho(y+e_2) < \mu$). Same holds for the pairs $y+e_1, t_0$ and

$y+e_3, t_0$. From this we see that $t_0 \overset{2}{\frown} y, t_0 \overset{2}{\frown} y+e_3, t_0 \overset{1}{\frown} y+e_1$. Analogously, we classify the contractions for A.2'.

Lemma 3.38. *Let $K \leq C_{5,1}$. There is no sequence $(y_k)_{k\in I}$ for suitable index set $I \subset \mathbb{N}_0$, with the following properties:*

1. *y_0 is defined, has $\rho(y_0) \leq K/(2+6\lambda), d(y_0+e_1, y_0+e_2) \leq \lambda K/(2+\lambda)\mu$,*
2. *If y_k is defined, and satisfies $\rho(y_k) \leq K\mu, d(y_0+e_1, y_0+e_2) \leq \lambda K\mu$, then y_k has diagram A.1 or A.1', and we define $y_{k+1} = y_k + e_i$, with $i = 1$ when diagram of y_k is A.1 and $i = 2$ otherwise.*

Proof of Lemma 3.38. By induction on k, we claim that y_k is defined and $\operatorname{diam}\{y_k, y_k+e_1, y_k+e_2\} \leq (3\lambda)^k K\mu/(2+6\lambda)$. This trivially holds for $k = 0$. Also, without loss of generality y_0 has diagram A.1.

Suppose that the claim holds for all k' not greater than k, where $k \geq 0$. Observe that $d(y_0, y_k) \leq d(y_0, y_1) + d(y_1, y_2) + \dots d(y_{k-1}, y_k) \leq (1 + 3\lambda + \dots + (3\lambda)^{k-1})K\mu/(2+6\lambda) < \frac{1}{(1-3\lambda)(2+6\lambda)}K\mu$. Now, contract y_0+e_3, y_k. It is contracted neither by 1 nor by 2, since we either get $\rho(y_0+e_1) < \mu$ or $\rho(y_0+e_2) < \mu$. Hence $y_k \overset{3}{\frown} y_0 + e_3$, so $d(y_k+e_3, y_0+e_3) \leq d(y_k+e_3, y_0+2e_3) + d(y_0+2e_3, y_0+e_3) \leq \frac{\lambda(3-6\lambda)}{(1-3\lambda)(2+6\lambda)}K\mu < 2\lambda K\mu$. Finally, we establish $\rho(y_k) \leq (2+6\lambda)K\mu/(2+6\lambda) = K\mu$, which combined with $d(y_k+e_1, y_k+e_2) \leq \lambda K\mu$ gives that y_k itself has diagram A.1 or A.1'. Hence y_{k+1} is defined, and $\operatorname{diam}\{y_{k+1}, y_{k+1}+e_1, y_{k+1}+e_2\} \leq 3\lambda \operatorname{diam}\{y_k, y_k+e_1, y_k+e_2\}$, as desired.

However, this shows that $(y_k)_{k\geq 0}$ is a 1-way Cauchy sequence, which is not allowed. Therefore, we reach a contradiction, and the end of the proof. $\square$

Corollary 3.39. *There exists a point y with $\rho(y) \leq 3C_3\mu, d(y+e_1, y+e_2) \leq 3\lambda C_3\mu$ with diagram A.2 or A.2'.*

Proof of Corollary 3.39. Suppose contrary, and let y_0 be a point with $\rho(y_0) \leq C_3\mu, d(y_0+e_1, y_0+e_2) \leq \lambda C_3\mu$, given by Proposition 3.26. We shall now define a sequence (y_k) inductively, as long as we can. The starting point y_0 is as above. Given y_k, provided it satisfies $\rho(y_k) \leq 3C_3\mu, d(y_k+e_1, y_k+e_2) \leq 3\lambda C_3\mu$, define y_{k+1} to be $y_k + e_1$ when y_k has diagram A.1 and $y_k + e_2$ if y_k has diagram A.1', (note that by assumption these two are the only permitted diagrams). But this gives a contradiction by Lemma 3.38 with $K = 3C_3$. $\square$

Corollary 3.40. *We have $d(t_0+e_1, t_0+e_2) > 5C_3\mu$.*

Proof of Corollary 3.40. Suppose contrary. In order to reach a contradiction, we shall obtain a Cauchy sequence as in the previous proof. Consider a point y with $\rho(y) \leq 36C_3\mu, d(y+e_1, y+e_2) \leq 36\lambda C_3\mu$. Assume that this point has diagram A.2. Recall that we have $t_0 \overset{1}{\frown} y+e_1, t_0 \overset{2}{\frown} y$. This gives $\rho(y+e_1) \leq C_{5,1}\mu$ and from contractions of $\{y\} \cup N(y)$ we get that $d(y+e_1+e_1, y+e_1+e_2) \leq \lambda C_{5,1}\mu$ holds as well, so $y+e_1$ has one of the four diagrams considered so far. However, we immediately see that it is not possible for $y+e_1$ to have diagram A.2, for $t_0 \overset{1}{\frown} y+e_1$.

Suppose that $y+e_1$ had diagram A.2'. Firstly, suppose that $y+e_1 \overset{3}{\frown} y+e_2+e_3$. Then contract $y, y+2e_3$. If it is by 3, we have $\rho(y+2e_3) < \mu$, otherwise we obtain $\rho(y+e_3) < \mu$. Hence $y+e_1 \overset{2}{\frown} y+e_2+e_3$. This further implies $y+e_1 \overset{2}{\frown} y+2e_2$ (or otherwise $\rho(y+2e_1) < \mu$). However $y+2e_2 \in S_3(x_0, C_5)$, so contract $y+e_2, t_0$ to get a contradiction.

Suppose now that y has diagram A.1 and $\rho(y) \leq 17C_3\mu, d(y+e_1, y+e_2) \leq 17\lambda C_3\mu$. If $y+e_1$ has diagram A.2, then $y+e_1 \overset{2}{\frown} t_0, y+e_1+e_3 \overset{2}{\frown} t_0, y+2e_1 \overset{1}{\frown} t_0$. But y has diagram A.1, so t_0 contracts with $y+e_1, y$ in the same direction, thus in e_2, and $t_0, y+e_3$ in the other, i.e. e_1. However, then $\operatorname{diam} N_1(x+2e_1) < 10\lambda C_5\mu$, which is in contradiction with Proposition 3.23 used with constant $10C_5$ after contracting $y, y+2e_1$.

Assume that $y+e_1$ has diagram A.2'. Thus $t_0 \overset{1}{\frown} y+e_1, t_0 \overset{1}{\frown} y+e_1+e_3$ and $t_0 \overset{2}{\frown} y+e_1+e_2$. As y has diagram A.1, we have $t_0 \overset{1}{\frown} y$ and $t_0 \overset{2}{\frown} y+e_3$. But, as $d(t_0+e_1, t_0+e_2) \leq 5C_3\mu$, we have $y+e_1+e_2$ $100C_3$-good, so by the previous discussion $y+e_1+e_2$ can only have diagram A.1 or A.1' (as $y+e_1$ is $36C_3$-good). If $y+e_1+e_2$ has diagram A.1 then $t_0 \overset{1}{\frown} y+e_1+e_2+e_3$, so $\rho(y+e_1) < \mu$, so we may assume $y+e_1+e_2$ has diagram A.1', which implies $t_0 \overset{1}{\frown} y+e_1+e_2+e_3$. Look at pairs $y+2e_1, y+2e_1+e_3$ and $y+2e_1+e_2, y+2e_1+e_3$, both have length at most $6C_3\mu$, so cannot be contracted by 2, as otherwise $d(t_0+e_1, t_0+e_2) < 10C_5\mu$. Suppose that at least one of these pairs is contracted by 1. Then apply Proposition 3.24 to $(y; y+3e_1, y+2e_1, y+e_1; y+e_2)$ with constant $10C_5$ (since $\lambda < 1/(8200C_1C_5)$), to see that $\rho(y+3e_3) < \mu$. Hence, the two considered pairs are contracted by 3. But, contract $y+e_2, y+2e_1+e_3$ to get $\rho(y+2e_1+e_3) < \mu$ or $d(t_0+e_1, t_0+e_2) < 200\lambda C_5\mu$ giving $\rho(y+e_2) < \mu$.

Now, start from y_0' with $\rho(y_0') \leq C_3\mu, d(y_0' + e_1, y_0' + e_2) \leq \lambda C_3\mu$, given by Proposition 3.26. If y_0' has diagram A.1 or A.1' set $y_0 = y_0'$, otherwise set $y_0 = y_0' + e_1$ if the diagram is A.2, and $y_0 = y_0' + e_2$ if the diagram is A.2'. Hence, y_0 satisfies $\rho(y_0) \leq 6C_3\mu, d(y_0 + e_1, y_0 + e_2) \leq 6\lambda C_3\mu$, and defining a sequence as in Lemma 3.38, gives a contradiction for $K = 17C_3$ by the discussion above. $\square$

Lemma 3.41. *Suppose that y_1, y_2 are two points with $\rho(y_1), \rho(y_2) \leq C_3\mu$. Then $d(y_1 + e_3, y_2 + e_3) \leq 40\lambda C_3\mu$.*

Proof of Lemma 3.41. Recall that we have a point y_0 with $\rho(y_0) \leq 6C_3\mu, d(y_0 + e_1, y_0 + e_2) \leq 6\lambda C_3\mu$, with diagram A.2 or A.2', given by Corollary 3.39. Without loss of generality it is A.2.

Let z be any point with $\rho(z) \leq C_3\mu$. We shall prove $d(y_0 + e_3, z + e_3) \leq 20\lambda C_3\mu$, which is clearly sufficient. Note that we have $d(z, x_0) \leq (C_3 + 2)\mu/(1 - \lambda) \leq C_5\mu, d(z, t_0) \leq d(z, x_0) + d(x_0, t_0) \leq (C_3 + 2)\mu/(1 - \lambda) + 3C_5\mu \leq 4C_5\mu$, and similarly $d(y_0, z) \leq 4C_5\mu$ and $y_0, z \in S_3(x_0, C_5)$.

Assume $t_0 \overset{1}{\frown} z$. Recall that $t_0 \overset{2}{\frown} y_0$. If $y_0 \overset{1}{\frown} z$, then $d(t_0 + e_1, t_0 + e_2) \leq d(t_0 + e_1, z + e_1) + d(z + e_1, y_0 + e_1) + d(y_0 + e_1, y_0 + e_2) + d(y_0 + e_2, t_0 + e_2) \leq \lambda 4C_5\mu + \lambda 7C_3/(1 - \lambda) + 6\lambda C_3\mu + 4\lambda C_5\mu < 5C_3\mu < d(t_0 + e_1, t_0 + e_2)$, which is a contradiction. Similarly we discard the case $y_0 \overset{2}{\frown} z$, as then $d(t_0 + e_1, t_0 + e_2) \leq d(t_0 + e_1, z + e_1) + d(z + e_1, z + e_2) + d(z + e_2, y_0 + e_2) + d(y_0 + e_2, t_0 + e_2) \leq 5C_3\mu$. Therefore, $y_0 \overset{3}{\frown} z$, so $d(y_0 + e_3, z + e_3) \leq \lambda 7C_3\mu/(1 - \lambda) < 8\lambda C_3\mu$.

Thus, we must have $z \overset{2}{\frown} t_0$. But we cannot have neither $y_0 + e_1 \overset{1}{\frown} z$ nor $y_0 + e_1 \overset{2}{\frown} z$, for otherwise we obtain $d(t_0 + e_1, t_0 + e_2) \leq d(t_0 + e_1, y_0 + 2e_1) + d(y_0 + 2e_1, z + e_2) + d(z + e_2, t_0 + e_2) \leq \lambda d(t_0, y_0 + e_1) + d(y_0 + 2e_1, y_0 + e_1 + e_2) + \lambda d(y + e_1, z) + 2\rho(z) + \lambda d(z, t_0) \leq 5C_3\mu$. Hence, we get $y_0 + e_1 \overset{3}{\frown} z$, so $d(y_0 + e_3, z + e_3) \leq \lambda d(y_0 + e_1, z) + d(y_0 + e_1 + e_3, y_0 + e_3) \leq 14\lambda C_3\mu + 6\lambda C_3\mu = 20\lambda C_3\mu$, as desired. $\square$

We are now ready to establish the final contradiction. By Proposition 3.26, we have points x_1, x_2, x_3 with whenever $\{i, j, k\} = [3]$, we have $\rho(x_i) \leq C_3\mu, d(x_i + e_j, x_i + e_k) \leq \lambda C_3\mu$. First of all, x_1, x_2, x_3 all belong to $S_3(x_0, C_5)$, since $d(x_0, x_i) \leq (C_3 + 2)\mu/(1 - \lambda)$. Suppose that for some i, j we have $t_0 \overset{1}{\frown} x_i$ and $t_0 \overset{2}{\frown} x_j$. Then, by the triangle inequality and FNI, $d(t_0 + e_1, t_0 + e_2) \leq d(t_0 + e_1, x_i + e_1) + d(x_i + e_1, x_i) + d(x_i, x_j) + d(x_j, x_j + e_2) + d(x_j + e_2, t_0 + e_2) \leq$

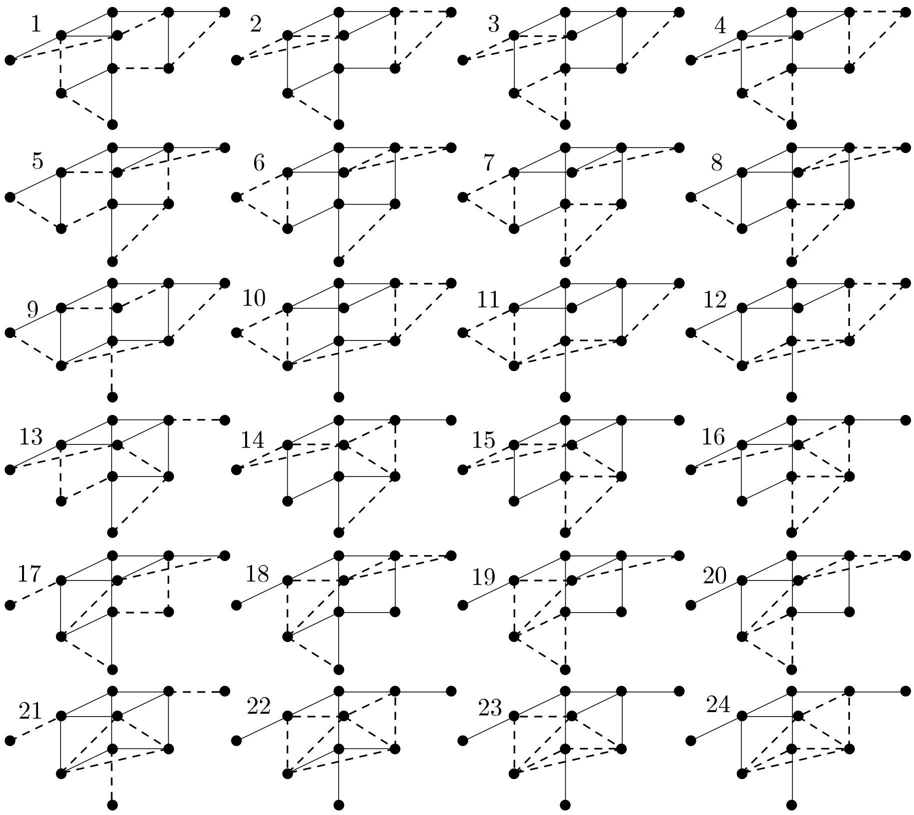


Figure 3.10: All possible contraction diagrams

$\lambda(d(t_0, x_0) + d(x_0, x_i)) + \rho(x_i) + (\rho(x_i) + \rho(x_j))/(1-\lambda) + \rho(x_j) + \lambda(d(x_j, x_0) + d(x_0, t_0)) \leq \lambda(3C_5\mu + (\rho(x_0) + \rho(x_i))/(1-\lambda)) + C_3\mu + 2C_3\mu/(1-\lambda) + C_3\mu + \lambda((\rho(x_j) + \rho(x_0))/(1-\lambda) + 3C_5\mu) \leq 5C_3\mu$, which is not possible, hence t_0 contracts with x_1, x_2, x_3 in the same direction, e_1 without loss of generality. But also Lemma 3.41 gives $\operatorname{diam}\{x_1 + e_3, x_2 + e_3, x_3 + e_3\} \leq 40\lambda C_3\mu$, and $\operatorname{diam}\{x_1 + e_1, x_2 + e_1, x_3 + e_1\} \leq 8\lambda C_5\mu$ so $\operatorname{diam} N(x_1) \leq 9\lambda C_5\mu$, which is a contradiction due to Proposition 3.23. □

Combine Corollary 3.34 with Propositions 3.35 and 3.36 to obtain a contradiction. □

3.8 Discussion of the Possible Contraction Diagrams

In this section we discuss the possible diagrams for contractions in the later part of the proof of Proposition 3.3. In this discussion we assume that the propositions preceding Proposition 3.25 all hold.

Let us start with a point x with $\rho(x) \leq K\mu$, for some $K \geq 1$. Consider first the contractions of the long edges, that is those of the form $x+e_i, x+e_j$, where i, j are distinct elements of $[3]$. If two such edges are contracted in the same direction, say k, then $\operatorname{diam} N(x+e_k) \leq 4\lambda K\mu$. Furthermore, we can contract $x, x+e_k$, to get $\rho(x_k) \leq (2+5\lambda)K\mu$, which is a contradiction due to Proposition 3.23, provided $\lambda < 1/(164C_1K)$, which we shall assume is the case. Thus, all three long edges must be contracted in different directions.

Contract now the short edges, i.e. those edges of the form $x, x+e_i$, for some $i \in [3]$. Given such an edge, there is a unique long edge $x+e_j, x+e_k$, such that $\{i,j,k\} = [3]$. We say that these edges are *orthogonal*. Suppose that a short edge $x+e_i$ is not contracted in the same direction as its orthogonal long edge. Then $x+e_i$ must be contracted in the same direction e_l as $x+e_i, x+e_j$, for some $j \neq i$. Let k be such that $\{i,j,k\} = [3]$. Then $x+e_k$ cannot be contracted in the same direction as $x+e_i$, as otherwise $\rho(x+e_l) \leq 3\lambda K\mu < \mu$, which is impossible. So, $x+e_k$ is contracted in the same direction as one of its nonorthogonal long edges. Hence $\operatorname{diam}\{x+e_l, x+e_l+e_i, x+e_l+e_j\}, \operatorname{diam}\{x+e_m, x+e_m+e_k, x+e_m+e_n\} \leq 3\lambda\rho(x)$ holds for some $m, n \in [3]$ where $m \neq l$ and $n \neq k$. From this we can conclude that contractions in $\{x\} \cup N(x)$ can only give the diagrams shown in Figure 3.8. There, an edge shown as dashed line implies that its length is at most $3\lambda\rho(x)$.

3.8.1 Diagrams in the proof of Proposition 3.26

As in the proof of Proposition 3.26 we consider a point y with $d(y+e_1, y+e_3) \leq \lambda C_{3,1}\mu$ and $\rho(y) \leq C_{3,1}\mu$, i.e. we set previously considered K to be $C_{3,1}$ instead, and so assume $\lambda < 1/(164C_1C_{3,1})$. Consider the possible diagrams of contractions of edges in $\{y\} \cup N(y)$. Recall that our assumption is that there is no point x with $\rho(x) \leq C_3\mu$ and $d(x+e_1, x+e_2) \leq \lambda C_3\mu$. We now describe how to reject all diagrams except 2, 4, 6, 11, 15 and 23.

1 Immediately we get $\rho(y + e_3) \leq 4\lambda C_{3,1}\mu < \mu$.

3 We have $\rho(y + e_1) \leq 4\lambda C_{3,1}\mu < \mu$.

5 Similarly to previous ones $\rho(y + e_1) \leq 7\lambda C_{3,1}\mu$.

7 We get $\rho(y + e_3) \leq 4\lambda C_{3,1}\mu < \mu$.

8 Have $\rho(y + e_2) \leq (2 + 3\lambda)C_{3,1}\mu, d(y + e_2 + e_1, y + e_2 + e_2) \leq 3\lambda C_{3,1}$, but we assume that there are no such points.

9 Diameter of $N(y)$ is at most $7\lambda C_{3,1}\mu$ and $\rho(y) \leq C_{3,1}\mu$ so apply Proposition 3.23, provided $\lambda < 1/(287C_1C_{3,1})$.

10 Diameter of $N(y)$ is at most $10\lambda C_{3,1}\mu$ and $\rho(y) \leq C_{3,1}\mu$ so apply Proposition 3.23, provided $\lambda < 1/(410C_1C_{3,1})$.

12 We apply Proposition 3.24 to $(y; y + e_2, y + e_1, y + e_3; y)$ with constant $9C_{3,1}$, so $\rho(y + e_2) \leq 144\lambda C_{3,1}\mu < \mu$, as long as $\lambda < 1/(7380C_1C_{3,1})$.

13 Use Proposition 3.22 to get $\rho(y + e_1) \leq (11 + 9\lambda)C_{3,1}\mu$ and $d(y + e_1 + e_1, y + e_1 + e_2) \leq 3\lambda C_{3,1}\mu$, as $\lambda < 1/(936C_{3,1})$. This is a contradiction as $C_3 > 12C_{3,1}$.

14 Apply Proposition 3.24 to $(y; y + e_3, y + e_2, y + e_1; y)$ with constant $9C_{3,1}$ to get $\rho(y + e_2) \leq 144\lambda C_{3,1}\mu$. Here we need $\lambda < 1/(7380C_1C_{3,1})$.

16 As 14.

17 As for 13, get $\rho(y + e_2) \leq (11 + 9\lambda)C_{3,1}\mu$ and $d(y + e_2 + e_1, y + e_2 + e_2) \leq 3\lambda C_{3,1}\mu$.

18 Apply Proposition 3.24 to $(y; y + e_1, y + e_3, y + e_2; y)$ with constant $9C_{3,1}$ to get $\rho(y + e_2) \leq 144\lambda C_{3,1}\mu < \mu$.

19 Apply Proposition 3.24 to $(y; y + e_1, y + e_3, y + e_2; y + e_3)$ with constant $9C_{3,1}$ to get $\rho(y+e_2) \leq (2+6\lambda)C_{3,1}\mu, d(y+e_2+e_1, y+e_2+e_2) \leq 3\lambda C_{3,1}\mu$.

20 As 18.

21 Use Proposition 3.22 to get $\rho(y+e_3) \leq (9+3\lambda)C_{3,1}\mu$ and $d(y+e_3+e_1, y+e_3+e_2) \leq 3\lambda C_{3,1}\mu$, as $\lambda < 1/(78C_{3,1})$.

22 Have $\operatorname{diam} N(y) \leq 7\lambda K\mu$ which is in contradiction with Proposition 3.23, when $\lambda < 1/(287C_1C_{3,1})$.

24 Apply Proposition 3.24 to $(y; y+e_1, y+e_2, y+e_3; y+e_2)$ with constant $6C_{3,1}$ to get $\rho(y+e_2) \leq 96\lambda C_{3,1}\mu$.

Therefore, we obtain that for the y given above, provided $\lambda < 1/(7380C_1C_{3,1})$, we can only have diagrams 2, 4, 6, 11, 15 and 23. However, in all of these diagrams we can classify contractions more precisely.

2 Observe that we cannot have $y+e_1 \overset{2}{\frown} y$ or $y+e_1 \overset{3}{\frown} y$ as the first one of these gives $\rho(y+e_2) \leq 10\lambda C_{3,1}\mu < \mu$, while the latter implies $\rho(y+e_1) \leq 10C_{3,1}\mu < \mu$. Hence $y+e_1 \overset{1}{\frown} y$. Similarly, we must have $y \overset{2}{\frown} y+e_3$, otherwise we get a point p with $\rho(p) \leq 10\lambda C_{3,1}\mu < \mu$.

4 As in 2, if we do not have $y \overset{3}{\frown} y+e_1$ and $y \overset{2}{\frown} y+e_2$, we obtain a point p with $\rho(p) \leq 10\lambda C_{3,1}\mu < \mu$.

6 As in 2, if we do not have $y \overset{2}{\frown} y+e_2$ and $y \overset{1}{\frown} y+e_3$, we obtain a point p with $\rho(p) \leq 10\lambda C_{3,1}\mu < \mu$.

11 If $y \overset{3}{\frown} y+e_3$, then $\rho(y+e_3) \leq 10\lambda C_{3,1}\mu < \mu$. On the other hand, if $y \overset{2}{\frown} y+e_3$, then $\operatorname{diam} N(y) \leq 8\lambda C_{3,1}\mu$ and $\rho(y) \leq C_{3,1}\mu$ which is impossible by Proposition 3.23, if $\lambda < 1/(328C_1C_{3,1})$. Thus, $y \overset{1}{\frown} y+e_3$, and in the same fashion $y \overset{3}{\frown} y+e_2$. Furthermore, apply Proposition 3.24 to $(y; y+e_2, y+e_1, y+e_3; y)$ with constant $6\rho(y)/\mu$ to get $d(y+e_2, y+e_1+e_2) \leq 96\lambda\rho(y)$.

15 As in 11, we obtain $y \overset{1}{\frown} y+e_1$ and $y \overset{3}{\frown} y+e_3$. Apply Proposition 3.24 to $(y; y+e_3, y+e_2, y+e_1; y)$ with constant $6\rho(y)/\mu$ to get $d(y+e_2, y+2e_2) \leq 96\lambda\rho(y)$.

23 As in 11, we obtain $y \overset{3}{\frown} y+e_1$ and $y \overset{1}{\frown} y+e_3$. Apply Proposition 3.24 to $(y; y+e_1, y+e_2, y+e_3; y)$ with constant $6\rho(y)/\mu$ to get $d(y+e_2, y+2e_2) \leq 96\lambda\rho(y)$.

3.9 Concluding Remarks

We now return to the (refuted) conjecture of Stein which stated that every contractive family had a common fixed point. Recall that Austin showed that the conjecture fails in general, but that it holds for families consisting of two commuting functions. Let us recollect once again the main results of this part of the thesis. These are Theorems 1.3 and 1.7, both extending Austin's results, and having rather contrasting conclusions.

Firstly, Theorem 1.3 tells us that, even with a strong topological restriction imposed on the underlying metric space X, we may still find a contractive family of two functions such that no composition has a fixed point. Therefore, trying to find a strengthening of Stein's conjecture that involves a topological condition on X is likely doomed to failure. On the other hand, Theorem 1.7 tells us that λ-contractive families of three commuting functions have a common fixed point (when λ is small enough). Recall also the remarkable Generalized Banach's Contraction theorem (Theorem 1.5), which states that contractive families of the form $\{f, f^2, \ldots, f^n\}$ always have a common fixed point. These two theorems give evidence that Austin's conjecture, stating that commuting contractive families necessarily have a common fixed point, should be true. In fact, an algebraic condition on functions in the considered family like the one in Austin's conjecture naturally defines the geometry of our problem. Namely, if the family is $\mathcal{F} = \{f_1, \ldots, f_n\}$ and we pick arbitrary point $x_0 \in X$ and consider compositions of length k applied to x_0, i.e. the set

$$S_k = \Big\{ f_{i_1} \circ f_{i_2} \circ \ldots \circ f_{i_k}(x_0) \colon i_1, i_2, \ldots, i_k \in [n] \Big\},$$

then the size of S_k is directly related to the algebraic properties of $\mathcal{F}$. In particular, if the family is commuting, then $|S_k| \leq n^k$, while in the general case, when there are no additional assumptions on $\mathcal{F}$, it may well be the case that $|S_k| \geq \exp(\Omega(k))$. In other words, S_k grows polynomially when $\mathcal{F}$ is commuting, rather than exponentially, and this should be very helpful for finding fixed points.

The rest of this section is devoted to the analysis of some aspects of the proof of Theorem 1.7 and we conclude the chapter with some questions and conjectures.

Recall that the starting point of our proof was to change our viewpoint by moving from the original space X with a λ-contractive family to a pseudometric space $(\mathbb{N}_0^3, d)$, with the property that for any $a, b \in \mathbb{N}_0^3$ there is some $i \in [3]$ such that $d(a + e_i, b + e_i) \leq \lambda d(a, b)$. Motivated by Austin's conjecture, we formulate the following one.

Conjecture 3.42. *Let n be a positive integer and λ a real with $0 \leq \lambda < 1$. Suppose that $(\mathbb{N}_0^n, d)$ is an n-*dimensional λ-contractive grid*, i.e. a pseudometric space with the property that given $x, y \in \mathbb{N}_0^n$ we have some $i \in [n]$ with $d(x + e_i, y + e_i) \leq \lambda d(x, y)$. Then there is a 1-way Cauchy sequence $(x_m)_{m \geq 1}$, i.e. $(x_m)_{m \geq 1}$ is Cauchy and $x_{m+1} - x_m \in \{e_1, e_2, \ldots, e_n\}$ holds for all m.*

Recall $\mu = \inf \rho(x)$, where x ranges over all points in the grid and set $\mu_\infty = \lim_{k\to\infty} \inf_{x \in A_k} \rho(x)$, where A_k is the n-way set generated by $(k, k, \ldots, k)$. We say that a pseudometric space is a *contractive grid* if it is n-dimensional λ-contractive grid, for some $0 \leq \lambda < 1$ and a positive integer n. Remember that μ plays a very important role in our proof, since $\mu = 0$ immediately gives rise to a 1-way Cauchy sequence (this is the content of Proposition 3.10).

Question 3.43. *Can $\mu > 0$ occur in a contractive grid?*

Question 3.44. *Can $\mu_\infty = \infty$ occur in a contractive grid?*

Even though Theorem 1.7 looks like an analytical statement, our proof is of a combinatorial nature, with the flavour of Ramsey theory. We remark that the proof of Generalized Banach Theorem (Theorem 1.5) in fact rests on Ramsey's Theorem. We suspect that the complete proof of Conjecture 3.42 should be based on a similar approach.

It might be interesting to examine some arguments used in the proof of Theorem 1.7 further, and we pose the following questions and conjectures. First, recall Proposition 3.11 and Corollary 3.18. The former states that a bounded 3-way set contains a bounded 2-way set of considerably smaller diameter, while the latter tells us that a 2-way set of small diameter induces a 3-way set of diameter which is not much larger.

Question 3.45. *Does an n-way set of bounded diameter necessarily contain an $n-1$-way set of much smaller diameter? In general, what is the relationship between the k-way sets and the $k+1$-way sets in higher dimensional grids?*

Finally, recall that Lemma 3.15 about colourings of edges of K_n in three colours played an important role in the proof. We conjecture the following generalization to be true.

Conjecture 3.46. *For each $k \geq 2$ there is a positive constant C_k with the following property. Given a k-colouring of the edges of K_n, we can find sets of vertices $A_1, A_2, \ldots, A_{k-1}$ which cover the vertex set, and colours $c_1, c_2, \ldots, c_{k-1} \in [k]$, such that $\operatorname{diam}_{c_i} G[A_i] \leq C_k$ holds for all $i \in [k-1]$.*

Part II

Graph Theory

4 Covering Complete Graphs by Monochromatically Bounded Sets

4.1 Introduction

Given a graph G, whose edges are coloured with a colouring $\chi\colon E(G) \to C$ (where adjacent edges are allowed to use the same colour), given a set of vertices A, and a colour $c \in C$, we write $G[A, c]$ for the subgraph induced by A and the colour c, namely the graph on the vertex set A and the edges $\{xy\colon x, y \in A, \chi(xy) = c\}$. In particular, when $A = V(G)$, we write $G[c]$ instead of $G[V(G), c]$. Finally, we also use the usual notion of the induced subgraph $G[A]$ which is the graph on the vertex set A with edges $\{xy\colon x, y \in A, xy \in E(G)\}$. We usually write $[n] = \{1, 2, \ldots, n\}$ for the vertex set of K_n.

Our starting point is the following conjecture of Gyárfás.

Conjecture 4.1 (Gyárfás [23], [25]). *Let k be fixed. Given any colouring of the edges of K_n in k colours, we can find sets $A_1, A_2, \ldots, A_{k-1}$ whose union is $[n]$, and colours $c_1, c_2, \ldots, c_{k-1}$ such that $K_n[A_i, c_i]$ is connected for each $i \in [k-1]$.*

This is an important special case of the well-known Lovász-Ryser conjecture, which we now state.

Conjecture 4.2 (Lovász-Ryser conjecture [33], [27]). *Let G be a graph, whose maximum independent set has size $\alpha(G)$. Then, whenever $E(G)$ is k-coloured, we can cover G by at most $(k-1)\alpha(G)$ monochromatic components.*

Conjectures 4.1 and 4.2 have attracted a great deal of attention. When it comes to the Lovász-Ryser conjecture, we should note the result of Aharoni ([1]), who proved the case of $k = 3$. For $k \geq 4$, the conjecture is still open. The special case of complete graphs was proved by Gyárfás ([24]) for $k \leq 4$, and by Tuza ([52]) for $k = 5$. For $k > 5$, the conjecture is open.

Let us also mention some results similar in the spirit to Conjecture 4.6. In [46], inspired by questions of Gyárfás ([23]), Ruszinkó showed that every k-colouring of edges of K_n has a monochromatic component of order at least $n/(k-1)$ and of diameter at most 5. This was improved by Letzter ([32]), who showed that in fact there are monochromatic triple stars of order at least $n/(k-1)$. For more results and questions along these lines, we refer the reader to surveys of Gyárfás ([23], [25]).

In a completely different direction, relating to contraction mappings on metric spaces, we recall Theorem 1.7, that was proved in Chapter 3. (We mention in passing that this chapter is self-contained, and in particular no knowledge of chapter 3 is assumed.)

Theorem 4.3 (Theorem 1.7)**.** *Let (X, d) be a complete metric space and let $\{f_1, f_2, f_3\}$ be a commuting λ-contractive family of operators on X, for a given $\lambda \in (0, 10^{-23})$. Then f_1, f_2, f_3 have a common fixed point.*

Some of the ingredients in the proof of Theorem 1.7 were the following simple lemmas. Note that Lemma 4.4 is in fact a classical observation due to Erdős and Rado.

Lemma 4.4. *Suppose that the edges of K_n are coloured in two colours. Then we may find a colour c such that $K_n[c]$ is connected and of diameter at most 3.*

Lemma 4.5. *Suppose that the edges of K_n are coloured in three colours. Then we may find colours c_1, c_2, (not necessarily distinct), and sets A_1, A_2 such that $A_1 \cup A_2 = [n]$, with $K_n[A_1, c_1], K_n[A_2, c_2]$ are each connected and of diameter at most 8.*

Recall also that a common generalization of these statements and a strengthening of Conjecture 4.1 was conjectured in Section 3.9.

Conjecture 4.6 (Conjecture 3.46)**.** *For every k, there is an absolute constant C_k such that the following holds. Given any colouring of the edges of K_n in k colours, we can find sets $A_1, A_2, \ldots, A_{k-1}$ whose union is $[n]$, and colours*

$c_1, c_2, \ldots, c_{k-1}$ *such that* $K_n[A_i, c_i]$ *is connected and of diameter at most* C_k*, for each* $i \in [k-1]$.

The main result of this chapter is

Theorem 4.7. *Conjecture 4.6 holds for 4 colours, and one may take* $C_4 = 160$.

4.1.1 An outline of the proof

We begin the proof by establishing the weaker Conjecture 4.1 for the case of 4 colours. Although this was proved by Gyárfás in [24], the reasons for giving a proof here are twofold. Firstly, we actually give a different reformulation of Conjecture 4.1 that has a more geometric flavour. The proof given here and the reformulation we consider emphasize the importance of the graph G_k, defined as the tensor product[1] of k copies of K_n, to Conjecture 4.1. Another reason for giving this proof is to make the chapter self-contained.

We also need some auxiliary results about colourings with 2 or 3 colours, like Lemmas 4.4 and 4.5 mentioned above. In particular, we generalize the case of 2 colours to complete multipartite graphs. Another auxiliary result we use is the fact that G_k essentially cannot have large very sparse graphs.

The main tool in our proof is the notion of c_3, c_4*-layer mappings*, where c_3, c_4 are two colours. For $P \subset \mathbb{N}_0^2$, this is a mapping $L\colon P \to \mathcal{P}(n)$, (where $[n]$ is the vertex set of our graph), with the property that

- **(i)** sets $L(A)$ partition $[n]$ as A ranges over P, and
- **(ii)** for $A, B \in P$ with $|A_1 - B_1|, |A_2 - B_2| \geq 2$, we have all edges between $L(A)$ and $L(B)$ coloured using only c_3, c_4.

This is a generalization of the idea that if we fix a vertex x_0 and we assign $A^{(x)} = (d_{c_1}(x_0, x), d_{c_2}(x_0, x)) \in \mathbb{N}_0^2$ to each vertex x, where d_{c_1}, d_{c_2} are distances in colours c_1, c_2 (which are the remaining two colours), then if $A^{(x)}, A^{(y)}$ satisfy $|A_1^{(x)} - A_1^{(y)}|, |A_2^{(x)} - A_2^{(y)}| \geq 2$, the edge xy cannot be coloured by c_1 or c_2.

Given a subset P' of the domain P, we say that it is k*-distant* if for all distinct

[1] Recall that the tensor product of graphs G and H is the graph on the vertex set $V(G) \times V(H)$ with edges of the form $(u, u'), (v, v')$ for all pairs of edges (u, v) in G and (u', v') in H.

$A, B \in P'$ we have $|A_1 - B_1|, |A_2 - B_2| \geq k$. Once we have all this terminology set up, we begin building up structure in our graph, essentially as follows:

Step 1. We prove that if a c_3, c_4-layer mapping has a 3-distant set of size at least 4, then Theorem 4.7 holds.

Step 2. We continue the analysis of distant sets, and prove essentially that if a c_3, c_4-layer mapping has a 6-distant set of size at least 3, then Theorem 4.7 holds.

Step 3. We prove Theorem 4.7 when every colour induces a connected subgraph.

Step 4. We prove Theorem 4.7 when any two monochromatic components of different colours intersect.

Step 5. We put everything together to finish the proof.

Organization of the chapter. In the next subsection, we briefly discuss a reformulation of Conjecture 4.1. In Section 4.2, we collect some auxiliary results, including results on 2-colourings of edges of complete multipartite graphs and the results on sparse subgraphs of G_k and independent sets in G_3. In Section 4.3, we prove Conjecture 4.1 for 4 colours, reproving a result of Gyárfás. The proof of Theorem 4.7 is given in Section 4.4, with subsections splitting the proof into the steps described above. Finally, we end the chapter with some concluding remarks in Section 4.5.

4.1.2 Another version of Conjecture 4.1

For each $l \in \mathbb{N}$, define the graph G_l with vertex set $\mathbb{N}_0^l$ by putting an edge between any two sequences that differ at every coordinate. Equivalently, G_l is the tensor product of l copies of $K_{\mathbb{N}_0}$ (the complete graph on the vertex set $\mathbb{N}_0$). We formulate the following conjecture.

Conjecture 4.8. *Given a finite set of vertices of $X \subset \mathbb{N}_0^l$, we can find l sets $X_1, \ldots, X_l \subseteq X$ that cover X and each X_i is either contained in a hyperplane of the form $\{x_j = c\}$ or $G_l[X_i]$ is connected.*

This conjecture is actually equivalent to Conjecture 4.1.

Proposition 4.9. *Conjectures 4.1 and 4.8 are equivalent for $k = l + 1$.*

Proof. Conjecture 4.1 implies Conjecture 4.8. Let $X \subset \mathbb{N}_0^l$ be a finite set. Let $n = |X|$ and define an $(l+1)$-colouring $\chi\colon E(K_n) \to [l+1]$ by setting $\chi(xy) = i$, where i is the smallest coordinate index such that $x_i = y_i$; otherwise, when x and y differ in all coordinates, set $\chi(xy) = l + 1$. If Conjecture 4.1 holds, we may find sets $A_1, A_2, \ldots, A_l$ that cover $[n]$, and colours $c_1, c_2, \ldots, c_l$ such that $K_n[A_i, c_i]$ are all connected. Fix now any i, and let $B \subset X$ be the set of vertices corresponding to A_i. If $c_i \le l$, then for any $x, y \in B$, there is a sequence of vertices $z_1, z_2, \ldots, z_m \in B$ such that $x_i = (z_1)_i = (z_2)_i = \cdots = (z_m)_i = y_i$, so $x_i = y_i$. Hence, B is subset of the plane $\{x_i = v\}$ for some value v. Otherwise, if $c = l+1$, that means that the edges of $K_n[A_i, c_i]$ correspond to edges of $G[B]$, so $G[B]$ is connected, as desired.

Conjecture 4.8 implies Conjecture 4.1. Let $\chi\colon E(K_n) \to [k]$ be any k-colouring of the edges of K_n. For every colour c, look at components $C_1^{(c)}, \ldots, C_{n_c}^{(c)}$ of $K_n[c]$. For each choice of $x_1, x_2, \ldots, x_{k-1}$ with $x_c \in [n_c]$ for $c \in [k-1]$, we define $C_x = C_{x_1, x_2, \ldots, x_{k-1}} = \cap_{c \in [k-1]} C_{x_c}^{(c)}$, which is the intersection of monochromatic components, one for each colour except k. Let $X \subset \mathbb{N}^{k-1}$ be the set of all $(k-1)$-tuples x for which C_x is non-empty. If Conjecture 4.8 holds, then we can find $A_1, A_2, \ldots, A_{k-1}$ that cover X such that each A_i is either contained in a hyperplane, or induces a connected subgraph of G_{k-1}. If $A_i \subset \{x_c = v\}$, then the corresponding intersection C_x is a subset of $C_v^{(c)}$ for each $x \in A_i$. On the other hand, if $G_{k-1}[A_i]$ is connected, then taking any adjacent $x, y \in G_{k-1}[A_i]$, we have that $x_c \ne y_c$ for all $c \in [k-1]$. Hence all the edges of between C_x and C_y are coloured by k. Hence, all the sets C_x for $x \in A_i$ are subset of the same component of $K_n[k]$. This completes the proof of the proposition. $\square$

4.2 Auxiliary Results

As suggested by its title, this section is devoted to deriving some auxiliary results. Firstly we extend Lemma 4.4 to complete multipartite graphs. The case of bipartite graphs is slightly different from the general case of more than 2 parts, and is stated separately. We also introduce additional notation. Given a colour c and vertices x, y we write $d_c(x, y)$ for the distance between x and y in $G[c]$. If they are not in the same c-component, we write $d_c(x,y)=\infty$. In particular, $d_c(x,y)<\infty$ means that x,y are in the same component of $G[c]$. Further, we write $B_c(x,r)$ for the *c-ball of radius r around x*, defined as $B_c(x,r)=\{y\colon d_c(x,y)\le r\}$, where c is a colour, x is a vertex, and r is a nonnegative integer. For any graph G, throughout the chapter, the *diameter* of G, written $\operatorname{diam} G$, is the supremum of all finite distances between two vertices of G. Thus, $\operatorname{diam} G=\infty$ only happens when G has arbitrarily long induced paths (as we focus on the finite graphs in this chapter, this will not occur). For a colour c and a set of vertices A, the *c-diameter* of A, written $\operatorname{diam}_c A$, is the diameter of $G[A,c]$. We use the standard notation for complete multipartite graphs, so $K_{n_1,n_2,\dots,n_r}$ stands for the graph with r vertex classes, of sizes $n_1,n_2\dots,n_r$, and all edges between different classes are present in the graph.

Lemma 4.10. *Suppose that the edges of $G=K_{n_1,n_2}$ are coloured in two colours. Then, one of the following holds:*

(i) *either there is a colour c, such that $G[c]$ is connected and of diameter at most 10, or*

(ii) *there are partitions $[n_1]=A_1\cup B_1$ and $[n_2]=A_2\cup B_2$ such that all edges in $A_1\times A_2\cup B_1\times B_2$ are of one colour, and all the edges in $A_1\times B_2\cup B_1\times A_2$ are of the other colour.*

Proof. Let χ be the given colouring. We start by observing the following. If there are two vertices v_1,v_2 such that for colour c_1 the inequality $6\le d_{c_1}(v_1,v_2)<\infty$ holds, then for every vertex u such that $\chi(uv_1)=c_1$, we must also have $d_{c_2}(u,v_1)\le 3$, where $c_2\ne c_1$ is the other colour. Indeed, let $v_1=w_0$, $w_1,w_2,\dots,$ $w_r=v_2$ be a minimal c_1-path from v_1 to v_2. Hence $r\ge 6$, the vertices w_i with the same parity of index belong to the same vertex class of $G=K_{n_1,n_2}$ and the edges $v_1w_3=w_0w_3$, w_3w_6, $w_6u\in E(G)$ are all of colour c_2 (otherwise, we get a contradiction to the fact that $d_{c_1}(w_i,v_2)=r-i$), implying that $d_{c_2}(v_1,u)\le 3$.

Now, suppose that a c_1-component C_1 has diameter at least 7. The observation above tells us that if a vertex y is adjacent to x_1, and $d_{c_2}(x_1,y)>1$, then $\chi(x_1,y)=c_1$, so $d_{c_2}(x_1,y)\le 3$. Hence, every vertex y adjacent to x_1 in G, satisfies $d_{c_2}(x_1,y)\le 3$. Similarly, any vertex y adjacent to x_2 satisfies $d_{c_2}(x_2,y)\le 3$. But, x_1,x_2 are in different vertex classes (as their c_1-distance is odd), so their neighbourhoods cover the whole vertex set, and x_1x_2 is an edge as well, from which we conclude that $G[c_2]$ is connected and of diameter at most 9. Thus, if any monochromatic component has diameter at least 7, the lemma follows, so assume that this does not occur.

Now we need to understand the monochromatic components. From the work above, it suffices to find monochromatic components of the desired structure, as the diameter is automatically bounded by 6. Suppose that there are at least 3 c_1-components, $X_1 \cup X_2, Y_1 \cup Y_2, Z_1 \cup Z_2$ with X_1, Y_1, Z_1 subsets of one class of K_{n_1,n_2} and X_2, Y_2, Z_2 subsets of the other. Let $u, v \in X_1 \cup Y_1 \cup Z_1$ be arbitrary vertices. Then we can find $w \in X_2 \cup Y_2 \cup Z_2$ in different c_1-component from u, v. Hence, $\chi(uw) = \chi(wv) = c_2$, so $d_{c_2}(u, v) \leq 2$. Therefore, both vertex classes of G are c_2-connected and consequently the whole graph is c_2-connected.

Finally, assume that each colour has exactly 2 monochromatic components. Let $[n_1] = A_1 \cup B_1, [n_2] = A_2 \cup B_2$ be such that $A_1 \cup A_2, B_1 \cup B_2$ are the c_1-components. Hence, $A_1 \cap B_1 = A_2 \cap B_2 = \emptyset$, and all edges in $A_1 \times B_2$ and $B_1 \times A_2$ are of colour c_2. Thus, sets $A_1 \cup B_2$ and $B_1 \cup A_2$ are c_2-connected and cover the vertices of G, so they must be the 2 c_2-components. Thus, all edges in $A_1 \times A_2$ and $B_1 \times B_2$ must be coloured by c_1, proving the lemma. □

Lemma 4.11. *Let $r \geq 3$, and suppose that $G = K_{n_1,n_2,\ldots,n_r}$ is a complete r-partite graph. Suppose that the edges of G are 2-coloured. Then, there is a colour c such that $G[c]$ is connected and of diameter at most C_r, where we can take $C_3 = 20$, and $C_r = 60$ for $r > 3$.*

Proof. **Assume first that $r = 3$.** Let A, B, C be the vertex classes. We shall use Lemma 4.10 throughout this part of the proof, applying it to every pair of vertex classes. We distinguish three cases, motivated by the possible outcomes of Lemma 4.10 (these cases are not identically the possible results of applying the lemma, but they do resemble the conclusion of the lemma).

