FORMALISING SZEMERÉDI'S REGULARITY LEMMA AND ROTH'S THEOREM ON ARITHMETIC PROGRESSIONS IN ISABELLE/HOL

CHELSEA EDMONDS, ANGELIKI KOUTSOUKOU-ARGYRAKI, AND LAWRENCE C. PAULSON

Department of Computer Science and Technology
University of Cambridge, UK

Abstract. We have formalised Szemerédi's Regularity Lemma and Roth's Theorem on Arithmetic Progressions, two major results in extremal graph theory and additive combinatorics, using the proof assistant Isabelle/HOL. For the latter formalisation, we used the former to first show the Triangle Counting Lemma and the Triangle Removal Lemma: themselves important technical results. Here, in addition to showcasing the main formalised statements and definitions, we focus on sensitive points in the proofs, describing how we overcame the difficulties that we encountered.

1. Introduction and Background

Szemerédi's Regularity Lemma and Roth's Theorem on Arithmetic Progressions are central results within extremal graph theory, additive combinatorics and, in a broader sense, number theory. They belong to a line of mathematical research which finds its origins in Ramsey theory [21]: van der Waerden's Theorem, proved in 1927 and referring to arithmetic progressions, can be regarded as a direct precursor:

Theorem 1. *(van der Waerden) For any given $c, k \in \mathbb{N}$, there exists a number N such that if the consecutive integers 1, 2, ..., N are coloured, each with one of c different colours, then there are at least k integers in arithmetic progression whose elements are all of the same colour.*

Less than a decade later, in 1936, Erdős and Turán introduced a conjecture [11] which was eventually proved in 1975 by Endre Szemerédi [32]—Gowers [20] discusses the background to this result—and today is known as Szemerédi's Theorem:

Theorem 2. *(Szemerédi) Every set of integers A with positive upper asymptotic density contains a k-term arithmetic progression for every $k \in \mathbb{N}$.*

The upper asymptotic density is a measure of the size of a set of integers.

Definition 1. *The* upper asymptotic density *of a set $A \subseteq \mathbb{Z}$ is defined as*

$$\limsup_{N \to \infty} \frac{|A \cap [1, N]|}{N}.$$

For example, the set of even numbers has density $1/2$, while the set of primes has density zero. It can be shown that the set of square-free integers has density $6/\pi^2$, which tells us that "most" integers are square-free.

Key words and phrases. interactive theorem proving, proof assistant, formalisation of mathematics, Isabelle/HOL, additive combinatorics, extremal graph theory, arithmetic progressions, number theory.
2020 Mathematics Subject Classification: 05C35, 05A17, 11P81, 03B35, 68V15, 68V20, 68V35.

Szemerédi's original proof was combinatorial, but many further proofs were given, most notably by Furstenberg in 1977 using ergodic theory [13] and by Gowers in 2001 using both Fourier analysis and combinatorics [16]. It is worth mentioning that Szemerédi's Theorem is a fundamental ingredient in the proof of the (2004) celebrated Green–Tao Theorem [22], which attests that the primes contain arbitrarily long arithmetic progressions. Although it does not directly follow from Szemerédi's Theorem, as the primes have zero asymptotic density in the integers, a Szemerédi-type statement plays a crucial rule in the proof, as noted by Conlon et al. [3].

Already in 1953, Klaus Roth had shown a special case of Szemerédi's Theorem, proving the aforementioned 1936 conjecture by Erdős and Turán [11] for the case of arithmetic progressions of length $k = 3$ [31]. His result, which is considered a milestone in additive combinatorics, is known as Roth's Theorem on Arithmetic Progressions:

Theorem 3. *(Roth) Every subset of the integers with positive upper asymptotic density contains a 3-term arithmetic progression.*

Roth's original proof [31] made use of Fourier analysis. However, a later proof follows a combinatorial approach: it relies on Szemerédi's Regularity Lemma, which Szemerédi proved in 1975 as a step towards his aforementioned Theorem 2 [4, 32]. Szemerédi first showed [32] a weaker version of the lemma for bipartite graphs, which was already sufficient to prove Theorem 2; later on, he showed the full lemma, for general graphs [33]. Essentially, Szemerédi's Regularity Lemma attests that for any large dense graph, we can partition its vertices into a bounded number of parts, so that edges between most different parts behave in a "random" way. To give a sense of what is meant by this notion of "randomness" on a quantitative level, we introduce the following definitions.

In the following, if G is a graph, $V(G)$ and $E(G)$ will denote the sets of its vertices and edges, respectively. Sometimes the notation $G = (V, E)$ will be used.

For sets of vertices X, $Y \subseteq V(G)$, let $e(X, Y)$ be the number of edges between X and Y. That is,

$$e(X, Y) = |\{(x, y) \in X \times Y : xy \in E(G)\}|.$$

Definition 2. *(Edge density) Given a graph G, for sets of vertices $X, Y \subseteq V(G)$, we define the edge density between X and Y to be*

$$d(X, Y) = \frac{e(X, Y)}{|X||Y|}.$$

Definition 3. *(ϵ-regular pair) Given a graph G and $\epsilon > 0$, for sets of vertices X, $Y \subseteq V(G)$, we call (X, Y) an ϵ-regular pair (in G) if for all $A \subseteq X$, $B \subseteq Y$ with $|A| \geq \epsilon|X|$, $|B| \geq \epsilon|Y|$, one has*

$$|d(A, B) - d(X, Y)| \leq \epsilon.$$

Taking the contrapositive: if the pair is not ϵ-regular, then the irregularity is witnessed by some $A \subseteq X$, $B \subseteq Y$ such that $|A| \geq \epsilon|X|$, $|B| \geq \epsilon|Y|$ and $|d(A, B) - d(X, Y)| > \epsilon$. We use *not ϵ-regular* and *ϵ-irregular* interchangeably.