Observation. Suppose that D, E, F is a permutation of A, B, C and that $D \cup E$ is contained in a c_1-component of diameter at most N_1, and for each colour, $D \cup F$ splits into two monochromatic components, all of diameter at most N_2. Then, $G[c_1]$ is connected and of diameter at most $N_1 + 2N_2$.

Case 1. Suppose that D, E, F is a permutation of A, B, C, and that Lemma

4.10 gives different outcomes when applied to pairs D, E and D, F. Then, by Observation, there is a colour c such that $G[c]$ is connected and of diameter at most 14. (We took $N_1 = 10$ and $N_2 = 2$.)

Case 2. Suppose that D, E, F is a permutation of A, B, C, and that Lemma 4.10 gives a single monochromatic component for each of pairs D, E and D, F. If we use the same colour c for both pairs, then $G[c]$ is connected and of diameter at most 20. Otherwise, let $D \cup E$ be c_1-connected, and let $D \cup F$ be c_2-connected, with $c_1 \neq c_2$. Apply Lemma 4.10 to E, F. If it results in a single monochromatic component, it must be of colour c_1 or c_2, so once again $G[c]$ has diameter at most 20 for some c. Finally, if $E \cup F$ splits in two pairs of monochromatic components, by Observation $G[c]$ has diameter at most 14, for some c.

Case 3. Lemma 4.10 gives the second outcome for each pair of vertex classes. Look at the complete bipartite graphs $G[A \cup B]$ and $G[A \cup C]$. Then, we have partitions $A = A_1 \cup A_2 = A'_1 \cup A'_2$, $B = B_1 \cup B_2$ and $C = C_1 \cup C_2$ such that all edges $(A_1 \times B_1) \cup (A_2 \times B_2) \cup (A'_1 \times C_1) \cup (A'_2 \times C_2)$ receive colour c_1, while the edges $(A_1 \times B_2) \cup (A_2 \times B_1) \cup (A'_1 \times C_2) \cup (A'_2 \times C_1)$ take the other colour c_2. If $\{A_1, A_2\} \neq \{A'_1, A'_2\}$, then we must have that some A_i intersects both A'_1, A'_2, or vice-versa. In particular, since any two vertices x, y in the same set among A_1, A_2, A'_1, A'_2 obey $d_{c_1}(x, y) \leq 2$, this means that for any two vertices $x, y \in A$, we have $d_{c_1}(x, y) \leq 6$. Now, every point in $B \cup C$ in on c_1-distance at most 1 from a vertex in A, so $G[c_1]$ is connected and of diameter at most 8. Hence, we may assume that $A_1 \cup A_2$ and $A'_1 \cup A'_2$ are the same partitions of A, and similarly for B and C, we get the same partition for both pairs of vertex classes involving each of B and C. Let $A = A_1 \cup A_2, B = B_1 \cup B_2, C = C_1 \cup C_2$ be these partitions, so the colouring is constant on each product $A_i \times B_j, A_i \times C_j, B_i \times C_j$, $i, j \in \{1, 2\}$. Renaming B_i, C_j, we may also assume that $A_1 \times B_1, A_2 \times B_2, A_1 \times C_1, A_2 \times C_2$ all receive colour c_1. Thus $A_1 \times B_2, A_2 \times B_1, A_1 \times C_2, A_2 \times C_1$ all receive colour c_2. But looking at the colour c of $B_1 \times C_2$, we see that $G[c]$ is connected and of diameter at most 5. This finishes the proof of the case $r = 3$, and we may take $C_3 = 20$.

Now suppose that $r > 3$**.** Let $V_1, V_2, \ldots, V_r$ be the vertex classes. Fix the vertex class V_r, and look at the 2-colouring χ' of the edges of K_{r-1} defined as follows: whenever $i, j \in [r-1]$ are distinct, then applying the case $r = 3$ of this lemma that we have just proved to the subgraph induced by $V_i \cup V_j \cup V_r$, we get a colour c such that $G[V_i \cup V_j \cup V_r, c]$ has diameter at most 20; we set $\chi'(ij) = c$. By Lemma 4.4, we have a colour c such that $K_{r-1}[c]$ is of diameter at most 3 for the colouring χ'. Returning to our original graph, we claim that $G[c]$ has diameter at most 60. Suppose that x, y are any two vertices of G. If any of these points lies in V_r, or if they lie in the same V_i, then we can pick i, j such that $y \in V_i \cup V_j \cup V_r$ and $\chi'(ij) = c$. Hence, by the definition of χ', we actually have $d_c(x, y) \leq 20$ in G. Now, assume that x, y lie in different vertex classes and outside of V_r. Let $x \in V_i, y \in V_j$. Under the colouring χ' of K_{r-1} we have that $d_c(ij) \leq 3$, so we have a sequence $i_1 = i, i_2, \dots, i_s = j$, with $s \leq 4$, such that $\chi'(i_1 i_2) = \cdots = \chi'(i_{s-1} i_s) = c$. For each t between 1 and s, pick a representative $x_t \in V_{i_t}$, with $x = x_1, y = x_s$. Then, $d_c(x_{t-1}, x_t) \leq 20$, so $d_c(x, y) = d_c(x_1, x_s) \leq 60$, as desired. □

4.2.1 Induced subgraphs of G_l

Recall that G_l is the graph on $\mathbb{N}^l$, with edges between pairs of points whose all coordinates differ. In this subsection we prove a few properties of such graphs, particularly focusing on G_3. We begin with a general statement, which will be reproved for specific cases with stronger conclusions.

Lemma 4.12. *If S is a set of vertices in G_l and the maximal degree of $G[S]$ is at most d, then the number of non-isolated vertices of $G[S]$ is at most $O_{l,d}(1)$.*

Proof. By Ramsey's theorem we have an integer N such that whenever $E(K_N)$ is coloured using $2^l - 1$ colours, there is a monochromatic K_{l+1}. Let S' be the set of non-isolated vertices in S. We show that $|S'| < (d^2 + d + 1)N$. Suppose contrary, since the maximal degree is at most d, we have a subset $S'' \subset S$ of size $|S''| \geq N$ such that sets $s \cup N(s)$ are disjoint for all $s \in S''$ (simply pick a maximal such subset, their second neighbourhoods must cover the whole S'). In particular, S'' is an independent set in G_l, so for every pair of vertices $x, y \in S$, the set $I(x, y) = \{i \in [l] \colon x_i = y_i\}$ is non-empty. Thus, $I \colon E(K_{S''}) \to \mathcal{P}(l) \setminus \{\emptyset\}$ is $2^l - 1$ colouring of the edges of a complete graph $K_{S''}$ on the vertex set S''. By Ramsey's theorem, there is a monochromatic clique on subset $T \subset S''$ of size at least $l + 1$, whose edges are coloured by some set $I_0 \neq \emptyset$. Take a vertex $t \in T$, and since t is not isolated and the neighbourhoods of vertices in S'' are disjoint, we can find $x \in S'$ such that tx is an edge, but $t'x$ is not for other $t' \in T$. Hence, $x_i \neq t_i$ for all $i \in [l]$ and for distinct $t', t'' \in T$ we have $t'_i = t''_i$ if and only if $i \in I_0$. Thus, $x_i \neq t'_i$ for all $t' \in T$ and $i \in I_0$. But, xt' is not an edge for $t' \in T \setminus \{t\}$, so we always have $i \in [l] \setminus I_0$ such that $x_i = t'_i$. But, for each $i \in I_0$, the values of t'_i are distinct for each $t' \in T$. Hence, for each i, there is at most one vertex $t' \in T \setminus \{t\}$ such that $x_i = t'_i$. Therefore $|T| - 1 \leq |[l] \setminus I_0| \leq l - 1$, so $|T| \leq l$, which is a contradiction. $\square$

We may somewhat improve on the bound in the proof of the lemma above by observing that for colour I_0 we only need a clique of size $l - |I_0| + 2$. Thus, instead of Ramsey number

$$R(\underbrace{l+1, l+1, \ldots, l+1}_{2^l - 1}),$$

we could use

$$R(l + 2 - |I_1|, l + 2 - |I_2|, \ldots, l + 2 - |I_{2^l - 1}|),$$

where I_i are the non-empty sets of $[l]$. But, even for paths in G_3, which we shall use later, taking $l = 3, d = 2$, we get the final bound of $7R(2, 3, 3, 3, 4, 4, 4)$, where 7 comes from $d^2 + d + 1$ factor we lose when moving from S' to S''. We now improve this bound.

Lemma 4.13. *If S is a set of vertices of G_3 such that $G_3[S]$ is a path, then $|S| \leq 30$.*

Proof. Let $S = \{s_1, s_2, \ldots, s_r\}$ be such that $s_1, s_2, \ldots, s_r$ is an induced path in G_3, so the only edges are $s_i s_{i+1}$.

Case 1. For all $i \in \{4, 5, \ldots, 10\}$, s_i coincides with one of s_1 or s_2 in at least two coordinates.

Since $s_1 s_2$ is an edge, s_1 and s_2 have all three coordinates different. Thus, for $i \in \{4, 5, \ldots, 10\}$, we have $(s_i)_c \in \{(s_1)_c, (s_2)_c\}$ for all coordinates c. Hence, there are only at most 6 possible choices of s_i (as $s_i \neq s_1, s_2$), so $r \leq 9$.

Case 2. There is $i_0 \in \{4, 5, \ldots, 10\}$ with at most one common coordinate with each of s_1, s_2. Since $s_1 s_{i_0}, s_2 s_{i_0}$ are not edges, w.l.o.g. we have $s_1 = (x_1, x_2, x_3), s_2 = (y_1, y_2, y_3), s_{i_0} = (x_1, y_2, z_3)$, where $x_i \neq y_i$, $z_3 \notin \{x_3, y_3\}$. Consider any point s_j, for $j \geq i_0 + 2$. It is not adjacent to any of s_1, s_2, s_{i_0}. If $(s_j)_1 = x_1$ and $(s_j)_2 \neq y_2$, then $(s_j)_3 = y_3$. Similarly, if $(s_j)_1 \neq x_1$ and $(s_j)_2 = y_2$, then $(s_j)_3 = x_3$. Also, if $(s_j)_1 \neq x_1, (s_j)_2 \neq y_2$, then $s_j = (y_1, x_2, z_3)$. Hence, for $j \geq i_0 + 2$, the point s_j is on one of the lines

$$(x_1, y_2, \cdot), (x_1, \cdot, y_3), (\cdot, y_2, x_3) \text{ or it is the point } (y_1, x_2, z_3),$$

where $(a, b, \cdot)$ stands for the line $\{(a, b, z) \colon z \text{ arbitrary}\}$, etc. Note that a point on $(x_1, y_2, \cdot)$ is not adjacent to any point on $(\cdot, y_2, x_3)$, and the same holds for lines $(x_1, y_2, \cdot)$ and $(x_1, \cdot, y_3)$. Hence, along out path, a point on the line $(x_1, \cdot, y_3)$ is followed either by a point on $(\cdot, y_2, x_3)$ or the point (y_1, x_2, z_3) (the latter may happen only once). In any case, if $|S| \geq 30$, then among $s_{i_0+2}, s_{i_0+3}, \ldots, s_{i_0+20}$, we must get a contiguous sequence $s_j, s_{j+1}, \ldots, s_{j+7}$ of points

$$s_j, s_{j+2}, s_{j+4}, s_{j+6} \in (x_1, \cdot, y_3), s_{j+1}, s_{j+3}, s_{j+5}, s_{j+7} \in (\cdot, y_2, x_3).$$

Finally, we look at $A = s_j, B = s_{j+2}, C = s_{j+5}, D = s_{j+7}$. These four points form an independent set, but $A \neq B$ gives $A_2 \neq B_2$, so one of $A_2 \neq y_2, B_2 \neq y_2$ holds, and similarly, one of $C_1 \neq x_1, D_1 \neq x_1$ holds as well. Choosing a point among A, B and a point among C, D for which equality does not hold gives an edge, which is impossible. $\square$

Finally, we study independent sets in G_3. Note that Lemma 4.12 in this case does not tell us anything about the structure of such sets. When we refer to line or planes, we always think of very specific cases, namely the lines are the sets of the form $\{x \colon x_i = a, x_j = b\}$ and the planes are $\{x \colon x_i = a\}$. Similarly, collinearity and coplanarity of points have a stronger meaning than the usual one, and imply that points lie on a common line or plane defined as above.

Lemma 4.14. *Let S be a set of vertices in G_3. If every two points of S are collinear, then S is a subset of a line. If every three points of S are coplanar, then S is a subset of a plane.*

Proof. We first deal with the collinear case. Take any pair of points, $x, y \in S$, w.l.o.g. they coincide in the first two coordinates. Take third point $z \in S$. If z

does not share the values of the first 2 coordinates with x and y, then we must have $x_3 = z_3 = y_3$, which is impossible. As z was arbitrary, we are done.

Suppose now that we have all triples coplanar. W.l.o.g. we have a non-collinear pair x, y, which only coincide in the first coordinate. Then all other points may only be in the plane $\{p\colon p_1 = x_1\}$. $\square$

Lemma 4.15. *(Structure of the independent sets of size 4.) Given an independent set I of G_3 of size 4, (at least) one of the following alternatives holds*

(S1) *I is coplanar,*

(S2) *$I = \{(a, b, c), (a', b', c), (a', b, c'), (a, b', c')\}$, where $a \neq a'; b \neq b'$ and $c \neq c'$,*

(S3) *up to permutation of coordinates $I = \{(a, b, c), (a, b, c'), (a, b', x), (a', b, x)\}$, where $a \neq a'; b \neq b'$ and $c \neq c'$.*

Proof. Suppose that $I = \{A, B, C, D\}$ is not a subset of any plane. We distinguish between two cases.

Case 1. There are no collinear pairs in I.

Let $A = (a, b, c)$. But AB is not an edge and not collinear so A and B differ in precisely two coordinates. Thus, w.l.o.g. $B = (a', b', c)$ where $a \neq a'$ and $b \neq b'$. If C_3 also equals c, then we must have $C_3 = (a'', b'', c)$ with a'' different from a, a' and b'' from b, b'. However, looking at D, we cannot have $D_3 = c$ as otherwise $I \subset \{x_3 = c\}$, so D must differ at all three coordinates from one of the points A, B, C, making them joined by an edge, which is impossible. Thus $C_3 = c'$, with $c' \neq c$. Since AC and BC are not edges, $C \in \{(a, b', c'), (a', b, c')\}$. The same argument works for D, so $D_3 = c'' \neq c$, and $D \in \{(a, b', c''), (a', b, c'')\}$. However, if $c' \neq c''$, then C, D are either collinear or adjacent in G_3, which are both impossible. Hence $c'' = c'$, and $\{C, D\} = \{(a, b', c'), (a', b, c')\}$, as desired.

Case 2. W.l.o.g. A and B are collinear.

Let $A = (a, b, c), B = (a, b, c')$ with $c \neq c'$. Since $\{x_1 = a\}$ does not contain the whole set I, we have w.l.o.g. $C_1 = a' \neq a$. If $C_2 \neq b$, then AC or BC is an edge, which is impossible. Therefore, $C_2 = b$. Hence $D_2 = b' \neq b$, and by similar argument $D_1 = a$. Finally CD is not an edge, so their third coordinate must be the same, proving the lemma. $\square$

Lemma 4.16. *(Structure of the independent sets of size 5.) Given an independent set I of G_3 of size 5, (at least) one of the following alternatives holds*

(i) *I is coplanar,*

(ii) *I is a subset of a union of three lines, all sharing the same point.*

Proof. List the vertices of I as x_1, x_2, x_3, x_4, x_5. W.l.o.g. x_1, x_2, x_3 are not coplanar. By the previous lemma, $\{x_1, x_2, x_3, x_i\}$ for $i = 4, 5$ may have structure **S2** or **S3**. But if both structures are **S2**, then we must have that in both quadruples, at each coordinate, each value appears precisely two times. This implies $x_4 = x_5$. Hence, w.l.o.g. $\{x_1, x_2, x_3, x_4\}$ has structure **S3**. Therefore, assume w.l.o.g. that

$$x_1 = (1,0,0), x_2 = (0,1,0), x_3 = (0,0,1), x_4 = (0,0,c')$$

for some $c' \neq 1$ (which corresponds to the choice $a = 0, a' = 1, b = 0, b' = 1, x = 0, c = 1$ in the previous lemma, swapping the roles of c and c' if necessary). Looking at $\{x_1, x_2, x_3, x_5\}$, if it had **S2** for its structure, we would get $x_5 = (1,1,1)$, which is adjacent to x_4, and thus impossible. Hence $\{x_1, x_2, x_3, x_5\}$ also has structure **S3**. Permuting the coordinates only permutes x_1, x_2, x_3, and does not change the number of zeros in x_5. Thus, w.l.o.g.

$$\begin{aligned}\{(1,0,0),(0,1,0),(0,0,1),x_5\} &= \{x_1, x_2, x_3, x_5\}\\ &= \{(d,e,f),(d,e,f'),(d',e,y),(d,e',y)\},\end{aligned}$$

for some $d \neq d', e \neq e', f \neq f'$. But in the first coordinate, only zero can appear three times, so $d = 0$. Similarly, $e = 0$, so $x_5 \in (0,0,\cdot)$, after a permutation of coordinates. Thus x_5 has at least 2 zeros, so our independent set I is a subset of the union of lines passing through the point $(0,0,0)$, as required. $\square$

4.3 Conjecture 4.1 for 4 Colours

In this short section we reprove a result of Gyárfás.

Theorem 4.17. *(Gyárfás) Conjecture 4.1 for 4 colours and Conjecture 4.8 for G_3 are true.*

Proof. By the equivalence of conjectures, it suffices to prove Conjecture 4.8 for G_3. Let X be the given finite set of vertices in G_3. Assume that $G_3[X]$ has at least 4 components, otherwise we are done immediately. By a *representatives set* we mean any set of vertices that contains at most one vertex from each component of X. A *complete representatives set* is a representatives set that intersects every component of X.

Observation 4.18. *If there are three collinear points, each in different component, then X can be covered by two planes. In particular, if two planes do not suffice, then among every three points in different components, there is a non-collinear pair.*

Proof. W.l.o.g. these are points $(0,0,1),(0,0,2),(0,0,3)$. Then, unless $X \subset \{x_1 = 0\} \cup \{x_2 = 0\}$, we have a point of the form (a,b,c) with a,b both non-zero, so it is a neighbour of at least two of the points we started with, contradicting the fact that they belong to different components. For the second part, recall that if every pair in a triple is collinear, then the whole triple lies on a line. $\square$

By the observation above, every representatives set of size at least 3 has a non-collinear pair. Suppose firstly that every complete representatives set is a subset of a plane. Pick a complete representatives set $\{x_1, x_2, \ldots, x_r\}$, with $x_i \in C_i$, where C_i are the components. W.l.o.g. x_1, x_2 is a noncollinear pair, therefore, it determines a plane π, forcing components $C_3, C_4, \ldots, C_r$ to be entirely contained in this plane. Hence, we may cover the whole set X by components C_1 and C_2, and the plane π. Therefore, we may assume that we have a representatives set of size three which does not lie in any plane.

Case 1. X has more than 4 components.

Let x_1, x_2, x_3 be a representatives set, $x_i \in C_i$, which is not coplanar. Then, for any choice of $y_4, \ldots, y_r$, such that $\{x_1, x_2, x_3, y_4, \ldots, y_r\}$ is a complete representatives set, we have 3 lines that meet in a single point, that contain all these points. Observe that this structure is determined entirely by x_1, x_2, x_3. Indeed, since these three points are not coplanar, they cannot coincide in any coordinate. However, since there are at least 5 components, x_1, x_2, x_3 extend to an independent set of size 5, which must be a subset of three lines sharing a point p. But we can identify p, since p_i must be the value that occurs precisely two times among

$(x_1)_i, (x_2)_i, (x_3)_i$, and hence the lines are $l_1 = px_1, l_2 = px_2, l_3 = px_3$. Thus, the union of lines l_1, l_2, l_3 contains whole components $C_4, \dots, C_r$ and $x_i \in l_i$. By the Observation above, each l_i has representatives from at most two components. Hence, the common point p of the lines l_1, l_2, l_3 cannot belong to X, as otherwise some line l_i would have three components meeting it. W.l.o.g. l_2, l_3 intersect two components, and l_1 may intersect 1 or 2. Then, picking any $y \in l_2$ in a different component than that of x_2 and any $z \in l_3$ with a component different from that of x_3, using the argument above applied to $\{x_1, y, z\}$ instead of $\{x_1, x_2, x_3\}$, we deduce that $C_2 \subset l_2$, $C_3 \subset l_3$. Thus, we actually have singleton components $C_2, C_3, \dots, C_r$. Finally, any point in C_1 must be either in the plane of l_2, l_3 or on the line l_1, so we can cover by two planes.

Case 2. X has precisely 4 components and there exists a coplanar complete representatives set.

Let x_1, x_2, x_3, x_4 be a complete representatives set, with $x_i \in C_i$. W.l.o.g. we have $x_i = (a_i, b_i, 0)$. As a few times before, we do not have a collinear triple among these 4 points, so each of the sequences $(a_i)_{i=1}^4$ and $(b_i)_{i=1}^4$ has the property that a value may appear at most twice in the sequence.

Suppose for a moment that each of these two sequences has at most one value that appears twice. Write v for the value that appears two times in (a_i), if it exists, and let v be the corresponding value for (b_i). If we take a point y outside the plane $(\cdot, \cdot, 0)$, then the number of appearances of y_1 in (a_i) and y_2 in (b_i) combined is at least three. So, either y_1 is the unique doubly-appearing value u for a_i or is $y_2 = v$, so the three planes $(u, \cdot, \cdot), (\cdot, v, \cdot)$ and $(\cdot, \cdot, 0)$ cover X.

Now, assume that w.l.o.g. has two doubly-appearing values, i.e. $a_1 = a_2 = u \neq a_3 = a_4 = v$. If y is outside the plane $(\cdot, \cdot, 0)$, then if $y_1 \neq u$, one of the pairs $x_1 y, x_2 y$ must be an edge, so $x_3 y$ and $x_4 y$ are not edges, so we must have $y_1 = v$. Similarly, if y is outside the plane $(\cdot, \cdot, 0)$ and $y_1 \neq v$, then $y_1 = u$. Hence, for all points $y \in X$, we have $y_1 \in \{u, v\}$ or $y_3 = 0$, and three planes cover once again.

Case 3. X has precisely 4 components, but no complete representatives set is coplanar.

Thus, by Lemma 4.15, every complete representatives set has either **S2** or **S3** as its structure. Observe that if **S2** is always the structure, then all the components are singleton, and we are done by taking a plane to cover two vertices. So, there is a representatives set with structure **S3**. Take such a representatives set x_1, x_2, a, b, w.l.o.g. $x_1 = (1,0,0), x_2 = (2,0,0)$. Take any y that shares the component with a, and any z that shares the component with b. Then, x_1, x_2, y, z is also a complete representatives set, so it is not coplanar. But, as x_1, x_2 are collinear, it may not have structure **S2**, so the structure must be **S3**, which forces $y_1 = z_1$. Hence, we can cover X by components of x and y and the plane $(a_1, \cdot, \cdot)$. This completes the proof. $\square$

Note that the theorem is sharp; we can take $X = \{0, e_1, e_2, e_3, e_1 + e_2, e_1 + e_3, e_2 + e_3\}$, where $e_1 = (1,0,0), e_2 = (0,1,0), e_3 = (0,0,1)$.

4.4 Conjecture 4.6 for 4 Colours

Recall, by the *diameter* of a colour c, written diam_c, we mean the maximal distance between vertices sharing the same component of $G[c]$. In the remaining part of the chapter, for a given 4-colouring $\chi\colon E(K_n) \to 4$, we say that χ *satisfies Conjecture 4.6 with (constant)* K if there are sets A_1, A_2, A_3 whose union is $[n]$ and colours c_1, c_2, c_3 such that each $K_n[A_i, c_i]$ is connected and of diameter at most K. Thus, our goal can be phrased as: there is an absolute constant K such that every 4-colouring χ of $E(K_n)$ satisfies Conjecture 4.6 with K.

We begin the proof of the main result by observing that essentially we may assume that at least two colours have arbitrarily large diameters. We argue by modifying the colouring slightly.

Lemma 4.19. *Suppose χ is a 4-colouring of $E(K_n)$ such that three colours have diameters bounded by N_1. Then χ satisfies Conjecture 4.6 with* $\max\{N_1, 30\}$.

Proof. Write $G = K_n$, and observe that if a point does not receive all 4 colours at its edges, we are immediately done. Let χ be the given colouring of the edges, and let colours 1, 2 and 3 have diameter bounded by N_1. We begin by modifying the colouring slightly. Let xy be any edge coloured by colour 4. If x and y share the same component in $G[c]$ for some $c \in \{1,2,3\}$, change the colour of xy to the colour c (if there is more than one choice, pick any). Note that such a modification does not change the monochromatic components, except possibly shrinking the components for the colour 4. Let χ' stand for the modified colouring.

Observe that the diameter of colour 4 in χ' is also bounded. Begin by listing all the components for colours $i \in \{1, 2, 3\}$ as $C_1^{(i)}, C_2^{(i)}, C_3^{(i)}, \ldots$. For $x \in \mathbb{N}^3$, consider the sets $C_x = C_{x_1,x_2,x_3} = C_{x_1}^{(1)} \cap C_{x_2}^{(2)} \cap C_{x_3}^{(3)}$. Let X be the set of all x such that $C_x \neq \emptyset$. If $G^{(\chi')}[4]$ (where the superscript indicates the relevant colouring) has an induced path $v_1, v_2, \ldots, v_r$, then if $x_i \in \mathbb{N}^3$ is defined to be such that $v_i \in C_{x_i}$, in fact $x_1, x_2, \ldots, x_r$ becomes an induced path in G_3. But Lemma 4.13 implies that $r \leq 30$. Hence, the 4-diameter in the colouring χ' is at most 30.

Applying Theorem 4.17 for the colouring χ', gives three monochromatic components that cover the vertex set, let these be $G^{(\chi')}[A_1, c_1]$, $G^{(\chi')}[A_2, c_2]$, $G^{(\chi')}[A_3, c_3]$, where the superscript indicates the relevant colouring. Using the same sets and colours, but returning to the original colouring, we have that $G^{(\chi)}[A_1, c_1]$, $G^{(\chi)}[A_2, c_2]$, $G^{(\chi)}[A_3, c_3]$ are all still connected, as 1-, 2- and 3-components are the same in χ and χ', while there can only be more 4-coloured edges in the colouring χ. Also, 1-, 2- and 3-diameters are bounded by N_1, and 4-diameters of sets may only decrease when returning to colouring χ', so the lemma follows. $\square$

Let us introduce some additional notions. Let $P \subset \mathbb{N}_0^2$ be a set, and let $L\colon P \to \mathcal{P}(n) \setminus \{\emptyset\}$ be a function with the property that $\{L(A)\colon A \in P\}$ form a partition of $[n]$ and there a two colours c_3, c_4 [2]such that whenever $A, B \in P$ and $|A_1 - B_1|, |A_2 - B_2| \geq 2$, then all edges between the sets $L(A)$ and $L(B)$ are coloured with c_3 and c_4 only. We call L a c_3, c_4-*layer mapping* and we refer to P as the *layer index set*. Further, we call a subset $S \subset P$ a k-*distant set* if for every two distinct points $A, B \in S$ we have $|A_1 - B_1|, |A_2 - B_2| \geq k$.

Let us briefly motivate this notion. Suppose that $K_n[c_1]$ and $K_n[c_2]$ are both connected. Fix a vertex x_0 and let $P = \{(d_{c_1}(x_0, v), d_{c_2}(x_0, v))\colon v \in [n]\} \subset \mathbb{N}_0^2$. Let $L(A) \colon= \{v \in [n]\colon (d_{c_1}(x_0, v), d_{c_2}(x_0, v)) = A\}$ for all $A \in P$ (this also motivates the choice of the letter L, we think of $L(A)$ as a *layer*). Then, if $x \in L(A), y \in L(B)$ for $A, B \in P$ with $|A_1 - B_1| \geq 2, |A_2 - B_2| \geq 2$, by triangle inequality, we cannot have $d_{c_1}(x, y) \leq 1$ nor $d_{c_2}(x, y) \leq 1$, so xy takes either the colour c_3 or the colour c_4. As we shall see, we may have more freedom in the

[2]This choice of indices was chosen on purpose – we shall first use colours c_1, c_2 to define P and L, and the remaining colours will be c_3 and c_4.

definition of P and L if there is more than one component in a single colour.

We now explore these notions in some detail, before using them to obtain some structural results on the 4-colourings that (for the moment) possibly do not satisfy Conjecture 4.6.

Lemma 4.20. *Let χ be a 4-colouring, L a c_3, c_4-*layer mapping *with layer index set P, and suppose that $\{A, B, C\} \subset P$ is a* 3*-distant set. Write $G = K_n$. Then the following hold.*

(1) *For some colour $c \in \{c_3, c_4\}$ we have $G[L(A) \cup L(B) \cup L(C), c]$ connected and of diameter at most 20.*

(2) *If additionally for c' such that $\{c, c'\} = \{c_3, c_4\}$ and some distinct $A', B' \in \{A, B, C\}$ we have $G[L(A') \cup L(B'), c']$ contained in a subgraph $H \subset G[c']$ that is connected and of diameter at most N_3, then the given colouring satisfies Conjecture 4.6 with* $\max\{40, N_3 + 20\}$.

Proof of Lemma 4.20. **(1):** Observe that all edges between $L(A), L(B), L(C)$ are of colours c_3 and c_4. This is a complete tripartite graph and by Lemma 4.11 w.l.o.g. $L(A) \cup L(B) \cup L(C)$ is c_3-connected and of c_3-diameter at most 20.

(2): W.l.o.g. $A' = A, B' = B$. Pick any $D \in P$. Note that since A, B, C are 3-distant, D is 2-distant from at least one of A, B, C (otherwise, by pigeonhole principle, for some A', B' among A, B, C and some index i, we have $|A'_i - D_i|, |B'_i - D_i| \leq 1$, so $|A'_i - B'_i| \leq 2$, which is impossible). Let $E \in \{A, B, C\}$ be such that D, E are 2-distant. Thus, all the edges between $L(D)$ and $L(E)$ are of colours c_3 and c_4, so Lemma 4.10 applies to $L(D) \cup L(E)$.

Let $P' \subset P$ be the set of all $D \in P$ such that Lemma 4.10 gives that either $L(D) \cup L(E)$ is c-connected and of c-diameter at most 10, or the second conclusion of that lemma holds. Hence, every vertex x in $L(D)$ for some $D \in P'$ is on c-distance at most 10 to a vertex in $L(A) \cup L(B) \cup L(C)$, which itself has c-diameter at most 20. Hence, $L(A) \cup L(B) \cup L(C) \cup (\cup_{D \in P'} L(D))$ is c-connected and of c-diameter at most 40.

For all other $D \in P \setminus P'$, Lemma 4.10 applied to $L(D) \cup L(E)$ for a relevant E implies that $L(D) \cup L(E)$ is c'-connected and of diameter at most 10. Let P'' be the set of $D \in P \setminus P'$ for which $E \in \{A, B\}$, and let $P''' = P \setminus (P' \cup P'')$

(for which therefore $E = C$). Hence, $H \cup (\cup_{D\in P''} L(D))$ is c'-connected and of c'-diameter at most N_3+20, and finally $L(C)\cup(\cup_{D\in P'''} L(D))$ is also c'-connected and of c'-diameter at most 20. Hence, taking

$$G[L(A) \cup L(B) \cup L(C) \cup (\cup_{D\in P'} L(D)), c],$$
$$H \cup G[(\cup_{D\in P''} L(D)), c'], \text{ and}$$
$$G[L(C) \cup (\cup_{D\in P'''} L(D)), c'],$$

proves the lemma. $\square$

Lemma 4.21. *Suppose that χ is a 4-colouring of $E(K_n)$ and that L is a c_3, c_4-layer mapping for some colours $c_3, c_4 \in [4]$ with a 3-distant set of size at least 4. Then c satisfies Conjecture 4.6 with constant 160.*

Proof. Write $G = K_n$. Suppose that some $A, B, C, D \in P$ are 3-distant. All edges between $L(A) \cup L(B) \cup L(C) \cup L(D)$ are of colours c_3 and c_4 only, so by Lemma 4.11 w.l.o.g. $G[L(A) \cup L(B) \cup L(C) \cup L(D), c_3]$ is connected and of diameter at most 60. Pick any $E \in P$. If E has difference at most 1 in absolute value in some coordinate from at least three points among A, B, C, D, by pigeonhole princple, there are A', B' among these four and coordinate i such that $|A'_i - E_i|, |B'_i - E_i| \leq 1$ so $|A'_i - B'_i| \leq 2$, which is impossible. Hence, E is 2-distant from at least two points $A'(E), B'(E)$ among A, B, C, D. Hence, $A'(E), B'(E), E$ is a 2-distant set, so edges between $L(A'(E)), L(B'(E))$ and $L(E)$ are of colours c_3 and c_4 only. By Lemma 4.11, for some colour $c(E) \in \{c_3, c_4\}$ we have $G[L(A'(E)) \cup L(B'(E)) \cup L(E), c(E)]$ connected and of diameter at most 20. We split P as follows: $P' \subset P$ is the set of all $E \in P$ such that $c(E) = c_3$, and for each pair π of A, B, C, D we define P_π as the set of all $E \in P$ such that $\{A'(E), B'(E)\} = \pi$ and $c(E) = c_4$. We now look at the set of all pairs π for which $P_\pi \neq \emptyset$.

Case 1: there are π_1, π_2 such that P_{π_1} and P_{π_2} are non-empty and $\pi_1 \cap \pi_2 \neq \emptyset$. W.l.o.g. $\pi_1 = \{A, B\}, \pi_2 = \{A, C\}$. For every $\pi = \{A', B'\}$ we already have $G[L(A') \cup L(B') \cup (\cup_{E\in P_\pi} L(E)), c_4]$ connected and of diameter at most 40. Hence, $G[L(A) \cup L(B) \cup L(C) \cup (\cup_{E\in P_{\pi_1}\cup P_{\pi_2}} L(E)), c_4]$ is also connected and of diameter at most 80. But, any other pair π must intersect A, B, C, so we have

$$G[\cup_\pi \left((\cup_{F\in\pi} L(F)) \cup (\cup_{E\in P_\pi} L(E))\right), c_4]$$

connected and of diameter at most 160, where $\cup_\pi$ ranges over all pairs. Taking additionally

$$G[L(A) \cup L(B) \cup L(C) \cup L(D) \cup (\cup_{E \in P'} L(E)), c_3]$$

proves the claim.

Case 2: all pairs π such that $P_\pi \neq \emptyset$ are disjoint. There are at most 2 such pairs. Thus, if we take

$$G[(\cup_{F \in \pi} L(F)) \cup (\cup_{E \in P_\pi} L(E)), c_4]$$

for such pairs π (these are connected and of diameter at most 40), and

$$G[L(A) \cup L(B) \cup L(C) \cup L(D) \cup (\cup_{E \in P'} L(E)), c_3],$$

the claim follows. □

Lemma 4.22. *Suppose that χ is a 4-colouring of $E(K_n)$ and that L is a c_3, c_4-layer mapping for some colours $c_3, c_4 \in [4]$ with a 7-distant set of size at least 3. Suppose additionally that $\{A_i : A \in P\}$ takes at least 28 values for each $i = 1, 2$. Then χ satisfies Conjecture 4.6 with constant 160.*

Proof. Let $\{A, B, C\}$ be a 7-distant set. Pick any other $D \in P$. If D is 3-distant from each of A, B, C, we obtain a 3-distant set of size 4, so by Lemma 4.21 we are done. Hence, for every $D \in P$ we have $E \in \{A, B, C\}$ such that $|E_i - D_i| \leq 2$ for some i. (Note that this is the main contribution to the constant 160 in the statement of the main result.)

Since $\{A, B, C\}$ is a 7-distant set, by Lemma 4.20, we have w.l.o.g. $G[L(A) \cup L(B) \cup L(C), c_3]$ connected and of diameter at most 20. We now derive some properties of $L(D)$ for points $D \in P$ be such that $|D_i - A_i|, |D_i - B_i|, |D_i - C_i| \geq 3$ for some $i \in \{1, 2\}$. (Note that such points exist by assumptions.)

Let D be such a point and let j be such that $\{i, j\} = \{1, 2\}$. Since the set $\{A, B, C\}$ is 7-distant, there are distinct $E_1, E_2 \in \{A, B, C\}$ such that $|D_j - (E_1)_j|, |D_j - (E_2)_j| \geq 3$. Thus, $\{D, E_1, E_2\}$ is also a 3-distant set. Applying Lemma 4.20 to $\{D, E_1, E_2\}$ implies that $G[L(D) \cup L(E_1) \cup L(E_2), c]$ is connected and of diameter at most 20, for some $c \in \{c_3, c_4\}$. However, if $c = c_4$, $G[L(E_1) \cup L(E_2), c_4]$ is contained in a subgraph of $G[c_4]$ which is connected and of diameter at most 20, so Lemma 4.20 (2) applies once again and the claim follows. Hence, we must have that $G[L(D) \cup L(E_1) \cup L(E_2), c_3]$ is connected and of diameter at most 20. In particular, whenever $D \in P$ satisfies $|D_i - A_i|, |D_i - B_i|, |D_i - C_i| \geq 3$ for some $i \in \{1, 2\}$, then every point in $L(D)$ is on c_3-distance at most 20 from $L(A) \cup L(B) \cup L(C)$.

By assumptions, $\{A_1 \colon A \in P\}$ takes at least 28 values. Hence, we can find $X \in P$ such that $|X_1 - A_1|, |X_1 - B_1|, |X_1 - C_1| \geq 5$. Similarly, there is $Y \in P$ such that $|Y_2 - A_2|, |Y_2 - B_2|, |Y_2 - C_2| \geq 5$. W.l.o.g $|X_2 - A_2| \leq 2$. If $|Y_1 - A_1| \leq 2$, then X, Y, B, C form a 3-distant set of size 4, and once again the claim follows from Lemma 4.21. Hence, w.l.o.g. $|Y_1 - B_1| \leq 2$. By the work above, we also have that every point in $L(X) \cup L(Y)$ is on c_3-distance at most 20 from $L(A) \cup L(B) \cup L(C)$. Note also that X, Y are 3-distant.

It remains to analyse $D \in P$ such that for both $i = 1, 2$ there is an $E \in \{A, B, C\}$ such that $|E_i - D_i| \leq 2$. We show that in all but one case on the choice of sets E, we in fact have $L(D)$ on bounded c_3-distance to $L(A) \cup L(B) \cup L(C)$. If we have an $E \in \{A, B, C\}$ such that both $|E_1 - D_1| \leq 2$ and $|E_2 - D_2| \leq 2$ hold, then taking E', E'' such that $\{E, E', E''\} = \{A, B, C\}$, we have D, E', E'' 3-distant, so Lemma 4.20 once again implies that every vertex in $L(D)$ is on c_3-distance at most 20 from $L(A) \cup L(B) \cup L(C)$ (or we are done by the second part of Lemma 4.20).

We distinguish the following cases.

- If $|D_1 - A_1| \leq 2, |D_2 - B_2| \leq 2$, then D, X, Y form a 3-distant set. Let us check this. We already have X, Y 2-distant. By triangle inequality, we obtain $|X_1 - D_1| \geq |X_1 - A_1| - |A_1 - D_1| \geq 3$, $|Y_1 - D_1| \geq |B_1 - A_1| - |B_1 - Y_1| - |D_1 - A_1| \geq 3$, $|D_2 - X_2| \geq |B_2 - A_2| - |B_2 - D_2| - |X_2 - A_2| \geq 3$ and $|Y_2 - D_2| \geq |Y_2 - B_2| - |B_2 - D_2| \geq 3$.

  We also know that $L(X) \cup L(Y)$ is contained in a subgraph $H \subset G[c_3]$ that is connected and of diameter at most 20, so applying Lemma 4.20 implies that we are done, unless $G[L(D) \cup L(X) \cup L(Y), c_3]$ is connected and of diameter at most 20. Hence $L(D)$ is on c_3-distance at most 40 from $L(A) \cup L(B) \cup L(C)$.

- If $|D_1 - C_1| \leq 2, |D_2 - B_2| \leq 2$, then the same argument we had in the case above proves that $L(D)$ is on c_3-distance at most 40 from $L(A) \cup L(B) \cup L(C)$.

- If $|D_1 - A_1| \leq 2, |D_2 - C_2| \leq 2$, then the same argument we had in the case above proves that $L(D)$ is on c_3-distance at most 40 from $L(A) \cup L(B) \cup L(C)$.

Finally, we define $P_1, P_2, P_3 \subset P$ as

$$P_1 = \{D \in P \colon |D_1 - B_1|, |D_2 - A_2| \leq 2\}$$
$$P_2 = \{D \in P \colon |D_1 - C_1|, |D_2 - A_2| \leq 2\}$$
$$P_3 = \{D \in P \colon |D_1 - B_1|, |D_2 - C_2| \leq 2\}$$

which are disjoint and if $D \in P \setminus (P_1 \cup P_2 \cup P_3)$ we know that $L(D)$ is on c_3-distance at most 40 from $L(A) \cup L(B) \cup L(C)$. Let also $L_i = \cup_{D \in P_i} L(D)$. Hence, since for $D \in P_1$ we have $|D_1 - C_1|, |D_2 - C_2| \geq 2$, all edges between $L(D)$ and $L(C)$ are coloured using c_3 and c_4, we actually have all edges between L_1 and $L(C)$ coloured using only these two colours. Applying Lemma 4.10 we have $G[L_1 \cup L(C), c]$ connected and of diameter at most 10 for some $c \in \{c_3, c_4\}$, or L_1 is on c_3-distance 1 from $L(A) \cup L(B) \cup L(C)$. Similarly, all edges between L_2 and Y, and all edges between L_3 and X only take the colours c_3 and c_4. Observe that if $D \in P_2, D' \in P_3$ then $|D_1 - D_1'| \geq |C_1 - B_1| - |C_1 - D_1| - |D_1' - B_1| \geq 3$. Similarly, $|D_2 - D_2'| \geq |A_2 - C_2| - |A_2 - D_2| - |D_2' - C_2| \geq 3$, so all edges between L_2 and L_3 are only of colours c_3 and c_4. Apply Lemma 4.10 to L_2 and $L(Y)$, implying that either $G[L_2 \cup L(Y), c_4]$ is connected and of diameter at most 10, or L_2 is on c_3-distance at most 30 from $L(A) \cup L(B) \cup L(C)$. Similarly, apply Lemma 4.10 to L_3 and $L(X)$, implying that either $G[L_3 \cup L(X), c_4]$ is connected and of diameter at most 10, or L_3 is on c_3-distance at most 30 from $L(A) \cup L(B) \cup L(C)$. Finally, let $V = \{v \in [n] \colon d_{c_3}(v, L(A) \cup L(B) \cup L(C)) \leq 40\}$, which is c_3-connected and of c_3-diameter at most 100. We distinguish the following cases.

- $L_2, L_3 \subset V$. In this case, we can take V and $G[L_1 \cup L(C), c]$ if necessary (otherwise $L_1 \subset V$).

- $L_2 \not\subset V, L_3 \subset V$. Thus, $G[L_2 \cup L(Y), c_4]$ is connected and of diameter at most 10, so taking $G[L_2 \cup L(Y), c_4]$ and V, and additionally $G[L_1 \cup L(C), c]$ if necessary, we are done.

- $L_2 \subset V, L_3 \not\subset V$. Thus, $G[L_3 \cup L(X), c_4]$ is connected and of diameter at most 10, so taking $G[L_3 \cup L(X), c_4]$ and V, and additionally $G[L_1 \cup L(C), c]$ if necessary, we are done.

- $L_2, L_3 \not\subset V$. In this case, we have $G[L_2 \cup L(Y), c_4]$ and $G[L_3 \cup L(X), c_4]$ connected and of diameter at most 10. Apply Lemma 4.10 to L_2 and L_3. If L_2 and L_3 are on c_4-distance at most 10, we may take $G[L_2 \cup L_3 \cup L(X) \cup L(Y), c_4]$, V and $G[L_1 \cup L(C), c]$ if necessary. Otherwise, we have $G[L_2 \cup L_3, c_3]$ is connected and of diameter at most 10. In this case, take $G[L_2 \cup L_3, c_3], V$ and $G[L_1 \cup L(C), c]$ if necessary.

This completes the proof of the lemma. □

Let us now briefly discuss a way of defining c_3, c_4-layer mappings. Pick two colours $c_1, c_2 \in [4]$, and take c_3, c_4 to be the remaining two colours. List all the vertices as $v_1, v_2, \ldots, v_n$. To each vertex, we shall assign two nonnegative integers, $D_1(v_i)$ and $D_2(v_i)$, initially marked as undefined. We apply the following procedure.

Step 1 Pick the smallest index i such that $D_1(v_i)$ or $D_2(v_i)$ is undefined. If there is no such i, terminate the procedure.

Step 2 For $j = 1, 2$, if $D_j(v_i)$ is undefined, pick an arbitrary value for it.

Step 3 For $j = 1, 2$, if $D_j(v_i)$ was undefined before the second step, for all vertices u in the same c_j-component of v_i set $D_j(u) := d_{c_j}(v_i, u) + D_j(v_i)$. Return to Step 1.

Upon the completion of the procedure, set $P = \{(D_1(v), D_2(v)) : v \in [n]\}$ and $L: P \to \mathcal{P}(n)$ as $L(x, y) := \{v \in [n] : (D_1(v), D_2(v)) = (x, y)\}$.

Claim. The mapping L above is well-defined and is a c_3, c_4-layer mapping.

Proof. Observe that each time we pick v_i whose one or two values are to be defined, we end up defining D_1 on one c_1-component or D_2 on one c_2-component or both. Hence, for every vertex v, the values $D_1(v), D_2(v)$ change precisely once from undefined to a nonnegative integer value. Thus, $(D_1(v), D_2(v))$ are well-defined and take values in $\mathbb{N}_0^2$, so P and L are well-defined and $L(A)$ forms a partition of $[n]$ as A ranges over P. Finally, consider an edge xy coloured by c_1. Let $D_1(x)$ be defined with v_i chosen in Step 2 (possibly $x = v_i$). Since xy is of colour c_1, these are in the same c_1-component, and hence $D_1(x) = d_{c_1}(v_i, x) + D_1(v_i)$ and $D_1(y) = d_{c_1}(v_i, y) + D_1(v_i)$. Therefore,

$$\begin{aligned}|D_1(x) - D_1(y)| &= |(d_{c_1}(v_i, x) + D_1(v_i)) - (d_{c_1}(v_i, y) + D_1(v_i))| \\ &= |d_{c_1}(v_i, x) - d_{c_1}(v_i, y)| \\ &\leq d_{c_1}(x, y) = 1\end{aligned}$$

hence, if $\chi(xy) = c_1$, then $|D_1(x) - D_1(y)| \leq 1$. Similarly, we get the corresponding statement for the colour c_2. It follows that if $A, B \in P$ are such that $|A_1 - B_1|, |A_2 - B_2| \geq 2$, then if $x \in L(A), y \in L(B)$, we have $(D_1(x), D_2(x)) = A, (D_1(y), D_2(y)) = B$, so xy is coloured by c_3 or c_4, as desired. □

4.4.1 Monochromatically connected case

Proposition 4.23. *Suppose that χ is a 4-colouring of $E(K_n)$ such that every colour induces a connected subgraph of K_n. Then χ satisfies Conjecture 4.6 with constant 160.*

Proof. Suppose contrary, in particular every colour has diameter greater than 160. Our main goal in the proof is to find a pair of vertices x', y' with a control over their 1-distance and 2-distance. We need both distances sufficiently large so that we can make a use of distant sets in 3, 4-layer mappings, and also bounded by a constant so that if a vertex is on small 1-distance from x', it is also on small 1-distance from y' and vice-versa. More precisely,

Lemma 4.24. *Suppose that there are vertices x', y' such that $d_1(x', y') \in \{6, 7, \ldots, 50\}$, $d_2(x', y') \in \{10, 11, \ldots, 20\}$. Then we obtain a contradiction.*

Proof. Pick any point $z \neq x', y'$. Apply the procedure for defining 3, 4-layer mapping starting from x'. If we obtain a 7-distant set of size at least 3, we obtain a contradiction with Lemma 4.22. Hence, the distances corresponding to

x', y', z cannot give such a set, so we must have one of

$$\begin{aligned} d_1(x', z) &\leq 6, \text{ or,} \\ |d_1(x', y') - d_1(x', z)| &\leq 6, \text{ or,} \\ d_2(x', z) &\leq 6, \text{ or,} \\ |d_2(x', z) - d_2(x', y)| &\leq 6. \end{aligned}$$

In particular, we must have $d_1(x', z) \leq 56$ or $d_2(x', z) \leq 26$. Recalling the definition of monochromatic balls, $B_1(x, 56)$ and $B_2(x, 26)$ cover all the vertices, giving a contradiction. □

Claim. There are x, y such that $d_1(x, y) \in \{25, 26, 27\}$ and $d_2(x, y) \geq 40$.