We are interested in partitions of a graph in which the number of irregular pairs is limited by the following formula:

Definition 4. *(ϵ-regular partition) Given a graph G and $\epsilon > 0$, a partition $P = \{V_1, \ldots, V_k\}$ of $V(G)$ is an ϵ-regular partition if*

$$\sum_{\substack{(i,j)\in[k]^2 \\ (V_i, V_j) \text{ not } \epsilon\text{-regular}}} |V_i||V_j| \leq \epsilon|V(G)|^2.$$

We can now formally state Szemerédi's Regularity Lemma:

Theorem 4. *(Szemerédi) For every $\epsilon > 0$, there exists a constant M such that every graph has an ϵ-regular partition of its vertex set into at most M parts.*

Szemerédi's Regularity Lemma has a number of significant applications that go far beyond the—already groundbreaking—proofs of Szemerédi's Theorem and Roth's Theorem: most notably, algorithmic applications within various areas of computer science. It is considered the cornerstone of extremal graph theory. Szemerédi gives an accessible overview and some interesting historical details [29]. Gowers has obtained quantitative results on the lower bound on the cardinality of the induced ϵ-regular partition [15]. Gowers [18, 19] and Rödl et al. [12, 25, 30] have proved various extensions of Szemerédi's Regularity Lemma to hypergraphs. On a different note, Terence Tao has studied Szemerédi's Regularity Lemma from a probability theory and information theory perspective [34].

This paper discusses our formalisations of Szemerédi's Regularity Lemma [8] and Roth's Theorem on Arithmetic Progressions [7] using Isabelle/HOL[1] [26]. Isabelle is a proof assistant (interactive theorem prover) supporting higher-order logic, among other formalisms. It is notable for its large library, the *Archive of Formal Proofs* (AFP), containing hundreds of entries of formalised mathematics in addition to hundreds more on theoretical computer science and formal verification. It offers powerful automation for both proving and disproving. Proofs can be written in a legible structured language called Isar. As of the writing of this article, the AFP contains 22 entries classified under graph theory and 30 under combinatorics (some of these possibly overlapping). Within combinatorics, we can mention our work formalising design theory [9, 10] and ordinal partition theory [6]. Notably, the aforementioned van der Waerden's Theorem was recently formalised in Isabelle/HOL by Kreuzer and Eberl [23].

For the formalisations described in this paper, we have built upon Noschinski's formalisation of the girth and chromatic number theorem [27], as it defines the basics of graph theory starting with elementary concepts such as `ugraphs`, `uedges`, `uverts` for undirected graphs and the sets of edges and vertices thereof respectively. Vertices are seen as natural numbers and edges as sets of natural numbers, so they are of type `nat` and `nat set` respectively. This library was initially chosen as it additionally provided foundations in probabilistic reasoning on graphs, which may have been required had we only followed Zhao's proof [35]. While this was ultimately unnecessary, this simple formalisation of undirected graphs proved easier to work with in comparison to other more extensive graph libraries in Isabelle which focus on directed graphs [28], which in turn tend to complicate formal reasoning on undirected graphs.

Our contribution begins by formalising a proof of Szemerédi's Regularity Lemma, following Yufei Zhao's online notes for a course taught recently at MIT [35]—these are now being reworked into a book [36]—as well as online notes written by Paul Russell from a combinatorics course taught at Cambridge by Timothy Gowers in 2004 [17]. This work is discussed in more detail in Section 2. Building on our formalisation of Szemerédi's Regularity Lemma [8] and following again the aforementioned set of notes supplemented by Bell et al. [1], we formalised the proofs of the Triangle Counting Lemma and the Triangle Removal Lemma (Section 3). Finally, we used these to prove Roth's Theorem on Arithmetic Progressions (Section 4). In Section 5, we include a general discussion on our comments and observations, summarising what we learned through the formalisation process and focussing on the difficulties we encountered. Independently, and around the same time with us, Yaël Dillies and

[1] `https://isabelle.in.tum.de`

Bhavik Mehta (also at Cambridge but in the Mathematics Department) formalised the aforementioned results in the Lean theorem prover [5]. Their formalisations[2] are pending full incorporation to mathlib, Lean's library of formalised mathematical proofs. We learned of their simultaneous work while we were halfway through our own formalisation. We briefly compare the two approaches in Section 6. Finally, Section 7 is a short conclusion.

We have written our proofs with care, trying to reveal the key insights, as we believe that formalised mathematics should not restrict to merely certifying claims, but should also clarify the proof ideas. In this paper we present only highlights, hoping that any missing elements are self-explanatory. Both of our formalisations can be found on the Archive of Formal Proofs (AFP) [7, 8]. The formal material presented below has been edited to improve readability.

2. Formalising Szemerédi's Regularity Lemma

2.1. **Defining the energy.** We start by presenting our Isabelle formalisations of the notions defined in Section 1. As mentioned, we build on the existing basic graph theory definitions defined by Noschinski [27].

Edge density is defined straightforwardly, following Def. 2 above.

```
definition
  "edge_density X Y G ≡ card(all_edges_between X Y G) / (card X * card Y)"
```

When speaking of ϵ-regular pairs, note that ϵ is actually a parameter and that one might refer to, say, an $\epsilon/3$-regular pair. Such a complicated syntax is achievable in Isabelle but at the cost of much syntactic hackery. The formal version therefore accepts ϵ as an ordinary argument. This is our formalised version of Def. 3:

```
definition "regular_pair X Y G ε
          ≡ ∀A B. A ⊆ X ∧ B ⊆ Y ∧
                  (card A ≥ ε * card X) ∧ (card B ≥ ε * card Y) ⟶
                   |edge_density A B G - edge_density X Y G| ≤ ε"
```