Proof of the claim. Suppose contrary, for every x, y such that $d_1(x, y) \in \{25, 26, 27\}$, we must have $d_2(x, y) \leq 39$. Pick any $y_1, y_2 \in [n]$ such that $\chi(y_1 y_2) = 1$. Since the 1-diameter is greater than 160, we can find $x \in [n]$ such that $d_1(x, y_1) = 26$. By triangle inequality, we also have $d_1(x, y_2) \in \{25, 26, 27\}$. Hence, $d_2(x, y_1), d_2(x, y_2) \leq 39$, from which we conclude that whenever an edge $y_1 y_2$ is coloured by 1, then $d_2(y_1, y_2) \leq 78$. Hence, taking any $x \in [n]$ the balls

$$B_2(x, 78), B_3(x, 1), B_4(x, 1)$$

cover the vertex set. However, these have diameter less than 160, which is a contradiction. □

Take x, y given by the claim above. Since the subgraph $G[2]$ is connected, there is a minimal 2-path $x = z_0, z_1, \ldots, z_r, z_{r+1} = y$ between x and y, with $r \geq 39$. Look at the vertices $z_{10}, z_{20}, \ldots, z_{10k}$ with k such that $10 \leq r - 10k < 20$. Consider x, y, z_{10i} for some $1 \leq i \leq k$ and check whether we can define $3, 4$-layer mapping so that these three points become a 7-distant set. Apply the procedure for defining $3, 4$-layers mapping, starting from x, i.e. we want to see whether $(0, 0), (d_1(x, y), d_2(x, y))$ and $(d_1(x, z_{10i}), d_2(x, z_{10i}))$ are 7-distant. If they are 7-distant, Lemma 4.22 gives us a contradiction. Since

$$\begin{aligned} d_1(x, y) \geq 25, d_2(x, y) &\geq 39 \\ 10 \leq d_2(x, z_{10i}) = 10i \leq 10k &< d_2(x, y) - 6 \end{aligned}$$

we must have either $d_1(x, z_{10i}) \leq 6$ or $|d_1(x, z_{10i}) - d_1(x, y)| \leq 6$ (implying $d_1(x, z_{10i}) \in \{19, 20, \ldots, 33\}$). Similarly, if we start from y instead of x in our procedure, we see that either $d_1(y, z_{10i}) \leq 6$ or $|d_1(y, z_{10i}) - d_1(x, y)| \leq 6$ (implying $d_1(y, z_{10i}) \in \{19, 20, \ldots, 33\}$) must hold.

Observe that for the vertex z_{10} we must have $d_1(x, z_{10}) \leq 6$. Otherwise, we would have $19 \leq d_1(x, z_{10}) \leq 33$ and $d_2(x, z_{10}) = 10$, resulting in a contradiction by Lemma 4.24 (applied to the pair x, z_{10}). For every z_{10i} we must have either the first inequality ($d_1(x, z_{10i}) \leq 6$) or the second ($19 \leq d_1(x, z_{10i}) \leq 33$), and we have that the first vertex among these, namely z_{10}, satisfies the first inequality. Suppose that there was an index i such that $z_{10(i+1)}$ obeys the second inequality, and pick the smallest such i. Then, by the triangle inequality, we would have

$$\begin{aligned} 13 &\leq d_1(z_{10(i+1)}, x) - d_1(x, z_{10i}) \leq d_1(z_{10i}, z_{10(i+1)}) \\ &\leq d_1(z_{10(i+1)}, x) + d_1(x, z_{10i}) \leq 39 \end{aligned}$$

and $d_2(z_{10i}, z_{10(i+1)}) = 10$, so Lemma 4.24 applies now to the pair $z_{10i}, z_{10(i+1)}$ and gives a contradiction. Hence, for all $i \leq k$ we must have the first inequality for z_{10i}. But then z_{10k} and y satisfy the conditions of Lemma 4.24, giving the final contradiction, since $10 \leq d_2(y, z_{10k}) < 20$ and

$$19 \leq d_1(y, x) - d_1(x, z_{10k}) \leq d_1(y, z_{10k}) \leq d_1(y, x) + d_1(x, z_{10k}) \leq 33.$$

This completes the proof. □

4.4.2 Intersecting monochromatic components

Proposition 4.25. *Suppose that $\chi\colon E(K_n) \to [4]$ is a 4-colouring with the property that, whenever C and C' are monochromatic components of different colours, and one of them has diameter at least 30 (in the relevant colour), then C and C' intersect. Then χ satisfies Conjecture 4.6 with constant 160.*

Proof. Suppose contrary, we have a colouring χ that satisfies the assumptions but for which the conclusion fails. By Lemma 4.19, we know that at least two colours have monochromatic diameters greater than 160. Let C_1 be such a component for colour c_1, and let C_2 be such a component for colour c_2, with $c_1 \neq c_2$. Further, by Proposition 4.23 we have a colour c' (which might equal one of c_1, c_2) with at least two components, w.l.o.g. $c_1 \neq c'$.

First, we find a pair of vertices x, y with the property that $10 \leq d_{c_1}(x, y) \leq 40$ and x, y are in different c'-components. We do this as follows. If there are a couple of vertices x_1, x_2 with $d_{c_1}(x_1, x_2) < 10$ that are in different c'-components, then, since c_1-diameter of C_1 is large, we can find $y \in C_1$ with $d_{c_1}(x_1, y) = 25$. Hence, $15 \leq d_{c_1}(x_2, y) \leq 35$, and y is in different c'-component from one of x_1, x_2, yielding the desired pair. Otherwise, we have that all pairs of vertices $x, y \in C_1$ with $d_{c_1}(x, y) \leq 30$ also share the same c'-component. But then, we must have the whole c_1-component C_1 contained in one c'-component, making it unable to intersect other c'-components, which is impossible. Hence, we have x, y in different c'-components, with $10 \leq d_{c_1}(x, y) \leq 40$.

Pick any vertex z outside $B_{c_1}(x, 50)$. Let c'', c''' be the two colours different from c_1, c'. We now apply our procedure for defining c'', c'''-layers mapping with vertices listed as $x, y, z, \ldots$. Note that $|D_1(x) - D_1(y)|, |D_1(x) - D_1(z)|, |D_1(y) - D_1(z)| \geq 10$ (recall the D_1, D_2 notation from the procedure). Hence, we get a 7-distant set, unless $d_{c'}(x, z) \leq 6$ or $d_{c'}(y, z) \leq 6$. Therefore, $B_{c_1}(x, 50)$, $B_{c'}(x, 6)$ and $B_{c'}(y, 6)$ cover the vertex set and we get a contradiction. $\square$

4.4.3 Final steps

In the final part of the proof, we show how to reduce the general case to the case of intersecting monochromatic components.

Theorem 4.26. *Conjecture 4.6 holds for 4 colours and we may take 160 for the diameter bounds.*

Proof. Let χ be the given 4-colouring of $E(K_n)$. Our goal is to apply Proposition 4.25. We start with an observation.

Observation 4.27. *Suppose that C is a c-component, which is disjoint from a c'-component C' with $c' \neq c$. Then for every pair of vertices $x, y \in C$ we have $d_c(x, y) \leq 6$ or $d_{c'}(x, y) \leq 6$, or the colouring satisfies Conjecture 4.6 with the constant 160.*

Proof of Observation 4.27. Pick $x, y \in C$ with $d_c(x, y) \geq 7$ and take arbitrary $z \in C'$. Apply our procedure for generating c_3, c_4-layers mapping to the list $x, y, z, \ldots$, with c_3, c_4 chosen to be the two colours different from c, c'. Since

z is in different c- and c'-components from x, y, these three vertices result in a 7-distant set, unless $d_{c'}(x, y) \leq 6$, as desired. $\square$

Proof of Observation 4.27. Pick $x, y \in C$ with $d_c(x, y) \geq 7$ and take arbitrary $z \in C'$. Apply our procedure for generating c_3, c_4-layers mapping to the list $x, y, z, \ldots$, with c_3, c_4 chosen to be the two colours different from c, c'. Since z is in different c- and c'-components from x, y, these three vertices result in a 7-distant set, unless $d_{c'}(x, y) \leq 6$, as desired. $\square$

Corollary 4.28. *Suppose that we have a c-component C, which is disjoint from a c'-component C' with $c' \neq c$ and has c-diameter at least 30. Then the colouring χ satisfies Conjecture 4.6 with the constant 160.*

Proof. By Observation 4.27 we are either done, or any two vertices $x, y \in C$ with $d_c(x, y) > 6$ satisfy $d_{c'}(x, y) \leq 6$. Furthermore, given any two vertices $x, y \in C$, since the c-diameter of C is at least 30, we can find $z \in C$ such that $d_c(x, z), d_c(y, z) \geq 7$, so by triangle inequality $d_{c'}(x, y) \leq 12$ holds for all $x, y \in C$.

Now, take an arbitrary vertex $v \in C$, let c'', c''' be the two remaining colours, and consider the sets

$$B_{c'}(v, 12), B_{c''}(v, 1), B_{c'''}(v, 1).$$

Given any $u \in [n]$, if vu is coloured by any of c', c'' or c''', it is already in the sets above. On the other hand, if uv is of colour c, then $v \in C$ so $d_{c'}(u, v) \leq 10$, thus $u \in B^{(c')}(v, 10)$. Thus, these sets cover the vertex sets and have monochromatic diameters at most 24, so we are done. $\square$

Finally, we are in the position to apply Proposition 4.25 which finishes the proof of the theorem. $\square$

4.5 Concluding Remarks

Apart from the main conjectures 4.1 (and its equivalent 4.8) and 4.6, here we pose further questions. Recall the auxiliary results appearing in Section 4.2. In that section we first discussed Lemmas 4.10 and 4.11, which were variants

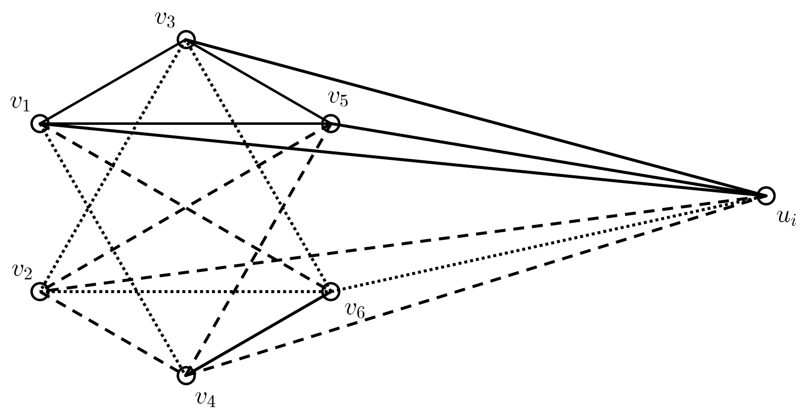


Figure 4.1: An example of 3-colouring of K_n with a matching of size 3 removed that cannot be covered by two monochromatic components.

of the main conjectures with different underlying graph instead of K_n. Recall that Lovasz-Ryser conjecture is also about different underlying graphs. Another natural question would be the following.

Question 4.29. *Let G be a graph, and let k be fixed. Suppose that $\chi\colon E(G) \to [k]$ is a k-colouring of the edges of G. For which G is it always possible to find $k-1$ monochromatically connected sets that cover the vertices of G? What bounds on their diameter can we take?*

Observe already that for 3 colours, the situation becomes much more complicated than that for 2 colours, where complete multipartite graphs behaved well. Consider the following example.

Pick $n+6$ vertices labeled as $v_1, v_2, \ldots, v_6$ and $u_1, u_2, \ldots, u_n$. Define the graph G to be the complete graph on these vertices from which 3 edges v_1v_2, v_3v_4 and v_5v_6 are removed. Define the colouring $\chi\colon E(G) \to [3]$ as follows.

- Edges of colour 1 are $v_1v_3, v_3v_5, v_1v_5, v_4v_6$ and v_1u_i, v_3u_i, v_5u_i for all i.
- Edges of colour 2 are $v_2v_4, v_2v_5, v_4v_5, v_1v_6$ and v_2u_i, v_4u_i for all i.
- Edges of colour 3 are $v_2v_3, v_2v_6, v_3v_6, v_1v_4$ and v_6u_i for all i.
- Edges of the form u_iu_j are coloured arbitrarily.

It is easy to check that this colouring has no covering of vertices by two monochromatic components. Is this essentially the only way the conjecture might fail for such a graph?

Question 4.30. *Let* $G = K_n \setminus \{e_1, e_2, e_3\}$ *be the complete graph with a matching of size three omitted. Suppose that* $\chi\colon E(G) \to [3]$ *is a 3-colouring of the edges such that no two monochromatic components cover* G*. Is such a colouring isomorphic to an example similar to the one above? What about* K_{2n} *with a perfect matching removed?*

Finally, recall that the one of the main contributions in the final bound in Theorem 4.7 came from Lemma 4.13 and that in general the Ramsey approach of Lemma 4.12 would give much worse value. It would be interesting to study the right bounds for this problem as well.

Question 4.31. *For fixed* l*, what is the maximal size of a set of vertices* S *of* G_l *such that* $G_l[S]$ *is a path? What about other families of graphs of bounded degree? In particular, for fixed* l *and* d*, what is the maximal size of a set of vertices* S *of* G_l *such that* $G_l[S]$ *is a connected graph whose degrees are bounded by* d*?*

5 Decomposing the Complete r-Graph

The work in this chapter is done in collaboration with Imre Leader and Ta Sheng Tan.

5.1 Introduction

The edge set of K_n, the complete graph on n vertices, can be partitioned into $n-1$ complete bipartite subgraphs: this may be done in many ways, for example by taking $n-1$ stars centred at different vertices. Graham and Pollak [21, 22] proved that the number $n-1$ cannot be decreased. Several other proofs of this result have been found, by Tverberg [53], Peck [42], and Vishwanathan [55, 56].

Generalising this to hypergraphs, for $n \geq r \geq 1$, let $f_r(n)$ be the minimum number of complete r-partite r-graphs needed to partition the edge set of $K_n^{(r)}$, the complete r-uniform hypergraph on n vertices (i.e., the collection of all r-sets from an n-set). Thus the Graham-Pollak theorem asserts that $f_2(n) = n-1$. For $r \geq 3$, an easy upper bound of $\binom{n-\lceil r/2\rceil}{\lfloor r/2\rfloor}$ may be obtained by generalising the star example above. Indeed, having ordered the vertices, consider the collection of r-sets whose $2^{\text{nd}}, 4^{\text{th}}, \ldots, (2\lfloor r/2\rfloor)^{\text{th}}$ vertices are fixed. This forms a complete r-partite r-graph, and the collection of all $\binom{n-\lceil r/2\rceil}{\lfloor r/2\rfloor}$ such is a partition of $K_n^{(r)}$. (There are many other constructions achieving the exact same value; see, for example Alon's recursive construction in [4].)

Alon [4] showed that $f_3(n) = n-2$. More generally, for each fixed $r \geq 1$, he showed that

$$\frac{2}{\binom{2\lfloor r/2\rfloor}{\lfloor r/2\rfloor}}(1+o(1))\binom{n}{\lfloor r/2\rfloor} \leq f_r(n) \leq (1-o(1))\binom{n}{\lfloor r/2\rfloor},$$

where the upper bound is from the construction above.

The best known lower bound for $f_r(n)$ was obtained by Cioabă, Küngden and

Verstraëte [12], who showed that $f_{2k}(n) \geq \frac{2\binom{n-1}{k}}{\binom{2k}{k}}$. For upper bounds for $f_r(n)$, the above construction is not sharp in general. Cioabă and Tait [13] showed that $f_6(8) = 9 < \binom{8-3}{3}$, and used this to give an improvement in a lower-order term, showing that $f_{2k}(n) \leq \binom{n-k}{k} - 2\left\lfloor \frac{n}{16} \right\rfloor \binom{\lfloor \frac{n}{2} \rfloor - k + 3}{k-3}$ for any $k \geq 3$. (We mention briefly that any improvement of $f_4(n)$ for any n will further improve the above upper bound. Indeed, one can check that $f_4(7) = 9 < \binom{7-2}{2}$, and this will imply that $f_r(n) \leq \binom{n - \lfloor r/2 \rfloor}{\lfloor r/2 \rfloor} - cn^{\lfloor r/2 \rfloor - 1}$ for some positive constant c. But note that, again, this is only an improvement to a lower-order term.)

Despite these improvements, the asymptotic bounds of Alon have not been improved. Perhaps the most interesting question was whether the asymptotic upper bound is the correct estimate.

Our aim here is to show that the asymptotic upper bound is not correct for each even $r \geq 4$. In particular, we will show that

$$f_4(n) \leq \frac{14}{15}(1 + o(1))\binom{n}{2},$$

and obtain the same improvement of $\frac{14}{15}$ for each even $r \geq 4$.

A key to our approach will be to consider a related question: what is the minimum number of (set-theoretic) products of complete bipartite graphs, that is, sets of the form $E(K_{a,b}) \times E(K_{c,d})$, needed to partition $E(K_n) \times E(K_n)$? There is an obvious guess, namely that we take the product of the complete bipartite graphs in the partitions of both K_ns. This gives a partition using $(n-1)^2$ products of complete bipartite graphs. But can we improve this? Writing $g(n)$ for the minimum value, it will turn out that, unlike for f_4, any improvement in the value of $g(n)$ for one n gives an asymptotic improvement for g as well. In this sense, this means that g is a 'better' function to investigate than f_4.

The plan of the chapter is as follows. In Section 5.2, we show how the function g is related to f_4, and give some related discussions. Then in Section 5.3, we investigate the simplest product of complete graphs: we attempt to partition the product set $E(K_3) \times E(K_n)$ into products of complete bipartite graphs. Although Section 5.3 is not strictly needed for our final bounds, it does provide several ideas and motivation for later work. In Section 5.4, we prove our main result on g and from this we deduce bounds on f_4. Finally, in Section 5.5, we mention some remarks and open problems.

We use standard graph and hypergraph language throughout the chapter. For an r-uniform hypergraph H, let $f_r(H)$ be the minimum number of complete r-partite r-uniform hypergraphs needed to partition the edge set of H. So $f_r\left(K_n^{(r)}\right)$ is just $f_r(n)$. A *minimal decomposition* of an r-graph H is a partition of the edge set of H into $f_r(H)$ complete r-partite r-graphs. A *block* is a (set-theoretic) product of the edge sets of two complete bipartite graphs. For graphs G and H, let $g(G,H)$ be the minimum number of blocks needed to partition the set $E(G)\times E(H)$. Thus $g(n)=g(K_n,K_n)$. Similarly, a *minimal decomposition* of $E(G)\times E(H)$ is a partition of the set into $g(G,H)$ blocks.

5.2 Products of complete bipartite graphs

We start by showing how g is related to f_4.

Proposition 5.1. *Let $\alpha>0$ be a constant. If $g(n)\le \alpha n^2$ for all n, then $f_4(n)\le \alpha(1+o(1))\frac{n^2}{2}$.*

Proof. We will show that

$$f_4(n)\le \alpha\binom{n^2}{2}+Cn\log n \tag{5.1}$$

for some sufficiently large C. This is clearly true for $n\le 4$. So assume $n>4$ and the inequality (5.1) holds for $1,2,\ldots,n-1$. We will consider the case when n is even; the case when n is odd is similar.

In order to decompose the edge set of $K_n^{(4)}$, we can split the n vertices into two equal parts, say $V\left(K_n^{(4)}\right)=A\cup B$, where $|A|=|B|=n/2$. The sets of 4-edges $\{e: e\subset A\}$ and $\{e: e\subset B\}$ can each be decomposed into $f_4(n/2)$ complete 4-partite 4-graphs; the sets of 4-edges $\{e: |e\cap A|=3\}$ and $\{e: |e\cap B|=3\}$ can each be decomposed into $f_3(n/2)$ complete 4-partite 4-graphs; while the remaining set of 4-edges $\{e: |e\cap A|=|e\cap B|=2\}$ can be decomposed into $g(n/2)$ complete 4-partite 4-graphs. So by the assumption of $g(n)$ and the induction hypothesis, we have

$$\begin{aligned}
f_4(n) &\le 2f_4(n/2) + g(n/2) + 2f_3(n/2) \\
&\le 2\left(\alpha\left(\frac{n^2}{8}\right) + \frac{Cn}{2}\log\left(\frac{n}{2}\right)\right) + \alpha\left(\frac{n}{2}\right)^2 + 2\left(\frac{n}{2} - 2\right) \\
&\le \alpha\left(\frac{n^2}{2}\right) + Cn\log n.
\end{aligned}$$

□

In the introduction to this chapter, we mentioned that any improvement in the upper bound of $f_4(n)$ from the easy upper bound of $\binom{n-2}{2}$, for one fixed n, will lead to an improvement for all (greater) values of n, but not an asymptotic improvement. However, very helpfully, this is not the case for g. Indeed, any improvement to $g(n)$ for one particular n leads to an asymptotic improvement. This is the content of the following simple proposition.

Proposition 5.2. *Suppose $g(K_a, K_b) < (a-1)(b-1)$ for some a and b. Then $g(n) \le \beta n^2$ for all n, for some constant $\beta < 1$.*

Proof. Suppose $g(K_a, K_b) = c < (a-1)(b-1)$ for some fixed a and b. Then, setting $\alpha = \frac{c}{(a-1)(b-1)}$, we will show that

$$g(K_{1+(a-1)i}, K_{1+(b-1)j}) \le \alpha((a-1)i)((b-1)j) = cij$$

for any $i, j \ge 1$. This will then imply that $g(1+(a-1)(b-1)k) \le \alpha((a-1)(b-1)k)^2$ for any $k \ge 1$, and hence

$$g(n) \le \alpha n^2 + Cn$$

for some constant C.

We proceed by induction on i. We will show the base case of $g(K_a, K_{1+(b-1)j}) \le cj$ by induction on j. The case $j = 1$ is true by assumption. So fix $j > 1$ and by induction, we have $g(K_a, K_{1+(b-1)(j-1)}) \le c(j-1)$.

Let $G = K_b$ be a subgraph of $K_{1+(b-1)j}$. Note that $K_{1+(b-1)j} - G$ (i.e., the graph $K_{1+(b-1)j}$ with the edges of G removed) is a blow-up of $K_{1+(b-1)(j-1)}$ by replacing one of its vertices with an empty graph on b vertices. So $g(K_a, K_{1+(b-1)j} -$

$G) = g(K_a, K_{1+(b-1)(j-1)}) \le c(j-1)$, implying

$$\begin{aligned} g(K_a, K_{1+(b-1)j}) &\le g(K_a, G) + g(K_a, (K_{1+(b-1)j} - G)) \\ &\le g(K_a, K_b) + c(j-1) \\ &\le cj. \end{aligned}$$

Now fix $i > 1$ and assume the theorem is true for $i - 1$. That is,

$$g(K_{1+(a-1)(i-1)}, K_{1+(b-1)j}) \le c(i-1)j$$

for all $j \ge 1$. To decompose $E(K_{1+(a-1)i}) \times E(K_{1+(b-1)j})$ for any fixed j, we first let $H = K_a$ and note that $K_{1+(a-1)i} - H$ is a blow-up of $K_{1+(a-1)(i-1)}$ by replacing one of its vertices with an empty graph on a vertices. Therefore,

$$\begin{aligned} g(K_{1+(a-1)i}, K_{1+(b-1)j}) &\le g(H, K_{1+(b-1)j}) + g((K_{1+(a-1)i} - H), K_{1+(b-1)j}) \\ &\le g(K_a, K_{1+(b-1)j}) + g(K_{1+(a-1)(i-1)}, K_{1+(b-1)j}) \\ &\le cj + c(i-1)j \\ &\qquad \text{(by the base case and induction hypothesis)} \\ &= cij. \end{aligned}$$

This completes the proof of the proposition. □

From Proposition 5.1 and Proposition 5.2, in order to improve the asymptotic upper bound on $f_4(n)$, it is enough to find a and b such that $g(K_a, K_b) < (a-1)(b-1)$.

The rest of this section is a digression (and so could be omitted if the reader wishes). The question of whether or not $g(n) = (n-1)^2$ has the flavour of a 'product' question. Indeed, it is an example of the following general question. Suppose we have a set X and a family $\mathcal{F}$ of some subsets of X, and we write $c(X, \mathcal{F})$ for the minimum number of sets in $\mathcal{F}$ needed to partition X. Is it true that $c(X \times Y, \mathcal{F} \times \mathcal{G}) = c(X, \mathcal{F})c(Y, \mathcal{G})$, where $\mathcal{F} \times \mathcal{G} = \{F \times G : F \in \mathcal{F}, G \in \mathcal{G}\}$?

This is certainly not *always* true. Indeed, for a simple example, let $X = \{1, 2, \ldots, 7\}$ and $\mathcal{F} = \{A \subset X : |A| = 1 \text{ or } 4\}$. Clearly, $c(X, \mathcal{F}) = 4$. But $X \times X$ can be partitioned into four 3 by 4 rectangles and a single point, giving $c(X \times X, \mathcal{F} \times \mathcal{F}) \le 13$.

However, there are a few cases where such a product theorem is known. For example, Alon, Bohman, Holzman, and Kleitman [5] proved that if X is a finite set of size at least 2, then any partition of X^n into proper boxes must consist of at least 2^n boxes. Here, a *box* is a subset of X^n of the form $B_1 \times B_2 \times \ldots \times B_n$, where each B_i is a subset of X. A box is *proper* if B_i is a proper subset of X for every i. Note that this corresponds to a product theorem where $\mathcal{F}$ is the family of all proper subsets of X. (There are also some related results by Ahlswede and Cai in [2, 3].)

Unfortunately, we have not been able to prove any product theorem that might relate to our problem about $g(n)$. Indeed, it seems difficult to extend the result of Alon, Bohman, Holzman, and Kleitman at all. For example, here are two closely related problems that we cannot solve.

A box is *odd* if its size is odd. Let X be a finite set such that $|X|$ is odd. We can partition X^n into 3^n odd proper boxes - can we do better?

Question 5.3. *Let X be a finite set such that $|X|$ is odd. Must any partition of X^n into odd proper boxes consist of at least 3^n boxes?*

We do not even see how to answer this question when $|X|= 5$.

A collection of proper boxes $B^{(1)}, B^{(2)}, \ldots, B^{(m)}$ of X^n is said to form a *uniform cover* of X^n if every point of X^n is covered the same number of times.

Question 5.4. *Let X be such that $|X|\geq 2$. Suppose $B^{(1)}, B^{(2)}, \ldots, B^{(m)}$ forms a uniform cover of X^n. Must we have $m \geq 2^n$?*

5.3 Decomposing $E(K_3) \times E(K_n)$

In this section, we investigate $g(K_3, K_n)$. As we know, we can decompose $E(K_3) \times E(K_n)$ using $2(n-1)$ blocks, and the question is whether we can improve this.

It turns out that the Graham-Pollak theorem actually gives some restriction on how small $g(K_3, K_n)$ can be. To be more precise, we will need a weighted version of the Graham-Pollak theorem. For the sake of completeness, we will include a proof here, although we stress that this is just a rewriting of the usual proof of the Graham-Pollak theorem.

Given a graph G and a real number α, we write $\alpha \cdot G$ for the weighted graph where each edge of G is given a weight of α. A collection of subgraphs $G_1, G_2, \ldots, G_m$ of K_n is a *weighted decomposition of* K_n if there exists real numbers $\alpha_1, \alpha_2, \ldots, \alpha_m$ such that for each edge e of K_n we have $\displaystyle\sum_{i:e\in G_i} \alpha_i = 1$. Note that the coefficients α_i are allowed to be negative.

Theorem 5.5. *The minimum number of complete bipartite graphs needed to form a weighted decomposition of K_n is $n-1$.*

Proof. Let the vertex set of K_n be $V = \{1, 2, \ldots, n\}$ and associate each vertex i with a real variable x_i. Let G be a complete bipartite subgraph of K_n with vertex classes X and Y. Then we can define $Q(G) = L(X) \cdot L(Y)$, where $L(A) = \sum_{i\in A} x_i$ for any subset $A \subset V$.

Suppose the bipartite graphs $G_k, 1 \leq k \leq q$ with vertex classes X_k and Y_k form a weighted decomposition of K_n. Then we must have

$$\sum_{i<j} x_i x_j = \sum_{k=1}^{q} \alpha_k L(X_k) L(Y_k)$$

for some real $\alpha_1, \alpha_2, \ldots, \alpha_q$. Rewriting the left-hand-side of the above equation, we have

$$\left(\sum_{i=1}^{n} x_i\right)^2 - \sum_{i=1}^{n} x_i^2 = 2\sum_{k=1}^{q} \alpha_k L(X_k) L(Y_k).$$

It follows that the linear subspace of $\mathbb{R}^n$ determined by the $q+1$ linear equations $\sum_{i=1}^{n} x_i = 0$ and $L(X_i) = 0, 1 \leq i \leq q$, must be the zero subspace. Hence $q + 1 \geq n$. $\square$

Proposition 5.6. *For $n \geq 2$ we have*

$$\frac{9}{5}(n-1) \leq g(K_3, K_n) \leq 2(n-1).$$

Proof. The upper bound has been explained already. For the lower bound, suppose the blocks $H_1, H_2, \ldots, H_q$ form a decomposition of $E(K_3) \times E(K_n)$. Then for each edge $e \in E(K_n)$, restricting the decomposition to the subset $E(K_3) \times e$, one of the following happens: either the three elements of $E(K_3) \times e$ decompose into three different H_i, or else two of the sets are in the same H_i for some i and the third set is in H_j for some $j \neq i$.

Let G_0 be the subgraph of K_n spanned by the set of e such that the first of these happens, and G_1, G_2, G_3 be the subgraphs of K_n spanned by the set of e for each of the three possible ways for the second case to happen, respectively. Thus in total we have

$$q \geq f_2(G_1) + f_2(G_2) + f_2(G_3) + f_2(G_0 \cup G_1) + f_2(G_0 \cup G_2) + f_2(G_0 \cup G_3). \quad (5.2)$$

Now, since G_0, G_1, G_2, G_2 form a partition of the edge set of K_n, we must have

$$f_2(G_i) + f_2(G_j) + f_2(G_0 \cup G_k) \geq n - 1 \quad (5.3)$$

for any $\{i, j, k\} = \{1, 2, 3\}$. Next, note that $1 \cdot (G_0 \cup G_i), 1 \cdot (G_0 \cup G_j), (-1) \cdot (G_0 \cup G_k), 2 \cdot G_k$ form a weighted decomposition of K_n for any $\{i, j, k\} = \{1, 2, 3\}$, so by Theorem 5.5, we must have

$$f_2(G_0 \cup G_1) + f_2(G_0 \cup G_2) + f_2(G_0 \cup G_3) + f_2(G_i) \geq n - 1 \quad (5.4)$$

for any $i = 1, 2, 3$.

Let $x = \frac{1}{3}(f_2(G_1) + f_2(G_2) + f_2(G_3))$ and $y = \frac{1}{3}(f_2(G_0 \cup G_1) + f_2(G_0 \cup G_2) + f_2(G_0 \cup G_3))$. Summing over different $\{i, j, k\}$ for inequality (5.3), we get $2x + y \geq n - 1$; while summing over different i for inequality (5.4), we get $x + 3y \geq n - 1$. This implies that $x + y \geq \frac{3}{5}(n - 1)$, and together with inequality (5.2), we conclude that

$$\begin{aligned} & q \geq 3x + 3y, \\ \text{i.e.} \quad & q \geq \frac{9}{5}(n - 1). \end{aligned}$$

□

Note that for any partition of K_n into G_0, G_1, G_2, G_3, we do obtain that $g(K_3, K_n)$ is at most the right-hand-side of (5.2).

We believe that the only restriction on $g(K_3, K_n)$ should be the restriction coming from the Graham-Pollak theorem, namely that $g(K_3, K_n) \geq \frac{9}{5}(n - 1)$. However, we have been unable to find any decomposition of $E(K_3) \times E(K_n)$ into fewer than $2(n - 1)$ blocks.

Question 5.7. *Does there exist a constant $\alpha < 2$ such that $g(K_3, K_n) \leq (\alpha + o(1))n$? In particular, can we take $\alpha = \frac{9}{5}$?*

5.4 Decomposing $E(K_4) \times E(K_n)$

The aim of this section is to find some a, b in which $E(K_a) \times E(K_b)$ can be partitioned into fewer than $(a-1)(b-1)$ blocks. In the previous section, we looked at decompositions of $E(K_3) \times E(K_n)$ by considering all the four possible ways to decompose $E(K_3)$ into complete bipartite graphs - this induced four subgraphs that partitioned the edge set of K_n.

Now, those decompositions of K_3 involved three 'large' complete bipartite subgraphs (namely, the copies of $K_{1,2}$), which between them form a 2-cover of K_3 (each edge of K_3 is in exactly two of them). However, this is in a sense 'wasteful', as by the Graham-Pollak theorem, we might expect to find a uniform cover by three 'large' complete bipartite subgraphs of K_4, rather than K_3.

This suggests that we should look at $E(K_4) \times E(K_n)$ instead of $E(K_3) \times E(K_n)$. It also suggests that, in each $E(K_4) \times e$, we do not allow *any* decomposition of K_4, but just four decompositions of K_4, three of which involve a 'large' complete bipartite subgraph and the fourth of which consists of single edges. More precisely, the first three decompositions of K_4 that we allow here are such that each consists of a 4-cycle and two independent edges. The three pairs of independent edges from these decompositions in turn form another decomposition of K_4 (into six complete bipartite graphs, each of which is a single edge).

Let C_1, C_2, C_3 be the three different 4-cycles of K_4 and let G_0, G_1, G_2, G_3 be the subgraphs of K_n (as in Proposition 5.6) whose edge sets partition the edge set of K_n. Then the sets $E(C_1) \times E(G_1), E(C_2) \times E(G_2), E(C_3) \times E(G_3), E(K_4 - C_1) \times E(G_0 \cup G_1), E(K_4 - C_2) \times E(G_0 \cup G_2), E(K_4 - C_3) \times E(G_0 \cup G_3)$ form a partition of $E(K_4) \times E(K_n)$. So $E(K_4) \times E(K_n)$ can be decomposed into

$$f_2(G_1) + f_2(G_2) + f_2(G_3) + 2f_2(G_0 \cup G_1) + 2f_2(G_0 \cup G_2) + 2f_2(G_0 \cup G_3)$$

blocks.

By the same argument as in Proposition 5.6, we have the following.

Proposition 5.8. *For $n \geq 2$, we have*

$$\frac{12}{5}(n-1) \leq g(K_4, K_n) \leq 3(n-1).$$

Again, it seems plausible that the only constraint on $g(K_4, K_n)$ is the one coming from the Graham-Pollak theorem.

Conjecture 5.9. $g(K_4, K_n) = \frac{12}{5}(1 + o(1))n$.

While we are unable to resolve this conjecture, we *are* able to find an example with $g(K_4, K_n) < 3(n-1)$. We start by observing that $G_0 \cup G_1, G_0 \cup G_2, G_0 \cup G_3$ form an *odd cover* of K_n (each edge of K_n appears an odd number of times). Now, it is known (see, e.g., [44]) that K_8 has an odd cover with four complete bipartite graphs. Indeed, the four $K_{3,3}$s with vertex classes $V_1 = \{1,3,5\} \cup \{2,4,6\}, V_2 = \{1,4,7\} \cup \{2,3,8\}, V_3 = \{2,5,7\} \cup \{1,6,8\}$ and $V_4 = \{3,6,7\} \cup \{4,5,8\}$ respectively form an odd cover of K_8. If we break the symmetry by deleting two vertices (vertices 6 and 8) from this odd cover of K_8, we obtain an odd cover of K_6 by four complete bipartite graphs, two of which are now disjoint. The union of these two disjoint complete bipartite graphs, together with the other two complete bipartite graphs, will be our $G_0 \cup G_1, G_0 \cup G_2, G_0 \cup G_3$. Remarkably, this does give rise to a decomposition of $E(K_4) \times E(K_6)$ into fewer than 15 blocks.

Proposition 5.10. *The set $E(K_4) \times E(K_6)$ can be decomposed into 14 blocks. In other words, $g(K_4, K_6) \leq 14 < (4-1)(6-1)$.*

Proof. Let G_0, G_1, G_2, G_3 be graphs that form a decomposition of K_6, defined as follows:

$$\begin{aligned}
&E(G_0) = \{12, 34\},\\
&E(G_0 \cup G_1) = \{ij : i \in \{1,3,5\}, j \in \{2,4\}\},\\
&E(G_0 \cup G_2) = \{ij : i \in \{1,4,6\}, j \in \{2,3\}\},\\
&E(G_0 \cup G_3) = \{ij : i \in \{3,6\}, j \in \{4,5\}\} \cup \{12, 15, 16\}.
\end{aligned}$$

By construction, we have $f_2(G_0 \cup G_1) = f_2(G_0 \cup G_2) = 1$, and $f_2(G_0 \cup G_3) = 2$, and a quick check shows that $f_2(G_1) = f_2(G_2) = f_2(G_3) = 2$. So from the discussion above we have

$$g(K_4, K_6) \leq \sum_{i=1}^{3} \left(f_2(G_i) + 2f_2(G_0 \cup G_i)\right) = 14.$$

□

Combining Proposition 5.1, Proposition 5.2 and Proposition 5.10, we obtain our main result.

Theorem 5.11. $f_4(n) \leq \frac{14}{15}(1 + o(1))\binom{n}{2}$.

5.5 Remarks and open problems

Proposition 5.10 (together with Proposition 5.2) implies that $g(n) \le \frac{14}{15}(1 + o(1))n^2$. We do not believe $\frac{14}{15}$ is the correct constant, but we are not able to improve it. What about a lower bound of $g(n)$? From Proposition 5.1, we know that if $g(n) = \alpha n^2(1 + o(1))$, then we have $f_4(n) \le \alpha(1 + o(1))\binom{n}{2}$. So we must have $\alpha \ge \frac{1}{3}$ from Alon's result on the lower bound of $f_4(n)$.

Here, we are able to give a small improvement, namely $\alpha \ge \frac{1}{2}$. For this, we will need a result by Reznick, Tiwari, and West [45] on decomposing tensor products of graphs into bipartite graphs. Recall that the tensor product $G * H$ of two graphs G and H has vertex set $\{(u, v) : u \in V(G), v \in V(H)\}$ with $(u_1, v_1) \sim (u_2, v_2)$ if and only if $u_1 \sim u_2$ in G and $v_1 \sim v_2$ in H.

Theorem 5.12 ([45]). *The minimum number of complete bipartite graphs needed to partition the edge set of $K_n * K_n$ is $(n-1)^2 + 1$.*

Proposition 5.13. *For $n \ge 2$, we have $g(n) \ge \left\lceil \frac{(n-1)^2+1}{2} \right\rceil$.*

Proof. Suppose we can decompose $E(K_n) \times E(K_n)$ into q blocks. For each of such blocks (say the parts from the left K_n are X_1, X_2 and the parts from the right K_n are Y_1, Y_2), we construct two complete bipartite graphs G_1 and G_2 as follows. The vertex classes of G_1 are $\{(x, y) : x \in X_1, y \in Y_1\}$ and $\{(x, y) : x \in X_2, y \in Y_2\}$; while the vertex classes of G_2 are $\{(x, y) : x \in X_1, y \in Y_2\}$ and $\{(x, y) : x \in X_2, y \in Y_1\}$.

Observe that these $2q$ complete bipartite graphs partition the edge set of the tensor product $K_n * K_n$. So by Theorem 5.12, we must have

$$q \ge \left\lceil \frac{(n-1)^2 + 1}{2} \right\rceil.$$

□

In general, for any fixed k, can we improve the upper bound of $(k-1)(n-1)$ on $g(K_k, K_n)$ in a manner similar to what we have considered for $k = 3$ and $k = 4$? It seems that perhaps there is no K_k having a 'better' allowed sets of decompositions than the four allowed decompositions of K_4 that we used in Section 5.4. If this is correct, perhaps $\frac{4}{5}$ is the right constant even for $g(n)$.

Question 5.14. *Is it true that $g(n) = \frac{4}{5}(1 + o(1))n^2$?*

Finally, let us turn our attention to the function f_r for $r > 4$. For fixed $r \geq 1$, let α_r be the smallest α such that $f_r(n) \leq \alpha(1 + o(1))\binom{n}{\lfloor r/2 \rfloor}$. Thus the initial construction gives $\alpha_r \leq 1$ for all r, while Theorem 5.11 says that $\alpha_4 \leq \frac{14}{15}$. This implies that $\alpha_r \leq \frac{14}{15}$ for all even r.

Theorem 5.15. *For each fixed $k \geq 2$, we have*

$$f_{2k}(n) \leq \frac{14}{15}(1 + o(1))\binom{n}{k}.$$

Proof. We use induction on k. By Theorem 5.11, the result is true for the base case $k = 2$. For larger k, the result is an easy consequence of the following inequality:

$$f_{2k+2}(n) \leq f_{2k}(n-2) + f_{2k}(n-3) + \ldots + f_{2k}(2k).$$

This inequality is obtained by ordering the n vertices and observing that the set of $(2k+2)$-edges whose second vertex is i, for any fixed $i \in \{2, 3, \ldots, n-2k\}$, may be decomposed into $f_{2k}(n-i)$ complete $(2k+2)$-partite $(2k+2)$-graphs. □

We do not see how to obtain a bound below 1 for α_r for r odd. But actually we would expect the following to be true.

Conjecture 5.16. *We have $\alpha_r \to 0$ as $r \to \infty$.*

To prove this, it would be sufficient to show that $\alpha_5 < 1$. Indeed, suppose $f_5(n) \leq (\alpha + o(1))\binom{n}{2}$ for some $\alpha < 1$. Let $r = 6k - 1$ and order the n vertices. We can decompose the complete r-graph on n vertices by considering the set of r-edges whose 6th, 12th, $\ldots, 6(k-1)$th are $i_1, i_2, \ldots, i_{k-1}$ respectively, where $i_1 \geq 6$ and $i_{k-1} \leq n-5$ and $i_j - i_{j-1} \geq 6$ for $2 \leq j \leq k-1$. For each such fixed $i_1, i_2, \ldots, i_{k-1}$, these r-edges can be decomposed into $f_5(i_1 - 1)f_5(i_2 - i_1 - 1)\ldots f_5(i_{k-1} - i_{k-2} - 1)f_5(n - i_{k-1})$ complete r-partite r-graphs. Summing over all possible choices of $i_1, i_2, \ldots, i_{k-1}$, we deduce that $f_{6k-1}(n) \leq (\alpha^k + o(1))\binom{n}{3k-1}$.

Annoyingly, we do not see how to use any of our arguments about f_4 for f_5.

Question 5.17. *Is $\alpha_5 < 1$? In other words, do we have $f_5(n) \leq (\alpha + o(1))\binom{n}{2}$ for some $\alpha < 1$?*

Part III

Combinatorics on Algebraic Structures

6 Points in Almost General Position

6.1 Introduction

A set of points in the plane is said to be *in general position* if it has no 3 collinear points, and *in almost general position* if there are no 4 collinear points. Let $\alpha(n)$ be the maximum k such that any set of n points in the plane in almost general position has k points in general position. In [15], Erdős asked for an improvement of the (easy) bounds $\sqrt{2n-1} \leq \alpha(n) \leq n$ (see equation (13) in the paper). This was done by Füredi [17], who proved $\Omega(\sqrt{n \log n}) \leq \alpha(n) \leq o(n)$.

In [11] Cardinal, Tóth and Wood considered the problem in $\mathbb{R}^3$. Firstly, let us generalize the notion of general position. A set of points in $\mathbb{R}^d$ is said to be in general position if there are no $d+1$ points on the same hyperplane, and in almost general position if there are no $d+2$ points on the same hyperplane. Let $\alpha(n,d)$ stand for the maximum integer k such that all sets of n points in $\mathbb{R}^d$ in almost general position contain a subset of k points in general position. Cardinal, Tóth and Wood proved that $\alpha(n,3) = o(n)$ holds. They noted that for a fixed $d \geq 4$, only $\alpha(n,d) \leq Cn$ is known, for a constant $C \in (0,1)$, and they asked whether $\alpha(n,d) = o(n)$. The goal of this chapter is to answer their question in all dimensions. In particular we prove the following.

Theorem 6.1. *For a fixed integer $d \geq 2$, we have $\alpha(n,d) = o(n)$.*

In fact, we are able to get better bounds for certain dimensions. This is the content of the next theorem.

Theorem 6.2. *Suppose that $d, m \in \mathbb{N}$ satisfy $2^{m+1} - 1 \leq d \leq 3 \cdot 2^m - 3$. Let $N \geq 1$. Then*

$$\alpha(2^N, d) \leq \left(\frac{25}{N}\right)^{1/2^{m+1}} 2^N.$$

It is worth noting the lower bound $\alpha(n,d) = \Omega_d((n \log n)^{1/d})$ due to Cardinal, Tóth and Wood ([11]), but we do not try to improve their bound in this chapter.

In [17] Füredi used the density Hales-Jewett theorem ([18], [14]) to establish $\alpha(n) = \alpha(n,2) = o(n)$. Here we reproduce his argument. By the density Hales-Jewett theorem, for a given $\epsilon > 0$, there is a positive integer N such that all subsets of $[3]^N$ of density ϵ contain a combinatorial line. Map the set $[3]^N$ to $\mathbb{R}^2$ using a generic linear map f to obtain a set $X = f([3]^N) \subseteq \mathbb{R}^2$. By the choice of f, collinear points in X correspond to collinear points in $[3]^N$, and f restricted to $[3]^N$ is injective. Therefore, X has no 4 points on a line, and so is in almost general position, but if $S \subseteq X$ has size at least $\epsilon|X|$, the set $f^{-1}(S) \subseteq [3]^N$ has density at least ϵ in $[3]^N$. Therefore, $f^{-1}(S)$ has a line, hence $S = f(f^{-1}(S))$ has 3 collinear points. Since $\epsilon > 0$ was arbitrary, this proves that $\alpha(n,2) = o(n)$.