The proofs will be concerned with partitions of the vertices of the given graph, `G`. In particular, we will need to collect all ϵ-irregular pairs among the members of any given partition, `P`:

```
definition "irregular_set ε G P
          ≡ {(R,S)|R S. R∈P ∧ S∈P ∧ ¬ regular_pair R S G ε}"
```

As mentioned above (Def. 4), a *regular partition* has "relatively few" irregular pairs, parameterised by ε:

```
definition "regular_partition ε G P
          ≡ partition_on (uverts G) P ∧
            (∑(R,S) ∈ irregular_set ε G P. card R * card S)
             ≤ ε * (card (uverts G))²"
```

We now formalise the key definitions referring to the *energy* with respect to subsets and/or (a) partition(s) of a graph. The notion of energy with respect to subsets of the vertices $U, W \subseteq V(G)$ is defined as follows:

```
definition "energy_graph_subsets U W G
          ≡ card U * card W * (edge_density U W G)² / (card (uverts G))²"
```

Now, considering *partitions* `P`, `Q` (instead of sets as above) we define the following notion of energy. As we discuss at the end of Section 5, instead of representing the partitions using indices for the parts, which was our first approach, in our final version of the formalisation we preferred to simply denote a partition as a set of sets, so the energy in terms of partitions was eventually defined as follows:

[2] https://github.com/leanprover-community/mathlib/tree/szemeredi/src/combinatorics/szemeredi

definition *"energy_graph_partitions G P Q*
≡ ∑R∈P. ∑S∈Q. energy_graph_subsets R S G"

Referring to a single partition of a single vertex set (which can be the entire vertex set of a graph) the *energy of the partition* (also referred to as *mean square density* [17]) is defined as follows:

abbreviation
"mean_square_density G P ≡ energy_graph_partitions G P P"

2.2. **Some elementary lemmas.** Let us look at some of the consequences of the definitions introduced. As usual with interactive theorem proving, it is helpful to prove a few trivial facts for every definition. Here are some of the more interesting results.

The following inequality concerns a partition *P* with *k* many parts of a vertex set *V* of a finite graph and is proved by induction on *k*. Although straightforward, the formal proof is over 30 lines long.

lemma *sum_partition_le:*
assumes *"finite_graph_partition V P k" "finite V"*
shows *"(∑R∈P. ∑S∈P. real (card R * card S)) ≤ (real(card V))²"*

This immediately yields the basic result that the mean square density is bounded by 1:

lemma *mean_square_density_bounded:*
assumes *"finite_graph_partition (uverts G) P k" "finite (uverts G)"*
shows *"mean_square_density G P ≤ 1"*

The following identity—relating the edge density of a graph *G* with respect to its vertex sets *U*, *W* to the edge densities with respect to a partition *P* of the vertex set *U* into *n* parts—ought to be straightforward, but the formal proof is nearly 50 lines, by induction on *n*.

lemma *edge_density_partition:*
assumes *"finite_graph_partition U P n"*
shows *"edge_density U W G = (∑X∈P. edge_density X W G * card X)/card U"*

This identity is used to prove a key lemma: that refining a partition of a vertex set cannot make the energy decrease. We follow Gowers's combinatorial proof, which is based on a direct calculation [17] and eschews probabilistic reasoning. (In contrast, Zhao's approach [35, 36] reasons about expected value.) The full version of the lemma considers partitions of two sets, but we save work by considering a partition of only one of the sets, then using symmetry to obtain the full result.

lemma *energy_graph_partition_half:*
assumes *"finite_graph_partition U P n"*
shows *"card U * (edge_density U W G)²*
*≤ (∑R∈P. card R * (edge_density R W G)²)"*

Here, we combine the two halves allowing both sides to be partitioned. The proof is straightforward (20 lines), using the previous result twice along with the commutativity of edge density. The following lemma states that partitioning subsets of the vertex set cannot make the energy decrease.

proposition *energy_graph_partition_increase:*
assumes *"finite_graph_partition U P k"*
and *"finite_graph_partition W Q l"*
shows *"energy_graph_partitions G P Q ≥ energy_graph_subsets U W G"*

In a similar spirit, the following result attests that refining partitions further cannot make the energy decrease (here partition *Q* refines partition *P* of the vertex set *V* while partition *Q'* refines partition *P'* of the vertex set *V'*) :

proposition *energy_graph_partitions_increase:*
assumes *"refines V Q P" "refines V' Q' P'"*
and *"finite V" "finite V'"*
shows *"energy_graph_partitions G Q Q' ≥ energy_graph_partitions G P P'"*

The following result is a special case of the above for a single partition:

corollary *mean_square_density_increase:*
assumes *"refines V Q P" "finite V"*
shows *"mean_square_density G Q ≥ mean_square_density G P"*

2.3. **The Energy Boost Lemma.** Having explored how the energy behaves with respect to partitioning subsets and to the further refining of partitions, we are ready to state the key Energy Boost Lemma [35, 36]: for a graph G, given a pair of vertex sets (U, W) that is *not* ϵ-regular and where the irregularity is witnessed by the pair (U', W') where $U' \subseteq U$ and $W' \subseteq W$, we partition U as $\{U', U \setminus U'\}$ and W as $\{W', W \setminus W'\}$ and the energy increases by at least

$$\frac{\epsilon^4 \, |U| \, |W|}{|V(G)|^2.}$$

The possibility that $U' = U$ or $W' = W$—not treated in any of our sources, as they all assumed the strict subset relation—slightly complicates the statement of the lemma. We must introduce the function *P2* to deal with degenerate partitions, ensuring that the empty set is never a member of a partition.

definition *"P2 X Y ≡ if X ⊂ Y then {X,Y-X} else {Y}"*

The proof is a messy 80 lines. Most of the effort goes into manipulating complicated summations, which can be tricky to do formally. Once again, Zhao [35, 36] employs probabilistic arguments in order to compare energies. We did not attempt that, preferring the simple calculation given by Gowers [17].

Note that the offending ϵ-irregular pair (U', W') is mentioned explicitly in the assumptions and conclusion.

proposition *energy_boost:*
fixes *ε::real* **and** *U W G*
defines *"alpha ≡ edge_density U W G"*
defines *"u ≡ λX Y. edge_density X Y G - alpha"*
assumes *"finite U" "finite W"*
and *"U' ⊆ U" "W' ⊆ W" "ε > 0"*
and *U': "card U' ≥ ε * card U"* **and** *W': "card W' ≥ ε * card W"*
and *gt: "|u U' W'| > ε"*
shows *"(∑A ∈ P2 U' U. ∑B ∈ P2 W' W. energy_graph_subsets A B G)*
≥ energy_graph_subsets U W G
*+ ε^4 * (card U * card W) / (card (uverts G))²"*

2.4. **Energy Boost Lemma for an irregular partition.** Having established the above result which refers to pairs that are not ϵ-regular, we build on it to prove a statement referring to a *partition* that is not ϵ-regular, that is, a partition that has ϵ-irregular pairs whose total size is too big (Def. 4). This crucial statement attests that for any ϵ-irregular partition *P* of the vertices of *G*, we can always find a refinement *Q* of *P* that increases the energy by at least ϵ^5, a small but positive quantity.

proposition *exists_refinement:*
assumes *"finite_graph_partition (uverts G) P k"* **and** *"finite (uverts G)"*
and *"¬ regular_partition ε G P"* **and** *"ε > 0"*
obtains *Q* **where** *"refines (uverts G) Q P"*
"mean_square_density G Q ≥ mean_square_density G P + ε^5"
"⋀R. R∈P ⟹ card {S∈Q. S ⊆ R} ≤ 2 ^ Suc k"
*"card Q ≤ k * 2 ^ Suc k"*

The formal proof is based on the Energy Boost Lemma and on lemmas on the energy behaviour with respect to subsets, partitions and refinements thereof that were presented in Section 2.2. It spans about 300 lines:

- About 50 lines for constructing the common refinement `Q` of `P`, using the previous Energy Boost Lemma and taking care to exploit symmetries.
- A further 30 lines for deriving some of its properties prior to proving the four claims in the theorem statement.
- Then 40 lines to show the first claim (that `Q` refines partition `P`).
- The second claim, about mean square density, requires more calculations involving summations and totals 90 lines.
- The third claim, a cap on the cardinality of the refinement of each member `R` of partition `P`, requires nearly 70 lines.
- The final claim, about the cardinality of `Q`, is easy: under 15 lines.

2.5. **Proving Szemerédi's Regularity Lemma itself.** The task is now straightforward. Whenever we have a partition that is *not* ϵ-regular, we repeatedly apply the lemma above, each time obtaining a refinement of the previous partition and increasing the energy by at least ϵ^5. The energy of any partition cannot exceed 1 (recall the lemma *mean_square_density_bounded* of Section 2.2), forcing termination after at most $\lceil \epsilon^{-5} \rceil$ iterations.

The formalisation of this argument is 75 lines long. Specifying the iterative construction—that at each step a new partition refines a previous one, that the energy increases and that the cardinality is bounded—seems to be unreasonably difficult. The iteration is formalised as a function on natural numbers and the properties above are proved by induction. It is tedious to reason about the existential claims made by the main lemma and that they continue to hold at the end. There should be a more concise and elegant formal proof.

Crucially, the upper bound on the number of iterations is independent of the graph G. It is given by a tower of exponentials, as is shown by iterating the previous lemma's bound on the size of the refined partition. We need the lemma $k\,2^{k+1} \leq 2^{2^k}$, and as its proof is a concise induction, we present it in full (Fig. 1).

The main statement (Theorem 4) is formalised in Isabelle as follows:

```
theorem Szemeredi_Regularity_Lemma:
  assumes "ε > 0"
  obtains M where
   "⋀G. card (uverts G) > 0 ⟹ ∃P. regular_partition ε G P ∧ card P ≤ M"
```

3. The Triangle Counting Lemma and the Triangle Removal Lemma

Triangles have long been valuable tools in graph theory, particularly in the context of extremal and probabilistic combinatorics. While for our purposes, the Triangle Counting Lemma and the Triangle Removal Lemma were required for the proof of Roth's Theorem, they also have numerous other applications. Hence, the formalisation of these lemmas is a valuable contribution in their own right. For both the Triangle Counting Lemma and Triangle Removal Lemma we use a mix of Zhao's notes [35] which clearly outlines the main intuition behind the proof, complemented by Bell and Grodzicki's notes [1] which provide additional detail on the exact calculations which take place.

3.1. **Triangle definitions.** We begin with some definitions. Firstly, we formalise the idea of a triangle in a graph:

```
definition "triangle_in_graph x y z G
          ≡ ({x,y} ∈ uedges G) ∧ ({y,z} ∈ uedges G) ∧ ({x,z} ∈ uedges G)"
```

```
lemma le_tower_2: "k * (2 ^ Suc k) ≤ 2^(2^k)"
proof (induction k rule: less_induct)
  case (less k)
  show ?case
  proof (cases "k ≤ Suc (Suc 0)")
    case False
    define j where "j = k - Suc 0"
    have kj: "k = Suc j"
      using False j_def by force
    then have §: "(2^j + 3) ≤ (2::nat) ^ k"
      by (simp add: Suc_leI le_less_trans not_less_eq_eq numeral_3_eq_3)
    have "k * (2 ^ Suc k) ≤ 6 * j * 2^j"
      using False by (simp add: kj)
    also have "... ≤ 6 * 2^(2^j)"
      using kj less.IH by force
    also have "... < 2^(2^j + 3)"
      by (simp add: power_add)
    also have "... ≤ 2^2^k"
      by (simp add: §)
    finally show ?thesis
      by simp
  qed (auto simp: le_Suc_eq)
qed
```