If one tries to generalize this argument to higher dimensions, by mapping $[m]^N$ to $\mathbb{R}^d$, then there will be m^{d-1} cohyperplanar points, and we must have $m^{d-1} = d+1$ to get almost general position. But the only positive integers that have this property are $(m,d) \in \{(3,2),(2,3)\}$. Taking $m=2, d=3$ gives $\alpha(n,3) = o(n)$, as observed by Cardinal, Tóth and Wood ([11]). For other choices of (m,d) we have too many cohyperplanar points as $m^{d-1} > d+1$. Overcoming this obstacle is our main goal.

Notation. Throughout this chapter, we write $[k]$ for the set $\{1,2,\dots,k\}$. By a *d-cube of edge length k* we mean a set of the form $\{v_0 + \lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_d v_d \colon \lambda_1, \lambda_2, \dots, \lambda_d \in \{0,1,2,\dots,k\}\}$, where $v_1, v_2, \dots, v_d$ are (not necessarily independent) vectors in a real vector space. A *d-dimensional combinatorial subspace* of $[N]^k$ is a set that consists of all $x \in [N]^k$ such that $x_i = a_i$ when $i \in I_0$, and x_i does not change when i ranges over I_j, for $j = 1,\dots,d$, where $I_0, I_1 \dots, I_d$ are some fixed sets that partition $[k]$, $I_1, I_2, \dots, I_d$ are non-empty and a_i for $i \in I_0$ are some fixed elements of $[N]$. Given vectors $v_0, v_1, \dots, v_r \in \mathbb{R}^d$, we say that they are *affinely dependent* if there are $\lambda_0, \lambda_1, \dots, \lambda_r \in \mathbb{R}$, not all zero, but adding up to zero, such that $\sum_{i=0}^{r} \lambda_i v_i = 0$. Finally, for a real vector spaces $\mathbb{R}^n$ we use the usual inner product $\langle x, y \rangle$ given by $\sum_{i=1}^{n} x_i y_i$, where x_i and y_i are coordinates of x and y with respect to the standard basis.

6.1.1 Organization of the chapter

Section 6.2 is devoted to the motivation of the arguments of this chapter and to the explanation of the approach taken in the proofs of the main results. In Section 6.3, we introduce the key notion for this chapter, *$\mathcal{F}$-incident sets*, where $\mathcal{F}$ is an arbitrary family of maps from $\mathbb{R}^N$ to $\mathbb{R}^d$. Roughly speaking, these are the sets that stay cohyperplanar under all maps in $\mathcal{F}$. In the same section, we prove Proposition 6.5, which provides us with an incidence removal function, a single function which makes all the non-$\mathcal{F}$-incident sets non-cohyperplanar.

In Section 6.4, we focus on the study of $\mathcal{F}_{N,d,m}$-incident sets, where $\mathcal{F}_{N,d,m}$ is a family of maps from $\mathbb{R}^N$ to $\mathbb{R}^d$ resembling polynomials of m^{th} degree. In particular, Lemma 6.7 shows that combinatorial subspaces and lines of a d-cube give rise to $\operatorname{span}\mathcal{F}_{N,d,m}$-incident sets. The rest of the section is devoted to deriving a characterization of $\mathcal{F}_{N,d,m}$-incident sets in terms of vectors given by products of coordinates. The proof of $\alpha(n,d) = o_d(n)$ is the result of work carried out in Section 6.2. That section also contains Lemma 6.11 which is the main tool used in the analysis of $\mathcal{F}_{N,d,m}$-incident sets. Finally, in Section 6.6, we improve the bounds for certain dimensions, using Lemma 6.16 in the analysis of $\mathcal{F}_{N,d,m}$-incident sets.

6.2 Motivation and the outline of the proof

Recall that the main obstacle to generalizing Füredi's argument to the higher dimensions is that $(d-1)$-cubes have too many cohyperplanar points. A (seemingly) possible way to get around this issue is to modify the initial set $[m]^N$ to a subset X, which does not have too many incidences, and yet some form of the Hales-Jewett theorem may still be applied to X. The desired set would once again be the image of X under a generic linear map from $\mathbb{R}^N \to \mathbb{R}^d$. It is tempting to try to remove certain points from each $(d-1)$-cube inside $[m]^N$, so that precisely $d+1$ out of the original m^{d-1} points remain. However, this is impossible for sufficiently large N, as the set $X \subseteq [m]^N$ gives a 2-colouring of $[m]^N$ (a point is blue if it is in X, red otherwise), and thus the Hales–Jewett theorem provides us with a monochromatic $(d-1)$-cube. Therefore, such an approach at least needs further modifications, if it can be made to work at all.

Having abandoned the first idea, it is natural to try to map $[m]^N$ under a map f which is more general than linear maps. Previously we used a generic linear map. In other words, this is a map f with the property that the only sets of size $d+1$ whose image under f is cohyperplanar in $\mathbb{R}^d$ are precisely the affinely dependent subsets of $[m]^N$ of size $d+1$. This leads us to the key notion of this chapter, namely that of *$\mathcal{F}$-incident sets*, which we now define. Let $\mathcal{F}$ be a family of functions from $\mathbb{R}^N$ to $\mathbb{R}^d$ (we shall use $\mathcal{F}$ instead of just the linear maps). We say that a set $S \subseteq \mathbb{R}^N$ is *$\mathcal{F}$-incident* if the multiset $f(S)$ is affinely dependent for all $f \in \mathcal{F}$. Crucially, like in the case of linear maps, we can a find a 'generic' map $f \in \operatorname{span} \mathcal{F}$, such that if $f(S)$ is affinely dependent then S is $\mathcal{F}$-incident. This is the content of Proposition 6.5. We refer to such a map as an 'incidence removal function'.

Once we have constructed an incidence removal function, the next aim is to study $\mathcal{F}$-incident sets for suitable $\mathcal{F}$. Our goal now is essentially the following: we want that each dense subset of $[m]^N$ contains an $\mathcal{F}$-incident set of size $d+1$ (which gives cohyperplanar sets with $d+1$ elements), but at the same time, that the image of $[m]^N$ under an incidence removal function does not contain $d+2$ cohyperplanar points. An easy way to fulfil the second requirement is to make sure that $\mathcal{F}$-incident sets of size $d+1$ cannot have intersection of size d. On the other hand, as in the case of linear maps, we use the density Hales-Jewett theorem to show that dense subsets contain the desired $\mathcal{F}$-incident sets, thus we want that the combinatorial subspaces are $(\operatorname{span} \mathcal{F})$-incident (note that here we need a stronger property of being $(\operatorname{span} \mathcal{F})$-incident instead of just $\mathcal{F}$-incident, as the incidence removal function belongs to a bigger family $\operatorname{span} \mathcal{F}$).

To give an idea of how we choose the family of functions $\mathcal{F}$ making the combinatorial lines $\operatorname{span} \mathcal{F}$-incident, observe the following identities that hold for arbitrary a, b:

$$\begin{aligned}
&\mathbf{1} \cdot 1 &&+ (-\mathbf{3}) \cdot 1 &&+ \mathbf{3} \cdot 1 &&+ (-\mathbf{1}) \cdot 1 &&= 0,\\
&\mathbf{1} \cdot a &&+ (-\mathbf{3}) \cdot (a+b) &&+ \mathbf{3} \cdot (a+2b) &&+ (-\mathbf{1}) \cdot (a+3b) &&= 0,\\
&\mathbf{1} \cdot a^2 &&+ (-\mathbf{3}) \cdot (a+b)^2 &&+ \mathbf{3} \cdot (a+2b)^2 &&+ (-\mathbf{1}) \cdot (a+3b)^2 &&= 0.
\end{aligned}$$

What is crucial here is that we have the same coefficients appearing in the three linear combinations above. Hence, if one looks at a function $f \colon \mathbb{R}^N \to \mathbb{R}^3$

of the form

$$f(x) = \begin{pmatrix} (\langle x, v_1\rangle + c_1)^2 \\ (\langle x, v_2\rangle + c_2)^2 \\ (\langle x, v_3\rangle + c_3)^2 \end{pmatrix} \tag{6.1}$$

for some $v_1, v_2, v_3 \in \mathbb{R}^N$ and reals c_1, c_2, c_3, then $f(x), f(x+y), f(x+2y), f(x+3y)$ are necessarily coplanar, as

$$\mathbf{1} \cdot f(x) + (-\mathbf{3}) \cdot f(x+y) + \mathbf{3} \cdot f(x+2y) + (-\mathbf{1}) \cdot f(x+3y) = 0$$

and the sum of coefficients is zero. Moreover, if g is any linear combination of functions of the form described above, then $g(x), g(x+y), g(x+2y), g(x+3y)$ are coplanar, owing to the fact that the same coefficients appear in the identities above.

In the case of $d = 2$, we used only linear maps and we had that the image of $[3]^N$ to the plane under a generic linear map is the desired set. In that case, the combinatorial lines in $[3]^N$ gave us collinear sets of points in the plane. Moving to the functions constructed from the polynomials of degree 2, the image of $[4]^N$ under a 'generic degree 2 function' to $\mathbb{R}^3$ has cohyperplanar sets of 4 points that are also images of combinatorial lines. After some analysis of the $\mathcal{F}$-incident sets for $\mathcal{F}$ given by equation (6.1), we are able to show that those sets have intersection of size at most 1, provided the size of sets is at most 4. The motivation for this step comes from the heuristics that we expect that our non-trivial $\mathcal{F}$-incident sets are precisely the relevant combinatorial subspaces (in this case the lines) and as such, they cannot have large intersection (in case of lines, they cannot share more than one point). This was the second requirement that we had, completing a sketch of the proof that $\alpha(n, 3) = o(n)$. This naturally extends to larger values of d.

Using different identities, we are able to get better bounds on $\alpha(n, d)$. For example, the fact that $x^2 + (x+a+b)^2 + (x+a+c)^2 + (x+b+c)^2 = (x+a)^2 + (x+b)^2 + (x+c)^2 + (x+a+b+c)^2$ holds for all x, a, b, c, enables us to use 3-dimensional combinatorial subspaces of $\{0,1\}^N$ as the sources of cohyperplanar sets. Generalizing this identity to higher degrees, we can use the higher-dimensional combinatorial subspaces as well. The better bounds on $\alpha(n, d)$ when these subspaces are used come from the better bounds for density

Hales-Jewett theorem [14] in the case of $\{0,1\}^N$ (the generalized Sperner's theorem).

When it comes to the analysis of $\mathcal{F}$-incident sets, let us first define precisely the families of functions that we shall consider in this chapter. For given $N, d, m \in \mathbb{N}$ we define the family $\mathcal{F}_{N,d,m}$ of functions $f\colon \mathbb{R}^N \to \mathbb{R}^d$ of the form $f_i(x) = (\langle x, u_i\rangle + c_i)^l$ for $i = 1, 2, \ldots, d$, for any $u_1, u_2, \ldots, u_d \in \mathbb{R}^N$, $c_1, c_2, \ldots, c_d \in \mathbb{R}$ and $1 \leq l \leq m$. The bulk of this chapter consists of studying the $\mathcal{F}_{N,d,m}$-incident sets.

6.2.1 Analysis and properties of $\mathcal{F}_{N,d,m}$-incident sets

The first important claim regarding the $\mathcal{F}_{N,d,m}$-incident sets is the characterization given by Proposition 6.9, which we explain here. To simplify the notation, we introduce the following notion. The terminology $(\leq m)$*-function to* S stands for any function $\varphi\colon A \to S$, where A has size at most m. Given a vector $x \in \mathbb{R}^N$ and a $(\leq m)$-function φ to $[N]$, we define $\varphi(x) = \prod_{a\in A} x_{\varphi(a)}$. Proposition 6.9 tells us that $\{x_0, x_1, \ldots, x_r\}$ for $r \leq d$ is $\mathcal{F}_{N,d,m}$-incident if and only if the vectors

$$\begin{pmatrix}\varphi_1(x_0)\\ \varphi_2(x_0)\\ \vdots\\ \varphi_r(x_0)\end{pmatrix}, \begin{pmatrix}\varphi_1(x_1)\\ \varphi_2(x_1)\\ \vdots\\ \varphi_r(x_1)\end{pmatrix}, \ldots, \begin{pmatrix}\varphi_1(x_r)\\ \varphi_2(x_r)\\ \vdots\\ \varphi_r(x_r)\end{pmatrix}$$

are affinely dependent for all $(\leq m)$-functions $\varphi_1, \varphi_2, \ldots, \varphi_r$. Then, in order to prove that our $\mathcal{F}_{N,d,m}$-incident sets cannot have large intersections, we use Lemmas 6.11 and 6.16. First we state Lemma 6.11 to illustrate its contrast to Proposition 6.9.

Lemma 6.3. *(Lemma 6.11) Let $m, r, N \in \mathbb{N}$. Suppose that $y_1, y_2, \ldots, y_r \in \mathbb{R}^N$ are vectors such that* $\operatorname{rank}\{y_1, y_2, \ldots, y_r\} + m - 1 \geq r$. *Suppose further that $y_1, y_2, \ldots, y_r$ are distinct and have non-zero coordinates. Then we may find $(\leq m)$-functions $\varphi_1, \varphi_2, \ldots, \varphi_r$ for which the vectors*

$$\begin{pmatrix}\varphi_1(y_1)\\ \varphi_2(y_1)\\ \vdots\\ \varphi_r(y_1)\end{pmatrix}, \begin{pmatrix}\varphi_1(y_2)\\ \varphi_2(y_2)\\ \vdots\\ \varphi_r(y_2)\end{pmatrix}, \ldots, \begin{pmatrix}\varphi_1(y_r)\\ \varphi_2(y_r)\\ \vdots\\ \varphi_r(y_r)\end{pmatrix}$$

are linearly independent.

The conclusions of Lemma 6.11 and Proposition 6.9 are almost exactly opposite. We only need to take care to pass from affine dependence to linear dependence (which is easy as a set $\{v_1, v_2, \ldots, v_r\}$ is linearly dependent if and only if $\{0, v_1, v_2, \ldots, v_r\}$ is affinely dependent). Hence, we use these two results along with some combinatorial arguments to deduce structural information about $\mathcal{F}_{N,d,m}$-incident sets, and in particular to show that such sets exhibit behaviour similar to combinatorial subspaces, as expected.

We now state Lemma 6.16, another crucial result in the study of $\mathcal{F}_{N,d,m}$-incidence. Note that it has a more combinatorial flavour than Lemma 6.11.

Lemma 6.4. *(Lemma 6.16) Let $m, k \in \mathbb{N}$. Given any distinct sets $X_1, X_2, \ldots, X_r \in \mathbb{N}^{(<\omega)}$, we can find sets $S_1, S_2, \ldots, S_r \subseteq \mathbb{N}^{(\leq m)}$ such that the matrix*

$$I = \begin{pmatrix} \mathbb{1}_{S_1 \subseteq X_1} & \mathbb{1}_{S_1 \subseteq X_2} & \cdots & \mathbb{1}_{S_1 \subseteq X_r} \\ \mathbb{1}_{S_2 \subseteq X_1} & \mathbb{1}_{S_2 \subseteq X_2} & \cdots & \mathbb{1}_{S_2 \subseteq X_r} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbb{1}_{S_r \subseteq X_1} & \mathbb{1}_{S_r \subseteq X_2} & \cdots & \mathbb{1}_{S_r \subseteq X_r} \end{pmatrix}$$

has $\dim \ker I = 0$ *if* $r < 2^{m+1}$, *and* $\dim \ker I \leq 1$ *if* $r < 3 \cdot 2^m$. *Here* $\mathbb{1}_{A \subseteq B}$ *takes value 1 if A is a subset of B, and zero otherwise.*

The subset relation here is actually quite natural. This comes from considering the $\mathcal{F}_{N,d,m}$-incident subsets of $\{0,1\}^N$. As we have seen above, when analysing $\mathcal{F}_{N,d,m}$-incidence, we are interested in the values of $\varphi(x)$ for $x \in \{0,1\}^N$ and $(\leq m)$-function φ to $[N]$. If we set $S = \operatorname{Im} \varphi$, then $\varphi(x) = \prod_{s \in S} x_s = \mathbb{1}_{S \subseteq X}$, where $X = \{i \colon x_i = 1\}$.

Finally, we note that studying the algebraic properties of such matrices may be of separate interest.

6.3 Definition and basic properties of $\mathcal{F}$-incidences

Throughout this section, $\mathcal{F}$ will stand for a family of maps from $\mathbb{R}^N$ to $\mathbb{R}^d$. Given such a family of functions $\mathcal{F}$, our goal is to understand the non-trivial affinely dependent sets of points in the images of $f \in \mathcal{F}$.

Recall that we say that points $s_1, s_2, \ldots, s_k \in \mathbb{R}^d$ (not necessarily distinct) are *affinely dependent* if there are $\lambda_1, \ldots, \lambda_k \in \mathbb{R}$ not all zero such that $\sum_{i=1}^k \lambda_i = 0$ and $\sum_{i=1}^k \lambda_i s_i = 0$. A k-tuple $S = (s_1, s_2, \ldots, s_k)$ of points in $\mathbb{R}^N$ is said to be *$\mathcal{F}$-incident* if for all $f \in \mathcal{F}$ we have $f(s_1), f(s_2), \ldots, f(s_k)$ affinely dependent. A set $S = \{s_1, s_2, \ldots, s_k\}$ of points in $\mathbb{R}^N$ is *$\mathcal{F}$-incident* if a corresponding k-tuple $(s_1, s_2, \ldots, s_k)$ is. Note that the order does not play a role in this definition, nor is the order of points important at any point in this chapter. The only reason why we use k-tuples is the possibility that some of $f(s_i)$ might overlap. (This issue could also be resolved using multisets.) Further, S is *minimal $\mathcal{F}$-incident* if it is $\mathcal{F}$-incident and no proper subset of S is $\mathcal{F}$-incident.

Proposition 6.5 (Incidence removal function). *Let $X \subseteq \mathbb{R}^N$ be a finite set and let $\mathcal{F}$ be a family of functions from $\mathbb{R}^N$ to $\mathbb{R}^d$. Then there is $f \in \operatorname{span} \mathcal{F}$ with the property that*

if $\{s_1, s_2, \ldots, s_k\}$ is not $\mathcal{F}$-incident, then $f(s_1), f(s_2), \ldots, f(s_k)$ are affinely independent. (†)

Furthermore, if $\mathcal{F}$ separates the points of X (i.e. for distinct $x, y \in X$ there is $f \in \mathcal{F}$ such that $f(x) \neq f(y)$), then there is $f \in \operatorname{span}\mathcal{F}$ which is injective on X, with the property (†).

The proof of the proposition is based on simple linear algebra and some easy facts regarding the vanishing of polynomials. It can be skipped at the first reading, the reader should only be aware of the existence of the incidence removal function and its properties.

Proof. Throughout this proof, for a function f and a set $S = \{s_1, s_2, \ldots, s_k\}$, we regard $f(S)$ as the multiset of elements $f(s_1), \ldots, f(s_k)$. So, if we say that $f(S)$ is affinely dependent, we mean $f(s_1), f(s_2), \ldots, f(s_k)$ are affinely dependent.

We start by establishing the existence of a map f with property (†). The second part of the proposition will follow from a simple argument later. Let $T_1, T_2, \ldots, T_m$ be the list of all subsets of X which are not $\mathcal{F}$-incident. Thus, for each index i we have a function $f_i \in \mathcal{F}$ such that $f_i(T_i)$ is affinely independent. We shall inductively construct functions $F_i \in \operatorname{span} \mathcal{F}$ such that all of

$F_i(T_1), F_i(T_2), \ldots, F_i(T_i)$ are affinely independent. Start by taking $F_1 = f_1$ for the case $i = 1$.

Suppose that we have $i \geq 1$ and a function $F_i \in \operatorname{span} \mathcal{F}$ such that each of $F_i(T_1), F_i(T_2), \ldots, F_i(T_i)$ is affinely independent. Assume that $i < m$, otherwise we are done. Also, if $F_i(T_{i+1})$ is already affinely independent, simply take $F_{i+1} = F_i$. Hence, w.l.o.g. $F_i(T_{i+1})$ is affinely dependent. We shall construct F_{i+1} as a linear combination $F_i + \lambda f_{i+1}$, where $\lambda > 0$ is a sufficiently small real, chosen so that it does not introduce new dependencies.

Let $u_1, u_2, \ldots, u_k \in \mathbb{R}^N$. Let $F^{(\lambda)} = F_i + \lambda f_{i+1}$ and suppose that $F^{(0)}(u_1)$, $F^{(0)}(u_2), \ldots,$ $F^{(0)}(u_k)$ are affinely independent. Then $F^{(0)}(u_2) - F^{(0)}(u_1), \ldots,$ $F^{(0)}(u_k) - F^{(0)}(u_1)$ are linearly independent.

Lemma 6.6. *Suppose that $v_1, \ldots, v_l \in \mathbb{R}^d$ are linearly independent. Then, we can find $I \subseteq [d]$ of size l such that $v_1, \ldots, v_l$ are still linearly independent when restricted to coordinates in I.*

Proof. Look at the $d \times l$ matrix $A = (v_1 v_2 \ldots v_l)$. Since $v_1, v_2, \ldots, v_l$ are linearly independent, the column rank of A is l. But the column rank is the same as the row rank, so we can find l linearly independent rows with indices $r_1, \ldots, r_l$. Take $I = \{r_1, \ldots, r_l\}$ and let A' be the matrix A restricted to rows in I. Then, the row rank of A' is l, so its column rank is l, as desired. $\square$

By Lemma 6.6 we can find a set of coordinates I of size $k - 1$ such that $F^{(0)}(u_2) - F^{(0)}(u_1)$, $F^{(0)}(u_3) - F^{(0)}(u_1), \ldots,$ $F^{(0)}(u_k) - F^{(0)}(u_1)$ are linearly independent after restriction to I. We restrict our attention to these coordinates only. Then we can define

$$p(\lambda) = \det(F^{(\lambda)}(u_2) - F^{(\lambda)}(u_1) \ldots F^{(\lambda)}(u_k) - F^{(\lambda)}(u_1)),$$

which is a polynomial in λ. Since $p(0) \neq 0$, by continuity we have $\delta > 0$ such that if $|\lambda| < \delta$ then $p(\lambda) \neq 0$. Therefore, $F^{(\lambda)}(u_1)$, $F^{(\lambda)}(u_2), \ldots,$ $F^{(\lambda)}(u_k)$ are affinely independent if $|\lambda| < \delta$. Note that we can now remove the restriction to coordinates of I, as this will not affect the affine independence.

We can apply this argument to all $T_1, \ldots, T_i$, to get $\delta > 0$ such that if $|\lambda| < \delta$ then $(F_i + \lambda f_{i+1})(T_j)$ is affinely independent for all $j = 1, \ldots, i$.

Now suppose that the choice $F_i + \lambda f_{i+1}$ does not work for us as F_{i+1}. Then, we must have $(F_i + \lambda f_{i+1})(T_{i+1})$ is affinely dependent for all $|\lambda| < \delta$. Thus if $\lambda > \delta^{-1}$ then $(\lambda F_i + f_{i+1})(T_{i+1})$ is affinely dependent. List the elements of T_{i+1} as $t_1, t_2, \ldots, t_r$. Now, apply Lemma 6.6 to $f_{i+1}(T_{i+1})$ to get a set of coordinates of size $r-1$, on which this set is still affinely independent, and use a similar polynomial to the one we had before, this time

$$q(\lambda) = \det((\lambda F_i + f_{i+1})(t_2 - t_1) \ldots (\lambda F_i + f_{i+1})(t_r - t_1)).$$

Then $q(0) \neq 0$, but $q(\lambda) = 0$ if $\lambda > \delta^{-1}$ which is a contradiction, and thus the first part of the proposition is proved.

For the last part, if $\mathcal{F}$ separates the points of X, observe that there are no two-element sets which are $\mathcal{F}$-incident. Hence, whenever $x, y \in X$ are distinct, their images $f(x)$ and $f(y)$ are affinely independent by the first part, so f is injective, as desired. □

6.4 Families of higher-degree maps and the resulting incident sets

Throughout the rest of the chapter we will focus on the family $\mathcal{F}_{N,d,m}$ of functions $f\colon \mathbb{R}^N \to \mathbb{R}^d$ of the form $f_i(x) = (\langle x, u_i \rangle + c_i)^l$ for $i = 1, 2, \ldots, d$, for any $u_1, u_2, \ldots, u_d \in \mathbb{R}^N$, $c_1, c_2, \ldots, c_d \in \mathbb{R}$ and $1 \leq l \leq m$.

We start by giving some examples of non-trivial $\operatorname{span} \mathcal{F}_{N,d,m}$-incident sets. The proofs are based on algebraic identities, which were described in the introduction. For the case of lines, we use the rank-nullity theorem to prove that there is an identity we are looking for, and in the case of combinatorial subspaces, we prove the identity explicitly.

Lemma 6.7. *(Examples of non-trivial* $\operatorname{span} \mathcal{F}_{N,d,m}$*-incident sets.)*

- ***(i)*** *(Lines.) For $x, y \in \mathbb{R}^N$, the $(m+2)$-tuple $(x + iy\colon i = 0, 1, \ldots, m+1)$ is* $\operatorname{span} \mathcal{F}_{N,d,m}$*-incident.*

- ***(ii)*** *(Combinatorial subspaces.) For $x_0, x_1, \ldots, x_{m+1} \in \mathbb{R}^N$, the 2^{m+1}-tuple $(x_0 + \sum_{i \in I} x_i\colon I \subseteq [m+1])$ is* $\operatorname{span} \mathcal{F}_{N,d,m}$*-incident.*

Proof. Lines. We show that there are $\lambda_0, \dots, \lambda_{m+1}$, not all zero, such that for all $f \in \mathcal{F}_{N,d,m}$ we have $\sum_{i=0}^{m+1} \lambda_i f(x+iy) = 0$ and $\sum_{i=0}^{m+1} \lambda_i = 0$. Then, the same linear combination shows that $f(x), f(x+y), \dots, f(x+(m+1)y)$ are affinely dependent for $f \in \operatorname{span} \mathcal{F}_{N,d,m}$. Before we proceed with the proof, observe that if $y = 0$ our line becomes degenerate and the $(m+2)$-tuple we consider is immediately $\mathcal{F}_{N,d,m}$-incident. Thus, we assume that $y \neq 0$.

Thus, we want a non-trivial sequence λ_i adding up to zero, such that for all $u \in \mathbb{R}^N, c \in \mathbb{R}, l \in [m]$ we have

$$\sum_{i=0}^{m+1} \lambda_i \left(\langle x+iy, u\rangle + c\right)^l = 0.$$

Expanding this expression using the binomial theorem and treating it as a polynomial in c, it becomes equivalent to

$$\sum_{i=0}^{m+1} \lambda_i \langle x+iy, u\rangle^l = 0$$

for all $u \in \mathbb{R}$ and $l = 0, 1, \dots, m$. Expanding further, this is equivalent to

$$\sum_{k=0}^{l} \binom{l}{k} \langle x, u\rangle^{l-k} \langle y, u\rangle^k \left(\sum_{i=0}^{m+1} \lambda_i i^k\right) = 0$$

for all $u \in \mathbb{R}$ and $l = 0, 1, \dots, m$. Hence, if $\lambda_0, \dots, \lambda_{m+1}$ satisfy

$$\sum_{i=0}^{m+1} \lambda_i i^l = 0$$

for all $l = 0, 1, \dots, m$, we are done. But by the rank-nullity theorem ('more variables than equations'), we must have a non-trivial solution to these equations, giving us the desired λ_i.

Combinatorial subspaces. As in the case of lines, we show that there are coefficients λ_I, for set-valued indices $I \subseteq [m+1]$ (including the $I = \emptyset$), not all zero, but adding up to zero, such that $\sum_{I \subseteq [m+1]} \lambda_I f(x_0 + \sum_{i \in I} x_i) = 0$, for all $f \in \mathcal{F}_{N,d,m}$, which suffices to prove the claim in the full generality. In this case, we can actually set $\lambda_I = (-1)^{|I|}$.

It is enough to show that for any $u \in \mathbb{R}^N, c \in \mathbb{R}, l \in [m]$ we have (in these sums, $I = \emptyset$ is included)

$$\sum_{I \subseteq [m+1]} (-1)^{|I|} \left(\langle x_0 + \sum_{i \in I} x_i, u \rangle + c \right)^l = 0.$$

But writing $a_0 = \langle x_0, u \rangle + c, a_i = \langle x_i, u \rangle$ for $i = 1, \ldots, m+1$, we see that it is sufficient to show

$$\sum_{I \subseteq [m+1]} (-1)^{|I|} \left(a_0 + \sum_{i \in I} a_i \right)^l = 0$$

for all $a_0, a_1, \ldots, a_{m+1} \in \mathbb{R}, l \in [m+1]$. This is the content of the next lemma.

Lemma 6.8. *Let $l, m \in \mathbb{N}, l \leq m$ and $a_0, a_1, \ldots, a_{m+1} \in \mathbb{R}$. Then*

$$\sum_{I \subseteq [m+1]} (-1)^{|I|} \left(a_0 + \sum_{i \in I} a_i \right)^l = 0.$$

Proof of Lemma 6.8. Note that

$$\sum_{I \subseteq [m+1]} (-1)^{|I|} \left(a_0 + \sum_{i \in I} a_i \right)^l = \sum_{k=0}^{l} \binom{l}{k} a_0^{l-k} \left(\sum_{I \subseteq [m+1]} (-1)^{|I|} \left(\sum_{i \in I} a_i \right)^k \right)$$

thus we only need to consider the case $a_0 = 0$. Proving the lemma in this case would tell us that

$$\sum_{I \subseteq [m+1]} (-1)^{|I|} \left(\sum_{i \in I} a_i \right)^k = 0$$

holds for all k, so the whole expression with arbitrary a_0 above would vanish.

Consider the expression

$$\sum_{I \subseteq [m+1]} (-1)^{|I|} \left(\sum_{i \in I} a_i \right)^l$$

as a polynomial of degree l in $a_1, \ldots, a_{m+1}$. The coefficient of $a_1^{d_1} a_2^{d_2} \ldots a_{m+1}^{d_{m+1}}$ is

$$\binom{l}{d_1, d_2, \ldots, d_{m+1}} \sum_{S \subseteq I \subseteq [m+1]} (-1)^{|I|},$$

where S is the set of indices i such that $d_i > 0$. Since $|S| \leq m$, the sum $\sum_{S \subseteq I \subseteq [m+1]} (-1)^{|I|}$ is zero, which finishes the proof. $\square$

Applying Lemma 6.8 completes the proof. $\square$

Before coming to a key proposition which describes the $\mathcal{F}_{N,d,m}$-incident sets, we introduce a couple of pieces of notation. If φ is a function from a set of size at most m to a set X, we say that φ is a *$(\leq m)$-function* to X. Given a $(\leq m)$-function $\varphi\colon A \to [N]$ and $x \in \mathbb{R}^N$, we write $\varphi(x) = \prod_{a\in A} x_{\varphi(a)}$. Here we allow an 'empty' function, i.e. a function φ from an empty set to $[N]$, defined by $\varphi(x) = 1$, for all $x \in \mathbb{R}^N$.

Proposition 6.9. *Let $r, d, m, N \in \mathbb{N}$, suppose $r \leq d$ and let $X = \{x_0, x_1, \ldots, x_r\}$ be a subset of $\mathbb{R}^N$. The following are equivalent.*

(i) *X is $\mathcal{F}_{N,d,m}$-incident.*

(ii) *Given any $(\leq m)$-functions $\varphi_1, \varphi_2, \ldots, \varphi_r$ to $[N]$, the vectors*

$$\begin{pmatrix} \varphi_1(x_0) \\ \varphi_2(x_0) \\ \vdots \\ \varphi_r(x_0) \end{pmatrix}, \begin{pmatrix} \varphi_1(x_1) \\ \varphi_2(x_1) \\ \vdots \\ \varphi_r(x_1) \end{pmatrix}, \ldots, \begin{pmatrix} \varphi_1(x_r) \\ \varphi_2(x_r) \\ \vdots \\ \varphi_r(x_r) \end{pmatrix}$$

are affinely dependent.

The proof of the proposition is a straightforward algebraic manipulation, mostly based on the fact that if a polynomial over the reals vanishes everywhere, then its coefficients are zero. The reader may consider skipping the proof in the first reading.

Proof. Start from the definition, **(i)** is equivalent to the vectors

$$\begin{pmatrix} (\langle x_0, u_1\rangle + c_1)^l \\ (\langle x_0, u_2\rangle + c_2)^l \\ \vdots \\ (\langle x_0, u_d\rangle + c_d)^l \end{pmatrix}, \begin{pmatrix} (\langle x_1, u_1\rangle + c_1)^l \\ (\langle x_1, u_2\rangle + c_2)^l \\ \vdots \\ (\langle x_1, u_d\rangle + c_d)^l \end{pmatrix}, \ldots, \begin{pmatrix} (\langle x_r, u_1\rangle + c_1)^l \\ (\langle x_r, u_2\rangle + c_2)^l \\ \vdots \\ (\langle x_r, u_d\rangle + c_d)^l \end{pmatrix}$$

being affinely dependent for any choice of parameters $c_1, c_2, \ldots, c_d \in \mathbb{R}$, u_1, $u_2, \ldots, u_d \in \mathbb{R}^N$ and $1 \leq l \leq m$. In particular, as $r \leq d$, this is further equivalent to vectors

$$\begin{pmatrix}(\langle x_1,u_1\rangle+c_1)^l-(\langle x_0,u_1\rangle+c_1)^l\\(\langle x_1,u_2\rangle+c_2)^l-(\langle x_0,u_2\rangle+c_2)^l\\\vdots\\(\langle x_1,u_r\rangle+c_r)^l-(\langle x_0,u_r\rangle+c_r)^l\end{pmatrix},\begin{pmatrix}(\langle x_2,u_1\rangle+c_1)^l-(\langle x_0,u_1\rangle+c_1)^l\\(\langle x_2,u_2\rangle+c_2)^l-(\langle x_0,u_2\rangle+c_2)^l\\\vdots\\(\langle x_2,u_r\rangle+c_r)^l-(\langle x_0,u_r\rangle+c_r)^l\end{pmatrix},\dots,$$
$$\begin{pmatrix}(\langle x_r,u_1\rangle+c_1)^l-(\langle x_0,u_1\rangle+c_1)^l\\(\langle x_r,u_2\rangle+c_2)^l-(\langle x_0,u_2\rangle+c_2)^l\\\vdots\\(\langle x_r,u_r\rangle+c_r)^l-(\langle x_0,u_r\rangle+c_r)^l\end{pmatrix}$$

being linearly dependent for all the choices of parameters. Hence, taking determinant, **(i)** is the same as

$$\det\big((\langle x_i,u_j\rangle+c_j)^l-(\langle x_0,u_j\rangle+c_j)^l\big)=0$$

for any choice of $u_1,\dots,u_r,c_1,\dots,c_r,l$. Expanding using binomial theorem, and writing S_r for the symmetric group on $[r]$, we obtain

$$\begin{aligned}0&=\sum_{\pi\in S_r}\operatorname{sgn}(\pi)\prod_{i=1}^r\big((\langle x_{\pi(i)},u_i\rangle+c_i)^l-(\langle x_0,u_i\rangle+c_i)^l\big)\\&=\sum_{\pi\in S_r}\operatorname{sgn}(\pi)\prod_{i=1}^r\left(\sum_{k=0}^l c_i^k\binom{l}{k}\big(\langle x_{\pi(i)},u_i\rangle^{l-k}-\langle x_0,u_i\rangle^{l-k}\big)\right)\\&=\sum_{0\le k_1,k_2,\dots,k_r\le l}c_1^{k_1}c_2^{k_2}\dots c_r^{k_r}\\&\qquad\prod_{i=1}^r\binom{l}{k_i}\left(\sum_{\pi\in S_r}\operatorname{sgn}(\pi)\prod_{i=1}^r\big(\langle x_{\pi(i)},u_i\rangle^{l-k_i}-\langle x_0,u_i\rangle^{l-k_i}\big)\right)\end{aligned}$$

However, this holds for any choice of $c_1,c_2,\dots,c_r\in\mathbb{R}$, so, when the expression above is viewed as a polynomial in variables $c_1,c_2,\dots,c_r$, we conclude that all its coefficients are zero. In other words, **(i)** is equivalent to the following. For any $0 \le k_1, k_2, \dots, k_r \le m$, and any $u_1, u_2, \dots, u_r \in \mathbb{R}^N$ we have

$$
\begin{aligned}
0 &= \sum_{\pi \in S_r} \operatorname{sgn}(\pi) \prod_{i=1}^{r} \left(\langle x_{\pi(i)}, u_i \rangle^{k_i} - \langle x_0, u_i \rangle^{k_i} \right) \\
&= \sum_{\pi \in S_r} \operatorname{sgn}(\pi) \prod_{i=1}^{r} \left(\left(\sum_{j=1}^{N} x_{\pi(i)j} u_{ij} \right)^{k_i} - \left(\sum_{j=1}^{N} x_{0j} u_{ij} \right)^{k_i} \right) \\
&= \sum_{\pi \in S_r} \operatorname{sgn}(\pi) \prod_{i=1}^{r} \left(\sum_{\varphi_i : [k_i] \to [N]} \left(\prod_{j=1}^{k_i} x_{\pi(i)\varphi_i(j)} u_{i\varphi_i(j)} - \prod_{j=1}^{k_i} x_{0\varphi_i(j)} u_{i\varphi_i(j)} \right) \right) \\
&= \sum_{\pi \in S_r} \operatorname{sgn}(\pi) \prod_{i=1}^{r} \left(\sum_{\varphi_i : [k_i] \to [N]} \left(\prod_{j=1}^{k_i} u_{i\varphi_i(j)} \right) \left(\prod_{j=1}^{k_i} x_{\pi(i)\varphi_i(j)} - \prod_{j=1}^{k_i} x_{0\varphi_i(j)} \right) \right) \\
&= \sum_{\varphi_1 : [k_1] \to [N], \dots, \varphi_r : [k_r] \to [N]} \left(\prod_{i=1}^{r} \prod_{j=1}^{k_i} u_{i\varphi_i(j)} \right) \\
&\qquad \left(\sum_{\pi \in S_r} \operatorname{sgn}(\pi) \prod_{i=1}^{r} \left(\prod_{j=1}^{k_i} x_{\pi(i)\varphi_i(j)} - \prod_{j=1}^{k_i} x_{0\varphi_i(j)} \right) \right) \\
&= \sum_{\varphi_1 : [k_1] \to [N], \dots, \varphi_r : [k_r] \to [N]} \left(\prod_{i=1}^{r} \varphi_i(u_i) \right) \left(\sum_{\pi \in S_r} \operatorname{sgn}(\pi) \prod_{i=1}^{r} (\varphi_i(x_{\pi(i)}) - \varphi_i(x_0)) \right)
\end{aligned}
$$

Now, look at the expression above as a polynomial in variables u_{ij}. Observe that if $\varphi_1, \varphi_2, \dots, \varphi_r$, $\psi_1, \psi_2, \dots, \psi_r$ are such that $\prod_{i=1}^{r} \varphi_i(u_i) = \prod_{i=1}^{r} \psi_i(u_i)$ as formal expressions, then we must have

$$
\sum_{\pi \in S_r} \operatorname{sgn}(\pi) \prod_{i=1}^{r} (\varphi_i(x_{\pi(i)}) - \varphi_i(x_0)) = \sum_{\pi \in S_r} \operatorname{sgn}(\pi) \prod_{i=1}^{r} (\psi_i(x_{\pi(i)}) - \psi_i(x_0))
$$

as well. This tells us that the coefficients of our polynomial are positive integer multiples of $\sum_{\pi \in S_r} \operatorname{sgn}(\pi) \prod_{i=1}^{r} (\varphi_i(x_{\pi(i)}) - \varphi_i(x_0))$. Once again, the polynomial over $\mathbb{R}$ vanishes everywhere if and only if its coefficients are zero, so we deduce that **(i)** holds if and only if for all ($\le m$)-functions $\varphi_1, \varphi_2, \dots, \varphi_r$ to $[N]$, we have

$$
\begin{aligned}
0 &= \sum_{\pi \in S_r} \operatorname{sgn}(\pi) \prod_{i=1}^{r} (\varphi_i(x_{\pi(i)}) - \varphi_i(x_0)) \\
&= \det_{1 \le i,j \le r} (\varphi_i(x_j) - \varphi_i(x_0))
\end{aligned}
$$

which says precisely that the vectors

$$\begin{pmatrix} \varphi_1(x_1)-\varphi_1(x_0) \\ \varphi_2(x_1)-\varphi_2(x_0) \\ \vdots \\ \varphi_r(x_1)-\varphi_r(x_0) \end{pmatrix}, \begin{pmatrix} \varphi_1(x_2)-\varphi_1(x_0) \\ \varphi_2(x_2)-\varphi_2(x_0) \\ \vdots \\ \varphi_r(x_2)-\varphi_r(x_0) \end{pmatrix}, \ldots, \begin{pmatrix} \varphi_1(x_r)-\varphi_1(x_0) \\ \varphi_2(x_r)-\varphi_2(x_0) \\ \vdots \\ \varphi_r(x_r)-\varphi_r(x_0) \end{pmatrix}$$

are linearly dependent, which is equivalent to **(ii)**, as desired. □

Proposition 6.10. *Let $r, d, m, N \in \mathbb{N}$ be given and suppose that $r \leq d$ holds. Suppose also that the set $\{x_0, x_1, \ldots, x_r\} \subseteq \mathbb{R}^N$ is $\mathcal{F}_{N,d,m}$-incident. Then, given any affine map $\alpha\colon \mathbb{R}^N \to \mathbb{R}^N$ and any $(\leq m)$-functions $\varphi_1, \varphi_2, \ldots, \varphi_r$ to $[N]$, the vectors*

$$\begin{pmatrix} \varphi_1(\alpha(x_0)) \\ \varphi_2(\alpha(x_0)) \\ \vdots \\ \varphi_r(\alpha(x_0)) \end{pmatrix}, \begin{pmatrix} \varphi_1(\alpha(x_1)) \\ \varphi_2(\alpha(x_1)) \\ \vdots \\ \varphi_r(\alpha(x_1)) \end{pmatrix}, \ldots, \begin{pmatrix} \varphi_1(\alpha(x_r)) \\ \varphi_2(\alpha(x_r)) \\ \vdots \\ \varphi_r(\alpha(x_r)) \end{pmatrix}$$

are affinely dependent.

On the other hand, if the set $\{x_0, x_1, \ldots, x_r\} \subseteq \mathbb{R}^N$ is not $\mathcal{F}_{N,d,m}$-incident, then, given any affine isomorphism $\alpha\colon \mathbb{R}^N \to \mathbb{R}^N$, we may find $(\leq m)$-functions $\varphi_1, \varphi_2, \ldots, \varphi_r$ to $[N]$, so that the vectors

$$\begin{pmatrix} \varphi_1(\alpha(x_0)) \\ \varphi_2(\alpha(x_0)) \\ \vdots \\ \varphi_r(\alpha(x_0)) \end{pmatrix}, \begin{pmatrix} \varphi_1(\alpha(x_1)) \\ \varphi_2(\alpha(x_1)) \\ \vdots \\ \varphi_r(\alpha(x_1)) \end{pmatrix}, \ldots, \begin{pmatrix} \varphi_1(\alpha(x_r)) \\ \varphi_2(\alpha(x_r)) \\ \vdots \\ \varphi_r(\alpha(x_r)) \end{pmatrix}$$

are affinely independent.

Proof. Suppose that an affine map $\alpha\colon \mathbb{R}^N \to \mathbb{R}^N$ is given. We may write it in the form $\alpha(x) = Ax + v$ for an $N \times N$ matrix A and a vector $v \in \mathbb{R}^N$. Given vectors $u_1, u_2, \ldots, u_r \in \mathbb{R}^N$, constants $c_1, c_2, \ldots, c_r \in \mathbb{R}$ and $1 \leq l \leq m$, we have

$$(\langle \alpha(x), u_i \rangle + c_i)^l = (\langle Ax + v, u_i \rangle + c_i)^l = (\langle x, A^T u \rangle + (\langle v, u_i \rangle + c_i))^l.$$

But then, since $x_0, x_1, \ldots, x_r$ are $\mathcal{F}_{N,d,m}$-incident, it follows that so are $\alpha(x_0)$, $\alpha(x_1), \ldots, \alpha(x_r)$. Apply Proposition 6.9 to $\alpha(x_0), \alpha(x_1), \ldots, \alpha(x_r)$, from which the first claim in the proposition follows.

For the second part, observe that if $\alpha(x_0), \alpha(x_1), \dots, \alpha(x_r)$ are $\mathcal{F}_{N,d,m}$-incident, then by the previous arguments, so are $x_0 = \alpha^{-1}(\alpha(x_0))$, $x_1 = \alpha^{-1}(\alpha(x_1)), \dots,$ $x_r = \alpha^{-1}(\alpha(x_r))$. Therefore, the points $\alpha(x_0)$, $\alpha(x_1), \dots, \alpha(x_r)$ are not $\mathcal{F}_{N,d,m}$-incident. Proposition 6.9 applies, and gives the desired $(\leq m)$-functions. □

6.5 Proof of $\alpha(n, d) = o_d(n)$

Lemma 6.11. *Let $m, r, N \in \mathbb{N}$. Suppose that $y_1, y_2, \dots, y_r \in \mathbb{R}^N$ are some vectors with the property that* $\operatorname{rank}\{y_1, y_2, \dots, y_r\} + m - 1 \geq r$*. Suppose further that $y_1, y_2, \dots, y_r$ are distinct and have non-zero coordinates. Then we may find $(\leq m)$-functions $\varphi_1, \varphi_2, \dots, \varphi_r$ for which the vectors*

$$\begin{pmatrix} \varphi_1(y_1) \\ \varphi_2(y_1) \\ \vdots \\ \varphi_r(y_1) \end{pmatrix}, \begin{pmatrix} \varphi_1(y_2) \\ \varphi_2(y_2) \\ \vdots \\ \varphi_r(y_2) \end{pmatrix}, \dots, \begin{pmatrix} \varphi_1(y_r) \\ \varphi_2(y_r) \\ \vdots \\ \varphi_r(y_r) \end{pmatrix}$$

are linearly independent.

Proof. We prove the lemma by induction, first on m, then on r. Observe that in the case when $m = 1$, for a $(\leq m)$-function φ, the resulting function $\varphi(x)$ is just evaluation of x at a chosen coordinate. Hence, for $m = 1$ we are actually asked to find a set of coordinates I of size r, such that y_i are still linearly independent when restricted to I. Applying Lemma 6.6 proves the claim in this case.

Suppose now that the claim holds for some $m' \geq 1$. Write $m = m' + 1$. For fixed m, we prove the lemma by induction on $r \geq 1$. If $r = 1$, then, take $\varphi \colon [1] \to [N]$, given by $\varphi(1) = 1$, so the vector $\varphi(y_1) = (y_1)_1$ is non-zero.

Suppose that the claim holds for some $r \geq 1$, and that $\{y_1, y_2, \dots, y_{r+1}\}$ satisfy the assumptions of the lemma.

Case 1. $y_{r+1} \notin \operatorname{span}\{y_1, y_2, \dots, y_r\}$. Then $r + 1 \leq \operatorname{rank}\{y_1, y_2, \dots, y_{r+1}\} + m - 1 = \operatorname{rank}\{y_1, y_2, \dots, y_r\} + m$, hence $\operatorname{rank}\{y_1, y_2, \dots, y_r\} + m - 1 \geq r$. By the induction hypothesis, we have ($\leq m$)-functions $\varphi_1, \varphi_2, \ldots, \varphi_r$ such that

$$\begin{pmatrix} \varphi_1(y_1) \\ \varphi_2(y_1) \\ \vdots \\ \varphi_r(y_1) \end{pmatrix}, \begin{pmatrix} \varphi_1(y_2) \\ \varphi_2(y_2) \\ \vdots \\ \varphi_r(y_2) \end{pmatrix}, \ldots, \begin{pmatrix} \varphi_1(y_r) \\ \varphi_2(y_r) \\ \vdots \\ \varphi_r(y_r) \end{pmatrix}$$

are linearly independent. Hence, there are unique scalars $\lambda_1, \lambda_2, \ldots, \lambda_r \in \mathbb{R}$ such that $\varphi_i(y_{r+1}) = \sum_{j=1}^r \lambda_j \varphi_i(y_j)$ holds for all $i = 1, \ldots, r$. But, the vector y_{r+1} is not in the span$\{y_1, \ldots, y_r\}$, and so $y_{r+1} \neq \sum_{j=1}^r \lambda_j y_j$. Hence, we can pick $\varphi_{r+1}\colon [1] \to [N]$ to be $\varphi(1) = c$, where c is the coordinate such that $(y_{r+1})_c \neq \sum_{j=1}^r \lambda_j (y_j)_c$, finishing the proof in this case.

Case 2. $y_{r+1} \in \operatorname{span}\{y_1, y_2, \ldots, y_r\}$. Then $r+1 \leq \operatorname{rank}\{y_1, y_2, \ldots, y_{r+1}\} + m - 1 = \operatorname{rank}\{y_1, y_2, \ldots, y_r\} + m - 1$, so

$$r \leq \operatorname{rank}\{y_1, y_2, \ldots, y_r\} + m - 2.$$

By the induction hypothesis, we have ($\leq m-1$)-functions $\varphi_1, \ldots, \varphi_r$ for which

$$\begin{pmatrix} \varphi_1(y_1) \\ \varphi_2(y_1) \\ \vdots \\ \varphi_r(y_1) \end{pmatrix}, \begin{pmatrix} \varphi_1(y_2) \\ \varphi_2(y_2) \\ \vdots \\ \varphi_r(y_2) \end{pmatrix}, \ldots, \begin{pmatrix} \varphi_1(y_r) \\ \varphi_2(y_r) \\ \vdots \\ \varphi_r(y_r) \end{pmatrix}$$

are linearly independent. As before, there are unique scalars $\lambda_1, \lambda_2, \ldots, \lambda_r \in \mathbb{R}$ such that $\varphi_i(y_{r+1}) = \sum_{j=1}^r \lambda_j \varphi_i(y_j)$ holds for all $i = 1, \ldots, r$.

We try to take φ_{r+1} to be some φ_i with an additional element in the domain, mapped to $c \in [N]$. If this works, we are done. Otherwise, for all $i = 1, \ldots, r$ and $c \in [N]$, we have $\varphi_i(y_{r+1})(y_{r+1})_c = \sum_{j=1}^r \lambda_j \varphi_i(y_j)(y_j)_c$. Since the coordinates are non-zero, we get

$$\varphi_i(y_{r+1}) = \sum_{j=1}^{r} (\lambda_j \cdot (y_j)_c/(y_{r+1})_c)\, \varphi_i(y_j).$$

But, by uniqueness of λ_j, we must have $\lambda_j \cdot (y_j)_c/(y_{r+1})_c = \lambda_j$ for all j, c. If some $\lambda_j \neq 0$, then for all c we get $(y_j)_c/(y_{r+1})_c = 1$, i.e. $y_{r+1} = y_j$ which is a contradiction, as our vectors are distinct. Otherwise, all the coefficients λ_j are 0, so $\varphi_1(y_{r+1}) = 0$, but coordinates of y_{r+1} are non-zero, resulting in a contradiction once again. $\square$

The next result is a corollary of the algebraic lemma we have just proved. It is consistent with the intuition we described in the introduction. There we said that we expected lines in $[m+1]^N$ to be the sources of the non-trivial $\mathcal{F}_{N,m+1,m}$-incident sets. In other words, a $\mathcal{F}_{N,m+1,m}$-incident set is either of size larger than $m+2$, and thus its image must be affinely dependent (by looking at dimension of the target space), or the set is on a line.

Corollary 6.12. *Suppose that $S \subseteq \mathbb{R}^N$ is $\mathcal{F}_{N,m+1,m}$-incident. Then, $|S| \geq m+2$ and if $|S| = m+2$, then S is a subset of a line.*

Proof. If $|S| \geq m+3$, we are done. Suppose now that $|S| \leq m+2$. Let $s_0, s_1, \dots, s_{m+1}$ be the elements of S. We can find an affine isomorphism $\alpha\colon \mathbb{R}^N \to \mathbb{R}^N$ such that $\alpha(s_0) = 0$, and $y_i = \alpha(s_i)$, for $i = 1, 2, \dots, m+1$, are distinct and have non-zero coordinates. By Proposition 6.10 (note that we may apply it because $|S|-1 \leq m+1$, and $m+1$ is the dimension of the target space), the vectors

$$\begin{pmatrix} \varphi_1(y_1) \\ \varphi_2(y_1) \\ \vdots \\ \varphi_{m+1}(y_1) \end{pmatrix}, \begin{pmatrix} \varphi_1(y_2) \\ \varphi_2(y_2) \\ \vdots \\ \varphi_{m+1}(y_2) \end{pmatrix}, \dots, \begin{pmatrix} \varphi_1(y_{m+1}) \\ \varphi_2(y_{m+1}) \\ \vdots \\ \varphi_{m+1}(y_{m+1}) \end{pmatrix}$$

are linearly dependent, for any choice of $(\leq m)$-functions $\varphi_1, \varphi_2, \dots, \varphi_{m+1}$ to $[N]$. Thus, Lemma 6.11 would give us contradiction, unless

$$\operatorname{rank}\{y_1, y_2, \dots, y_{m+1}\} + m - 1 \leq m.$$

So $\operatorname{rank}\{y_1, y_2, \dots, y_{m+1}\} \leq 1$, and as $y_1 \neq 0$, there are scalars $\lambda_1, \dots, \lambda_{m+1}$ such that $y_i = \lambda_i y_1$ holds for all $i = 1, \dots, m+1$. But, since α is an affine isomorphism, the points $s_0 = \alpha^{-1}(0)$, $s_1 = \alpha^{-1}(y_1), \dots,$ $s_{m+1} = \alpha^{-1}(y_{m+1})$ are on a line, as desired. □

Theorem 6.13. *For $d, n \in \mathbb{N}$, $d \geq 2$, we have $\alpha(n,d) = o_d(n)$.*

Proof. For notational consistency with previous results, we set $m = d-1$. Let $\epsilon > 0$ be arbitrary and let N be sufficiently large so that ϵ-density Hales-Jewett theorem holds for the combinatorial lines in $[m+2]^N$. Let $X = [m+2]^N$, and let f be the function given by Proposition 6.5 applied to X and $\mathcal{F}_{N,m+1,m}$. Since

$\mathcal{F}_{N,m+1,m}$ separates the points of X, we may assume that f is injective on X. Finally, let $Y = f(X) \subseteq \mathbb{R}^{m+1}$. We claim that Y has no more than $m+2$ points in a hyperplane, and that all subsets of Y of size at least $\epsilon|Y|$ have a hyperplane containing $m+2$ points.

There are no more than $m+2$ points of Y on a hyperplane. Look at a hyperplane H and suppose that Y has $m+3$ points $y_1, \ldots, y_{m+3}$ inside H. Look at a maximal affinely independent subset of $y_1, \ldots, y_{m+3}$, w.l.o.g. this is $y_1, y_2, \ldots, y_r$ for some r. Since H is m-dimensional affine subspace, we have $r \leq m+1$. So $S_1 = \{y_1, y_2, \ldots, y_r, y_{m+2}\}$ is affinely dependent, and has size at most $m+2$. Then, by the definition of f and Proposition 6.5, $T_1 = f^{-1}(S_1)$ is $\mathcal{F}_{N,m+1,m}$-incident. Since f is a bijection from X onto its image, T_1 has size at most $m+2$, so by Corollary 6.12, T_1 is a subset of a line, and $|T_1| = m+2$ and $r = m+1$. Applying the same arguments to $S_2 = \{y_1, \ldots, y_r, y_{m+3}\}$ and $T_2 = f^{-1}(S_2)$, we have that T_2 is also a subset of a line and has size $m+2$ and also $|T_1 \cap T_2| = m+1$. But, as $T_1, T_2 \subseteq [m+2]^N$, this is impossible and we have a contradiction, so Y has no more than $m+2$ points on a hyperplane.

Dense subsets of Y are not in general position. Let $S \subseteq Y$ have size at least $\epsilon|Y|$. Then $T = f^{-1}(S)$ has a combinatorial line L by the density Hales-Jewett theorem. Hence, $f(L) \subseteq S$ and S has $m+2$ points that lie on the same hyperplane, by Lemma 6.7. This finishes the proof. □

6.6 Better bounds for certain dimensions

In this section, we provide better bounds on $\alpha(n,d)$ for certain dimensions d. The key difference in this approach is the use of a more efficient version of density Hales-Jewett theorem, which we now state.

Theorem 6.14 (Generalized Sperner's Theorem, [14], Theorem 2.3)**.** *Let $\mathcal{A}$ be a collection of subsets of $[n]$ that contains no d-dimensional combinatorial subspace. Then the size of $\mathcal{A}$ is at most $(25/n)^{1/2^d} 2^n$.*

Here, we consider the points in $\{0,1\}^N \subseteq \mathbb{R}^N$, which we also interpret as subsets of $[N]$. Observe that, given an $(\leq m)$-function φ to $[N]$, with image $S \subseteq [N]$ and a point $x \in \{0,1\}^N$ corresponding to $X \subseteq [N]$ (by setting $X :=$

$\{i \in [N]\colon x_i = 1\})$, we have

$$f(x) = \mathbb{1}_{S \subseteq X},$$

where, for a general property P, the value of $\mathbb{1}_P$ is 1, when P holds, and zero otherwise. Hence, we can reinterpret Proposition 6.10 in the language of sets as follows. Suppose that $\emptyset, X_1, X_2, \ldots, X_r$ correspond to $r+1$ points in $\{0,1\}^N$ which are not $\mathcal{F}_{N,d,m}$-incident (so the first point is 0). Then, there are sets $S_1, S_2, \ldots, S_r \subseteq [N]$ of size at most m, for which the vectors

$$\begin{pmatrix} \mathbb{1}_{S_1 \subseteq \emptyset} \\ \mathbb{1}_{S_2 \subseteq \emptyset} \\ \vdots \\ \mathbb{1}_{S_r \subseteq \emptyset} \end{pmatrix}, \begin{pmatrix} \mathbb{1}_{S_1 \subseteq X_1} \\ \mathbb{1}_{S_2 \subseteq X_1} \\ \vdots \\ \mathbb{1}_{S_r \subseteq X_1} \end{pmatrix}, \begin{pmatrix} \mathbb{1}_{S_1 \subseteq X_2} \\ \mathbb{1}_{S_2 \subseteq X_2} \\ \vdots \\ \mathbb{1}_{S_r \subseteq X_2} \end{pmatrix}, \ldots, \begin{pmatrix} \mathbb{1}_{S_1 \subseteq X_r} \\ \mathbb{1}_{S_2 \subseteq X_r} \\ \vdots \\ \mathbb{1}_{S_r \subseteq X_r} \end{pmatrix}$$

are affinely independent. If all the sets S_i are non-empty, then the vectors

$$\begin{pmatrix} \mathbb{1}_{S_1 \subseteq X_1} \\ \mathbb{1}_{S_2 \subseteq X_1} \\ \vdots \\ \mathbb{1}_{S_r \subseteq X_1} \end{pmatrix}, \begin{pmatrix} \mathbb{1}_{S_1 \subseteq X_2} \\ \mathbb{1}_{S_2 \subseteq X_2} \\ \vdots \\ \mathbb{1}_{S_r \subseteq X_2} \end{pmatrix}, \ldots, \begin{pmatrix} \mathbb{1}_{S_1 \subseteq X_r} \\ \mathbb{1}_{S_2 \subseteq X_r} \\ \vdots \\ \mathbb{1}_{S_r \subseteq X_r} \end{pmatrix}$$

are linearly independent. Now we show that actually no set S_i is empty. Otherwise, w.l.o.g. $S_1 = S_2 = \cdots = S_k = \emptyset$ and the others are non-empty, so after subtracting the vector $(\mathbb{1}_{S_1 \subseteq \emptyset} \mathbb{1}_{S_2 \subseteq \emptyset} \ldots \mathbb{1}_{S_r \subseteq \emptyset})^T$ from each vector $(\mathbb{1}_{S_1 \subseteq X_i} \mathbb{1}_{S_2 \subseteq X_i} \ldots \mathbb{1}_{S_r \subseteq X_i})^T$ with $i \geq 1$, we obtain that

$$\begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ \mathbb{1}_{S_{k+1} \subseteq X_1} \\ \vdots \\ \mathbb{1}_{S_r \subseteq X_1} \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ \mathbb{1}_{S_{k+1} \subseteq X_2} \\ \vdots \\ \mathbb{1}_{S_r \subseteq X_2} \end{pmatrix}, \ldots, \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ \mathbb{1}_{S_{k+1} \subseteq X_r} \\ \vdots \\ \mathbb{1}_{S_r \subseteq X_r} \end{pmatrix}$$

are linearly independent, which is not possible (when viewed as a matrix, the row rank is less than r). We sum up this discussion as the following observation.

Observation 6.15. *Suppose that the sets* $\emptyset, X_1, X_2, \ldots, X_r \subseteq [N]$ *correspond to* $r+1$ *points that are not* $\mathcal{F}_{N,d,m}$*-incident. Then, there are non-empty sets* $S_1, S_2, \ldots, S_r \subseteq \mathbb{N}$ *of size at most* m *such that the vectors*

$$\begin{pmatrix} \mathbb{1}_{S_1 \subseteq X_1} \\ \mathbb{1}_{S_2 \subseteq X_1} \\ \vdots \\ \mathbb{1}_{S_r \subseteq X_1} \end{pmatrix}, \begin{pmatrix} \mathbb{1}_{S_1 \subseteq X_2} \\ \mathbb{1}_{S_2 \subseteq X_2} \\ \vdots \\ \mathbb{1}_{S_r \subseteq X_2} \end{pmatrix}, \ldots, \begin{pmatrix} \mathbb{1}_{S_1 \subseteq X_r} \\ \mathbb{1}_{S_2 \subseteq X_r} \\ \vdots \\ \mathbb{1}_{S_r \subseteq X_r} \end{pmatrix}$$

are linearly independent.

Viewing these vectors together as an $r \times r$ matrix, we have found that the nullity of this matrix is related to the notion of $\mathcal{F}_{N,d,m}$-incidence. This motivates the study of the nullity of such matrices in general. Before stating the lemma which contains some basic results regarding this problem, we introduce some notation.

Given sets $A_1, A_2, \ldots, A_r, B_1, B_2, \ldots, B_s \in \mathbb{N}^{(<\omega)}$, we write

$$I(A_1, A_2, \ldots, A_r; B_1, B_2, \ldots, B_s)$$

for the $s \times r$ matrix with entries $I_{ij} = \mathbb{1}_{B_i \subseteq A_j}$. Further, we define

$$K(A_1, A_2, \ldots, A_r; B_1, B_2, \ldots, B_s)$$

for the kernel of I and

$$n(A_1, A_2, \ldots, A_r; B_1, B_2, \ldots, B_s)$$

for the nullity of I. Also, if A, B are finite sequences of finite sets, of lengths r and s, we write $I(A, B) = I(A_1, A_2, \ldots, A_r; B_1, B_2, \ldots, B_s)$, and similarly we define $K(A, B), n(A, B)$.

Lemma 6.16. *Let* $m, k \in \mathbb{N}$*. Given any distinct sets* $X_1, X_2, \ldots, X_r \in \mathbb{N}^{(<\omega)}$*, we can find sets* $S_1, S_2, \ldots, S_r \subseteq \mathbb{N}^{(\leq m)}$ *which enjoy the following property.*

(i) $n(X_1, X_2, \ldots, X_r; S_1, S_2, \ldots, S_r) = 0$*, provided* $r < 2^{m+1}$*.*

(ii) $n(X_1, X_2, \ldots, X_r; S_1, S_2, \ldots, S_r) \leq 1$*, provided* $r < 3 \cdot 2^m$*.*

We prove the lemma by induction and (ideas related to) compressions, and in fact use the part (**i**) in order to deduce the part (**ii**). As it will be stressed in the proof, there is a subtlety in proving $n(X_1, X_2, \ldots, X_r; S_1, S_2, \ldots, S_r) \leq 1$. Namely, the naive application of induction could only give $n(X_1, X_2, \ldots, X_r; S_1, S_2, \ldots, S_r) \leq 2$, and we actually use the first part of the lemma to obtain the required saving of 1 on the right hand side.

Proof. Part (i). We prove the claim by induction on $\sum_{i=1}^{r}|X_i|$. If this is zero, then we have $r = 1$ and $X_1 = \emptyset$, so just take $S_1 = \emptyset$.

Suppose that the lemma holds for smaller values of $\sum_{i=1}^{r}|X_i|$. Let $x \in \mathbb{N}$ be any element that is contained in at least one of the sets X_i. Denote by $\{Y_1, Y_2, \ldots, Y_u\}$ the collection of sets given by $\{X_i \setminus \{x\} : i = 1, \ldots, r\}$, and further let $\{Z_1, \ldots, Z_v\}$ be the set $\{X_i : x \notin X_i, X_i \cup \{x\} = X_j \text{ for some } j\}$. Thus $v \leq u$ and $u + v = r$. By the induction hypothesis, there are relevant sets $S_1, \ldots, S_u \in \mathbb{N}^{(\leq m)}$ for $Y_1, \ldots, Y_u$. Also, since $v \leq r/2 < 2^m$, we have relevant sets $S'_{u+1}, \ldots S'_r \in \mathbb{N}^{(\leq m-1)}$ for $Z_1, Z_2, \ldots, Z_v$, and note that w.l.o.g. none of $S_1, S_2, \ldots, S_u, S'_{u+1}, \ldots, S'_r$ contains x. Set $S_{u+i} = S'_{u+i} \cup \{x\}$ for all $i = 1, \ldots, v$. We claim that the sets $S_1, S_2, \ldots, S_r$ have the desired property. So far, we know that for all i, $|S_i| \leq m$ holds.

Let $(\lambda_1 \lambda_2 \ldots \lambda_r)^T$ be an element of the kernel $K(X, S)$. We can rewrite this as $\sum_{j : S_i \subseteq X_j} \lambda_j = 0$ for all $i = 1, 2, \ldots, r$. Define $\mu_i = \sum_{j : Y_i = X_j \setminus \{x\}} \lambda_j$, for each $i = 1, \ldots, u$. Then, recalling that $x \notin S_i$ for $i \leq u$, we have $\sum_{j : S_i \subseteq Y_j} \mu_j = \sum_{j : S_i \subseteq X_l} \lambda_l = 0$ for all $i = 1, 2, \ldots, u$. Since $n(Y_1, Y_2, \ldots, Y_u; S_1, S_2, \ldots, S_u) = 0$, we infer $\mu_j = 0$ for all j. Returning to the definition of μ_i, we have that whenever j is such that $x \in X_j$, but $X_j \setminus \{x\}$ is not any of the sets X_l, then there is i such that $\lambda_j = \mu_i$, so λ_j must vanish.

Hence, for $i > u$, we have that $x \in S_i$ and $\sum_j \lambda_j \mathbb{1}_{S_i \subseteq X_j} = 0$, when the sum is taken over all j such that $x \in X_j$, but $X_j \setminus \{x\}$ is not any of the sets X_l. Set $\nu_i = -\lambda_j$ for $Z_i = X_j$, which by previous work is the same as $\nu_i = \lambda_l$ for l such that $X_l \setminus \{x\} = Z_i$ and $x \in X_l$. Therefore, for $i > u$, we have

$$\sum_{j : S'_i \subseteq Z_j} \nu_j = \sum_{j : S_i \subseteq Z_j \cup \{x\}} \nu_j = \sum_{j : S_i \subseteq X_j} \lambda_j = 0$$

with no additional restrictions on j apart those written in the sums. Hence, the vector $(\nu_1\nu_2\dots\nu_v)^T$ must lie inside $K(Z_1, Z_2, \dots, Z_v; S'_{u+1}, S'_{u+2}, \dots, S'_r)$. But thus kernel is trivial, so all $\nu_i = 0$. Finally, this implies that $\lambda_i = 0$ holds for the remaining i, as desired.

Part (ii). We follow similar steps as in the previous part. However, we have to be slightly careful, since the previous argument unchanged would give us that $K(X_1, X_2, \dots, X_r; S_1, S_2, \dots, S_r)$ is essentially a sum of kernels of similar matrices for $Y_1, Y_2, \dots, Y_u$ and $Z_{u+1}, Z_{u+2}, \dots, Z_r$. This way, we could be 1 dimension short of the desired goal, as this argument only allows us to deduce $n(X_1, X_2, \dots, X_r; S_1, S_2, \dots, S_r) \leq 2$, so we have to be more efficient. In order to overcome this issue, we shall apply the part (i) of the lemma.

We prove the claim by induction on $\sum_{i=1}^r |X_i|$. If this is zero, then we have $r = 1$ and $X_1 = \emptyset$, so just take $S_1 = \emptyset$.

Suppose that the lemma holds for smaller values of $\sum_{i=1}^r |X_i|$. Let $x \in \mathbb{N}$ be any element that is contained in at least one of the sets X_i. Denote by $\{Y_1, Y_2, \dots, Y_u\}$ the collection of sets given by $\{X_i \setminus \{x\}: i = 1, \dots, r\}$, and further let $\{Z_1, \dots, Z_v\}$ be the set $\{X_i: x \notin X_i, X_i \cup \{x\} = X_j \text{ for some } j\}$. Thus $v \leq u$ and $u + v = r$. Pick the sets $S_1, S_2, \dots, S_u \in \mathbb{N}^{(\leq m)}$ such that $U = K(Y_1, Y_2, \dots, Y_u; S_1, S_2, \dots, S_u)$ is of minimum dimension. Further, pick the sets $S'_{u+1}, S'_{u+2}, \dots, S'_r \in \mathbb{N}^{(\leq m-1)}$ such that $V = K(Z_1, Z_2, \dots, Z_v; S'_{u+1}, S'_{u+2}, \dots, S'_r)$ is of minimum dimension. W.l.o.g. we may assume that $x \notin S_i, S'_j$. Finally, set $S_{u+i} = S'_{u+i} \cup \{x\}$ for $i = 1, \dots, v$. All S_i have size at most m.

By the induction hypothesis, we have $\dim U \leq 1$ and, since $v \leq r/2 < 3{\cdot}2^{m-1}$, we also have $\dim V \leq 1$. However, we can make a saving of one dimension as promised. Suppose that $\dim U = \dim V = 1$. Then, by the part (i), since U, V are of the minimum possible dimension, we must have $u \geq 2^{m+1}$ and $v \geq 2^m$, which is a contradiction as $u + v = r < 3 \cdot 2^m$. Therefore, $\dim U + \dim V \leq 1$. We shall now finish the proof by similar arguments as in the previous case, however we need to treat the cases when $\dim U = 1$ and $\dim V = 1$ separately.

We may reorder $X_1, X_2, \dots, X_r$, if necessary, to have $Y_i = X_i \setminus \{x\}$, for $i = 1, 2, \dots, u$, and $Z_i = X_{u+i} \setminus \{x\}$ with $x \in X_{u+i}$ for $i = 1, 2, \dots, v$. Furthermore, we may also assume that $Z_i = X_{u-v+i}$ with $x \notin X_{u-v+i}$ for $i = 1, 2, \dots, v$. Now proceed as in the part (i), with the argument modified to deal with the possibly non-trivial kernels. Suppose that $\lambda_1, \dots, \lambda_r \in \mathbb{R}$ are such that $\sum_{j:S_i \subseteq X_j} \lambda_j = 0$ for all $i = 1, 2, \dots, r$. Define $\mu_i = \sum_{j:Y_i = X_j \setminus \{x\}} \lambda_j$, for each $i = 1, \dots, u$, thus

$$\mu_i = \begin{cases} \lambda_i & \text{if } i \leq u - v \\ \lambda_i + \lambda_{i+v} & \text{if } u - v < i \leq u \end{cases}$$

Then we have $\sum_{j:S_i \subseteq Y_j} \mu_j = 0$ for all $i = 1, 2, \dots, u$. This thus gives $\mu \in U$. Next, set $\nu_i = \lambda_j$ for $Z_i = X_j$, i.e. $\nu_i = \lambda_{u+i}$ for $i = 1, 2, \dots, v$. We have (note the restriction on the index $j \in [u - v]$ in some of the sums)

$$\begin{aligned} 0 &= \sum_{j:S_i \subseteq X_j} \lambda_j \\ &= \sum_{j:S_i' \cup \{x\} \subseteq Z_j \cup \{x\}} \nu_j + \sum_{j \in [u-v]:S_i \subseteq X_j} \lambda_j \\ &= \sum_{j:S_i' \subseteq Z_j} \nu_j + \sum_{j \in [u-v]:S_i \subseteq X_j} \lambda_j \end{aligned} \tag{6.2}$$

for all $i = u + 1, \dots, r$. Note also that we can express λ_i in terms of μ_i and ν_i as follows

$$\lambda_i = \begin{cases} \mu_i & \text{if } i \leq u - v \\ \mu_i - \nu_{i+v-u} & \text{if } u - v < i \leq u \\ \nu_{i-u} & \text{if } u < i \end{cases} \tag{6.3}$$

Case 1. $\dim U = 0, \dim V = 1$.

As $U = \{0\}$, we must have all $\mu_j = 0$. Therefore, $\lambda_j = 0$ for $j \leq u - v$, which implies that

$$\sum_{j:S_i' \subseteq Z_j} \nu_j = 0$$

for all $i = 1, 2, \dots, u$. Therefore, $\nu \in V$. Using the expressions (6.3), we see that we can express any given $\lambda \in K(X_1, X_2, \dots, X_r;\ S_1, S_2, \dots, S_r)$ as a sum of vectors in two subspaces of $\mathbb{R}^r$, isomorphic to U and V, so $K(X_1, X_2, \dots, X_r;$ $S_1, S_2, \dots, S_r)$ is a subset of at most 1-dimensional subspace, as desired.

Case 2. $\dim V = 0, \dim U = 1$.

Now, the scalars μ_j might be non-trivial. On the other hand, due to the equation (6.2) we have

$$\sum_{j:S_i' \subseteq Z_j} \nu_j = - \sum_{j \in [u-v]:S_i \subseteq X_j} \lambda_j,$$

which, combined with the fact that $V = \{0\}$, implies that ν_j are uniquely determined by the choice of μ_j. Finally, relationships in (6.3) show once again that λ_j lies in an (at most) 1-dimensional subspace, as desired. $\square$

The following corollary is just a modification of the lemma in the case when all the sets are non-empty. The need for this additional technicality comes from Observation 6.15.

Corollary 6.17. *Let $m, k \in \mathbb{N}$. Given any distinct non-empty sets $X_1, X_2, \ldots, X_r \in \mathbb{N}^{(<\omega)}$, we can find non-empty sets $S_1, S_2, \ldots, S_r \subseteq \mathbb{N}^{(\leq m)}$ which enjoy the following property.*

(i) *$n(X_1, X_2, \ldots, X_r; S_1, S_2, \ldots, S_r) = 0$, provided $r < 2^{m+1} - 1$.*

(ii) *$n(X_1, X_2, \ldots, X_r; S_1, S_2, \ldots, S_r) \leq 1$, provided $r < 3 \cdot 2^m - 1$.*

Proof. In both cases, we apply Lemma 6.16 to distinct sets $\emptyset, X_1, X_2, \ldots, X_r$ to find sets $S_0, S_1, \ldots, S_r$ of size at most m such that

$$n(\emptyset, X_1, X_2, \ldots, X_r; S_0, S_1, S_2, \ldots, S_r) \leq q,$$

where $q = 0$ if $r < 2^{m+1} - 1$, and $q = 1$ if $r < 3 \cdot 2^m - 1$. We now show that, starting from

$$n(\emptyset, X_1, X_2, \ldots, X_r; S_0, S_1, S_2, \ldots, S_r) \leq q,$$

we can reorder the sets S_i so that

$$n(X_1, X_2, \ldots, X_r; S_1, S_2, \ldots, S_r) \leq q,$$

which finishes the proof.

Let I be the matrix $I(\emptyset, X_1, X_2, \ldots, X_r; S_0, S_1, S_2, \ldots, S_r)$. By the rank-nullity theorem, the rank of I (which is also the column rank) is at least $r + 1 - q$. If all the sets S_i are non-empty, then the first column of I is zero. Removing the first row from I, we get a matrix with the column rank also $\geq r + 1 - q$, thus having the row rank also $\geq r + 1 - q$. Remove the first row, the remaining matrix is $I(X_1, X_2, \ldots, X_r; S_1, S_2, \ldots, S_r)$ and it has the row rank at least $r - q$. Thus its rank is at least $r - q$, so by the rank-nullity theorem, $n(X_1, X_2, \ldots, X_r; S_1, S_2, \ldots, S_r) \leq q$, as desired.

On the other hand, if $S_0 = \emptyset$ (after reordering if necessary), remove the first row from I, to get a matrix with the row rank at least $r - q$, and whose first column is zero. But removing the first column does not change the column rank, and we end up with the matrix $I(X_1, X_2, \ldots, X_r;\ S_1, S_2, \ldots, S_r)$ of the column rank $\geq r - q$, which by the rank-nullity theorem gives

$$n(X_1, X_2, \ldots, X_r; S_1, S_2, \ldots, S_r) \leq q,$$

as desired. □

The next corollary is tailored to the analysis of the $\mathcal{F}_{N,d,m}$-incident sets (see Corollary 6.20).

Corollary 6.18. *Suppose that $X_1, X_2, \ldots, X_r \in \mathbb{N}^{(<\omega)}$ are distinct, $t \leq r$ and $S_1, S_2, \ldots, S_t \in \mathbb{N}^{(<\omega)}$ satisfy*

$$n(X_1, X_2, \ldots, X_t; S_1, S_2, \ldots, S_t) = 0.$$

Provided $r < 3 \cdot 2^m$, we can find sets $S_{t+1}, S_{t+2}, \ldots,\ S_r \in \mathbb{N}^{(\leq m)}$ such that

$$n(X_1, X_2, \ldots, X_r; S_1, S_2, \ldots, S_r) \leq 1.$$

If $r < 3 \cdot 2^m - 1$ and the sets X_i are non-empty, then additionally, the sets $S_{t+1}, S_{t+2}, \ldots, S_r$ can be chosen to be non-empty.

Proof. Apply the part **(ii)** of Lemma 6.16, to get sets $T_1, T_2, \ldots, T_r \in \mathbb{N}^{(\leq m)}$ such that

$$n(X_1, X_2, \ldots, X_r; T_1, T_2, \ldots, T_r) \leq 1,$$

or Corollary 6.17 to make the sets T_i non-empty, provided $r < 3 \cdot 2^m - 1$ holds and the sets X_i are non-empty. Look at the $(t + r) \times r$ matrix $I(X_1, X_2, \ldots, X_r;$ $S_1, S_2, \ldots, S_t,\ T_1, T_2, \ldots, T_r)$. We shall remove t rows from those corresponding to $T_1, T_2, \ldots, T_r$ to get the desired matrix. The following row-removal lemma does this for us.

Lemma 6.19. *Suppose that A is an $(r + t) \times r$ matrix with the first t rows linearly independent and $t \leq r$. Then we can remove t rows from the last r rows of A, so that the kernel of A is not affected.*

Proof. If $I \subseteq [r+t]$, let A_I stand for the matrix formed from the rows of A with indices in I. Starting from the set $I = [r+s]$, we shall iteratively remove elements greater than t from I, so that at each step we have $\ker A_I = \ker A$.

Suppose that we have $I \subseteq [r+t]$ with $[t] \subseteq I$, but $|I|> r$, such that $\ker A_I = \ker A$ holds. If we can pick an element $x \in I \setminus [t]$, so that $\ker A_{I\setminus\{x\}} = \ker A_I$, we are done. Otherwise, no such x works. Observe that if a row v^T of A_I is a linear combination of the other rows, then it can be removed from A_I. To spell it out, write v_i^T for i^{th} row of A and suppose that $v_i^T = \sum_{j\in I\setminus\{i\}} \lambda_j v_j^T$. Then, if $\mu \in \ker A_{I\setminus\{i\}}$, we have $\mu \cdot v_i^T = \sum_{j\in I\setminus\{i\}} \lambda_j \mu \cdot v_j^T = 0$. So $\ker A_{I\setminus\{x\}} = \ker A_I$.

Thus, the vectors $v_1^T, \dots, v_t^T$ are linearly independent, and $v_i \notin \operatorname{span}\{v_j\colon j \in I \setminus \{i\}\}$ for $i \in I \setminus [t]$. But, then, $|I| > r$ and the rows of I are linearly independent vectors of the dimension r, which is a contradiction. Hence, we can proceed, until we reach $|I| = r$, as desired. ∎

The matrix

$$I(X_1, X_2, \dots, X_r; S_1, S_2, \dots, S_t, T_1, T_2, \dots, T_r)$$

satisfies the conditions of the lemma since $n(X_1, X_2, \dots, X_t;\ S_1, S_2, \dots, S_t) = 0$. By applying the lemma, we can pick $S_{t+1}, S_{t+2}, \dots, S_r$ among the sets in $T_1, T_2, \dots, T_r$ so that

$$\begin{aligned}
&n(X_1, X_2, \dots, X_r; S_1, S_2, \dots, S_r)\\
=&n(X_1, X_2, \dots, X_r; S_1, S_2, \dots, S_t, T_1, T_2, \dots, T_r)\\
\le&n(X_1, X_2, \dots, X_r; T_1, T_2, \dots, T_r)\\
\le&1.
\end{aligned}$$

∎

Similarly to Corollary 6.12, the next corollary is consistent with the somewhat vague idea that the combinatorial subspaces are the source of the non-trivial $\mathcal{F}_{N,d,m}$-incident sets. In particular, we show that the $\mathcal{F}_{N,d,m}$-incident sets behave like the combinatorial subspaces when it comes to taking unions – the size of a union of two $\mathcal{F}_{N,d,m}$-incident sets of size 2^{m+1} is at least $3 \cdot 2^m$.

Corollary 6.20. *Let $d, m \in \mathbb{N}$ be given.*

(i) *If $T \subseteq \{0,1\}^N$ is $\mathcal{F}_{N,d,m}$-incident, then $|T| \geq \min\{d+2, 2^{m+1}\}$.*

(ii) *If $T_1, T_2 \subseteq \{0,1\}^N$ are distinct, of size at most $d+1$ and minimal (w.r.t. inclusion) $\mathcal{F}_{N,d,m}$-incident, then $|T_1 \cup T_2| \geq 3 \cdot 2^m$.*

Proof. Part (i). Suppose that $T = \{x_0, x_1, x_2, \dots, x_r\} \subseteq \{0,1\}^N$ is $\mathcal{F}_{N,d,m}$-incident and that $r < 2^{m+1} - 1, d+1$. Note that, for a fixed set A, the map $X \mapsto X \Delta A$, induces a reflection $\alpha\colon \mathbb{R}^N \to \mathbb{R}^N$ (with the natural correspondence between sets and points in $\{0,1\}^N$). In particular, taking A to be the set of non-zero coordinates of x_0, we have an affine isomorphism α that preserves the cube $\{0,1\}^N$ and sends x_0 to zero. Let $X_i \subseteq [N]$ be the set corresponding to $\alpha(x_i)$, i.e. the set of indices j such that $\alpha(x_i)_j = 1$. As $r < 2^{m+1} - 1$, Corollary 6.17 yields non-empty sets $S_1, S_2, \dots, S_r \subseteq [N]$ of size at most m, such that

$$n(X_1, X_2, \dots, X_r; S_1, S_2, \dots, S_r) = 0.$$

Choosing $(\leq m)$-functions $\varphi_1, \varphi_2, \dots, \varphi_r$ with images $S_1, S_2, \dots, S_r$ respectively, we obtain that the vectors

$$\begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \begin{pmatrix} \varphi_1(\alpha(x_1)) \\ \varphi_2(\alpha(x_1)) \\ \vdots \\ \varphi_r(\alpha(x_1)) \end{pmatrix}, \begin{pmatrix} \varphi_1(\alpha(x_2)) \\ \varphi_2(\alpha(x_2)) \\ \vdots \\ \varphi_r(\alpha(x_2)) \end{pmatrix}, \dots, \begin{pmatrix} \varphi_1(\alpha(x_r)) \\ \varphi_2(\alpha(x_r)) \\ \vdots \\ \varphi_r(\alpha(x_r)) \end{pmatrix}$$

are affinely independent. But, as $r \leq d$, Proposition 6.10 applies to T, affine map α and functions $\varphi_1, \varphi_2, \dots, \varphi_r$, which tells us that these vectors are affinely dependent, which is a contradiction. Thus $|T| = r + 1 \geq \min\{2^{m+1}, d+2\}$ as desired.

Part (ii). If T_1, T_2 are disjoint, then by part (i), $|T_1 \cup T_2| \geq 2^{m+2}$, so we are done. Thus, assume that some t_0 belongs to both sets. Pick an affine isomorphism $\alpha\colon \mathbb{R}^N \to \mathbb{R}^N$ which sends t_0 to zero and preserves the cube $\{0,1\}^N$ (given by a suitable reflection). Let $X_1, X_2, \dots, X_t$ be the sets that correspond to the non-zero points of $\alpha(T_1 \cap T_2)$. Next, let $X_{t+1}, \dots, X_{t+r_1}$ be the sets that correspond to points in $\alpha(T_1 \setminus T_2)$ and let $X_{t+r_1+1}, \dots, X_{t+r_1+r_2}$ be the sets corresponding to points of $\alpha(T_2 \setminus T_1)$. If $|T_1 \cup T_2| \geq 3 \cdot 2^m$, we are done. Otherwise $1 + t + r_1 + r_2 = |T_1 \cup T_2| < 3 \cdot 2^m$.

Since they are minimal and distinct, T_1, T_2 cannot contain one another. So $T_1 \cap T_2$ is a proper subset of T_1 and hence it is not $\mathcal{F}_{N,d,m}$-incident. Therefore, by Observation 6.15, we can find non-empty sets $S_1, S_2, \ldots, S_t \in \mathbb{N}^{(\leq m)}$ such that

$$n(X_1, X_2, \ldots, X_t; S_1, S_2, \ldots, S_t) = 0.$$

Applying Corollary 6.18 (as $r + t_1 + t_2 < 3 \cdot 2^m - 1$), we obtain non-empty sets $S_{t+1}, \ldots, S_{t+r_1+r_2} \in \mathbb{N}^{(\leq m)}$ such that

$$n(X_1, X_2, \ldots, X_{r+t_1+t_2}, S_1, S_2, \ldots, S_{r+t_1+t_2}) \leq 1.$$

Now, take any $(\leq m)$-functions $\varphi_1, \ldots, \varphi_{t+r_1+r_2}$ to $[N]$ with images $S_1, S_2, \ldots, S_{t+r_1+r_2}$, and let $x_i \in T_1 \cup T_2$ be the point such that the set X_i corresponds to $\alpha(x_i)$. Write y_i for the vector $(y_i)_j = \varphi_j(x_i)$, $j = 1, 2, \ldots, t + r_1 + r_2$. Thus, $y_1, y_2, \ldots, y_t$ are linearly independent and the rank of $y_1, y_2, \ldots, y_{t+r_1+r_2}$ is at least $t + r_1 + r_2 - 1$. Since $|T_1| \leq d + 1$, we can apply Proposition 6.10 to T_1, map α and functions $f_1, \ldots, f_{t+r_1}$. Note that since the sets S_i are non-empty, we have $f_i(0) = 0$ for all i. Thus, vectors $y_1, y_2, \ldots, y_{t+r_1}$ have rank at most $t + r_1 - 1$. Similarly, the rank of the vectors $y_1, y_2, \ldots, y_t, y_{t+r_1+1}, \ldots, y_{t+r_1+r_2}$ is at most $t + r_2 - 1$.

To obtain a contradiction, look at

$$\begin{aligned}
U &= \operatorname{span}\{y_1, y_2, \ldots, y_{t+r_1}\}, \\
V &= \operatorname{span}\{y_1, y_2, \ldots, y_t, y_{t+r_1+1}, y_{t+r_1+2}, \ldots, y_{t+r_1+r_2}\}, \\
W &= \operatorname{span}\{y_1, y_2, \ldots, y_{t+r_1+r_2}\}, \text{ and} \\
Z &= \operatorname{span}\{y_1, y_2, \ldots, y_t\}.
\end{aligned}$$

Thus, $\dim Z = t$, $\dim U \leq t + r_1 - 1$, $\dim V \leq t + r_2 - 1$, $\dim W \geq t + r_1 + r_2 - 1$, $Z \subseteq U, V \subseteq W$ and $W = U + V$. Therefore $W/Z = U/Z + V/Z$. Finally,

$$\begin{aligned}
r_1 + r_2 - 1 &\leq \dim W - \dim Z = \dim W/Z \\
&\leq \dim U/Z + \dim V/Z \leq r_1 - 1 + r_2 - 1 = r_1 + r_2 - 2,
\end{aligned}$$

which is a contradiction. □

Theorem 6.21. *Suppose that $d, m \in \mathbb{N}$ satisfy $2^{m+1} - 1 \leq d \leq 3 \cdot 2^m - 3$. Let $N \geq 1$. Then*

$$\alpha(2^N, d) \leq \left(\frac{25}{N}\right)^{1/2^{m+1}} \cdot 2^N.$$

Proof. Let $X = \{0,1\}^N \subseteq \mathbb{R}^N$. Applying Proposition 6.5, we obtain a function $f \in \operatorname{span} \mathcal{F}_{N,d,m}$, which is a bijection onto its image when restricted to X and such that if $S \subseteq f(X)$ is affinely dependent then $f^{-1}(S)$ is $\mathcal{F}_{N,d,m}$-incident. Let $Y = f(X)$. Note that $|Y|= 2^N$, since f is injective on X. We claim that the set Y has no more than $d+1$ points on the same hyperplane, but all sufficiently large subsets of Y have $d+1$ cohyperplanar points.

No more than $d+1$ points on a hyperplane. Suppose that we have a cohyperplanar set $S = \{s_1, s_2, \ldots, s_{d+2}\} \subseteq Y$. Pick a maximal affinely independent subset $S' \subseteq S$. W.l.o.g. $S' = \{s_1, \ldots, s_r\}$, for some r. As S' is a subset of a hyperplane, we have $r \leq d$. Look at $S'_1 = S' \cup \{s_{d+1}\}$. By the choice of S', the set S'_1 is not affinely independent. By the choice of f, the preimage $f^{-1}(S'_1)$ is $\mathcal{F}_{N,d,m}$-incident. Find a subset T_1 of $f^{-1}(S'_1)$ which is minimal $\mathcal{F}_{N,d,m}$-incident, and arbitrary point p in T_1. We also have $S'_2 = S \setminus \{p\}$ affinely dependent, as it is a subset of a hyperplane of size at $d+1$. By the choice of f, $f^{-1}(S'_2)$ is $\mathcal{F}_{N,d,m}$-incident, and has a minimal $\mathcal{F}_{N,d,m}$-incident subset T_2. Note that $p \in T_1 \setminus T_2$, so T_1, T_2 are distinct, and $|T_1|, |T_2|\leq d+1$. The part **(ii)** of Corollary 6.20 applies to give $d+2 = |S|\geq |T_1 \cup T_2|\geq 3 \cdot 2^m > d+2$, which is a contradiction.

Dense subsets are not in general position. Let $T \subseteq Y$ be a set of size at least $\left(\frac{25}{N}\right)^{1/2^{m+1}} 2^N$. Then, by Theorem 6.14, $f^{-1}(T)$ contains an $(m+1)$-dimensional combinatorial subspace. Applying Lemma 6.7, we have that the points of $T = f(f^{-1}(T))$ are affinely dependent. Adding any $d+1-2^{m+1}$ points to the set T proves the claim. $\square$

6.7 Conclusion

Even though there are now some non-trivial lower bounds on $\alpha(n,d)$ ([11]), the gap between the lower and the upper bounds is still very large. Of course, the main question still is to determine the $\alpha(n,d)$. Regarding the current lower bounds on $\alpha(n,2)$, both in [17] and in [11], we note that their proofs are based on some relatively general probabilistic estimates of the independence number of hypergraphs. However, these approaches used very little of the structure of the given sets of points. In fact, possible algebraic properties of such sets have not been exploited. For example, if X is a set of points with no more than 3 on a line, but with no dense set in general position, we can expect that plenty of pairs of points in X have a unique third point in X on the line spanned by the pair. This gives rise to an algebraic operation: given two points x_1, x_2 of X, set $x_1 * x_2$ to be the third point of X on their line, if such a point exists. Of course, there is an issue of how to define $x_1 * x_2$ for all pairs, but at least for plenty of pairs it can be defined. Hopefully, if X is a set for which the value $\alpha(|X|, 2)$ is attained, we could deduce some properties of the operation $*$.

Returning to the estimates for $\alpha(n, d)$, the current situation with the upper bounds is that we have infinitely many d, for which $\alpha(n, d)/n = O(1/log^{\beta_d} n)$ for some $\beta_d > 0$, while for infinitely many other d, the bounds for $\alpha(n, d)/n$ currently come from the general density Hales–Jewett theorem, and are roughly comparable to the inverse of the Ackermann function. It is most certainly far from truth that $\alpha(n, d)/n$ is close to either of these estimates for any d. However, it would already be interesting to understand the relationship between the values of $\alpha(n, d)$ for consecutive dimensions d.

Question 6.22. *What is the relationship between $\alpha(n, d)$ and $\alpha(n, d + 1)$?*

Finally, one of the key tools in this chapter were the algebraic lemmas 6.11 and 6.16. It could be of interest to study further how the quantities like $n(X_1, X_2, \ldots, X_r; S_1, S_2, \ldots, S_r)$ depend on the structure of the sequences $X_1, \ldots, X_r$ and $S_1, \ldots, S_r$.

7 Small Sets with Large Difference Sets

7.1 Introduction

The problem of comparing different expressions involving the same subset A of an abelian group G (e.g. $A + A$ and $A - A$) is one of the central topics in additive combinatorics. For example, one of the starting points in the study of this field is the Plünnecke-Ruzsa inequality that bounds $|kA - lA|$ in terms of $|A|$ and $|A + A|$.

Theorem 7.1 (Plünnecke-Ruzsa inequality [43], [47]). *Let A be a subset of an abelian group. Then, for any $k, l \geq 1$ we have*

$$|kA - lA||A|^{k+l-1} \leq |A + A|^{k+l}.$$

To illustrate the difficulties in determining the right bounds for such inequalities, we note that even for the comparison of $|A + A|$ and $|A - A|$ the right exponents are not known. In fact, the best known lower bounds for $|A + A|$ in terms of $|A - A|$ have not changed for more than 40 years.

Theorem 7.2 (Freiman, Pigaev [16], Ruzsa [49]). *Let A be a subset of an abelian group. Then $|A - A|^{3/4} \leq |A + A|$.*

In the opposite direction, the best known lower bound is given by the following result.