FIGURE 1. Statement and proof that $k\,2^{k+1} \leq 2^{2^k}$

A triangle-free graph is simply defined as one where there exist no such `x`, `y`, and `z` satisfying the above definition. We also define the set of all triangles formed by taking vertices from three (not necessarily distinct) sets:

```
definition "triangle_triples X Y Z G
          ≡ {(x,y,z) ∈ X × Y × Z. triangle_in_graph x y z G}"
```

Note that the triangle definition assumes that the *well-formed* assumption holds between `uedges` and `uverts`: that every edge of `G` joins two vertices of `G`. The `triangle_in_graph` definition can also be formally reasoned on using the alternative `neighbor_in_graph` definition to capture that assumption.

```
definition "neighbor_in_graph x y G
          ≡ (x ∈ uverts G ∧ y ∈ uverts G ∧ {x,y} ∈ uedges G)"
```

It can clearly be seen that for the definitions above, the ordering of the vertices of the vertex set will not affect the result of either definition. However, we do note that based on the `triangle_triples` definition, if the sets `X`, `Y` and `Z` are not disjoint, a triangle may appear more than once (using a different ordering). This is in line with the proof of the Triangle Counting Lemma in Zhao's notes [35], which requires ordered triples.

However, this causes issues in later proofs where we are interested in counting the purely distinct triangles. In this case we define a function `mk_triangle_set` to convert a triple to a set of size 3, and further define the `triangle_set`, which mirrors the `triangle_triples` definition but for unordered triples.

3.2. **Triangle Counting Lemma.** Using these definitions, we are now ready to formalise the Triangle Counting Lemma, which provides a minimum bound on the number of triangles in a graph.

Lemma 1. *(Triangle Counting Lemma) Given a graph G, let $X, Y, Z \subseteq V(G)$ so that $(X, Y), (Y, Z), (Z, X)$ are all ϵ-regular pairs for some $\epsilon > 0$. Assuming that*

$d(X,Y), d(X,Z), d(Z,Y) \geq 2\epsilon$, the number of triples $(x,y,z) \in X \times Y \times Z$ such that x, y, z form a triangle in G is at least

$$(1-2\epsilon)(d(X,Y)-\epsilon)(d(X,Z)-\epsilon)(d(Y,Z)-\epsilon)|X||Y||Z|.$$

The proof, as presented by Zhao [35], has four main components.

(1) Given a regular pair (X,Y), we have an upper bound of $\epsilon|X|$ on the number of vertices in X which have fewer than $(d(X,Y)-\epsilon)|Y|$ neighbours, i.e. which have a negligible neighbourhood size in Y.
(2) Using (1) on the regular pairs (X,Y) and (X,Z) from the lemma assumptions, we establish a lower bound on a subset of X where all elements which meet the minimum bound on neighbourhood size in Y and Z.
(3) We establish a lower bound for the number of edges between the neighbourhoods of X in Y and Z.
(4) We combine (2) and (3) to establish a lower bound on the total number of triangles in the graph.

We first show (1) in the lemma *regular_pair_neighbor_bound*.

```
lemma regular_pair_neighbor_bound:
  fixes ε::real
  assumes "finite (uverts G)"
  assumes "X ⊆ uverts G" and "Y ⊆ uverts G" and "card X > 0"
    and "uwellformed G" and "ε>0"
    and "regular_pair X Y G ε" and "edge_density X Y G ≥ 2*ε"
  shows "card{x ∈ X. card (neighbors_ss x Y G)
                   < (edge_density X Y G - ε) * card Y}  <  ε * card X"
```

The proof required a case split to first reason on the trivial case (not considered by any of our sources) where there are no vertices in *X* meeting the negligible neighbourhood size condition. The main case proceeded by contradiction as described in our sources. Bell and Grodzicki's notes [1] proved valuable in this case, providing much more detail on the calculations taking place, which formed the basis of the proof. It should be noted that it was this proof which first raised the issue of the strict versus non-strict subset use in the regular pair definition, which we discuss further in Section 5.

This lemma could now be used to perform (2) within the formal proof of the Triangle Counting Lemma. For (3), we establish a technical auxiliary lemma:

```
lemma all_edges_btwn_neighbor_sets_lower_bound:
  fixes ε::real
  assumes "X ⊆ uverts G" "Y ⊆ uverts G" "Z ⊆ uverts G"
    and "ε>0"  "finite (uverts G)" "uwellformed G"
    and "finite X" "finite Y" "finite Z"
    and "regular_pair X Y G ε" "regular_pair Y Z G ε" "regular_pair X Z G ε"
    and "edge_density X Y G ≥ 2*ε" "edge_density X Z G ≥ 2*ε"
        "edge_density Y Z G ≥ 2*ε"
    and "card (neighbors_ss x Y G) ≥ (edge_density X Y G - ε) * card Y"
    and "card (neighbors_ss x Z G) ≥ (edge_density X Z G - ε) * card Z"
    and "x ∈ X"
 shows "card(all_edges_between (neighbors_ss x Y G) (neighbors_ss x Z G) G)
      ≥ (edge_density Y Z G - ε)
        * card (neighbors_ss x Y G) * card (neighbors_ss x Z G)"
```

This requires some set-up in the proof, but is relatively straightforward.