Theorem 7.3 (Hennecart, Robert, Yudin [28]). *There exist arbitrarily large sets $A \subset \mathbb{Z}$ such that $|A+A| \leq |A-A|^{\alpha+o(1)}$, where $\alpha := \log(2)/\log(1+\sqrt{2}) \approx 0.7864$.*

In 1973, Haight [26] found for each k and $\epsilon > 0$, an integer q and a set $A \subset \mathbb{Z}_q$ such that $A - A = \mathbb{Z}_q$ and $|kA| \leq \epsilon q$. Recently, Ruzsa [48] gave a similar construction, and observed that Haight's work even gives a constant $\alpha_k > 0$ for each k with the property that there are arbitrarily large q with sets $A \subset \mathbb{Z}_q$ such that $A - A = \mathbb{Z}_q$ and $|kA| \leq q^{1-\alpha_k}$. The ideas in both constructions are relatively similar, but Ruzsa's argument is considerably more concise.

In [41], Nathanson applied Ruzsa's method to construct sets $A \subset R$ with $A - A = R$, but kA small, for rings R that are more general than $\mathbb{Z}_q$. In the same paper, he posed the following question. Given a polynomial $F(x_1, x_2, \ldots, x_n)$ with coefficients in $\mathbb{Z}$, and a set $A \subset \mathbb{Z}_N$, write $F(A) = \{F(a_1, a_2, \ldots, a_n) \colon a_1, \ldots, a_n \in A\}$. His question can be stated as: given two polynomials F, G over $\mathbb{Z}$ and $\epsilon > 0$, does there exist arbitrarily large N and a set $A \subset \mathbb{Z}_N$ such that $F(A) = \mathbb{Z}_N$, but $|G(A)| < \epsilon N$?[1]

Let us now state the main result of this chapter, which answers the first interesting cases of Nathanson's question. Once again we recall the notation

$$A^2 + kA = \{a_1a_2 + b_1 + b_2 + \cdots + b_k : a_1, a_2, b_1, \ldots, b_k \in A\},$$

and more generally,

$$lA^2 + kA = \{a_1a_2 + \cdots + a_{2l-1}a_{2l} + b_1 + b_2 + \cdots + b_k : a_1, a_2, \ldots, a_{2l}, b_1, \ldots, b_k \in A\}.$$

Theorem 7.4. *Given $k \in \mathbb{N}_0$ and any $\epsilon > 0$, there is a natural number q and a set $A \subset \mathbb{Z}_q$ such that*

$$A - A = \mathbb{Z}_q, \ \text{but } |A^2 + kA| \leq \epsilon q.$$

In fact we prove rather more.

Theorem 7.5. *For $l \in \{1, 2, 3\}$, any $k \in \mathbb{N}_0$ and any $\epsilon > 0$, there is a natural number q and a set $A \subset \mathbb{Z}_q$ such that*

$$A - A = \mathbb{Z}_q, \ \text{but } |lA^2 + kA| < \epsilon q.$$

Moreover, we can take q to be a product of distinct primes, and we can take the smallest prime dividing q to be arbitrarily large.

[1] Actually, Nathanson poses this question for more general rings R, but for $R = \mathbb{Z}$, the formulation we give here is a natural one.

We shall discuss each of the cases $l = 1, 2, 3$ separately. Note also an interesting phenomenon in the opposite direction. Namely, if we are not allowed freedom in the choice of the modulus, a statement like the theorem above cannot hold. The reason is that, by a result of Glibichuk and Rudnev (Lemma 1 in [19]) whenever $A \subset \mathbb{F}_p$ for a prime p, is a set of size at least $|A| > \sqrt{p}$, then $10A^2 = \mathbb{F}_p$ (and $A - A = \mathbb{F}_p$ certainly implies $|A| > \sqrt{p}$). Hence, unlike the linear case, already for quadratic expressions we have strong obstructions.

In fact, this problem is comparable in spirit to the sum-product phenomenon, which can be stated as the following notable theorem.

Theorem 7.6 (Bourgain, Katz, Tao [10], Sum-product estimate.)**.** *Let $\delta > 0$ be given. Then there is $\epsilon > 0$ such that whenever $A \subset \mathbb{Z}_q$ for a prime q satisfies*

$$q^{\delta} < |A| < q^{1-\delta},$$

then one has

$$\max\{|A^2|, |2A|\} \geq |A|^{1+\epsilon}.$$

Remarkably, this was further generalized to arbitrary modulus q.

Theorem 7.7 (Bourgain [9], Sum-product estimate for composite moduli)**.** *Given q, q' such that $q'|q$, write $\pi_{q'}$ for the natural projection from $\mathbb{Z}_q \to \mathbb{Z}_{q'}$.*

Let $\delta > 0$ be given. We then have $\epsilon, \eta > 0$ such that the following holds. Whenever $A \subset \mathbb{Z}_q$ satisfies

$$|A| \leq q^{1-\delta}$$

and,

$$|\pi_{q'}(A)| \geq q'^{\delta} \text{ for all } q'|q, \text{ with } q' \geq q^{\eta},$$

then

$$\max\{|A^2|, |2A|\} \geq |A|^{1+\epsilon}.$$

Hence, the sum-product phenomenon still holds even in general residue rings of integers. Given the similarity with our problem, it could be that the result of Glibichuk and Rudnev stated above holds in the more general setting as well. (Note that if $A - A = \mathbb{Z}_q$, then A satisfies the technical condition in Theorem 7.7.)

Conjecture 7.8. *There is l such that whenever $A \subset \mathbb{Z}_q$ and $A - A = \mathbb{Z}_q$, then we have $lA^2 + lA = \mathbb{Z}_q$.*

7.2 Overview of the Construction

We begin the work in this chapter by reviewing Ruzsa's construction and generalizing its main ideas slightly to the context of polynomial expressions in A. As it turns out, to be able to construct a set A such that $A - A = \mathbb{Z}_q$, but $|lA^2+kA|= o(q)$, it will suffice to consider expressions which are sums of terms of the form $\alpha_i(x_i)+cx_i$, $(\alpha_i(x_i)+cx_i)(\alpha_i(x_i)+c'x_i)$ and $(\alpha_i(x_i)+cx_i)(\alpha_j(x_j)+c'x_j)$, with $c, c' \in \{0, 1\}$ and then to choose the maps so that the number of values attained by each expression is small. For example, one of the expressions that we have to consider already for the case $l = 1$ is $\alpha_1(x_1)\alpha_2(x_2) + \alpha_1(x_1) + x_1 + \alpha(x_3)$. This discussion takes place in Section 7.3 and the rest of the chapter is devoted to constructions of maps for various expressions.

In Section 7.4, we construct sets A such that $A - A = \mathbb{Z}_q$ but $A^2 + kA$ is small. In this construction, we come to a basic version of one of the main ideas, which we call the *identification of coordinates*. Very roughly, if q is a product of distinct prime $p_1p_2 \dots p_n$, using approximate homomorphisms between $\mathbb{Z}_{p_i}$ and $\mathbb{Z}_{p_j}$, we can essentially treat $\mathbb{Z}_q$ as a vector space of dimension n. Then, although we might not ensure that each coordinate attains few values, we can ensure that their sum attains few values.

In Section 7.5, we construct sets A such that $A - A = \mathbb{Z}_q$ but $2A^2 + kA$ is small. There, we improve our results for the expression that involve a single variable using a variant of Weyl's equidistribution theorem for polynomials. Using this result, the identification of coordinates is developed further and we conclude this section with the strongest form of the identification of coordinates.

The final part of the construction, finding sets A with $3A^2 + kA$ small, is carried out in Section 7.6. There, we also touch upon some limitations of our usual approach and therefore develop different ideas to treat some of the remaining expressions. Namely, for certain choices of coefficients, in the expression

$$(\alpha(x) + c_1x)(\beta(y) + c_2y) + (\alpha(x) + c_3x)(\beta(y) + c_4y) + (\alpha(x) + c_5x)(\gamma(z) + c_6z)$$

the identification of coordinates cannot work. For this expression, we give a different, probabilistic argument, which is a form of dependent random choice.

The final section is devoted to some open problems and questions that naturally arise, including the motivation for some of these. We have tried to organize our proof so that the methods used naturally develop from the case $A^2 + kA$ to the case $3A^2 + kA$, highlighting the new difficulties that arise and why the earlier arguments are not powerful enough for the later expressions.

7.3 Overview of Ruzsa's argument and Initial Steps

We now briefly discuss Ruzsa's construction of sets $A \subset \mathbb{Z}_q$ such that $A - A = \mathbb{Z}_q$, but $|kA| = o(q)$. His ideas will be important for the later constructions given in this chapter.

Let us first analyse the requirement that $A - A = \mathbb{Z}_q$. Given any $x \in \mathbb{Z}_q$, we thus have $y \in A$ such that $y + x \in A$. If we write $\varphi(x)$ for such a y, this yields a map $\varphi : \mathbb{Z}_q \to \mathbb{Z}_q$ with the property that all $\varphi(x)$ and $\varphi(x) + x$ are contained in A. Removing all other elements from A does not change the equality $A - A = \mathbb{Z}_q$, and it can only make kA smaller, so Ruzsa's starting point is to consider a set A of the form

$$\{\varphi(x) : x \in \mathbb{Z}_q\} \cup \{\varphi(x) + x : x \in \mathbb{Z}_q\},$$

where φ is map from $\mathbb{Z}_q$ to itself. We shall do the same here as well, and throughout the chapter we will devote ourselves to finding suitable modulus q and maps on $\mathbb{Z}_q$.

Thus, we have to understand how to find a suitable q and a map φ which then give rise to the desired set A. Let us now examine the elements of kA. These are sums $a_1 + a_2 + \cdots + a_k$, where $a_i \in A$. But each element of A is either $\varphi(x)$ or $\varphi(x) + x$ for some $x \in \mathbb{Z}_q$. Hence, elements of kA are of the form

$$\sum_{i \in I} \varphi(x_i) + \sum_{i \notin I} (\varphi(x_i) + x_i)$$

for a subset $I \subset [k]$ and $x_1, x_2, \ldots, x_k$. Immediately we see that the number of different expressions here is bounded in terms of k (in fact, it equals 2^k). Further, we consider which of the x_i are equal, grouping the corresponding terms $\varphi(x_i)$ and $\varphi(x_i) + x_i$ together, and renaming the variables along the path to $y_1, y_2, \ldots, y_s$. Hence, every element of kA is of the form

$$\sum_{i=1}^{s} (a_i \varphi(y_i) + b_i y_i), \tag{7.1}$$

where $s \leq k$, $k \geq a_i \geq b_i \geq 0$ and all $y_1, \ldots, y_s$ are different. Once again, treating y_i as formal variables, the number of expressions we wrote is bounded in terms of k. The plan now is to make sure that each such expression attains a small number of values, so that in total only at most ϵq values attained.

Ruzsa's main idea in the construction is the *separation of functions*, which we now discuss. In all these expressions we have the same map φ occurring. However, we can turn the problem of constructing a single function φ that works for all expressions into a much easier problem of constructing a function for each expression separately. We first list all the expressions of the form (7.1), sorted in the ascending order by the number of variables appearing. Thus, our list start from expressions of the form $a\varphi(y) + b$. Next, we split q as a product of coprime numbers $q = q_1 q_2 \ldots q_r$, with one q_i for each expression so that by Chinese Remainder Theorem we have $\mathbb{Z}_q = \mathbb{Z}_{q_1} \oplus \mathbb{Z}_{q_2} \oplus \ldots \oplus \mathbb{Z}_{q_r}$.

We promise that however we choose an expression and values of y_i, we get at least one zero coordinate (which need not depend on the expression) and we call this **ZCP** (Zero Coordinate Promise). If i^{th} expression has only one variable appearing, thus it is of the form $a\varphi(y)+by$, we can easily ensure **ZCP** by setting the i^{th} component of the function as $\varphi_i(y) = -ba^{-1}y_i$. Now, take any expression

$$\sum_{i=1}^{s}(a_i\varphi(y_i) + b_i y_i),$$

and assume that for every such expression with fewer than s variables **ZCP** holds. Let q' be the product of q_i for the expressions with fewer than s variables. Note that, if we are given $y_1, y_2, \ldots, y_s$, and if any two among them have the same value in $\mathbb{Z}_{q'}$, by induction hypothesis, **ZCP** already holds. Hence, we may assume not only that $y_1, y_2, \ldots, y_s$ are different, but that they are different modulo q'. Write y'_i for the residue of y_i mod q'. Then, looking at j^{th} coordinate, we have to define φ_j such that

$$\sum_{i=1}^{s}(a_i\varphi_j(y'_i, (y_i)_j) + b_i(y_i)_j)$$

equals zero for all choices of $y_1, \ldots, y_s$ such that y'_i are different. But, we can rewriting $\varphi_j(y'_i, (y_i)_j)$ as $\varphi_{j,y'_i}((y_i)_j)$ already tells us that we are actually looking for a new function for each variable! Hence, our goal is to find s functions

$\varphi_{j,y'_1}, \dots \varphi_{j,y'_s}$ such that the expression is once again zero. But linear maps once again work.

We start our own work by slightly generalizing Ruzsa's idea to the polynomial setting. In what follows, by an *i-degree term* we think of a product of i terms of the from $\alpha_j(x_j)$ or $(\alpha_j(x_j)+x_j)$, the only rule being that indices of the map and the the variable to which it is applied (and the variable which is possibly added) coincide. For example, $(\alpha_1(x_1)+x_1)\alpha_2(x_2)^2$ and $\alpha_1(x_1)(\alpha_2(x_2)+x_2)(\alpha_3(x_3)+x_3)$ are both 3-degree terms, but $\alpha_1(x_2)\alpha_2(x_3)\alpha_3(x_1)$ is not, since the indices are not valid.

Proposition 7.9. *Let k be given, and let $a_1, a_2, \dots, a_k \in \mathbb{N}$. Suppose that for every $\epsilon > 0$ and every formal expression E in functions α_i and variables x_i of the form*

$$\textit{sum of } a_k \textit{ of } k\textit{-degree terms} + \textit{sum of } a_{k-1} \textit{ of } (k-1)\textit{-degree terms} + \dots$$
$$+ \textit{ sum of } a_1 \textit{ of } 1\textit{-degree terms},$$

we can find a modulus q, which is a product of arbitrarily large distinct primes, and functions $\theta_i : \mathbb{Z}_q \to \mathbb{Z}_q$, so that the E takes at most ϵq values in $\mathbb{Z}_q$, when the functions θ_i are substituted in E. Then, for every $\epsilon > 0$, there is a modulus Q, product of arbitrarily large distinct primes, and a set $A \subset \mathbb{Z}_Q$ such that $A - A = \mathbb{Z}_Q$ and

$$|a_k A^k + a_{k-1}A^{k-1} + \dots + a_1 A| \leq \epsilon Q.$$

Proof. We proceed as in the Ruzsa's construction (except that we do not insist on only having zero value in a coordinate, as a small number of values suffices). As before, we sort the expressions by the number of variables appearing, and process them in groups of those having the same number of a variables. We now turn to details.

Let $N = a_1 + a_2 + \dots + a_k$. Let $E_1, E_2, \dots, E_r$ be all the expressions in variables $y_1, y_2, \dots, y_N$ of the following form. Each expression is a sum of a_k terms, each being a product of k short terms $\varphi(y_i)$ or $\varphi(y_i)+y_i$, followed by a_{k-1} terms which are products of $k-1$ short terms, etc. with a final contribution of a_1 terms, each being $\varphi(y_i)$ or $\varphi(y_i) + y_i$. As in the discussion before, these are all expressions that naturally arise from $a_k A^k + \dots + a_1 A$, when A is defined as $\{\varphi(x)\colon x \in \mathbb{Z}_Q\} \cup \{\varphi(x) + x\colon x \in \mathbb{Z}_Q\}$. Comparing these expressions with the expressions in the assumptions of this proposition, we have that here only a single formal function appears, while in the other expressions we have a separate function for each variable. Let $m_0 = 0, m_1, m_2, \dots, m_N = r$ be indices such that if $m_i < j \leq m_{i+1}$, then the number of different variables among $(y_t)_{t=1}^N$ appearing in the expression E_j is exactly $i+1$.

Fix an increasing sequence $0 < \epsilon_1 < \epsilon_2 < \dots < \epsilon_N = \epsilon$. We inductively construct moduli $Q_1, Q_2, \dots, Q_N$ and functions $\varphi_i : Q_i \to Q_i$ such that for every $i \leq N$ we have that union of all images of expressions $E_1, E_2, \dots, E_{m_i}$ (that is, all expressions having at most i variables) takes at most $\epsilon_i Q_i$ values (when φ_i is substituted in the expressions).

Base case: $i = 1$**.** By the assumption, for every expression E_i that has only one variable, we have moduli q_i with arbitrarily large distinct prime factors, and a map $\theta_i^{(1)}$, such that E_i takes only at most $\epsilon_1 q_i / m_1$ values. Thus, w.l.o.g. $q_1, q_2, \dots, q_{m_1}$ are all coprime, with distinct arbitrarily large prime factors. We set $Q_1 = q_1 q_2 \dots q_{m_1}$ and identify $\mathbb{Z}_{Q_1}$ with $\mathbb{Z}_{q_1} \oplus \mathbb{Z}_{q_2} \oplus \dots \oplus \mathbb{Z}_{q_{m_1}}$, and we define φ_1 coordinate-wise as $\varphi_{1,i}(x) := \theta_i^{(1)}(x_i)$, where x_i is i-th coordinate of x. Note that union of all values attained by these m_1 expressions with this definition of Q_1 and φ_1 has size bounded by

$$\sum_{i=1}^{m_1} |\operatorname{Im} E_i| \leq \sum_{i=1}^{m_1} \frac{\epsilon_1 q_i}{m_1} \frac{Q_1}{q_i} = \epsilon_1 Q_1,$$

as desired. (Here we write $\operatorname{Im} E_i$ for the resulting image of the expression E_i, and we have a trivial bound for it; the expression may only take at most $\epsilon_1 q_i / m_1$ values on the i^{th} coordinate.)

Inductive step. Suppose now that we have found $\varphi_s : \mathbb{Z}_{Q_s} \to \mathbb{Z}_{Q_s}$ such that in total all expressions with at most s variables have a small image V_s, i.e. only at most $\epsilon_s Q_s$ values are attained. We shall construct Q_{s+1} as a product $Q_s R_{m_s+1} R_{m_s+2} \dots R_{m_{s+1}}$, where R_i is an auxiliary modulus for the expression E_i, with the property that either E_i takes one of the small number of values on $\mathbb{Z}_{Q_s}$ or a value in another small set in $\mathbb{Z}_{R_i}$. Here we use Ruzsa's *separation of functions* idea.

Fix an expression E_i with exactly $s+1$ variables. If we take values of these variables restricted to $\mathbb{Z}_{Q_s}$, and it happens so that at least two such values coincide, then using the map φ_s the value of the expression E_i (also restricted to $\mathbb{Z}_{Q_s}$) is actually a value of one of the expressions we already considered, with at most s variables, so it lies in the small set V_s. Hence, we only need to consider the choices of $y_1, y_2, \ldots, y_{s+1}$ (w.l.o.g. these are the variables that appear) which differ in $\mathbb{Z}_{Q_s}$. We split the expression E_i further into cases on y_i mod Q_s, thus into further $L \leq Q_s^{s+1}$ cases. Pick an arbitrary choice C of $s+1$ distinct values in Q_s. Look back at E_i and change every appearance of $\varphi(y_t)$ by $\alpha_t(y_t)$. By assumptions, we have a choice of an integer r_C with arbitrarily large distinct prime factors and maps $\theta_t^{(C)}$ such that the modified E_i takes only at most $(\epsilon_{s+1}-\epsilon_s)r_C/((m_{s+1}-m_s)Q_s^{s+1})$ values in $\mathbb{Z}_{r_C}$. Finally, define R_i as the product of all these r_C, and $(\varphi_{s+1})_i(x)$ as follows: for every C, take $(\varphi_{s+1})_i(x)$ at the coordinate corresponding to r_C to be zero if x modulo $\mathbb{Z}_{Q_s}$ is not in C, otherwise, if it is the j-th residue, set $(\varphi_{s+1})_i(x) := \theta_j^{(C)}(x')$, where x' is the coordinate of x corresponding to r_C. It remains to check the size of images.

For every expression and every choice of values of $y_1, y_2, \ldots, y_N$, we either end up in $A_s \times \mathbb{Z}_{R_{m_s+1}} \times \mathbb{Z}_{R_{m_s+2}} \times \ldots \times \mathbb{Z}_{R_{m_{s+1}}}$, which has size at most $\epsilon_s Q_{s+1}$, or one of the coordinates is in a fixed subset of $\mathbb{Z}_{R_t}$ of size at most $(\epsilon_{s+1}-\epsilon_s)R_t/(m_{s+1}-m_s)$. Summing everything together, the image has at most $\epsilon_{s+1}Q_{s+1}$ values as desired. $\square$

The rest of the chapter is therefore devoted to finding moduli q and maps $\alpha_i\colon \mathbb{Z}_q \to \mathbb{Z}_q$ under which the expressions like $(\alpha_1(x_1)+x_1)(\alpha_2(x_2)+x_2)+\alpha_3(x_3)^2$ do not take too many values. Along the way, we also discuss related problems and questions.

Notation. Throughout the chapter, Greek letters α, β and γ will be used for the maps appearing in the expressions. The following functions will be frequently used in our construction. For a prime p, we use the standard projection homomorphism $\pi_p\colon \mathbb{Z} \to \mathbb{Z}_p$, which sends integer x to $x + p\mathbb{Z}$. Next, we define $\iota_p\colon \mathbb{Z}_p \to \mathbb{Z}$ by sending $x \in \mathbb{Z}_p$ to the integer $\iota_p(x) \in \{0, 1, \ldots, p-1\} \subset \mathbb{Z}$ such that $\pi_p \circ \iota_p(x) = x$. For two primes p and q, we also define the map $\mathrm{mod}_{p,q}\colon \mathbb{Z}_p \to \mathbb{Z}_q$ given by $\mathrm{mod}_{p,q} = \pi_q \circ \iota_p$. Finally, in any abelian group Z, and functions $f, g\colon S \to G$, from a set S to Z, we write $f \stackrel{M}{=} g$ to mean that

$\{f(s) - g(s)\colon s \in S\}$ is a set of size at most M. In particular, $f \overset{O(1)}{=} g$ means that $\{f(s) - g(s)\colon s \in S\}$ has a bounded size as S grows.

7.4 Sets A with small $A^2 + kA$

The main result of this section is the case $l = 1$ of Theorem 7.5.

Theorem 7.10. *For any $k \in \mathbb{N}_0$ and any $\epsilon > 0$, there is a natural number q, which is a product of distinct, arbitrarily large primes, and a set $A \subset \mathbb{Z}_q$ such that $A - A = \mathbb{Z}_q$, while $|A^2 + kA| < \epsilon q$.*

Proof. We start from Proposition 7.9. To be able to construct $A \subset \mathbb{Z}_q$ with full difference set, but small $A^2 + kA$, we need to handle the expressions that are sums of the *quadratic part* which is a product of two terms of the form $\alpha_i(x_i) + x_i$ or $\alpha_i(x_i)$, and a *linear part* which is itself a sum of k summands, each being of the form $\alpha_i(x_i) + x_i$ or $\alpha_i(x_i)$. Note that for the terms in the linear part whose variables do not appear in the quadratic part, we can define the corresponding maps α_i to be affine so that the variables involved cancel out. Therefore, w.l.o.g. we only consider expressions whose all variables already appear in the quadratic part. Note also that for the quadratic part we have two cases: either only one variable, w.l.o.g. x_1, appears, or exactly two variables, w.l.o.g. x_1 and x_2, appear. We treat these cases separately.

Case 1: only one variable in the quadratic part. Thus, our goal now is to show that if we are given a quadratic expression featuring only one variable, we can find a modulus and function, so that the expression takes a small number of values. In fact, here we do more and prove the claim for expressions of arbitrary degree.

Lemma 7.11. *Let $d \in \mathbb{N}$ be given, and let $p > d$ be a prime. Then, given any maps $c_0, c_1, \ldots, c_d\colon \mathbb{Z}_p \to \mathbb{Z}_p$ and any set $F \subset \mathbb{Z}_p$ of size less than p/d, we can find another map $\alpha\colon \mathbb{Z}_p \to \mathbb{Z}_p$ such that the expression*

$$c_d(x)\alpha(x)^d + \ldots c_1(x)\alpha(x) + c_0(x)$$

does not take a value in F for any x that has at least one of $c_1(x)$, $c_2(x), \ldots,$ $c_d(x)$ non-zero.

Proof. Suppose that for some x, for every choice of $v = \alpha(x)$ we have $c_d(x)v^d + \dots c_1(x)v + c_0(x) \in F$. By the pigeonhole principle, some value $f \in F$ is hit at least $d+1$ times. Thus, the polynomial (in v)

$$c_d(x)v^d + \dots c_1(x)v + c_0(x) - f$$

has at least $d+1$ zeros, making it a zero polynomial. Hence $c_1(x), c_2(x), \dots, c_d(x)$ are simultaneously zero, proving the lemma. □

Corollary 7.12. *Let E be an arbitrary $\mathbb{Z}$-linear combination of terms of the form $\alpha(x)^i x^j$, where at least one of such terms with $i > 0$ appears. Given any $\epsilon > 0$, we can find a modulus q, which is a product of distinct arbitrarily large primes, and a map $\alpha\colon \mathbb{Z}_q \to \mathbb{Z}_q$ such that under α the expression E takes at most ϵq values in $\mathbb{Z}_q$.*

Proof. Rewrite E by grouping together a $\mathbb{Z}$-linear combination of x^j that appear next to each $\alpha(x)^i$. Thus, we can write E as $\alpha(x)^d f_d(x) + \dots + \alpha(x) f_1(x) + f_0(x)$, where each $f_i(x)$ is a polynomial in x over $\mathbb{Z}$, and at least one of $f_1, f_2, \dots, f_d$ is not a zero polynomial. Let $D = \max \deg f_i$. Pick distinct arbitrarily large primes $p_1, p_2, \dots, p_t$, all w.l.o.g. larger than $2d(D+1)$ and absolute values of coefficients of $f_1, f_2, \dots, f_d$ (so that non-zero polynomials do not become zero modulo p_i). By Lemma 7.11, we may find a map $\alpha_i\colon \mathbb{Z}_{p_i} \to \mathbb{Z}_{p_i}$ for each i such that the image of E has size at most $(1-1/d)p_i + 1$, when the variable x ranges over values such that polynomials $f_1, f_2, \dots, f_d$ are not simultaneously zero. But there are at most D values of x such that $f_1(x) = \dots = f_d(x) = 0$, so we conclude that modulo each p_i, the expression E may take at most $(1-1/d)p_i + D + 1 \leq (1-1/2d)p_i$ values. Finally, set $q = p_1 p_2 \dots p_t$ and take $\alpha\colon \mathbb{Z}_q \to \mathbb{Z}_q$ to be $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_t)$, where we as usual identify $\mathbb{Z}_q$ with $\mathbb{Z}_{p_1} \oplus \mathbb{Z}_{p_2} \oplus \dots \oplus \mathbb{Z}_{p_t}$. Hence, modulo q, the expression takes at most $(1-1/2d)^t q$ values. Taking t large enough so that $(1-1/2d)^t < \epsilon$ proves the corollary. □

The case 1 now follows by applying Corollary 7.12.

Case 2: the quadratic part has two variables. The quadratic part must look like a product of two terms, each being either $\alpha_i(x_i) + x_i$ or $\alpha_i(x_i)$. By suitably renaming the variables, and adding x_i to $\alpha_i(x_i)$ if necessary, w.l.o.g. we only need to consider the case when the quadratic part is $\alpha_1(x_1)\alpha_2(x_2)$, and the whole expression is

$$\alpha_1(x_1)\alpha_2(x_2) + L_1(x_1) + L_2(x_2)$$

where each $L_i(x_i)$ is a $\mathbb{Z}$-linear combination of $\alpha_i(x_i)$ and x_i. Note also that if $L_i(x_i)$ is nonzero, then $\alpha_i(x_i)$ appears with a nonzero coefficient.

We have come to an important point, and one of the key ideas, which we now explain. We have to construct q and maps $\alpha_1, \alpha_2 \colon \mathbb{Z}_q \to \mathbb{Z}_q$ such that $\alpha_1(x_1)\alpha_2(x_2)+L_1(x_1)+L_2(x_2)$ takes $o(q)$ values. Suppose for a moment that the linear terms L_i are both zero. Then, we have an easy way to make $\alpha_1(x_1)\alpha_2(x_2)$ constant, by setting one of the α_i to be zero. However, such an approach cannot work in the case when L_1, L_2 are not zero, as it would force one of the L_i to be an affine map, which is surjective. As a way to overcome this, we can use both $\alpha_1 = 0$ and $\alpha_2 = 0$ to get additional freedom. Thus, we set $q = q_1q_2$, where q_1, q_2 are coprime products of distinct primes, identify $\mathbb{Z}_q$ with $\mathbb{Z}_{q_1} \oplus \mathbb{Z}_{q_2}$, and set α_1 to be zero on the first coordinate, and α_2 to be zero on the second coordinate. Hence if $L_1(x_1) = \lambda_1\alpha_1(x_1) + \mu_1 x_1$ and $L_2(x_2) = \lambda_2\alpha_2(x_2) + \mu_2 x_2$, then the expression becomes

$$(\mu_1(x_1)_1 + \lambda_2(\alpha_2)_1(x_2) + \mu_2(x_2)_1, \lambda_1(\alpha_1)_2(x_1) + \mu_1(x_1)_2 + \mu_2(x_2)_2)\,. \tag{7.2}$$

We now want to find $(\alpha_1)_2$ and $(\alpha_2)_1$ so that the expression (7.2) does not take too many values in $\mathbb{Z}_{q_1} \oplus \mathbb{Z}_{q_2}$. Suppose for a moment that instead of coprime q_1 and q_2 we actually had $q_1 = q_2$. Then, we could have simply taken

$$(\alpha_1)_2(x_1) := -\lambda_1^{-1}\mu_1((x_1)_1 + (x_1)_2)$$

and

$$(\alpha_2)_1(x_2) := -\lambda_2^{-1}\mu_2((x_2)_1 + (x_2)_2),$$

which ensures that every value taken by the expression is of the form $(v, -v)$ and hence it is in small subset $\{(x, y) : x + y = 0\}$ of $\mathbb{Z}_{q_1} \oplus \mathbb{Z}_{q_1}$. It turns out that we can use the same approach even if $q_1 \neq q_2$. We shall refer to this idea as the *identification of coordinates*, which will appear at other places in this chapter as well. The following proposition and its proof formalize this discussion. We slightly change the notation to make the reading easier.

Proposition 7.13. *(Basic identification of coordinates.) Let $\lambda_0, \lambda_1, \lambda_2, \mu_1, \mu_2 \in \mathbb{Z}$ be given and let $p \leq q$ be primes greater than $|\lambda_1|, |\lambda_2|$. Suppose that if $\lambda_1 = 0$ then $\mu_1 = 0$ and if $\lambda_2 = 0$ then $\mu_2 = 0$. Then we have $\alpha, \beta\colon \mathbb{Z}_p \oplus \mathbb{Z}_q \to \mathbb{Z}_p \oplus \mathbb{Z}_q$ such that*

$$f\colon (x, y) \mapsto \lambda_0\alpha(x)\beta(y) + \lambda_1\alpha(x) + \mu_1 x + \lambda_2\beta(y) + \mu_2 y$$

takes at most $O(q)$ values, when x, y range over all pairs of values in $\mathbb{Z}_p \oplus \mathbb{Z}_q$.

Recall the definition of map ι_p as the natural embedding of $\mathbb{Z}_p$ into $\mathbb{Z}$, the natural projection $\pi_p\colon \mathbb{Z} \to \mathbb{Z}_p$, and finally, the composition $\mathrm{mod}_{p,q}\colon \mathbb{Z}_p \to \mathbb{Z}_q$, given by $\mathrm{mod}_{p,q} = \pi_q \circ \iota_p$. Before proceeding with the proof, it is useful to note some easy properties of the maps ι_p and $\mathrm{mod}_{p,q}$.

Lemma 7.14. *Let p, p', p_1, p_2, p_3 be primes. Then*

(1) *Given $z \in \mathbb{Z}$, we have $p | \iota_p(\pi_p(z)) - z$. Also, $\iota_p(\pi_p(z)) \leq z$, when $z \geq 0$.*

(2) *Given $x, y \in \mathbb{Z}_p$, we have $\iota_p(x) + \iota_p(y) - \iota_p(x + y) \in \{0, p\}$.*

(3) *Given $x, y \in \mathbb{Z}_p$, we have*

$$\mathrm{mod}_{p,p'}(x) + \mathrm{mod}_{p,p'}(y) - \mathrm{mod}_{p,p'}(x + y) \in \{0, \pi_{p'}(p)\} \subset \mathbb{Z}_{p'}.$$

(4) *Provided that $p_3 < (t + 1)p_2$, we have*

$$\begin{aligned} &\mathrm{mod}_{p_2,p_1} \circ \mathrm{mod}_{p_3,p_2}(x) - \mathrm{mod}_{p_3,p_1}(x) \\ &\qquad\qquad \in \{-t\pi_{p_1}(p_2), -(t - 1)\pi_{p_1}(p_2), \ldots, 0\} \subset \mathbb{Z}_{p_1}. \end{aligned}$$

Proof. **(1)** Applying π_p, we have $\pi_p(\iota_p(\pi_p(z)) - z) = \pi_p \circ \iota_p(\pi_p(z)) - \pi_p(z) = 0$, thus $p | \iota_p(\pi_p(z)) - z$. If $z \geq 0$, then $\iota_p(\pi_p(z)) - z \leq p - 1$, so the claim follows.

(2) Let $x' = \iota_p(x), y' = \iota_p(y) \in \mathbb{Z}$. Note that $\pi_p(x' + y') = x + y$ and $x' + y' \in \{0, 1, \ldots, 2p - 2\}$. From definition, $\pi_p(\iota_p(x + y)) = x + y$ and $\iota_p(x + y) \in \{0, 1, \ldots, p - 1\}$. Hence, if we set $v = \iota_p(x) + \iota_p(y) - \iota_p(x + y)$, we have $p | v$ and $v \in \{-(p - 1), -(p - 2), \ldots, 2p - 2\}$, so $v \in \{0, p\}$.

(3) The statement follows by applying $\pi_{p'}$ to $\iota_p(x) + \iota_p(y) - \iota_p(x + y) \in \{0, p\}$, noting that $\pi_{p'}$ is an additive homomorphism and recalling that $\mathrm{mod}_{p,p'} = \pi_{p'} \circ \iota_p$.

(4) From the definition, we have

$$\begin{aligned}&\operatorname{mod}_{p_2,p_1}\circ\operatorname{mod}_{p_3,p_2}(x)-\operatorname{mod}_{p_3,p_1}(x)\\=&\pi_{p_1}(\iota_{p_2}(\pi_{p_2}(\iota_{p_3}(x))))-\pi_{p_1}(\iota_{p_3}(x))\\=&\pi_{p_1}(\iota_{p_2}(\pi_{p_2}(\iota_{p_3}(x)))-\iota_{p_3}(x)).\end{aligned}$$

Write $v=\iota_{p_2}(\pi_{p_2}(\iota_{p_3}(x)))-\iota_{p_3}(x)$. Using the previous work, we know that $p_2|v$, $v\geq-(p_3-1)$ and $v\leq 0$, since $\iota_{p_3}(x)\geq 0$. So $v\in\{-tp_2,-(t-1)p_2,\dots,0\}$, and the claim follows after applying π_{p_1}. $\square$

Proof of Proposition 7.13. Observe immediately that if $\lambda_0=0$, we can ensure that $\lambda_1\alpha(x)+\mu_1 x=0$ and $\lambda_2\beta(y)+\mu_2 y=0$, proving the claim. Therefore, we may assume $\lambda_0\neq 0$, w.l.o.g. $\lambda_0=1$. If $\mu_1=\mu_2=0$ holds, then the function becomes $f\colon(x,y)\mapsto\alpha(x)\beta(y)+\lambda_1\alpha(x)+\lambda_2\beta(y)$, which can be made zero, by choosing zero maps for α and β. If exactly one of μ_1,μ_2 vanishes, $\mu_1=0$ say, then we can pick β to ensure that $\lambda_2\beta(y)+\mu_2 y=0$, and set $\alpha(x)=0$ to get $f=0$. From now on, assume that $\lambda_1,\lambda_2,\mu_1,\mu_2\neq 0$.

Set $\alpha_1(x)=0$ and $\beta_2(y)=0$. This makes $\alpha(x)\beta(y)=0$ for all choices of x,y. It remains to pick $\alpha_2(x),\beta_1(y)$ so that $(\mu_1x_1+\lambda_2\beta_1(y)+\mu_2y_1,\lambda_1\alpha_2(x)+\mu_1x_2+\mu_2y_2)$ takes a small number of values.

Set $\beta_1(y)=-\lambda_2^{-1}(\mu_1\operatorname{mod}_{q,p}(y_2)+\mu_2y_1)$ and $\alpha_2(x)=-\lambda_1^{-1}(\mu_2\operatorname{mod}_{p,q}(x_1)+\mu_1x_2)$. Hence f becomes

$$f(x,y)=(\mu_1(x_1-\operatorname{mod}_{q,p}(y_2)),\mu_2(y_2-\operatorname{mod}_{p,q}(x_1))).$$

Let $\Phi\colon\mathbb{Z}_p\oplus\mathbb{Z}_q\to\mathbb{Z}$ be given by $\Phi(u,v)=\iota_p(\mu_1^{-1}u)+\iota_q(\mu_2^{-1}v)$, noting that $\mu_1,\mu_2\neq 0$. Then,

$$\Phi(f(x,y))=\iota_p(x_1-\operatorname{mod}_{q,p}(y_2))+\iota_q(y_2-\operatorname{mod}_{p,q}(x_1)).$$

Fixing the set $S=\{-p,0,p\}+\{-q,0,q\}$, from Lemma 7.14 we have

$$\begin{aligned}&\iota_p(x_1-\operatorname{mod}_{q,p}(y_2))+\iota_q(y_2-\operatorname{mod}_{p,q}(x_1))\\\in&\,\iota_p(x_1)-\iota_p(\operatorname{mod}_{q,p}(y_2))+\iota_q(y_2)-\iota_q(\operatorname{mod}_{p,q}(x_1))+S\end{aligned}$$

or, under our notation introduced earlier,

$$\begin{aligned}\Phi(f(x,y))\overset{O(1)}{=}&\iota_p(x_1)-\iota_p(\operatorname{mod}_{q,p}(y_2))+\iota_q(y_2)-\iota_q(\operatorname{mod}_{p,q}(x_1))\\=&\iota_p(x_1)-\iota_q(\pi_q(\iota_p(x_1)))+\iota_q(y_2)-\iota_p(\pi_p(\iota_q(y_2)))\end{aligned}$$

Lemma 7.14 also implies that $\iota_p(\pi_p(v)) \overset{O(\frac{q}{p})}{=} v$ and $\iota_q(\pi_q(v)) \overset{O(1)}{=} v$, when $|v|= O(q)$, from which we conclude that

$$\Phi(f(x,y)) \overset{O(\frac{q}{p})}{=} \iota_p(x_1) - \iota_p(x_1) + \iota_q(y_2) - \iota_q(y_2) = 0,$$

so the image of the function f is a subset of a preimage of Φ of a set of size $O(1)$. Fibres of Φ are of size at most p, so the claim follows. $\square$

Applying Proposition 7.13 finishes the proof of Theorem 7.10. $\square$

7.4.1 Using affine maps in the case of two variables

In this subsection, we further discuss some quadratic expressions involving two variables. A natural map we can try is an affine map $x \mapsto ax + b$, for constants a, b. However, if we look at expression $\alpha(x)\beta(y) + \alpha(x) + x + \beta(y) + y$, which was among the ones necessary to discuss in the proof of Theorem 7.10, it is easy to see that choosing affine maps from $\mathbb{Z}_q$ to $\mathbb{Z}_q$ for α and β yields full image, for every q. In the following discussion, we ask ourselves the question when we can use such maps to get a small image of the function defined by the expression.

As we shall see later, in the construction of A with small $2A^2 + kA$, one of the expressions we shall consider has quadratic part of the form $\alpha_1(x_1)\alpha_2(x_2) + (\alpha_1(x_1) + c_1x_1)(\alpha_2(x_2) + c_2x_2)$, with $c_1, c_2 \neq 0$. It turns out that in this case the affine maps can be used as desired maps. We discuss these maps before the construction of A with small $2A^2 + kA$, so that we can focus better on the new ideas needed for that case.

Lemma 7.15. *(Affine maps solution.) Let $\nu_1, \nu_2 \neq 0$ and $\lambda_1, \lambda_2, \mu_1, \mu_2$ be integers. Then, for any prime p greater than absolute values of all the given integers, we can find affine maps $\alpha, \beta\colon \mathbb{Z}_p \to \mathbb{Z}_p$ such that*

$$\alpha(x)\beta(y) + (\alpha(x) + \nu_1x)(\beta(y) + \nu_2y) + \lambda_1\alpha(x) + \mu_1x + \lambda_2\beta(y) + \mu_2y$$

is constant.

Proof. Let $\alpha(x) := ax + b$ and $\beta(y) := cy + d$, with a, b, c, d to be determined. With this choice of maps, the expression above becomes

$$\begin{aligned}&(ac + (a + \nu_1)(c + \nu_2))xy + (2ad + d\nu_1 + \lambda_1 a + \mu_1)x \\ +&(2bc + b\nu_2 + \lambda_2 c + \mu_2)y \quad + (2bd + \lambda_1 b + \lambda_2 d).\end{aligned}$$

Hence, we need to make sure that

$$\begin{aligned}2ac + \nu_2 a + \nu_1 c + \nu_1\nu_2 &= 0,\\ 2ad + \nu_1 d + \lambda_1 a + \mu_1 &= 0,\\ 2bc + \nu_2 b + \lambda_2 c + \mu_2 &= 0.\end{aligned}$$

This is equivalent to

$$\begin{aligned}b &= -(\lambda_2 c + \mu_2)/(2c + \nu_2),\\ a &= -(\nu_1 c + \nu_1\nu_2)/(2c + \nu_2),\\ d &= \left(\mu_1(2c + \nu_2) - \lambda_1\nu_1(c + \nu_2)\right)/(\nu_1\nu_2)\,.\end{aligned}$$

Hence, we can pick a, b, c, d so that affine maps make our expression equal to constant if and only if ν_1, ν_2 are non-zero. $\square$

7.5 Sets A with small $2A^2 + kA$

This section is devoted to the proof of the case $l = 2$ of Theorem 7.5.

Theorem 7.16. *For any $k \in \mathbb{N}_0$ and any $\epsilon > 0$, there is a natural number q, which is a product of distinct, arbitrarily large primes, and a set $A \subset \mathbb{Z}_q$ such that $A - A = \mathbb{Z}_q$, while $|2A^2 + kA| < \epsilon q$.*

Proof. The approach here is similar to the one in the proof of Theorem 7.10, however the expressions that arise in this case are more complicated and require new ideas. Once again, the proof is based on Proposition 7.9. As before, we split all expressions in their quadratic and linear parts, and we may assume that if a variable appears at all in an expression, it must appear in the quadratic part. Next, we consider all the possible cases for the quadratic part, and explain how to make the image of the expression small in each case separately. They are listed sorted by the support size and then by structure. We also have the freedom of renaming the variables. Again, we change the notation slightly; instead of x_1, x_2, x_3, x_4 and $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ we use x, y, z, w and $\alpha, \beta, \gamma, \delta$ respectively. The possible cases, w.l.o.g. are (all the c_i are in $\{0, 1\}$)

1. Support of size 1.
   (a) The non-linear part must look like $(\alpha(x)+c_1x)(\alpha(x)+c_2x)+(\alpha(x)+c_3x)(\alpha(x)+c_4x)$.
2. Support of size 2. We have a few possibilities here.
   (a) $(\alpha(x)+c_1x)(\alpha(x)+c_2x)+(\alpha(x)+c_3x)(\beta(y)+c_4y)$
   (b) $(\alpha(x)+c_1x)(\beta(y)+c_2y)+(\alpha(x)+c_3x)(\beta(y)+c_4y)$
   (c) $(\alpha(x)+c_1x)(\alpha(x)+c_2x)+(\beta(y)+c_3y)(\beta(y)+c_4y)$
3. Support of size 3. We have a couple of possibilities here.
   (a) $(\alpha(x)+c_1x)(\alpha(x)+c_2x)+(\beta(y)+c_3y)(\gamma(z)+c_4z)$
   (b) $(\alpha(x)+c_1x)(\beta(y)+c_2y)+(\alpha(x)+c_3x)(\gamma(z)+c_4z)$
4. Support of size 4.
   (a) The non-linear part must look like $(\alpha(x)+c_1x)(\beta(y)+c_2y)+(\gamma(z)+c_3z)(\delta(w)+c_4w)$.

We discuss each of these case separately. However, we use a different order than stated above and deal with easier cases first.

Case 1(a). This is immediate from Corollary 7.12.

Case 2(b). If $c_1 = c_3$ or $c_2 = c_4$, modifying $\alpha(x)$ by adding a suitable multiple λx to it, and modifying $\beta(y)$ accordingly, we may assume that the quadratic expression is exactly $2\alpha(x)\beta(y)$, which we have already done in Proposition 7.13 (notice that the condition on coefficients in that proposition is satisfied). Hence, w.l.o.g. $c_1 \neq c_3$ and $c_2 \neq c_4$. Then, (after a suitable modification of α_i by affine maps to make $c_1 = c_2 = 0$, $c_3, c_4 \neq 0$), we can apply Lemma 7.15, to finish the proof in this case.

Case 2(c). The whole expression in this case is of the form $f_1(x)+f_2(y)$, where f_1 is a polynomial of degree at most 2 in x and $\alpha(x)$ and f_2 is a polynomial of degree at most 2 in y and $\beta(y)$. Note that we cannot use our arguments about single variable expressions here, as we would only get two sets $S_1, S_2 \subset \mathbb{Z}_q$ of size $o(q)$ such that f_i always takes values in S_i, so we would only know that the whole expression takes values in $S_1 + S_2$ which could easily be the whole set of residues. Instead, we recall that the polynomials always attain a small value. This is the content of the next lemma, which is a well-known consequence of Weyl's inequality on exponential sums. Similar results appear in [20], we include a proof for completeness.

Lemma 7.17. *Let d be fixed. Then there is an absolute constant C_d such that the following holds. Let p be a prime, and let $a_d, a_{d-1}, \ldots, a_0 \in \mathbb{Z}_p$ be given, with a_d non-zero. Then the polynomial $a_d x^d + \cdots + a_1 x + a_0$ attains a value in $\{-C_d p^{1-2^{-d}}, \ldots, C_d p^{1-2^{-d}}\}$.*

Write $e_p(t)$ for the function $\exp(2\pi i t/p)$. The proof uses discrete Fourier transforms of functions $f\colon \mathbb{Z}_p \to \mathbb{C}$, which we define as $\hat{f}\colon \mathbb{Z}_p \to \mathbb{C}$ with $\hat{f}(r) = \sum_{x \in \mathbb{Z}_p} f(x) e_p(-rx)$. We refer readers to [20] for more details.

Proof. Write $f(x)$ for the polynomial $a_d x^d + \cdots + a_1 x + a_0$. We begin by stating (a special case of) Weyl's inequality.

Theorem 7.18 (Weyl's inequality, Lemma 2.4 in [54])**.** *For every $\epsilon > 0$, and $d \in \mathbb{N}$, there is a constant $C_{\epsilon,d}$ such that for all primes p*

$$\left| \sum_{x \in \mathbb{Z}_p} e_p(g(x)) \right| \leq C_{\epsilon,d} p^{1+\epsilon-2^{1-d}}$$

holds for every polynomial $g \in \mathbb{Z}_p[X]$ of degree d.