Finally, (4) is completed within the proof of the *triangle_counting_lemma*, for which we give the Isabelle lemma statement below.

```
theorem triangle_counting_lemma:
  fixes ε::real
```

```
assumes "X ⊆ uverts G" "Y ⊆ uverts G" "Z ⊆ uverts G"
  and "ε>0"  "finite (uverts G)" "uwellformed G"
  and "regular_pair X Y G ε" "regular_pair Y Z G ε" "regular_pair X Z G ε"
  and "edge_density X Y G ≥ 2*ε" "edge_density X Z G ≥ 2*ε"
      "edge_density Y Z G ≥ 2*ε"
shows "card (triangle_triples X Y Z G)
    ≥ (1 - 2*ε) * ((edge_density X Y G) - ε) * ((edge_density X Z G) - ε)
                * ((edge_density Y Z G) - ε) * card X * card Y * card Z"
```

While the proof required a number of additional steps to manage sum and inequality manipulations, it was relatively straightforward to complete. Once again, these manipulations closely followed Bell and Grodzicki [1]. While the level of detail in these notes was helpful, the formalisation picked up on a number of minor errors in stages (3) and (4) in particular. For example, there was an *and* instead of *or* in one of the set definitions, a *plus* instead of a *minus* in one of the lower bound results, and in one summation the summation was presented to be over pairs of sets, rather than the cardinality of the edges between these sets.

3.3. **Triangle Removal Lemma.** The Triangle Removal Lemma is the first direct application of our formalisation of Szemerédi's Regularity Lemma, which was presented in Section 2. It gives a maximum bound on the number of triangles which must be removed such that a graph can be considered *triangle-free*:

Lemma 2. *(Triangle Removal Lemma) For all $\epsilon > 0$, there exists $\delta > 0$ such that any graph on N vertices with less than or equal to δN^3 triangles can be made triangle-free by removing at most ϵN^2 edges.*

This lemma is frequently expressed in the language of Landau symbols as follows: any graph G on N vertices with $o(N^3)$ triangles can be made triangle-free by removing $o(N^2)$ edges. We chose to prove it in the concrete form above, since it was not clear how to formalise a proof of the Landau version.

Zhao [35] presents an intuitive recipe for applying Szemerédi's Regularity Lemma to prove the Triangle Removal Lemma, which we mirror in our formalisation:

(1) *Partition:* We use Szemerédi's Regularity Lemma to obtain an ϵ-regular partition of the vertices.
(2) *Clean:* We remove edges that "behave poorly" within the ϵ-regular structure imposed. Specifically, this includes edges between irregular pairs, pairs with low edge density, and pairs where one part is small.
(3) *Count:* We use the Triangle Counting Lemma to establish a contradiction and show that the "cleaned" graph is triangle-free.

We first define the concepts of a regular graph, a dense graph, and a decent graph. These three collectively express that a given graph (with a partition of its vertex set) has been cleaned as described in Step (2). These definitions are used within the proof to improve readability and simplify reasoning.

A *regular graph* has been partitioned such that all pairs are regular.

```
definition "regular_graph P G ε
        ≡ ∀R S. R∈P ⟶ S∈P ⟶ regular_pair R S G ε"
```

A *dense graph* satisfies a minimum density for its non-empty edge sets.

```
definition "edge_dense X Y G ε
          ≡ all_edges_between X Y G = {} ∨ edge_density X Y G ≥ ε"
definition "dense_graph P G ε ≡ ∀R S. R∈P ⟶ S∈P ⟶ edge_dense R S G ε"
```

A *decent graph* satisfies a minimum size for partition members that are connected by at least one edge.

```
definition "decent X Y G η
          ≡ all_edges_between X Y G = {} ∨ (card X ≥ η ∧ card Y ≥ η)"
```

```
definition "decent_graph P G η ≡ ∀R S. R∈P ⟶ S∈P ⟶ decent R S G η"
```

Additionally, we introduce a lemma to convert between a cardinality bound on our two triangle representations (ordered and unordered). This is essential after applying the Triangle Counting Lemma in the proof of the Triangle Removal Lemma, mentioned in Zhao's proof as the way of managing any "overcounting" which may occur.

```
lemma card_convert_triangle_rep:
  assumes "X ⊆ uverts G" and "Y ⊆ uverts G" and "Z ⊆ uverts G"
  and     "finite (uverts G)" "uwellformed G"
  shows "card (triangle_set G) ≥
         1/6 * card {(x,y,z) ∈ X×Y×Z. triangle_in_graph x y z G}"
```

We now present the Isabelle version of the Triangle Removal Lemma:

```
theorem triangle_removal_lemma:
  fixes ε :: real
  assumes "ε > 0"
  shows "∃δ::real > 0. ∀G. card(uverts G) > 0 ⟶ uwellformed G ⟶
         card (triangle_set G) ≤ δ * card(uverts G) ^ 3 ⟶
         (∃G'. triangle_free_graph G' ∧ uverts G' = uverts G ∧
                uedges G' ⊆ uedges G ∧
                card (uedges G - uedges G') ≤ ε * (card (uverts G))²)"
```

The formal proof first discharges the trivial case where $\varepsilon \geq 1$, when all edges can be deleted. This case is not considered explicitly in any of our sources, although the main proof requires $\varepsilon < 1$.

For the main case, we follow Zhao's recipe. The application of Szemerédi's Regularity Lemma is straightforward, enabling us to obtain an upper bound `M0` on a regular partition for any arbitrary graphs `G`. We further define `D0`, as a strict upper bound on δ, which is important in deriving a contradiction at the end of the proof. Following this application, we derive a number of useful facts on the partition which are used later in the proof.

Step (2) is where the formal proof begins to get complicated. For each of the classes of edges that "behave poorly", we define a variable representing the set of those edges, and establish an upper bound on the cardinality of each of these sets. This counting proved quite fiddly in a formal environment, reinforcing observations made during our previous work formalising counting proofs on combinatorial structures [9]. As such, the *clean* stage of our formal proof was significantly longer than the more intuitive reasoning used by both Zhao [35] and Bell–Grodzicki [1].

The formal proof can now obtain a new graph excluding these edges. The final stage of our proof matches Step (3), showing that this cleaned graph must be triangle-free. Again, this required some fiddly counting reasoning using the bounds established in Step (2). To help structure this reasoning, we show that the new graph obtained is regular, dense, and decent (as per our earlier Isabelle definitions), with Bell and Grodzicki's notes proving particularly useful here. Having met these conditions, the Triangle Counting Lemma can now be applied and through the use of the `card_convert_triangle_rep` lemma we come to a contradiction and finish the proof as required.

4. Formalising Roth's Theorem on Arithmetic Progressions

We tackled this development in three stages: the Diamond-Free Lemma, then a technical lemma containing the main construction, and finally the result itself (Theorem 3). In this section, we show a few highlights of the formal proof.

4.1. **The Diamond-Free Lemma.**

The Triangle Removal Lemma implies a key corollary, which in the literature is often referred to as a Ruzsa-Szemerédi bound or

the *Diamond-Free Lemma*. First we formalise the property of being a graph every edge of which belongs to precisely one triangle:

```
"unique_triangles G
  ≡ ∀e ∈ uedges G. ∃!T. ∃x y z.
                  T = {x,y,z} ∧ triangle_in_graph x y z G ∧ e ⊆ T"
```

Now we can state the corollary.

Corollary 1. *For all $\epsilon > 0$, there exists a $N > 0$, so that any graph G with more than N vertices and such that every edge of G lies in a unique triangle, we have that $|E(G)| \leq \epsilon |V(G)|^2$.*

```
corollary Diamond_free:
  fixes ε :: real
  assumes "0 < ε"
  shows "∃N>0. ∀G. card(uverts G) > N ⟶ uwellformed G ⟶
          unique_triangles G ⟶ card (uedges G) ≤ ε * (card (uverts G))²"
```

The above claim can be rephrased in the language of Landau symbols as follows: given a graph G on N vertices so that every edge of G lies in a unique triangle, G has $o(N^2)$ edges.

Zhao offers a six-line proof of Corollary 1, but the formal version, which does not follow Zhao's notation with Landau symbols, is well over a hundred lines. It proceeds as follows. Let $\epsilon > 0$ be given. Use the Triangle Removal Lemma with $\epsilon/3$ to obtain some suitable $\delta > 0$ and then pick some integer $N \geq \frac{1}{3\delta}$. Let $G = (V, E)$ be given such that $|V| > N$. Half of the formal development goes to showing that (by the assumption of unique triangles) G has exactly three times as many edges as it has triangles. Thus, the number of triangles is bounded above by $|V|^2/3$ and therefore by $\delta |V|^3$. Removing at most $(\epsilon/3)\,|V|^2$ edges from G yields a triangle-free version G'. A triangle of G clearly cannot involve any edges of G', so the number of triangles in G is bounded by the number of edges that were removed from G, from which $|E| \leq \epsilon |V|^2$ follows.

The Isabelle proof is largely straightforward except regarding the unique triangles property and converting between the triangle $\{x, y, z\}$ and the corresponding triplet of edges for the counting argument. This is a typical example of a trivial fact ("three times as many edges as triangles") that is cumbersome to formalise.

Corollary 1 will be employed in the proof of Theorem 3. Its statement and Isabelle formalisation are presented below.

4.2. **Roth's Theorem: the main argument.** We begin by defining 3-term arithmetic progressions. The definition is polymorphic, and the formal development uses both natural number and integer versions.

```
definition progression3 :: "'a::comm_monoid_add ⇒ 'a ⇒ 'a set"
  where "progression3 k d ≡ {k, k+d, k+d+d}"
```

Roth's theorem is equivalent to the statement that any set free of 3-term arithmetic progressions must be "small" in a certain sense:

Theorem 5. *(Roth) For every $\epsilon > 0$, there exists a $M \in \mathbb{N}$ so that for all $N \geq M$, for any subset of the naturals A with $A \subseteq \{0, \ldots, N-1\}$, if A does not contain a 3-term arithmetic progression, then $|A| < \epsilon N$.*

Thus for any set A as above, the cardinality of A is $o(N)$, that is, A is "small". However, as before, we work in terms of a given $\epsilon > 0$ rather than using Landau notation.

The Isabelle/HOL formalisation comprises nearly 500 lines. The formalised statement follows.

```
lemma RothArithmeticProgressions_aux:
  fixes ε::real
  assumes "ε > 0"
  obtains M where "∀N ≥ M. ∀A ⊆ {..<N}.
            (∄k d. d>0 ∧ progression3 k d ⊆ A) ⟶ card A < ε * real N"
```

As mentioned earlier, Corollary 1 (the Diamond-Free Lemma) will be employed in the proof. We start by taking $A \subseteq \{0, \ldots, N-1\}$ assuming that A contains no 3-term arithmetic progression. We embed A into a cyclic group: $A \subseteq \mathbb{Z}/M\mathbb{Z}$, where $M = 2N + 1$. We then construct a tripartite graph G so that each of its three parts is a copy of $\mathbb{Z}/M\mathbb{Z}$. We then show that each edge of G lies in exactly one triangle, and therefore by Corollary 1 we get a bound on the number of edges of G, and thus, by construction, on the cardinality of A too.

The formalisation of the tripartite graph G is interesting. We need to make three disjoint copies of the natural numbers below M. Since the vertices of a graph are already natural numbers, we use a bijection between $\mathbb{N} \times \mathbb{N}$ and $\mathbb{N}$. The library function `prod_encode` maps a pair of natural numbers to a natural number, and `prod_decode` is its inverse.