Write $F(x)$ for the number of times the polynomial f attains the value x. Hence, by Weyl's inequality, there is a constant C, independent of p such that $|\hat{F}(r)| \leq Cp^{1-2^{-d}}$ for $r \neq 0$, and $\hat{F}(0) = p$. Let I be the interval $\{-k, -k+1, \ldots, k\}$. Suppose that f attains no value in $\{-2k, -2k+1, \ldots, 2k\}$. We have

$$\sum_x F(x) I * I(x) = 0.$$

Applying Parseval's formula and noting that $\hat{I}(r) \in \mathbb{R}$, we get that

$$0 = \sum_r \hat{F}(r)\hat{I}(r)^2 = \hat{F}(0)\hat{I}(0)^2 + \sum_{r \neq 0} \hat{F}(r)\hat{I}(r)^2 = p(2k+1)^2 + \sum_{r \neq 0} \hat{F}(r)\hat{I}(r)^2.$$

Thus,

$$p(2k+1)^2 \leq \sum_{r\neq 0} |\hat{F}(r)| \hat{I}(r)^2 \leq \left(\max_{r\neq 0} |\hat{F}(r)| \right) \sum_s \hat{I}(s)^2 \leq Cp^{1-2^{-d}} p(2k+1).$$

From this we conclude that $2k+1 \leq Cp^{1-2^{-d}}$, as desired. □

Write N for $C_d p^{1-2^{-d}}$. Now, consider $f_1(x)$ as a polynomial in $\alpha(x)$ for every fixed x. The lemma guarantees that we can define $\alpha(x)$ so that $f_1(x) \in \{-N, -N+1, \ldots, N\}$. Similarly, for every y, we can pick $\beta(y)$ so that $f_2(y) \in \{-N, -N+1, \ldots, N\}$, hence we always have $f_1(x) + f_2(y) \in \{-2N, -2N+1, \ldots, 2N\}$, as desired.

Case 3(a). We shall take q of the form $q_1q_2q_3$, where q_1, q_2, q_3 are coprime, and each q_i is a product of distinct arbitrarily large primes. As always, we identify $\mathbb{Z}_q \cong \mathbb{Z}_{q_1} \oplus \mathbb{Z}_{q_2} \oplus \mathbb{Z}_{q_3}$, and we aim to use the identification of coordinates idea. Thus, we set $\alpha_1(x) := -c_1x_1, \alpha_2(x) := -c_2x_2$, so that $(\alpha(x)+c_1x)(\alpha(x)+c_2x)$ has second and third coordinates equal to zero. We also set $\beta_1(y) := -c_3y_1, \beta_3(y) := -c_3y_3$ and $\gamma_2(z) := -c_4z_2, \gamma_3(z) := -c_4z_3$. Note that we still have freedom of choice for $\alpha_3, \beta_2, \gamma_1$. Let the linear part of the expression be $d_1\alpha(x) + d_2x + d_3\beta(y) + d_4y + d_5\gamma(z) + d_6z$, where the coefficients d_i have the property that $d_{2i} \neq 0$ implies $d_{2i-1} \neq 0$ (since the linear part comes from $\mathbb{N}$-linear combination of $\alpha(x)$ and $\alpha(x) + x$, etc.). The expression becomes

$$\Big((-d_1c_1 + d_2)x_1 + (-d_3c_3 + d_4)y_1 + d_5\gamma_1(z) + d_6z_1,$$
$$(-d_1c_2 + d_2)x_2 + d_3\beta_2(y) + d_4y_2 + (-c_4d_5 + d_6)z_2,$$
$$(\alpha_3(x) + c_1x_3)(\alpha_3(x) + c_2x_3)$$
$$+ d_1\alpha_3(x) + d_2x_3 + (-d_3c_3 + d_4)y_3 + (-d_5c_4 + d_6)z_3\Big).$$

We combine the identification of coordinates idea with the fact that polynomials have relatively dense sets of values in the next proposition.

Proposition 7.19 (Strong version of the identification of coordinates)**.** *Fix $n, d \in \mathbb{N}$. Then there are constants $\epsilon, C > 0$ such that the following holds. Let $d_1, d_2, \ldots, d_n \in \mathbb{N}$ all be at most d. Let $2p_n > p_1 \geq p_2 \geq \ldots \geq p_n$ be primes. Write $r = p_1p_2\ldots p_n$. Next, let $f_{i,j}\colon \mathbb{Z}_r \to \mathbb{Z}_{p_j}$ be arbitrary maps for every $1 \leq i, j \leq n$. Let for every $1 \leq i \leq n$, $c_i \in \mathbb{Z}_{p_i}^\times$. Finally, let $g_{i,j}\colon \mathbb{Z}_r \to \mathbb{Z}_{p_i}$*

be also arbitrary functions for every $1 \leq i \leq n, 1 \leq j \leq d_i - 1$. Then, we can find maps $\alpha_i \colon \mathbb{Z}_r \to \mathbb{Z}_{p_i}$ such that the expression

$$\begin{aligned}
\Big(&f_{1,1}(x_1) + f_{2,1}(x_2) + \cdots + f_{n,1}(x_n) + c_1\alpha_1(x_1)^{d_1} \\
&\qquad + g_{1,d_1-1}(x_1)\alpha_1(x_1)^{d_1-1} + \cdots + g_{1,1}(x_1)\alpha_1(x_1), \\
&f_{1,2}(x_1) + f_{2,2}(x_2) + \cdots + f_{n,2}(x_n) + c_2\alpha_2(x_2)^{d_2} \\
&\qquad + g_{2,d_2-1}(x_2)\alpha_2(x_2)^{d_2-1} + \cdots + g_{2,1}(x_2)\alpha_2(x_2), \\
&\vdots \\
&f_{1,n}(x_1) + f_{2,n}(x_2) + \cdots + f_{n,n}(x_n) + c_n\alpha_n(x_n)^{d_n} \\
&\qquad + g_{n,d_n-1}(x_n)\alpha_n(x_n)^{d_n-1} + \cdots + g_{n,1}(x_n)\alpha_n(x_n)\Big)
\end{aligned}$$

takes at most $Cp_n^{-\epsilon}p_1p_2\dots p_n$ values as $x_1, x_2, \dots, x_n$ range over all values in $\mathbb{Z}_r$.

Throughout the chapter, we will use the prime number theorem (Theorem 12.2 on the page 304 and equation (12.27) on the page 305 in [29]) without explicitly mentioning it.

Proof. Write q for p_n (in fact any prime close to $p_1, p_2, \dots, p_n$ would work). The main idea is to pick $\alpha_1, \dots, \alpha_n$ so that every value $(v_1, v_2, \dots, v_n)$ attained by the expression satisfies $\sum_{i=1}^n \mod_{p_i,q}(v_i) \in S$, for a small subset $S \subset \mathbb{Z}_q$. Partitioning $\mathbb{Z}_{p_1} \oplus \mathbb{Z}_{p_2} \oplus \ldots \oplus \mathbb{Z}_{p_n}$ into cosets of $\{0\} \times \ldots \times \{0\} \times \mathbb{Z}_{p_n}$, we see the set of values of the expression can take only at most $|S|$ values on each coset, and thus a small number of values in total.

We use Lemma 7.17 in order to define α_i. Recall that the lemma gives $C', \epsilon > 0$ such that every non-constant polynomial of degree at most d in $\mathbb{Z}_{p_i}$ for any i, takes a value in $\{0, 1, \dots, C'q^{1-\epsilon}\}$ (modify the constant coefficient if necessary). For every i, we define α_i as follows. We apply the lemma for every fixed $x_i \in \mathbb{Z}_{p_1} \oplus \mathbb{Z}_{p_2} \oplus \ldots \oplus \mathbb{Z}_{p_n}$ to the polynomial

$$c_i t^{d_i} + \sum_{j=1}^{d_i-1} g_{i,j}(x_i)t^j + \sum_{j=1}^{n} \mathrm{mod}_{p_j,p_i}(f_{i,j}(x_i)).$$

Hence, we can pick t, such that this expression takes value in $\{0, 1, \dots, C'q^{1-\epsilon}\} \subset \mathbb{Z}_{p_i}$. We set $\alpha_i(x_i) := t$. Therefore, we have defined $\alpha_i \colon \mathbb{Z}_{p_1} \oplus \mathbb{Z}_{p_2} \oplus \ldots \oplus \mathbb{Z}_{p_n} \to \mathbb{Z}_{p_i}$, so that

$$\operatorname{mod}_{p_i,q}\left(c_i\alpha_i(x_i)^{d_i}+\sum_{j=1}^{d_i-1}g_{i,j}(x_i)\alpha_i(x_i)^j+\sum_{j=1}^{n}\operatorname{mod}_{p_j,p_i}(f_{i,j}(x_i))\right)\in S\subset\mathbb{Z}_q,$$

where $S=\operatorname{mod}_{p_i,q}(\{0,1,\dots,C'q^{1-\epsilon}\})=\{0,1,\dots,C'q^{1-\epsilon}\}$. To finish the proof, we apply Lemma 7.14.

Note that we have

$$\begin{aligned}
&\sum_{i=1}^{n}\operatorname{mod}_{p_i,q}\left(\sum_{j=1}^{n}f_{j,i}(x_j)+c_i\alpha_i(x_i)^{d_i}+\sum_{j=1}^{d_i-1}g_{i,j}(x_i)\alpha_i(x_i)^j\right)\\
&\overset{O_n(1)}{=}\sum_{i=1}^{n}\left(\sum_{j=1}^{n}\operatorname{mod}_{p_i,q}(f_{j,i}(x_j))+\operatorname{mod}_{p_i,q}(c_i\alpha_i(x_i)^{d_i})+\sum_{j=1}^{d_i-1}\operatorname{mod}_{p_i,q}(g_{i,j}(x_i)\alpha_i(x_i)^j)\right)\\
&\overset{O_n(1)}{=}\left(\sum_{i=1}^{n}\sum_{j=1}^{n}\operatorname{mod}_{p_j,q}\circ\operatorname{mod}_{p_i,p_j}(f_{j,i}(x_j))\right)\\
&\qquad+\left(\sum_{i=1}^{n}\left(\operatorname{mod}_{p_i,q}(c_i\alpha_i(x_i)^{d_i})+\sum_{j=1}^{d_i-1}\operatorname{mod}_{p_i,q}(g_{i,j}(x_i)\alpha_i(x_i)^j)\right)\right)\\
&=\left(\sum_{i=1}^{n}\sum_{j=1}^{n}\operatorname{mod}_{p_i,q}\circ\operatorname{mod}_{p_j,p_i}(f_{i,j}(x_i))\right)\\
&\qquad+\left(\sum_{i=1}^{n}\left(\operatorname{mod}_{p_i,q}(c_i\alpha_i(x_i)^{d_i})+\sum_{j=1}^{d_i-1}\operatorname{mod}_{p_i,q}(g_{i,j}(x_i)\alpha_i(x_i)^j)\right)\right)\\
&=\sum_{i=1}^{n}\operatorname{mod}_{p_i,q}\left(\operatorname{mod}_{p_j,p_i}(f_{i,j}(x_i))+c_i\alpha_i(x_i)^{d_i}+\sum_{j=1}^{d_i-1}g_{i,j}(x_i)\alpha_i(x_i)^j\right)\in nS
\end{aligned}\tag{7.3}$$

We conclude that values $(v_1,v_2,\dots,v_n)$ attained by the expression with the maps α_i defined as above satisfy

$$\sum_{i=1}^{n}\operatorname{mod}_{p_i,q}(v_i)\in nS+T,$$

for a set T of size at most $O_n(1)$. Since $nS=\{0,1,\dots,nC'q^{1-\epsilon}\}\subset\mathbb{Z}_q$, the expression takes at most $O_{n,d}(p_1p_2\dots p_{n-1}p_n^{1-\epsilon})$ values, as desired. □

The case 3(a) now follows from a straightforward application of Proposition 7.19.

We deal with the remaining cases in a similar fashion.

Case 2(a). Let the linear part of the expression be $\lambda_1\alpha(x)+\mu_1 x+\lambda_2\beta(y)+\mu_2 y$. We shall take $q = q_1q_2$, for coprime q_1 and q_2, with $\mathbb{Z}_q \cong \mathbb{Z}_{q_1} \oplus \mathbb{Z}_{q_2}$. We set $\alpha_1(x) := -c_3x_1$ and $\beta_2(y) := -c_4y_2$. It remains to choose $\alpha_2\colon \mathbb{Z}_{q_1} \oplus \mathbb{Z}_{q_2} \to \mathbb{Z}_{q_2}$ and $\beta_1\colon \mathbb{Z}_{q_1} \oplus \mathbb{Z}_{q_2} \to \mathbb{Z}_{q_1}$ so that the expression

$$\begin{aligned}
&\Big((c_1-c_3)(c_2-c_3)x_1^2 - c_3\lambda_1x_1 + \mu_1x_1 + \lambda_2\beta_1(y) + \mu_2y_1,\\
&\quad(\alpha_2(x)+c_1x_2)(\alpha_2(x)+c_2x_2) + \lambda_1\alpha_2(x) + \mu_1x_2 - c_4\lambda_2y_2 + \mu_2y_2\Big)\\
=&\Big((c_1-c_3)(c_2-c_3)x_1^2 + (\mu_1 - c_3\lambda_1)x_1 + \mu_2y_1 + \lambda_2\beta_1(y),\\
&\quad c_1c_2x_2^2 + \mu_1x_2 + (\mu_2 - c_4\lambda_2)y_2 + \alpha_2(x)^2 + ((c_1+c_2)x_2 + \lambda_1)\alpha_2(x)\Big)
\end{aligned}$$

takes small number of values. But, recalling that $\lambda_2 = 0$ implies $\mu_2 = 0$, this follows directly from Proposition 7.19, and we may take q_1, q_2 to be prime.

Case 3(b). Let the linear part of the expression be $\lambda_1\alpha(x) + \mu_1x + \lambda_2\beta(y) + \mu_2y+\lambda_3\gamma(z)+\mu_3z$. We shall take $q = q_1q_2q_3$, for coprime q_1, q_2 and q_3, with $\mathbb{Z}_q \cong \mathbb{Z}_{q_1}\oplus\mathbb{Z}_{q_2}\oplus\mathbb{Z}_{q_3}$. We set $\alpha_1(x) := -c_1x_1, \alpha_2(x) := -c_3x_2, \beta_2(y) := -c_2y_2, \beta_3(y) := -c_2y_3, \gamma_1(z) := -c_4z_1$ and $\gamma_3(z) := -c_4z_3$. It remains to choose $\alpha_3\colon \mathbb{Z}_{q_1} \oplus \mathbb{Z}_{q_2} \oplus \mathbb{Z}_{q_3} \to \mathbb{Z}_{q_3}, \beta_1\colon \mathbb{Z}_{q_1} \oplus \mathbb{Z}_{q_2} \oplus \mathbb{Z}_{q_3} \to \mathbb{Z}_{q_1}$ and $\gamma_2\colon \mathbb{Z}_{q_1} \oplus \mathbb{Z}_{q_2} \oplus \mathbb{Z}_{q_3} \to \mathbb{Z}_{q_2}$ so that the expression

$$\begin{aligned}
\Big(&(-c_1\lambda_1+\mu_1)x_1 + \lambda_2\beta_1(y) + \mu_2y_1 + (-c_4\lambda_3+\mu_3)z_1,\\
&(-c_3\lambda_1+\mu_1)x_2 + (-c_2\lambda_2+\mu_2)y_2 + \lambda_3\gamma_2(z) + \mu_3z_2,\\
&\lambda_1\alpha_3(x) + \mu_1x_3 + (-c_2\lambda_2+\mu_2)y_3 + (-c_4\lambda_3+\mu_3)z_3\Big)
\end{aligned}$$

takes small number of values. Once again, recalling that $\lambda_i = 0$ implies $\mu_i = 0$, this follows directly from Proposition 7.19, and we may take q_1, q_2 and q_3 to be prime.

Case 4(a). Let the linear part of the expression be $\lambda_1\alpha(x) + \mu_1x + \lambda_2\beta(y) + \mu_2y + \lambda_3\gamma(z) + \mu_3z + \lambda_4\delta(w) + \mu_4w$. We shall take $q = q_1q_2q_3q_4$, for coprime

q_1, q_2, q_3 and q_4, with $\mathbb{Z}_q \cong \mathbb{Z}_{q_1} \oplus \mathbb{Z}_{q_2} \oplus \mathbb{Z}_{q_3} \oplus \mathbb{Z}_{q_4}$. We set

$$\begin{aligned}
\beta_1(y) &:= -c_2 y_1, & \gamma_1(z) &:= -c_3 z_1, & \delta_1(w) &:= -c_4 w_1, \\
\alpha_2(x) &:= -c_1 x_2, & \gamma_2(z) &:= -c_3 z_2, & \delta_2(w) &:= -c_4 w_2, \\
\alpha_3(x) &:= -c_1 x_3, & \beta_3(y) &:= -c_2 y_3, & \delta_3(w) &:= -c_4 w_3, \\
\alpha_4(x) &:= -c_1 x_4, & \beta_4(y) &:= -c_2 y_4, & \gamma_4(z) &:= -c_3 z_4.
\end{aligned}$$

We use Proposition 7.19 to find $\alpha_1, \beta_2, \gamma_3, \delta_4$ so that the expression

$$\begin{gathered}
(\lambda_1 \alpha_1(x) + \mu_1 x_1 + (-c_2\lambda_2 + \mu_2) y_1 + (-c_3\lambda_3 + \mu_3) z_1 + (-c_4\lambda_4 + \mu_4) w_1, \\
(-c_1\lambda_1 + \mu_1) x_2 + \lambda_2 \beta_2(y) + \mu_2 y_2 + (-c_3\lambda_3 + \mu_3) z_2 + (-c_4\lambda_4 + \mu_4) w_2, \\
(-c_1\lambda_1 + \mu_1) x_3 + (-c_2\lambda_2 + \mu_2) y_3 + \lambda_3 \gamma_3(z) + \mu_3 z_3 + (-c_4\lambda_4 + \mu_4) w_3, \\
(-c_1\lambda_1 + \mu_1) x_4 + (-c_2\lambda_2 + \mu_2) y_4 + (-c_3\lambda_3 + \mu_3) z_4 + \lambda_4 \delta_4(w) + \mu_4 w_4)
\end{gathered}$$

takes small number of values. This completes the proof of Theorem 7.16. □

7.5.1 Further discussion of the identification of coordinates idea

As we have seen in the proof of Theorem 7.16, Proposition 7.19 was used in a very similar fashion for several cases of expressions. The goal of this short subsection is to take this approach further and see what expressions can be handled using this idea.

We temporarily return to the notation of x_i for the variables and α_i for the maps. The value of x_i at coordinate c is denoted by $x_{i,c}$. Observe that when we use Proposition 7.19, we have to pick some of the maps $\alpha_{i,c}$ to cancel out the mixed quadratic terms like $\alpha_{1,c}(x_1)(\alpha_{2,c}(x_2)+x_{2,c})$. In the proof of Theorem 7.16 in the last few cases, given an expression, we used a different coordinate c for every variable x_i, and we picked $\alpha_{j,c}$ for $j \neq i$, so that the mixed quadratic terms disappear. Our goal now is to put all these ideas together in a single proposition. First, we need to set up some useful definitions.

Fix an expression E in variables $x_1, x_2, \dots, x_n$. Define a graph G_E on vertices $\{x_1, x_2, \dots, x_n\}$ by adding an edge $x_i x_j$ for every term of the form $(\alpha_i(x_i) + cx_i)(\alpha_j(x_j) + dx_j)$ with $i \neq j$, with multiple edges allowed (so $x_i x_j$ appears the same number of times the relevant terms occur in E).

Proposition 7.20. *(Acyclic version of the identification of the coordinates.) Let E be a quadratic expression such that G_E has no cycles (in particular, no repeated edges). Then there is an absolute constant $\epsilon > 0$ such that the following holds. We can find q, a product of distinct, arbitrarily large primes, and maps $\alpha_1, \ldots, \alpha_n : \mathbb{Z}_q \to \mathbb{Z}_q$ such that E takes at most $O(q^{1-\epsilon})$ values.*

Proof. As promised, we will take $q = q_1 q_2 \ldots q_n$, with q_i coprime products of distinct primes, suitably chosen. As always, view $\mathbb{Z}_q$ as the direct sum $\mathbb{Z}_{q_1} \oplus \ldots \oplus \mathbb{Z}_{q_n}$. Let $c \in [n]$ be an arbitrary coordinate. We start from x_c and traverse the graph G_E. (If G_E is disconnected, pick arbitrary vertices in all other components to start the traversal from. For each such starting vertex x_i, $i \neq c$, set $\alpha_{i,c} = 0$.) Since the graph is acyclic, we reach every variable at most once, and we visit every edge. When we move along the edge $x_i x_j$, from x_i to x_j, that means that there is a term $(\alpha_i(x_i) + a x_i)(\alpha_j(x_j) + b x_j)$ in the expression, and we set $\alpha_{j,c}(x_j) := -b x_{j,c}$, to make the term vanish. Since this is the first time we reach x_j, there are no issues with defining $\alpha_{j,c}$.

After this procedure, we have defined $\alpha_{i,j}$ for $i \neq j$, so that for every coordinate c, the expression E_c no longer has mixed quadratic terms. We still have the freedom of choosing $\alpha_{c,c}$, so we now may apply Proposition 7.19 to finish the proof. □

As we shall see later, depending on the structure of the graph G_E, it is not always possible to choose some of the maps $\alpha_{i,c}$ so that the mixed quadratic terms vanish, so there is no obvious way to make Proposition 7.20 more general.

7.6 Sets A with small $3A^2 + kA$

In this section we prove the final case of the main theorem.

Theorem 7.21. *For any $k \in \mathbb{N}_0$ and any $\epsilon > 0$, there is a natural number q, which is a product of distinct, arbitrarily large primes, and a set $A \subset \mathbb{Z}_q$ such that $A - A = \mathbb{Z}_q$, while $|3A^2 + kA| < \epsilon q$.*

Proof. We proceed like in the proofs of Theorems 7.10 and 7.16, except that the details become once again more complicated and the ideas we developed so far, culminating in Proposition 7.20, do not suffice. As usual, the proof is based on Proposition 7.9. We split all expressions in their quadratic and linear parts, and we may assume that if a variable appears at all in an expression, it must appear in the quadratic part. In the first part of the discussion of the possible expressions, we use the notation x_i for variables and α_i for maps, as there can be up to 6 variables involved. Later, we again switch to x, y, z and α, β, γ notation.

Firstly, by Corollary 7.12, we only need to consider expressions with at least two variables. Next, we use Proposition 7.20 to treat the expressions with at least 4 variables. We look at the graph G_E. Note that if we have an isolated vertex x_i in G_E, since x_i appears in the quadratic part, we must have term of the form $(\alpha_i(x_i) + c_1x_i)(\alpha_i(x_i) + c_2x_i)$ in E. Hence, the number of isolated vertices v_{is} plus the number of edges e is at most 3, which is the number of quadratic terms in E.

Expression E with exactly 6 variables. We look at G_E. It is a graph on 6 vertices, with $v_{is} + e \leq 3$. Hence, it is a perfect matching, which is acyclic, so Proposition 7.20 applies.

Expression E with exactly 5 variables. Looking at G_E, which is a graph on 5 vertices with $v_{is} + e \leq 3$, we see that at most one vertex can have degree greater than 1. The graph G_E is acyclic, so Proposition 7.20 applies.

Expression E with exactly 4 variables. Once again, we analyse G_E. It is a graph on 4 vertices with $v_{is} + e \leq 3$. The only way to get a cycle is if the graph has a double edge x_1x_2 and an edge x_3x_4 (after a suitable renaming of variables). Thus, the quadratic part of E is of the form

$$\begin{aligned}
&(\alpha_1(x_1) + c_1x_1)(\alpha_2(x_2) + c_2x_2) \\
+&(\alpha_1(x_1) + c'_1x_1)(\alpha_2(x_2) + c'_2x_2) \\
+&(\alpha_3(x_3) + c_3x_3)(\alpha_4(x_4) + c_4x_4),
\end{aligned}$$

where $c_1, c_2, c'_1, c'_2, c_3, c_4 \in \{0, 1\}$. If $c_1 = c'_1$ or $c_2 = c'_2$, we can rewrite the quadratic part as a linear combination of only two quadratic terms, so that the graph G_E becomes a matching, and therefore acyclic. Thus, assume that $c_1 \neq c'_1$ and $c_2 \neq c'_2$. But, using the affine maps solution from Lemma 7.15 we can cancel all the terms in E that involve x_1 and x_2. Then, w.l.o.g. E becomes an expression with quadratic term

$$(\alpha_3(x_3) + c_3x_3)(\alpha_4(x_4) + c_4x_4)$$

which we have already done using the basic version of the identification of coordinates idea in Lemma 7.13.

Hence, we may assume that the expression E has either two or three variables. We treat these cases separately. From now on, we use the notation x, y, z for the variables and α, β, γ for maps.

7.6.1 E HAS TWO VARIABLES x AND y

Observe that if there is at most one mixed quadratic term $(\alpha(x)+c_1x)(\beta(y)+c_2y)$ in the quadratic part, then once again Proposition 7.20 applies. Hence, we may assume that there are at least two such terms in E. Suppose now that there all three quadratic terms are of this form, hence the quadratic part is

$$(\alpha(x) + c_1x)(\beta(y) + c_2y) + (\alpha(x) + c_3x)(\beta(y) + c_4y) + (\alpha(x) + c_5x)(\beta(y) + c_6y),$$

where $c_1, c_2, \dots, c_6 \in \{0, 1\}$. This constraint on the coefficients is crucial. By pigeonhole principle, there are at least two equal coefficients among c_1, c_3, c_5, w.l.o.g. $c_1 = c_3$. The quadratic part of E may be written as

$$(\alpha(x) + c_1x)(2\beta(y) + (c_2 + c_4)y) + (\alpha(x) + c_5x)(\beta(y) + c_6y),$$

which we treat using Lemma 7.13 if this factorizes further, or using Lemma 7.15 otherwise.

It remains to treat the case when there are exactly two mixed terms, so the quadratic part is w.l.o.g.

$$(\alpha(x) + c_1x)(\alpha(x) + c_2x) + (\alpha(x) + c_3x)(\beta(y) + c_4y) + (\alpha(x) + c_5x)(\beta(y) + c_6y).$$

However, we can no longer use the affine maps to cancel out quadratic terms to modify the expression and then apply Proposition 7.20. Instead, we have to use a different argument, which unfortunately gives significantly worse bounds.

Lemma 7.22. *Let E be a quadratic expression with quadratic part of the form*

$$n_1\alpha(x)^2 + \alpha(x)(n_2x + n_3\beta(y) + n_4y) + x(n_5x + n_6\beta(y) + n_7y),$$

with $n_1, n_2, \ldots, n_7 \in \mathbb{Z}$ and $n_1, n_3 \neq 0$. Then, for every sufficiently large prime p, we can find $\alpha, \beta \colon \mathbb{Z}_p \to \mathbb{Z}_p$ such that the expression does not attain every value in $\mathbb{Z}_p$.

Immediately, we have the following corollary.

Corollary 7.23. *Let E be a quadratic expression with quadratic part of the form*

$$n_1\alpha(x)^2 + \alpha(x)(n_2x + n_3\beta(y) + n_4y) + x(n_5x + n_6\beta(y) + n_7y),$$

with $n_1, n_2, \ldots, n_7 \in \mathbb{Z}$ and $n_1, n_3 \neq 0$. Let $\epsilon > 0$. Then, there is q, product of distinct, arbitrarily large primes, and maps $\alpha, \beta \colon \mathbb{Z}_q \to \mathbb{Z}_q$ such that the expression attains at most ϵq values.

Proof. Let N be the bound in Lemma 7.22 such that for all primes $p > N$ we have $\alpha^{(p)}, \beta^{(p)} \colon \mathbb{Z}_p \to \mathbb{Z}_p$ such that the expression evades one value, i.e. all values are confined to a set S_p of size $p-1$. If we now take $q = p_1p_2 \ldots p_n$, a product of distinct primes greater than N, then, once again identifying $\mathbb{Z}_q \cong \mathbb{Z}_{p_1} \oplus \ldots \oplus \mathbb{Z}_{p_n}$, and defining $\alpha, \beta \colon \mathbb{Z}_q \to \mathbb{Z}_q$ coordinatewise using $\alpha^{(p_i)}, \beta^{(p_i)}$, we have that the expression in $\mathbb{Z}_q$ attains values in $S_{p_1} \times S_{p_2} \times \ldots \times S_{p_n}$. Hence, it takes at most $(p_1 - 1) \ldots (p_n - 1)$ values. A standard calculation reveals that for n sufficiently large, the number of values becomes $o(q)$. (The p that appears in the sums and products below ranges over primes only.) Indeed,

$$\begin{aligned}\prod_{N<p<M} \frac{p-1}{p} &= \exp\left(\sum_{N<p<M} \log\left(1 - \frac{1}{p}\right)\right) = \exp\left(\sum_{N<p<M} -\frac{1}{p} + O\left(\frac{1}{p^2}\right)\right) \\ &= O\left(\exp\left(-\sum_{N<p<M} \frac{1}{p}\right)\right) \to 0\end{aligned}$$

as $M \to \infty$, since $\sum_p \frac{1}{p} = \infty$. □

Proof of Lemma 7.22. Let $\lambda_1\alpha(x) + \mu_1x + \lambda_2\beta(y) + \mu_2y$ be the linear part of the expression. The proof is based on a dependent random choice argument. We will define $\alpha \colon \mathbb{Z}_p \to \mathbb{Z}_p$ essentially by setting each $\alpha(y)$ uniformly independently at random (for technical reasons, for every x we will forbid one value in $\mathbb{Z}_p$). Our aim is to define β accordingly so that the expression evades zero value. Hence, for every y, we want to find $\beta(y)$ such that there is no x with

$$\begin{aligned}\beta(y)&(n_3\alpha(x)+n_6x+\lambda_2)\\+\alpha(x)&(n_1\alpha(x)+n_2x+n_4y+\lambda_1)\\+n_5x^2&+n_7xy+\mu_1x+\mu_2y=0.\end{aligned}\tag{7.4}$$

In other words, provided $n_3\alpha(x)+n_6x+\lambda_2\neq 0$ always, we want a value of $\beta(y)$ such that

$$\begin{aligned}\beta(y)\neq -\frac{1}{n_3\alpha(x)+n_6x+\lambda_2}\Big(&y(n_4\alpha(x)+n_7x+\mu_2)\\&+\alpha(x)(n_1\alpha(x)+n_2x+\lambda_1)+n_5x^2+\mu_1x\Big),\end{aligned}\tag{7.5}$$

for all $x\in\mathbb{Z}_p$. Hence, this becomes the requirement that for every fixed y, the set

$$\begin{aligned}S_y{:}=\Big\{-\frac{1}{n_3\alpha(x)+n_6x+\lambda_2}\Big(&y(n_4\alpha(x)+n_7x+\mu_2)\\&+\alpha(x)(n_1\alpha(x)+n_2x+\lambda_1)+n_5x^2+\mu_1x\Big){:}\,x\in\mathbb{Z}_p\Big\}\end{aligned}$$

is not the whole set $\mathbb{Z}_p$. We now define $\alpha\colon\mathbb{Z}_p\to\mathbb{Z}_p$ by setting each $\alpha(x)$ independently to be a uniform random variable on $\mathbb{Z}_p\setminus\{-\frac{n_6x+\lambda_2}{n_3}\}$ (which is fine, as $n_3\neq 0$).

Let B_y be the event that the set S_y is the whole $\mathbb{Z}_p$, i.e. for every v there is x such that

$$\begin{aligned}0=&v\,(n_3\alpha(x)+n_6x+\lambda_2)\\&+\Big(y(n_4\alpha(x)+n_7x+\mu_2)+\alpha(x)(n_1\alpha(x)+n_2x+\lambda_1)+n_5x^2+\mu_1x\Big).\end{aligned}\tag{7.6}$$

Suppose that B_y occurs. We cannot use the same x for two values of v, so by counting, for every v, we have exactly one $x=x(v)$ such that (7.6) holds. Suppose that we already know this permutation $x(v)=\pi(v)$. The equation is further equivalent to

$$\begin{aligned}n_1\alpha(\pi(v))^2&+\alpha(\pi(v))(n_2\pi(v)+n_4y+n_3v+\lambda_1)+n_5\pi(v)^2+n_6\pi(v)v\\&+n_7\pi(v)y+\mu_1\pi(v)+y\mu_2+v\lambda_2=0.\end{aligned}$$

Hence, for every v, we know that $\alpha(\pi(v))$ must take one of the two values depending only on v, since $n_1\neq 0$. So, given π, there are at most 2^p choices for

α. Hence, the probability of B_y is $\mathbb{P}(B_y) \leq p!\,2^p/(p-1)^p$. By Stirling's formula,

$$\mathbb{P}(B_y) = O\left(\sqrt{p}\left(\frac{2}{e}\right)^p\right).$$

By the union bound, the probability $\mathbb{P}(\cup_y B_y) = o(1)$, so there is a choice of α such that for all y we have $S_y \neq \mathbb{Z}_p$. For such α, we can define β so that the expression does not attain every value, proving the lemma. $\square$

Returning to our main argument, the case when the quadratic part is of the form

$$(\alpha(x)+c_1x)(\alpha(x)+c_2x)+(\alpha(x)+c_3x)(\beta(y)+c_4y)+(\alpha(x)+c_5x)(\beta(y)+c_6y).$$

follows directly from Corollary 7.23, since $n_1 = 1, n_3 = 2$.

7.6.2 E has three variables

Finally, we address the case when the quadratic part of E has exactly three variables. Once again, we only need to consider the situation when G_E has a cycle. We know that G_E is a graph on three vertices, with $v_{is} + e \leq 3$. The only such graphs that have cycles are xy, xy (a repeated edge and an isolated vertex), xy, xy, xz (a repeated edge and an additional edge) and xy, yz, zx (a cycle of length 3).

G_E is a repeated edge. In this case, the quadratic part of the expression is w.l.o.g.

$$(\alpha(x)+c_1x)(\beta(y)+c_2y)+(\alpha(x)+c_3x)(\beta(y)+c_4y)+(\gamma(z)+c_5z)(\gamma(z)+c_6z).$$

If $c_1 = c_3$ or $c_2 = c_4$, we can further factorize the expression and apply Proposition 7.20, to finish the proof. Thus assume that $c_1 \neq c_3$ and $c_2 \neq c_4$.

Let the linear part of the expression be $\lambda_1\alpha(x)+\mu_1x+\lambda_2\beta(y)+\mu_2y+\lambda_3\gamma(z)+\mu_3z$. Fix a prime p, and apply Lemma 7.15 to the expression

$$(\alpha(x)+c_1x)(\beta(y)+c_2y)+(\alpha(x)+c_3x)(\beta(y)+c_4y)+\lambda_1\alpha(x)+\mu_1x+\lambda_2\beta(y)+\mu_2y$$

to make it constant. Hence, it remains to pick $\gamma\colon \mathbb{Z}_p \to \mathbb{Z}_p$ so that the expression

$$(\gamma(z)+c_5z)(\gamma(z)+c_6z)+\lambda_3\gamma(z)+\mu_3z$$

attains a small number of values, which we can ensure if we apply Lemma 7.17 for each z to the polynomial $\gamma(z)^2 + (c_5 z + c_6 z + \lambda_3)\gamma(z) + c_5 c_6 z^2 + \mu_3 z$. Provided p is large enough, $\gamma(z)$ can be chosen so that the value of the polynomial is small. This completes the proof in this case.

G_E **is a 3-cycle.** In this case, the quadratic part of E has three mixed terms, one for each pair of variables among x, y, z. More precisely, it is

$$(\alpha(x) + c_1 x)(\beta(y) + c_2 y) + (\beta(y) + c_3 y)(\gamma(z) + c_4 z) + (\gamma(z) + c_5 z)(\alpha(x) + c_6 x),$$

where $c_1, \ldots, c_6 \in \{0, 1\}$. Let the linear part be

$$\lambda_1 \alpha(x) + \mu_1 x + \lambda_2 \beta(y) + \mu_2 y + \lambda_3 \gamma(z) + \mu_3 z.$$

First, assume that no further factorization is possible, i.e. $c_1 \neq c_6, c_2 \neq c_3$ and $c_4 \neq c_5$. We set $\alpha(x) = -c_1 x + d_1, \beta(y) = -c_3 y + d_2, \gamma(z) = -c_5 z + d_3$, so that the expression becomes

$$\begin{aligned} &d_1((c_2 - c_3)y + d_2) + d_2((c_4 - c_5)z + d_3) + d_3((c_6 - c_1)x + d_1) \\ &+ (\mu_1 - c_1\lambda_1)x + (\mu_2 - c_3\lambda_2)y + (\mu_3 - c_5\lambda_3)z + (\lambda_1 d_1 + \lambda_2 d_2 + \lambda_3 d_3). \end{aligned}$$

Rearranging further, we obtain

$$\begin{aligned} &x(d_3(c_6 - c_1) + \mu_1 - c_1\lambda_1) + y(d_1(c_2 - c_3) + \mu_2 - c_3\lambda_2) \\ &+ z(d_2(c_4 - c_5) + \mu_3 - c_5\lambda_3) + (\lambda_1 d_1 + \lambda_2 d_2 + \lambda_3 d_3 + d_1 d_2 + d_2 d_3 + d_3 d_1). \end{aligned}$$

Setting $d_1 = \frac{\mu_2 - c_3\lambda_2}{c_3 - c_2}$, $d_2 = \frac{\mu_3 - c_5\lambda_3}{c_5 - c_4}$ and $d_3 = \frac{\mu_1 - c_1\lambda_1}{c_1 - c_6}$, the expression becomes constant.

Now, suppose that w.l.o.g. $c_1 = c_6$. Assume for now that $(c_3 - c_2)(c_4 - c_5) = 0$, we will address the case when this product does not vanish later. The expression becomes

$$\begin{aligned} (\alpha(x) + c_1 x)&(\beta(y) + c_2 y + \gamma(z) + c_5 z) + (\beta(y) + c_3 y)(\gamma(z) + c_4 z) \\ &+ \lambda_1 \alpha(x) + \mu_1 x + \lambda_2 \beta(y) + \mu_2 y + \lambda_3 \gamma(z) + \mu_3 z. \end{aligned}$$

We use the identification of coordinates approach. We will take $q = p_1 p_2 p_3$, where $p_1 < p_2 < p_3 < 2p_1$ are arbitrarily large primes. Identify $\mathbb{Z}_q \cong \mathbb{Z}_{p_1} \oplus \mathbb{Z}_{p_2} \oplus \mathbb{Z}_{p_3}$. Our first step is to set

$$\alpha_1(x) = -c_1 x_1, \beta_1(y) = -c_3 y_1 + 1 - \lambda_3, \alpha_2(x) = -c_1 x_2, \gamma_2(z) = -c_4 z_2 + 1 - \lambda_2.$$

This way, the quadratic terms vanish in the first two coordinates, and we still have freedom of choosing β_2, γ_1 to cancel the linear terms in y, z. We want to do the same for α_3, so we set $\beta_3(y) = -c_2 y_3 + 1 - \lambda_1, \gamma_3(z) = -c_5 z_3$. However, with such a choice, the third coordinate of the expression is

$$\begin{aligned}
&(1-\lambda_1)(\alpha_3(x) + c_1 x_3) + ((c_3 - c_2)y_3 + 1 - \lambda_1)((c_4 - c_5)z_3) + \lambda_1 \alpha_3(x) + \mu_1 x_3 \\
&\qquad + y_3(\mu_2 - \lambda_2 c_2) + z_3(\mu_3 - \lambda_3 c_5) + \lambda_2(1 - \lambda_1) \\
=\,&\alpha_3(x) + ((1-\lambda_1)c_1 + \mu_1)x_3 + (c_3 - c_2)(c_4 - c_5)y_3 z_3 + (\mu_2 - \lambda_2 c_2)y_3 \\
&\qquad + (\mu_3 - \lambda_3 c_5 + (1 - \lambda_1)(c_4 - c_5))z_3 + \lambda_2(1 - \lambda_1).
\end{aligned}$$

Since $(c_3 - c_2)(c_4 - c_5) = 0$, the expression becomes

$$\begin{aligned}
\Big(&(\mu_1 - c_1\lambda_1)x_1 + (\mu_2 - c_3\lambda_2)y_1 + \gamma_1(z) + (\mu_3 + (1-\lambda_3)c_4)z_1 + \lambda_2(1-\lambda_3), \\
&(\mu_1 - c_1\lambda_1)x_2 + \beta_2(y) + (\mu_2 + c_3(1-\lambda_2))y_2 + (\mu_3 - c_4\lambda_3)z_2 + \lambda_3(1-\lambda_2), \\
&\alpha_3(x) + ((1-\lambda_1)c_1 + \mu_1)x_3 + (\mu_2 - \lambda_2 c_2)y_3 \\
&\qquad\qquad\qquad\qquad + (\mu_3 - \lambda_3 c_5 + 1 - \lambda_1)z_3 + \lambda_2(1-\lambda_1)\Big).
\end{aligned}$$

We may now apply the identification of coordinates idea, using Proposition 7.19, to finish the proof in this case.

Now assume that $(c_3 - c_2)(c_4 - c_5) \neq 0$. We shall take $q = p_1p_2p_3p_4p_5$ and use the additional fourth and fifth coordinates to cancel out the y_3z_3 term. Also, using the prime number theorem, we can find arbitrarily large primes such that $p_1 < \cdots < p_5 < p_1 + O(\log p_i)$. In the work below it will be essential that all the primes are close in value (although it will not be important to have them this close). Writing E also for the resulting map defined by α, β, γ and the expression, our aim is to show that

$$\sum_{i=1}^{5} \operatorname{mod}_{p_i, p_3}(E_i)$$

takes few values in $\mathbb{Z}_{p_3}$.

We use the same choices of $\alpha_1, \alpha_2, \beta_1, \beta_3, \gamma_2, \gamma_3$ as in the case when $(c_3 - c_2)(c_4 - c_5) = 0$. Next, we set $\alpha_4(x) = -c_1 x_4, \beta_4(y) = -\operatorname{mod}_{p_3,p_4}(y_3) -$

$c_3y_4, \gamma_4(y) = \mathrm{mod}_{p_3,p_4}(z_3) - c_4z_4$. Observe that

$$\begin{aligned}
&\mathrm{mod}_{p_4,p_3}\left((\beta_4(y) + c_3y_4)(\gamma_4(y) + c_4z_4)\right) + \mathrm{mod}_{p_3,p_3}(y_3z_3) \\
=&\ \mathrm{mod}_{p_4,p_3}(-\mathrm{mod}_{p_3,p_4}(y_3)\,\mathrm{mod}_{p_3,p_4}(z_3)) + y_3z_3 \\
=&\ \pi_{p_3} \circ \iota_{p_4}(-\pi_{p_4} \circ \iota_{p_3}(y_3)\pi_{p_4} \circ \iota_{p_3}(z_3)) + y_3z_3
\end{aligned}$$

Let $\overline{y_3} = \iota_{p_3}(y_3)$ and $\overline{z_3} = \iota_{p_3}(z_3)$. Hence $\overline{y_3}, \overline{z_3} \in \{0, 1, \ldots, p_3 - 1\}$ are integers such that $\pi_{p_3}(\overline{y_3}) = y_3$ and $\pi_{p_3}(\overline{z_3}) = z_3$ hold. We also have

$$\iota_{p_4}(-\pi_{p_4} \circ \iota_{p_3}(y_3)\pi_{p_4} \circ \iota_{p_3}(z_3)) = \iota_{p_4}(-\pi_{p_4}(\overline{y_3})\pi_{p_4}(\overline{z_3})) = \iota_{p_4}(\pi_{p_4}(-\overline{y_3}\,\overline{z_3})).$$

But $\iota_{p_4}(\pi_{p_4}(-\overline{y_3}\,\overline{z_3}))$ is an integer $w \in \{0, 1, \ldots, p_4 - 1\}$ such that $\pi_{p_4}(w) = \pi_{p_4}(-\overline{y_3}\,\overline{z_3})$, thus $w = -\overline{y_3}\,\overline{z_3} + p_4t$, for $t = \lceil \frac{\overline{y_3}\,\overline{z_3}}{p_4} \rceil$. Therefore, with this choice of t we have

$$\begin{aligned}
&\mathrm{mod}_{p_4,p_3}((\beta_4(y) + c_3y_4)(\gamma_4(y) + c_4z_4)) + \mathrm{mod}_{p_3,p_3}(y_3z_3) \\
=&\ \pi_{p_3} \circ \iota_{p_4}(-\pi_{p_4} \circ \iota_{p_3}(y_3)\pi_{p_4} \circ \iota_{p_3}(z_3)) + y_3z_3 \\
=&\ \pi_{p_3}(-\overline{y_3}\,\overline{z_3} + p_4t) + \pi_{p_3}(\overline{y_3})\pi_{p_3}(\overline{z_3}) \\
=&\ \pi_{p_3}(p_4t) = \pi_{p_3}((p_4 - p_3)t)
\end{aligned}$$

Proceeding further, we use the fifth coordinate to approximate $(p_4 - p_3)t$. To this end, write $M = \lfloor \sqrt{p_4} \rfloor$, $\overline{y_3} = uM + u', \overline{z_3} = vM + v'$, where $u', v' \in \{0, 1, \ldots, M - 1\}$, $u, v = O(M)$. Observe that uv is a good approximation to t

$$\begin{aligned}
|t - uv| = \left| \lceil \frac{\overline{y_3}\,\overline{z_3}}{p_4} \rceil - uv \right| &\leq 1 + \left| \frac{\overline{y_3}\,\overline{z_3} - p_4uv}{p_4} \right| \\
&= 1 + \left| \frac{(uM + u')(vM + v') - p_4uv}{p_4} \right| \\
&\leq 1 + \left| \frac{u'vM + uv'M + u'v'}{p_4} \right| + \left| \frac{uv(p_4 - M^2)}{p_4} \right| \leq C_1\sqrt{p_4}
\end{aligned}$$

for some absolute constant C_1, since $u, v, u', v', M, |p_4 - M^2| = O(\sqrt{p_4})$. Therefore, we set $\alpha_5 = -c_1x_5, \beta_5(y) = -\pi_{p_5}(u) - c_3y_5, \gamma_5(z) = \pi_{p_5}(v(p_4 - p_3)) - c_4z_5$. Note that β_5, γ_5 are well defined, as u depends on y only, and v depends on z only. With β_5 and γ_5 so defined we have

$$\begin{aligned}
&\mathrm{mod}_{p_5,p_3}((\beta_5(y) + c_3y_5)(\gamma_5(z) + c_4z_5)) + \pi_{p_3}(t(p_4 - p_3)) \\
=&\ \pi_{p_3}(\iota_{p_5}(-\pi_{p_5}(u)\pi_{p_5}(v(p_4 - p_3))) + t(p_4 - p_3)) \\
=&\ \pi_{p_3}(\iota_{p_5}(\pi_{p_5}(-uv(p_4 - p_3))) + t(p_4 - p_3))
\end{aligned}$$

We also have that $\iota_{p_5}(\pi_{p_5}(-uv(p_4-p_3)))$ is an integer $s \in \{0,1,\ldots,p_5-1\}$ such that $\pi_{p_5}(s) = \pi_{p_5}(-uv(p_4-p_3))$, thus $s = -uv(p_4-p_3) + p_5 t'$, where $t' = \lceil \frac{uv(p_4-p_3)}{p_5} \rceil \leq C_2 \log p_3$, for an absolute constant C_2. Therefore,

$$\begin{aligned}
&\operatorname{mod}_{p_5,p_3}((\beta_5(y)+c_3y_5)(\gamma_5(z)+c_4z_5)) + \pi_{p_3}(t(p_4-p_3)) \\
=&\pi_{p_3}(\iota_{p_5}(\pi_{p_5}(-uv(p_4-p_3))) + t(p_4-p_3)) \\
=&\pi_{p_3}(-uv(p_4-p_3) + p_5t' + t(p_4-p_3)) \\
=&\pi_{p_3}((t-uv)(p_4-p_3) + p_5t')
\end{aligned}$$

Summing up the work done so far we conclude that

$$\begin{aligned}
&\operatorname{mod}_{p_3,p_3}(y_3z_3) + \operatorname{mod}_{p_4,p_3}(\beta_4(y)+c_3y_4)(\gamma_4(y)+c_4z_4)) \\
&\qquad + \operatorname{mod}_{p_5,p_3}((\beta_5(y)+c_3y_5)(\gamma_5(z)+c_4z_5)) \\
=&y_3z_3 + \operatorname{mod}_{p_4,p_3}(-\operatorname{mod}_{p_3,p_4}(y_3)\operatorname{mod}_{p_3,p_4}(z_3)) \\
&\qquad + \operatorname{mod}_{p_5,p_3}(\pi_{p_5}(-uv(p_4-p_3))) \in S_1,
\end{aligned}$$

where $S_1 \subset \mathbb{Z}_{p_3}$ is the set defined by $\{\pi_{p_3}(a(p_4-p_3)+p_5b)\colon a,b \in \mathbb{Z}, |a|\leq C_1\sqrt{p_4}, |b|\leq C_2 \log p_3\}$. In particular $|S_1|= O(\sqrt{p_3}\log^2 p_3)$. Finally, we put everything together, using Lemma 7.14. Recall the definitions (the maps β_4, γ_4 and γ_5 below are slightly modified to cancel the term $(c_3-c_2)(c_4-c_5)y_3z_3$ instead of just y_3z_3)

$$\begin{aligned}
\alpha_1(x) &= -c_1x_1, \beta_1(y) = -c_3y_1 + 1 - \lambda_3, \\
\alpha_2(x) &= -c_1x_2, \gamma_2(z) = -c_4z_2 + 1 - \lambda_2, \\
\beta_3(y) &= -c_2y_3 + 1 - \lambda_1, \gamma_3(z) = -c_5z_3, \\
\alpha_4(x) &= -c_1x_4, \beta_4(y) = -(c_3-c_2)\operatorname{mod}_{p_3,p_4}(y_3) - c_3y_4, \\
&\qquad \gamma_4(y) = (c_4-c_5)\operatorname{mod}_{p_3,p_4}(z_3) - c_4z_4, \\
&\alpha_5 = -c_1x_5, \beta_5(y) = -\pi_{p_5}(u) - c_3y_5, \\
&\qquad \gamma_5(z) = \pi_{p_5}(v(p_4-p_3)(c_3-c_2)(c_4-c_5)) - c_4z_5.
\end{aligned}$$

Thus, $\sum_{i=1}^5 \operatorname{mod}_{p_i,p_3}(E_i)$ equals

$$\begin{aligned}
=&\sum_{i=1}^5 \operatorname{mod}_{p_i,p_3}\Big((\alpha_i(x)+c_1x_i)(\beta_i(y)+c_2y_i+\gamma_i(z)+c_5z_i) \\
&+(\beta_i(y)+c_3y_i)(\gamma_i(z)+c_4z_i) \\
&+\lambda_1\alpha_i(x)+\mu_1x_i+\lambda_2\beta_i(y)+\mu_2y_i+\lambda_3\gamma_i(z)+\mu_3z_i\Big)
\end{aligned}$$

$$
\begin{aligned}
&= \operatorname{mod}_{p_1,p_3}\Big(\gamma_1(z) + (\mu_1 - c_1\lambda_1)x_1 + (\mu_2 - c_3\lambda_2)y_1 \\
&\qquad + (\mu_3 + c_4(1-\lambda_3))z_1 + \lambda_2(1-\lambda_3)\Big) \\
&\quad + \operatorname{mod}_{p_2,p_3}\Big(\beta_2(y) + (\mu_1 - c_1\lambda_1)x_2 + (\mu_2 + c_3(1-\lambda_2))y_2 \\
&\qquad + (\mu_3 - c_4\lambda_3)z_2 + \lambda_3(1-\lambda_2)\Big)
\end{aligned}
$$

$$
\begin{aligned}
&+ \alpha_3(x) + y_3z_3(c_3-c_2)(c_4-c_5) + x_3(c_1(1-\lambda_1)+\mu_1) + (\mu_2 - \lambda_2c_2)y_3 \\
&+ ((1-\lambda_1)(c_4-c_5) - c_5\lambda_3 + \mu_3)z_3 + \lambda_2(1-\lambda_1) \\
&+ \operatorname{mod}_{p_4,p_3}\Big(- (c_3-c_2)(c_4-c_5)\operatorname{mod}_{p_3,p_4}(y_3)\operatorname{mod}_{p_3,p_4}(z_3) \\
&\quad + (\mu_1 - \lambda_1c_1)x_4 - (c_3-c_2)\lambda_2\operatorname{mod}_{p_3,p_4}(y_3) \\
&\quad + (\mu_2 - c_3\lambda_2)y_4 + (c_4-c_5)\lambda_3\operatorname{mod}_{p_3,p_4}(z_3) + (\mu_3 - \lambda_3c_4)z_4\Big) \\
&+ \operatorname{mod}_{p_5,p_3}\Big(- \pi_{p_5}(u)\pi_{p_5}(v(p_4-p_3)(c_3-c_2)(c_4-c_5)) \\
&\quad + (\mu_1 - \lambda_1c_1)x_5 - \lambda_2\pi_{p_5}(u) + (\mu_2 - \lambda_2c_3)y_5 \\
&\quad + \lambda_3\pi_{p_5}(v(p_4-p_3)(c_3-c_2)(c_4-c_5)) + (\mu_5 - \lambda_3c_4)z_5\Big) \\
&\overset{O(1)}{=} \pi_{p_3}\Big(\iota_{p_3}(\alpha_3(x)) + (\mu_1 - c_1\lambda_1)\iota_{p_1}(x_1) + (\mu_1 - c_1\lambda_1)\iota_{p_2}(x_2) \\
&\quad + (c_1(1-\lambda_1)+\mu_1)\iota_{p_3}(x_3) + (\mu_1 - \lambda_1c_1)\iota_{p_4}(x_4) + (\mu_1 - \lambda_1c_1)\iota_{p_5}(x_5) \\
&\quad + \iota_{p_2}(\beta_2(y)) + (\mu_2 - c_3\lambda_2)\iota_{p_1}(y_1) + (\mu_2 + c_3(1-\lambda_2))\iota_{p_2}(y_2) \\
&\quad + (\mu_2 - \lambda_2c_2)\iota_{p_3}(y_3) - (c_3-c_2)\lambda_2\iota_{p_4}(\operatorname{mod}_{p_3,p_4}(y_3)) \\
&\quad + (\mu_2 - c_3\lambda_2)\iota_{p_4}(y_4) - \lambda_2\iota_{p_5}(\pi_{p_5}(u)) + (\mu_2 - \lambda_2c_3)\iota_{p_5}(y_5) \\
&\quad + \iota_{p_1}(\gamma_1(z)) + (\mu_3 + c_4(1-\lambda_3))\iota_{p_1}(z_1) + (\mu_3 - c_4\lambda_3)\iota_{p_2}(z_2) \\
&\quad + ((1-\lambda_1)(c_4-c_5) - c_5\lambda_3 + \mu_3)\iota_{p_3}(z_3) + (c_4-c_5)\lambda_3\iota_{p_4}(\operatorname{mod}_{p_3,p_4}(z_3)) \\
&\quad + (\mu_3 - \lambda_3c_4)\iota_{p_4}(z_4) + \lambda_3\iota_{p_5}(\pi_{p_5}(v(p_4-p_3)(c_3-c_2)(c_4-c_5))) \\
&\quad + (\mu_5 - \lambda_3c_4)\iota_{p_5}(z_5)\Big) \\
&+ (c_3-c_2)(c_4-c_5)\Big(y_3z_3 - \operatorname{mod}_{p_4,p_3}(\operatorname{mod}_{p_3,p_4}(y_3)\operatorname{mod}_{p_3,p_4}(z_3)) \\
&\quad - \operatorname{mod}_{p_5,p_3}(\pi_{p_5}(uv(p_4-p_3)))\Big).
\end{aligned}
$$

Finally, we set $\alpha_3, \beta_2, \gamma_1$ to cancel the linear x, y, z terms respectively:

$$
\begin{aligned}
\alpha_3(x) = -\pi_{p_3}(&(\mu_1 - c_1\lambda_1)\iota_{p_1}(x_1) + (\mu_1 - c_1\lambda_1)\iota_{p_2}(x_2) \\
&+ (c_1(1-\lambda_1)+\mu_1)\iota_{p_3}(x_3) + (\mu_1 - \lambda_1c_1)\iota_{p_4}(x_4) + (\mu_1 - \lambda_1c_1)\iota_{p_5}(x_5))
\end{aligned}
$$

$$\begin{aligned}\beta_2(y) = -\pi_{p_2}((\mu_2 - c_3\lambda_2)\iota_{p_1}(y_1) + (\mu_2 + c_3(1-\lambda_2))\iota_{p_2}(y_2) \\ + (\mu_2 - \lambda_2 c_2)\iota_{p_3}(y_3) - (c_3 - c_2)\lambda_2\iota_{p_4}(\mathrm{mod}_{p_3,p_4}(y_3)) \\ + (\mu_2 - c_3\lambda_2)\iota_{p_4}(y_4) - \lambda_2\iota_{p_5}(\pi_{p_5}(u)) + (\mu_2 - \lambda_2 c_3)\iota_{p_5}(y_5)))\end{aligned}$$

$$\begin{aligned}\gamma_1(z) = -\pi_{p_1}((\mu_3 + c_4(1-\lambda_3))\iota_{p_1}(z_1) + (\mu_3 - c_4\lambda_3)\iota_{p_2}(z_2) \\ + ((1-\lambda_1)(c_4 - c_5) - c_5\lambda_3 + \mu_3)\iota_{p_3}(z_3) + (c_4 - c_5)\lambda_3\iota_{p_4}(\mathrm{mod}_{p_3,p_4}(z_3)) \\ + (\mu_3 - \lambda_3 c_4)\iota_{p_4}(z_4) + \lambda_3\iota_{p_5}(\pi_{p_5}(v(p_4 - p_3)(c_3 - c_2)(c_4 - c_5))) \\ + (\mu_5 - \lambda_3 c_4)\iota_{p_5}(z_5)))\end{aligned}$$

With this choice of α, β, γ we have

$$\begin{aligned}\sum_{i=1}^{5} \mathrm{mod}_{p_i,p_3}(E_i) \overset{O(1)}{=} (c_3 - c_2)(c_4 - c_5)\Big(y_3 z_3 \\ - \mathrm{mod}_{p_4,p_3}(\mathrm{mod}_{p_3,p_4}(y_3)\,\mathrm{mod}_{p_3,p_4}(z_3)) - \mathrm{mod}_{p_5,p_3}(\pi_{p_5}(uv(p_4 - p_3)))\Big)\end{aligned}$$

which takes small number of values.

G_E is has a repeated edge and another single edge. In this case, the quadratic part of the expression is w.l.o.g.

$$(\alpha(x) + c_1x)(\beta(y) + c_2y) + (\alpha(x) + c_3x)(\beta(y) + c_4y) + (\alpha(x) + c_5x)(\gamma(z) + c_6z).$$

If $c_1 = c_3$ or $c_2 = c_4$, we can further factorize the expression and apply Proposition 7.20, to finish the proof. Thus assume that $c_1 \neq c_3$ and $c_2 \neq c_4$. Since all $c_i \in \{0, 1\}$, we must have $c_5 \in \{c_1, c_3\}$, so w.l.o.g. $c_5 = c_1$.

We now discuss a limitation of the usual approach based on the identification of coordinates idea. Basically, we always try to cancel out the quadratic terms by taking some of the $\alpha_i, \beta_i, \gamma_i$ to be affine, while we use the rest to cancel out the linear terms in x_i, y_i, z_i. Let us try the same strategy here. Temporarily we work in $\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \ldots \oplus \mathbb{Z}_p$ to ignore the difficulties that arise from moving from one modulus to another one. For technical reasons, we use a slightly unusual indexing of $n+2$ coordinates by $-1, 0, \ldots, n$. Start by using the coordinate -1 to get a free γ_{-1} which is later used to cancel the linear terms involving z. Thus, we set $\alpha_{-1}(x) = -c_1x_{-1}$ and $\beta_{-1}(y) = -c_4y_{-1}$. Similarly, try to use the coordinate 0 to get a free β_0 map. Rewriting the expression as

$$\beta(y)(2\alpha(x) + (c_1 + c_3)x) + y((c_2 + c_4)\alpha(x) + (c_1c_2 + c_3c_4)x) + (\alpha(x) + c_5x)(\gamma(z) + c_6z),$$

we see that we need to set $\alpha_0(x) = -\frac{c_1+c_3}{2}x_0 + C$, for a constant C and $\gamma_0(z) = -c_6 z_0$. The issue is that we get a term $x_0 y_0$ with a non-zero coefficient. The natural thing to do now is to try to cancel somehow this term. During this digression, we forget about the linear terms (in any case, we can cancel them by remaining free $\alpha_i, \beta_i, \gamma_i$).

The most natural thing is to set $\gamma_i(z) = -c_6 z_i$ for $i = 1, 2, \ldots, n$ (as further mixed quadratic terms involving z seem even harder to cancel). Hence, the question is whether we can find linear maps $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n$, each a linear combination of $x_0, x_1, \ldots, x_n$ or $y_0, y_1, \ldots, y_n$ such that (w.l.o.g. $c_1 = c_2 = 0$ and $c_3 = c_4 = 1$)

$$\sum_{i=1}^{n} \alpha_i(x)\beta_i(x) + (\alpha_i(x) + x_i)(\beta_i(y) + y_i) = 0. \tag{7.7}$$

Write $\alpha_i(x) = \sum_{j=0}^{n} A_{ij} x_j$ and $\beta_i(y) = \sum_{j=0}^{n} B_{ij} y_j$. Let δ_{ij} equal 1 if $i = j$ and zero otherwise. Expanding the (7.7) we obtain

$$\begin{aligned}
&\sum_{i=1}^{n} \left(\left(\sum_{j=0}^{n} A_{ij} x_j \right) \left(\sum_{k=0}^{n} B_{ik} y_k \right) + \left(\sum_{j=0}^{n} (A_{ij} + \delta_{ij}) x_j \right) \left(\sum_{k=0}^{n} (B_{ik} + \delta_{ik}) y_k \right) \right) \\
&= \sum_{j=0}^{n} \sum_{k=0}^{n} \left(\sum_{i=1}^{n} 2A_{ij}B_{ik} + A_{ij}\delta_{ik} + \delta_{ij}B_{ik} + \delta_{ij}\delta_{ik} \right) x_j y_k.
\end{aligned} \tag{7.8}$$

Hence, we require that for every $j, k \in \{0, 1, \ldots, n\}$, which are not both zero, we have $\sum_{i=1}^{n} 2A_{ij}B_{ik} + A_{ij}\delta_{ik} + \delta_{ij}B_{ik} + \delta_{ij}\delta_{ik} = 0$, while for $j = k = 0$ this expression is non-zero (to cancel the initial $x_0 y_0$ term). We now define two $(n+1)\times(n+1)$ matrices P, Q, with entries indexed by $\{0, 1 \ldots, n\} \times \{0, 1, \ldots, n\}$, by setting $P_{ji} = A_{ij}$ when $i \geq 1$ and $P_{j0} = 0$, and $Q_{ik} = B_{ik}$ if $i \geq 1$ and $Q_{0k} = 0$. Let I' be the matrix of all zeros except $I'_{ii} = 1$ for $i \geq 1$, and let J be the matrix consisting of zeros only, except $J_{00} = 1$. We rewrite (7.8) as a matrix equation

$$2PQ + PI' + QI' + I' = \lambda J$$

for some non-zero λ. However, this is the same as

$$(2P + I')(2Q + I') = 2\lambda J - I'.$$

But comparing ranks we have

$$\begin{aligned}\operatorname{rank}(2\lambda J - I') = \operatorname{rank}((2P + I')(2Q + I')) \leq& \operatorname{rank}(2P + I')\\ \leq& n < n + 1 = \operatorname{rank}(2\lambda J - I')\end{aligned}$$

which is a contradiction. Hence, this case requires a different approach.

Finally, we construct the desired maps for this expression. By adding linear terms to α, β, γ, we may assume that the expression is

$$\begin{gathered}\alpha(x)\beta(y) + (\alpha(x) + c_1 x)(\beta(y) + c_2 y) + \alpha(x)\gamma(z)\\ +\lambda_1\alpha(x) + \mu_1 x + \lambda_2\beta(y) + \mu_2 y + \lambda_3\gamma(z) + \mu_3 z\end{gathered} \tag{7.9}$$

for some coefficients $c_1, c_2 \in \{-1, 1\}, \lambda_1, \lambda_2, \lambda_3 \in \mathbb{N}_0, \mu_1, \mu_2, \mu_3 \in \mathbb{Z}$. Let us begin by observing that in most cases there is a rather simple solution, which strangely we could not generalize to work for all choices of coefficients. Try setting $\alpha(x) = A, \beta(y) = -c_2 y + B$, for some constants A, B and suppose we work in $\mathbb{Z}_q$, where q is a product of distinct, arbitrarily large primes (so that all the coefficients and related expressions are coprime with q). With these choices, the expression (7.9) becomes

$$\begin{aligned}&A(-c_2 y + B) + (A + c_1 x)B + A\gamma(z) + \lambda_1 A + \mu_1 x + \lambda_2(-c_2 y + B)\\ &\quad + \mu_2 y + \lambda_3\gamma(z) + \mu_3 z\\ =&y(-c_2 A - c_2\lambda_2 + \mu_2) + x(c_1 B + \mu_1) + \gamma(z)(A + \lambda_3)\\ &\quad + \mu_3 z + (2AB + \lambda_1 A + \lambda_2 B).\end{aligned}$$

Further, set $B = -\mu_1 c_1$, (recall that $c_1, c_2 \in \{-1, 1\}$ so $c_1^{-1} = c_1, c_2^{-1} = c_2$) so that the coefficient of x above vanishes. We try to pick A such that coefficient of y also becomes zero, setting $A = c_2\mu_2 - \lambda_2$. If $A + \lambda_3 \neq 0$, then we can pick γ_3 to cancel the z term, and the expression actually becomes constant.

Otherwise, assume that $c_2\mu_2 - \lambda_2 + \lambda_3 = 0$. The following proposition solves the problem of making the image of expressions that satisfy this relationship miss at least some values. The complete result which says that the image can be made small is then a consequence of a simple number-theoretic calculation.

Proposition 7.24. *Let $c_1, c_2, \lambda_1, \lambda_2, \lambda_3, \mu_1, \mu_2, \mu_3 \in \mathbb{Z}$ be some fixed coefficients, such that $c_1, c_2 \in \{-1, 1\}$ and $c_2\mu_2 - \lambda_2 + \lambda_3 - c_2 \neq 0$. Then, for all sufficiently large primes p, q, obeying $q < p < 2q$, we may find maps $\alpha, \beta, \gamma \colon \mathbb{Z}_{pq} \to \mathbb{Z}_{pq}$ such that the expression (7.9) misses at least $p - q$ values.*

Proof. As always, $\mathbb{Z}_{pq}$ is viewed as $\mathbb{Z}_p \oplus \mathbb{Z}_q$. In the first coordinate, we set $\alpha_1(x) = c_2\mu_2 - \lambda_2 - c_2, \beta_1(y) = -c_2 y - \mu_1 c_1, \gamma_1(z) = \frac{-\mu_3 z + \delta_1(z) + D}{c_2\mu_2 + \lambda_3 - \lambda_2 - c_2}$, with $\delta_1(z)$ to be chosen and a constant D. After a suitable choice of D, the first coordinate of the expression becomes $y_1 - \delta_1(z)$.

On the other hand, we shall use the second coordinate to evade some of the values. To this end, we generalize Lemma 7.22, with a similar proof.

Lemma 7.25. *Let S be a set, and q a prime. Let $f\colon S \to \mathbb{Z}_q$ be any map, and let $c_1, c_2, \lambda_1, \lambda_2, \mu_1, \mu_2 \in \mathbb{Z}$ be any coefficients. Then, provided $|S|q^2 \cdot q! < (q-1)^q$ we may pick $\alpha, \beta_s\colon \mathbb{Z}_q \to \mathbb{Z}_q$ for all $s \in S$, such that*

$$\alpha(x)\beta_s(y) + (\alpha(x) + c_1 x)(\beta_s(y) + c_2 y) + \lambda_1\alpha(x) + \mu_1 x + \lambda_2\beta_s(y) + \mu_2 y + f(s) \quad (7.10)$$

never takes value zero.

Proof of Lemma 7.25. We proceed similarly as in the proof of Lemma 7.22, starting by defining each $\alpha(x)$ independently, uniformly at random in $\mathbb{Z}_q \setminus \{-2^{-1}(c_1 x + \lambda_2)\}$, with this single value omitted for technical reasons.

For each y and $s \in S$, we want to pick $\beta_s(y)$, so that (7.10) does not vanish for any x. Let $E_{y,s}$ be the event that we cannot do this, i.e. that, having fixed y, s for every value β, we can find x such that

$$\alpha(x)\beta + (\alpha(x) + c_1 x)(\beta + c_2 y) + \lambda_1\alpha(x) + \mu_1 x + \lambda_2\beta + \mu_2 y + f(s). \quad (7.11)$$

If $E_{y,s}$ occurs, observe that (7.11) cannot hold for distinct β_1, β_2 with the same choice of x, since this equation can be rewritten as

$$\beta(2\alpha(x) + c_1 x + \lambda_2) + y(c_2\alpha(x) + c_1 c_2 x + \mu_2) + \lambda_1\alpha(x) + \mu_1 x + f(s)$$

and by the choice of α, the coefficient of β is never zero. Hence, if $\pi\colon \mathbb{Z}_q \to \mathbb{Z}_q$ is the map that sends each β to the corresponding value of x for which the (7.11) vanishes, we must have π injective, which is thus a bijection.

Suppose furthermore that we know π as well. Note that in this case we can almost determine α. Indeed, for all β we have

$$\begin{aligned}
0 =& \beta(2\alpha(\pi(\beta)) + c_1\pi(\beta) + \lambda_2) + y(c_2\alpha(\pi(\beta)) + c_1 c_2\pi(\beta) + \mu_2) \\
&+ \lambda_1\alpha(\pi(\beta)) + \mu_1\pi(\beta) + f(s) \\
=& \alpha(\pi(\beta))(2\beta + yc_2 + \lambda_1) + \beta(c_1\pi(\beta) + \lambda_2) + y(c_1 c_2\pi(\beta) + \mu_2) + \mu_1\pi(\beta) + f(s)
\end{aligned}$$

Substituting $\beta = \pi^{-1}(\beta')$, we obtain

$$\alpha(\beta')(2\pi^{-1}(\beta')+yc_2+\lambda_1)+\pi^{-1}(\beta')(c_1\beta'+\lambda_2)+y(c_1c_2\beta'+\mu_2)+\mu_1\beta'+f(s)=0$$

for all $\beta' \in \mathbb{Z}_q$, so $\alpha(\beta')$ is uniquely determined for all β' such that $2\pi^{-1}(\beta') + yc_2 + \lambda_1 \neq 0$, i.e. for $q-1$ values. So there are at most q ways to pick α, and in conclusion, the probability of $E_{y,s}$ is $\mathbb{P}(E_{y,s}) \leq q \cdot q!\,/(q-1)^q$. Finally, we have

$$\mathbb{P}(\cup_{y,s}E_{y,s}) \leq \sum_{y,s} \mathbb{P}(E_{y,s}) \leq |S|q^2 \frac{q!}{(q-1)^q} < 1,$$

so it is possible to choose α for which all other maps can be defined so that (7.10) never vanishes. $\square$

Set $\gamma_2 = 0$. Let $\overline{y_1} = \iota_p(y_1), t = \iota_q(\mu_3 z_2) \in \mathbb{Z}$. We define $\delta_1(z) = \pi_p(t)$, so the first coordinate becomes $\pi_p(\overline{y_1} - t)$. We set $f\colon \mathbb{Z}_p \to \mathbb{Z}_q$, by $f(y_1) = \pi_q(\overline{y_1})$. Apply Lemma 7.25 to $\mathbb{Z}_q$, $S = \mathbb{Z}_p$, and the expression

$$\begin{gathered}\alpha_2(x_2)\beta_{2,y_1}(y_2) + (\alpha_2(x_2) + c_1x_2)(\beta_{2,y_1}(y_2) + c_2y_2)\\ +\lambda_1\alpha_2(x_2) + \mu_1x_2 + \lambda_2\beta_{2,y_1}(y_2) + \mu_2y_2 + f(y_1)\end{gathered}$$

to define $\alpha_2, \beta_{2,y_1}\colon \mathbb{Z}_q \to \mathbb{Z}_q$ to make it non-zero always. Note that we may apply the lemma since $pq^2q! < (q-1)^q$, whenever $q < p < 2q$, for sufficiently large q. We define $\beta_2(y)$ as $\beta_{2,y_1}(y_2)$. Finally, we show that values $(\pi_p(r), -\pi_q(r)) \in \mathbb{Z}_p \oplus \mathbb{Z}_q$ are not attained for $r \in \{0, 1, \ldots, p-q-1\}$.

Suppose that $r \in \{0, 1, \ldots, p-q-1\}$ and suppose that the expression takes value $(\pi_p(r), -\pi_q(r))$. Thus, the first coordinate gives $\pi_p(\overline{y_1} - t) = \pi_p(r)$, so p divides $\overline{y_1} - t - r$, so either $\overline{y_1} \leq t + r - p$, $\overline{y_1} = t + r$, or $\overline{y_1} \geq t + r + p$. But, $\overline{y_1} \in \{0, 1, \ldots, p-1\}, t \in \{0, 1, \ldots, q-1\}$ and $r \in \{0, 1, \ldots, p-q-1\}$, so we must have $\overline{y_1} = t + r$.

Next, let v stand for the value of

$$\begin{aligned}\alpha_2(x_2)\beta_{2,y_1}(y_2)+&(\alpha_2(x_2) + c_1x_2)(\beta_{2,y_1}(y_2) + c_2y_2)\\ &+\lambda_1\alpha_2(x_2) + \mu_1x_2 + \lambda_2\beta_{2,y_1}(y_2) + \mu_2y_2.\end{aligned}$$

By the definition of α_2, β_{2,y_1}, we always have $v + f(y_1) \neq 0$. If the second coordinate equals $-\pi_q(r)$, then we have $0 = v + \mu_3z_2 + \pi_q(r) = v + \pi_q(t) + \pi_q(r) = v + \pi_q(t + r) = v + \pi_q(\overline{y_1}) = v + f(y_1)$, which is impossible. $\square$

Corollary 7.26. *Let $c_1, c_2, \lambda_1, \lambda_2, \lambda_3, \mu_1, \mu_2, \mu_3 \in \mathbb{Z}$ be some fixed coefficients, such that $c_1, c_2 \in \{-1, 1\}$ and $c_2\mu_2 - \lambda_2 + \lambda_3 - c_2 \neq 0$. Let $\epsilon > 0$ be any small real. Then, we can find q, a product of arbitrarily large distinct primes and maps $\alpha, \beta, \gamma \colon \mathbb{Z}_q \to \mathbb{Z}_q$ such that the expression (7.9) takes at most ϵq values in $\mathbb{Z}_q$.*

Proof. We proceed as follows. Look at all the primes $2^k < q_1 < q_2 < \cdots < q_m < (1 + \frac{1}{3})2^k$ and $(1 + \frac{2}{3})2^k < p_1 < p_2 < \cdots < p_n < 2^{k+1}$. For k sufficiently large, by the prime number theorem, $n, m \geq \Omega(2^k/k)$. For k sufficiently large, pairs of primes p_i, q_i satisfy the conditions of Proposition 7.24, which we apply to obtain $\alpha_i, \beta_i, \gamma_i \colon \mathbb{Z}_{p_iq_i} \to \mathbb{Z}_{p_iq_i}$ so that the expression (7.9) misses at least $p_i - q_i$ values in $\mathbb{Z}_{p_iq_i}$. In other words, the expression (7.9) takes at most $(1 - \frac{1}{10p_i})p_iq_i$ values in $\mathbb{Z}_{p_iq_i}$. Let $P_k = \{p_1, p_2, \ldots, p_{\min\{m,n\}}\}$, and let Q_k be the product of all p_iq_i. Viewing $\mathbb{Z}_{Q_k}$ as a direct sum of $\mathbb{Z}_{p_iq_i}$, we can therefore define $\alpha, \beta, \gamma \colon \mathbb{Z}_{Q_k} \to \mathbb{Z}_{Q_k}$ coordinatewise using $\alpha_i, \beta_i, \gamma_i$, so that the expression (7.9) attains at most $\prod_{p \in P_k}(1 - \frac{1}{10p})Q_k \leq \exp(-\frac{c}{k})Q_k$ values in $\mathbb{Z}_{Q_k}$, for some positive constant c.

Finally, taking $\mathbb{Z}_{Q_k} \oplus \mathbb{Z}_{Q_{k+1}} \oplus \ldots \oplus \mathbb{Z}_{Q_N}$, and using the maps α, β, γ on each $\mathbb{Z}_{Q_i}$ separately, makes the expression (7.9) take at most $\prod_{i=k}^{N} \exp(-\frac{c}{i}) = \exp(-c\sum_{i=k}^{N} \frac{1}{i})$ proportion of values in $\mathbb{Z}_{Q_k} \oplus \mathbb{Z}_{Q_{k+1}} \oplus \ldots \oplus \mathbb{Z}_{Q_N}$, which goes to zero as N goes to infinity, as desired. □

This finishes the proof of Theorem 7.21. □

7.7 Concluding remarks

We conclude the chapter with some problems and several questions related to the ingredients used in our construction. Firstly, the main question here is still the following.

Question 7.27. *Suppose that $A \subset \mathbb{Z}_q$ has $A - A = \mathbb{Z}_q$ and let $a_k, a_{k-1}, \ldots, a_1 \in \mathbb{N}$. How small can $a_kA^k + a_{k-1}A^{k-1} + \cdots + a_1A$ be? What is the answer when q is square-free/product of $O(1)$ primes/prime? When can we get a power saving, i.e. $|a_kA^k + a_{k-1}A^{k-1} + \cdots + a_1A| \leq q^{1-\epsilon}$?*

The next natural question is about the number of values attained by expressions.

Question 7.28. *Let $k \in \mathbb{N}$ be given. We consider expressions in variables $x_1, x_2, \ldots, x_k$ and maps $\alpha_1(x_1), \alpha_2(x_2), \ldots, \alpha_k(x_k)$. Let E be any $\mathbb{N}$-linear combination of products of terms of the form $\alpha_i(x_i)$ or $\alpha_i(x_i) + x_i$. Is there a choice of a $q \in \mathbb{N}$ and maps $\alpha_i \colon \mathbb{Z}_q \to \mathbb{Z}_q$ such that E attains only $o(q)$ values in $\mathbb{Z}_q$? Is there a choice for which we have a power-saving, i.e. E attains only $O(q^{1-\epsilon})$ values? What if q is square-free/product of $O(1)$ primes/prime?*

We remark that in our construction, there was a power-saving choice for most of the expressions. In fact, the only ones for which our arguments do not lead to a power-saving are

$$\begin{aligned}\alpha(x)^2 + &\alpha(x)\beta(y) + (\alpha(x) + x)(\beta(y) + y)\\ &+\lambda_1\alpha(x) + \mu_1 x + \lambda_2\beta(y) + \mu_2 y + \lambda_3\gamma(z) + \mu_3 z\end{aligned}$$

and

$$\begin{aligned}\alpha(x)\gamma(z) + &\alpha(x)\beta(y) + (\alpha(x) + x)(\beta(y) + y)\\ &+\lambda_1\alpha(x) + \mu_1 x + \lambda_2\beta(y) + \mu_2 y + \lambda_3\gamma(z) + \mu_3 z,\end{aligned}$$

(for a specific choice of λ_i, μ_i).

Returning once again to the identification of coordinates idea, it turns out that Proposition 7.13 is nearly optimal for some expressions, provided p and q are close. Namely, consider expression $E = \alpha'(x)\beta'(y) + (\alpha'(x) + x) + (\beta'(y) + y) + 1$. Putting $\alpha(x) = \alpha'(x) + 1, \beta(y) = \beta'(y) + 1$, the expression becomes $E = \alpha(x)\beta(y) + x + y$.

Observation 7.29. *Let p and q be distinct primes. Given any maps $\alpha, \beta \colon \mathbb{Z}_{pq} \to \mathbb{Z}_{pq}$, the expression $\alpha(x)\beta(y) + x + y$ attains at least $\Omega(\min\{p, q\})$ values in $\mathbb{Z}_{pq}$.*

Proof. We begin by observing that if $\alpha(x)$ is not invertible for some choice of x, viewing $\mathbb{Z}_{pq}$ as $\mathbb{Z}_p \oplus \mathbb{Z}_q$, for some coordinate $c \in \{1, 2\}$, we have $E_c = x_c + y_c$. Letting y_c vary, we obtain at least $\min\{p, q\}$ values.

Therefore, assume that all $\alpha(x)$ are invertible in $\mathbb{Z}_{pq} \cong \mathbb{Z}_p \oplus \mathbb{Z}_q$. Fix some x. Consider all values $v_1, v_2, \ldots, v_r$ of $E(x, y)$, (where $E(x, y)$ is evaluation of the expression for the given choice of x, y), as y ranges over $\mathbb{Z}_{pq}$. We may assume $r \leq \frac{1}{10}\min\{p, q\}$, otherwise we are done. Hence, we obtain a partition $Y_1 \cup Y_2 \cup \ldots \cup Y_r = \mathbb{Z}_{pq}$, where $E(x, y) = v_i$ if $y \in Y_i$. Call a pair y_1, y_2 *invertible* if $y_1 - y_2$ is invertible in $\mathbb{Z}_{pq}$. Observe that in each set Y_i, there are at least $\max\{|Y_i|(|Y_i|-p-q+1)/2, 0\}$ invertible pairs. However, if $E(x,y_1) = E(x,y_2)$ for an invertible pair y_1, y_2, then $\alpha(x)\beta(y_1)+y_1 = \alpha(x)\beta(y_2)+y_2$, so $\beta(y_1)-\beta(y_2)$ is invertible, and $\alpha(x) = \frac{y_1-y_2}{\beta(y_2)-\beta(y_1)}$. Thus, for every invertible pair y_1, y_2 there is a value $w(y_1, y_2)$ such that $E(x,y_1) = E(x,y_2)$ implies $\alpha(x) = w(y_1,y_2)$.

For a fixed w, take x such that $\alpha(x) = w$, and consider the partition $Y_1 \cup \ldots \cup Y_r = \mathbb{Z}_{pq}$ as above. Firstly, take R to be the set of indices i such that $|Y_i| \geq 2(p+q)$. Thus, $\sum_{i\notin R}|Y_i| < r \cdot 2(p+q) \leq \frac{1}{5}\min\{p,q\}(p+q) \leq \frac{2}{5}pq$. Hence, $\sum_{i\in R}|Y_i| > \frac{3}{5}pq$. Therefore, we obtain that the number of invertible pairs $\{y_1, y_2\}$ that have value $w(y_1,y_2) = \alpha(x) = w$ is at least

$$\begin{aligned}\sum_{i=1}^{r}\max\{|Y_i|(|Y_i|-p-q+1)/2, 0\} &\geq \sum_{i\in R}|Y_i|(|Y_i|-p-q+1)/2 \\ &\geq \sum_{i\in R}|Y_i|(p+q)/2 \geq \frac{3}{10}pq(p+q).\end{aligned}$$

If α attains at most $2(p+q)$ values, we simply consider $E(x,y)$ for fixed y. The expression then attains at least $pq/2(p+q)$ values, thus the claim follows, so we may assume that α attains more than $2(p+q)$ values. But then, for every value w of α, we have at least $\frac{3}{10}pq(p+q)$ invertible pairs $\{y_1,y_2\}$ with $w(y_1,y_2) = w$, so the total number of invertible pairs is at least $\frac{3}{10}pq(p+q)\cdot 2(p+q) > p^2q^2$, which is a contradiction. $\square$

It could be interesting to better understand the minimum image size for this expression. Furthermore, recall that in the case of prime modulus, our understanding of the right size of image is much weaker. In fact, the arguments we provided can merely prove that maps α and β can be chosen so that this expression is not surjective (just apply Lemma 7.25 to the expression $\alpha(x)\beta(y) + (\alpha(x)+x) + (\beta(y)+y) + 1$ which we saw is equivalent to the expression discussed).

Let us temporarily change the variables to u and v, so we consider the expression $\alpha(u)\beta(v) + u + v$ (we keep x and y for their traditional meaning of coordinates in the plane). For the lower bounds on the image size, all we can say follows from a finite field version of Szemerédi-Trotter theorem. This was first proved by Bourgain, Katz and Tao [10]. We state the version of Stevens and de Zeeuw [50], with state-of-the-art bounds.

Theorem 7.30 (Finite fields Szemerédi-Trotter theorem [50])**.** *Let $\mathcal{L}$ be a set of p lines and let $\mathcal{P}$ be a set of p points in the plane $\mathbb{Z}_p \times \mathbb{Z}_p$. Then there are at most $O(p^{22/15})$ point-line incidences.*

Given maps α and β we may define set of lines $\mathcal{L} = \Big\{\{y = -\alpha(u)x - u\} \colon u \in \mathbb{Z}_p\Big\}$ and a set of points $\mathcal{P} = \{(\beta(v), v)\}$. Then, our expression takes value c if and only if there is an incidence between lines in $\mathcal{L}$ and points in $\mathcal{P} - (0, c)$ (the set of points gets translated by $(0, -c)$). Let $f \colon \mathbb{Z}_p \to \mathbb{N}_0$ be the number of incidences between these two sets for the given c. We then have

$$p^2 = |\mathcal{P}||\mathcal{L}| = \sum_c f(c).$$

Theorem 7.30 bounds the maximum such a function can attain from above by $O(p^{22/15})$. Thus, the support of this function must have size at least $\Omega(p^{8/15})$, which is very far from the upper bounds. Hence, we pose the following question.

Question 7.31. *Let $\alpha, \beta \colon \mathbb{Z}_p \to \mathbb{Z}_p$ be maps and p prime. What is the smallest number of values that the expression $\alpha(x)\beta(y) + x + y$ must attain?*

We expect that the answer is $p^{1-o(1)}$ and we would not be surprised even if the set of non-values had size $p^{o(1)}$.

Finally, we pose the question of improving the bounds in Lemma 7.11.

Question 7.32. *Suppose that $c_1, c_2, \ldots, c_d$ are never simultaneously zero. How large a set F in Lemma 7.11 can we take?*

Bibliography

[1] R. Aharoni, *Ryser's conjecture for tripartite 3-graphs*, Combinatorica **21** (2001), 1–4.

[2] R. Ahlswede and N. Cai, *On extremal set partitions in Cartesian product spaces*, Combin. Probab. Comput. **2** (1993), 211–220.

[3] R. Ahlswede and N. Cai, *On partitioning and packing products with rectangles*, Combin. Probab. Comput. **3** (1994), 429–434.

[4] N. Alon, *Decomposition of the complete r-graph into complete r-partite r-graphs*, Graphs Combin. **2** (1986), 95–100.

[5] N. Alon, T. Bohman, R. Holzman and D.J. Kleitman, *On partitions of discrete boxes*, Discrete Math. **257** (2002), 255–258.

[6] A. D. Arvanitakis, *A proof of the generalized Banach contraction conjecture*, Proc. Amer. Math. Soc. **131** (2003), 3647–3656.

[7] T. Austin, *On contractive families and a fixed-point question of Stein*, Mathematika **52** (2005), 115–129.

[8] S. Banach, *Sur les opérations dans les ensembles abstraits et leur application aux équations intégrales*, Fund. Math. **3** (1922), 133–181.

[9] J. Bourgain, *The sum-product theorem in $\mathbb{Z}_q$ with q arbitrary*, J. Anal. Math. **106** (2008), 1–93.

[10] J. Bourgain, N. Katz and T. Tao, *A sum-product estimate in finite fields, and applications*, Geom. Funct. Anal. **14** (2004), 27–57.

[11] J. Cardinal, C. Tóth and D.R. Wood, *General position subsets and independent hyperplanes in d-space*, J. Geom. **108** (2017), 33–43.

[12] S.M. Cioabă, A. Küngden and J. Verstraëte, *On decompositions of complete hypergraphs*, J. Combin. Theory Ser. A **116** (2009), 1232–1234.

[13] S.M. Cioabă and M. Tait, *Variations on a theme of Graham and Pollak*, Discrete Math. **313** (2013), 665–676.

[14] D.H.J. Polymath, *A new proof of the density Hales–Jewett theorem*, Annals of Math. **175** (2012), 1283–1327.

[15] P. Erdős, *On some metric and combinatorial geometric problems*, Discrete Math. **60** (1986), 147–153.

[16] G.A. Freiman and V.P. Pigaev, *The relation between the invariants R and T* (in Russian), Kalinin. Gos. Univ. Moscow (1973), 172–174.

[17] Z. Füredi, *Maximal independent subsets in Steiner systems and in planar sets*, SIAM J. Discrete Math. **4** (1991), 196–199.

[18] H. Furstenberg and Y. Katznelson, *A density version of the Hales–Jewett theorem*, J. Anal. Math. **57** (1991), 64–119.

[19] A.A. Glibichuk, *Sums of powers of subsets of an arbitrary finite field*, Izvestiya: Mathematics **75** (2011), 253–285.

[20] W.T. Gowers, *A new proof of Szemerédi's theorem*, Geom. Funct. Anal. **11** (2001), 465–588.

[21] R.L. Graham and H.O. Pollak, *On the addressing problem for loop switching*, Bell Labs Tech. J. **50** (1971), 2495–2519.

[22] R.L. Graham and H.O. Pollak, *On embedding graphs in squashed cubes*, Graph Theory and Applications, Lecture Notes in Mathematics **303**, Springer, 1972, pp. 99–110.

[23] A. Gyárfás, *Large monochromatic components in edge-colorings of graphs: a survey*, Ramsey Theory: Yesterday, Today, and Tomorrow, Progress in Mathematics **285**, Birkhäuser Boston 2010, 77–96.

[24] A. Gyárfás, *Partitions, coverings and blocking sets in hypergraphs* (in Hungarian) Commun. Comput. Autom. Inst. Hungar. Acad. Sci. **71** (1977), 62 pp.

[25] A. Gyárfás, *Vertex covers by monochromatic pieces – a survey of results and problems.* Discrete Math. **339** (2016), 1970–1977.

[26] J.A. Haight, *Difference covers which have small k-sums for any k*, Mathematika **20** (1973), 109–118.

[27] J.R. Henderson, *Permutation decomposition of* $(0-1)$ *matrices and decomposition transversals.* Ph.D. Thesis, Caltech, 1971.

[28] F. Hennecart, G. Robert and A. Yudin, *On the number of sums and differences*, Astérisque **258** (1999), 173–178.

[29] A. Ivić, *The Riemann Zeta-Function. Theory and Applications.* Dover Publications, New York, 2003, reprint of the 1985 original, pp. 304–305.

[30] J.R. Jachymski, B. Schroder and J.D.Jr. Stein, *A connection between fixed-point theorems and tiling problems*, J. Combin. Theory Ser. A **87** (1999), 273–286.

[31] I. Leader, L. Milićević, T.S. Tan, *Decomposing the complete r-graph*, J. Combin. Theory Ser. A **154** (2018) 21–31.

[32] Sh. Letzter, *Large monochromatic triple stars in edge colourings*, J. Graph Theory **80** (2015), 323–328.

[33] L. Lovász, *A kombinatorika minimax tételeiről (On minimax theorems in combinatorics)*, Mat. Lapok **26** (1975), 209–264.

[34] J. Merryfield, B. Rothschild and J.D.Jr. Stein, *An application of Ramsey's theorem to the Banach contraction mapping principle*, Proc. Amer. Math. Soc. **130** (2002), 927–933.

[35] J. Merryfield and J.D.Jr. Stein, *A generalization of the Banach Contraction Mapping Theorem*, J. Math. Anal. Appl. **273** (2002), 112–120.

[36] L. Milićević, *Contractive families on compact spaces*, Mathematatika **60** (2014), 444–462.

[37] L. Milićević, *Commuting contractive families*, Fund. Math. **231** (2015), 225–272.

[38] L. Milićević, *Covering complete graphs by monochromatically bounded sets*, submitted.

[39] L. Milićević, *Sets in almost general position*, Combin. Probab. Comput. **26** (2017), 720–745.

[40] L. Milićević, *Small sets with large difference sets*, submitted.

[41] M.B. Nathanson, *The Haight-Ruzsa method for sets with more differences than multiple sums*, preprint, https://arxiv.org/abs/1604.03015

[42] G. Peck, *A new proof of a theorem of Graham and Pollak*, Discrete Math. **49** (1984), 327–328.

[43] H. Plünnecke, *Eine zahlentheoretische anwendung der graphtheorie*, J. Reine Angew. Math. **243** (1970), 171–183.

[44] J. Radhakrishnan, P. Sen and S. Vishwanathan, *Depth-3 arithmetic circuits for $S^2_n(X)$ and extensions of the Graham-Pollak Theorem*, FST TCS 2000: Foundations of Software Technology and Theoretical Computer Science, New Delhi, Lecture Notes in Computer Science **1974**, Springer, 2000, pp. 176–187.

[45] B. Reznick, P. Tiwari and D.B. West, *Decomposition of product graphs into complete bipartite subgraphs*, Discrete Math. **57** (1985), 189–193.

[46] M. Ruszinko, *Large components in r-edge-colorings of K_n have diameter at most five*, J. Graph Theory **69** (2012), 337–340.

[47] I.Z. Ruzsa, *An application of graph theory to additive number theory*, Scientia, Ser. A **3** (1989), 97–109.

[48] I.Z. Ruzsa, *More differences than multiple sums*, preprint, https://arxiv.org/abs/1601.04146

[49] I.Z. Ruzsa, *On the cardinality of $A+A$ and $A-A$*, Coll. Math. Soc. János Bolyai, **18** Combinatorics (Keszthely, 1976), Akadémiai Kiadó (Budapest, 1979), 933–938.

[50] S. Stevens and F. de Zeeuw, *An improved point-line incidence bound over arbitrary fields*, Bull. London Math. Soc. **49** (2017), 842–858.

[51] J.D.Jr. Stein, *A systematic generalization procedure for fixed-point theorems*, Rocky Mountain J. Math. **30** (2000), 735–754.

[52] Zs. Tuza, *On special cases of Ryser's Conjecture.* Manuscript.

[53] H. Tverberg, *On the decomposition of K_n into complete bipartite graphs*, J. Graph Theory **6** (1982), 493–494.

[54] R.C. Vaughan, *The Hardy-Littlewood Method (2nd ed.)*, Cambridge Tracts in Mathematics **125**, Cambridge University Press, 1997, p. 11.

[55] S. Vishwanathan, *A polynomial space proof of the Graham-Pollak theorem*, J. Combin. Theory Ser. A **115** (2008), 674–676.

[56] S. Vishwanathan, *A counting proof of the Graham-Pollak Theorem*, Discrete Math. **313** (2013), 765–766.