The first function creates a part (vertex set) of G from a given label (0, 1 or 2) and the numbers below M. The other two return the label (or the original number below M, respectively) given a vertex of G.

```
  define part_of where "part_of ≡ λξ. (λi. prod_encode (ξ,i)) ‘ {..<M}"
  define label_of_part where "label_of_part ≡ λp. fst (prod_decode p)"
  define from_part where "from_part ≡ λp. snd (prod_decode p)"
```

We prove some obvious identities relating these functions, and then define the three parts X, Y, Z of G:

```
  let ?X = "part_of 0"
  let ?Y = "part_of (Suc 0)"
  let ?Z = "part_of (Suc (Suc 0))"
```

Defining the edges of G isn't easy. Zhao says (referring to the set A above)

> Connect a vertex $x \in X$ to a vertex $y \in Y$ if $y - x \in A$. Similarly, connect $z \in Z$ with $y \in Y$ if $z - y \in A$. Finally, connect $x \in X$ with $z \in Z$ if $(z - x)/2 \in A$. Because we picked M to be odd, 2 is invertible modulo M and this last step makes sense.

To formalise these difference relations, it seems easier to work in the type of integers. The function `int` is the obvious embedding from the natural numbers. Note that division by 2 has been expressed in terms of multiplication by $N + 1$.

```
  define "diff ≡ λa b. (int a - int b) mod (int M)"
  define "diff2 ≡ λa b. ((int a - int b) * int(Suc N)) mod (int M)"
```

We need a dozen lines simply to prove this trivial fact (and more facts are needed):

```
  have "diff y x = int a ⟷ y = (x + a) mod M" if "y < M" "a∈A"
```

An auxiliary function captures the requirement that an edge set needs to connect specific parts of the tripartite graph satisfying a given difference relation:

```
  define Edges where "Edges ≡ λX Y df.
      {{x,y}| x y. x∈X ∧ y∈Y ∧ df(from_part y)(from_part x) ∈ int‘A}"
```

Finally, Zhao's definition of G is straightforward:

```
  define XY where "XY ≡ Edges ?X ?Y diff"
  define YZ where "YZ ≡ Edges ?Y ?Z diff"
  define XZ where "XZ ≡ Edges ?X ?Z diff2"
  define G where "G ≡ (?X ∪ ?Y ∪ ?Z, XY ∪ YZ ∪ XZ)"
```

Unfortunately, that this construction satisfies the obvious properties is tricky even to formalise, let alone to prove. Consider the following claim:

```
have uniq: "∃i<M. ∃d∈A. ∃x ∈ {p,q,r}. ∃y ∈ {p,q,r}. ∃z ∈ {p,q,r}.
              x = prod_encode(0, i)
            ∧ y = prod_encode(1, (i+d) mod M)
            ∧ z = prod_encode(2, (i+d+d) mod M)"
  if T: "triangle_in_graph p q r G" for p q r
```

It is a characterisation of an arbitrary triangle $\{p, q, r\}$ in G. The claim is that p, q, r can be permuted as $x \in X$, $y \in Y$, $z \in Z$ so that there is one vertex in each of the three parts of the graph (in order!), and that x, y, z encode the arithmetic progression i, $i+d$, $i+2d$ for $i < M$ and $d \in A$. Zhao devotes two sentences to this claim. The formal proof takes more than 50 lines. It takes us to a key milestone:

```
have "unique_triangles G"
```

The proof that each edge of G lies in a unique triangle is four sentences in Zhao's presentation and more than 180 lines in Isabelle/HOL, requiring a case analysis with three quite similar proofs depending on the edge: `e ∈ XY`, `e ∈ YZ` or `e ∈ XZ`.

Zhao's proof [35] concludes as follows (*Corollary 3.18* is our Corollary 1):

> Then Corollary 3.18 implies that G has $o(M^2)$ edges. But by construction G has precisely $3M|A|$ edges. Since $M = 2N + 1$, it follows that $|A|$ is $o(N)$ as claimed.

We have 100+ lines of Isabelle to go. First, a simple proof that $|E| \leq \epsilon/12\,|V|^2$:

```
have *: "card (uedges G) ≤ ε/12 * (card (uverts G))²"
  using X <X < card (uverts G)> <unique_triangles G> <uwellformed G>
  by blast
```

Next, a result that will let us show that the edge sets `XY`, `YZ`, `XZ` all have cardinality $M|A|$. The defining relation is abstracted as `df`. The proof takes some effort!

```
have card_Edges: "card (Edges (part_of ξ) (part_of ζ) df) = M * card A"
  if "ξ ≠ ζ" and df_cancel: "∀a∈A. ∀i<M. ∃j<M. df j i = int a"
             and df_inj: "∀a. inj_on (λx. df x a) {..<M}"  for ξ ζ df
```

Having got this far, the rest is plain sailing. The edge sets are trivially shown to be disjoint, from which we obtain $|E| = 3M|A|$ and therefore $|A| \leq \epsilon N$.

```
have "card (uedges G) = 3 * M * card A"
  by (simp add: G_def card_Un_disjnt)
then have "card A ≤ ε * (real M / 4)"
  using * <0 < M> by (simp add: cardG card_edges power2_eq_square)
also have "... < ε * N"
  using <N>0> by (simp add: M_def assms)
finally show "card A < ε * N" .
```

4.3. **Roth's Theorem: the final version.** The version of Roth's Theorem presented as Theorem 3 in Section 1, that is, formulated using the notion of upper asymptotic density, essentially constitutes the contrapositive of the lemma proved above: if A is in a certain sense "big enough" then it must contain a 3-term arithmetic progression.

```
theorem RothArithmeticProgressions:
  assumes "upper_asymptotic_density A > 0"
  shows "∃k d. d>0 ∧ progression3 k d ⊆ A"
```

The notion of upper asymptotic density is in the development *Ergodic Theory* from the Archive of Formal Proofs [14]. Assuming the negation of the conclusion, it is easy to contradict the assumption.

5. Some Difficulties

Much of the effort in this project had not to do with the formalisation itself but with ascertaining precisely what to formalise. Although this material is considered mathematics of central importance, sources are conflicting about the basic definitions.

The first problematic definition is *edge density*, Def. 2:

$$d(X,Y) = \frac{e(X,Y)}{|X||Y|}.$$

In one draft of his notes, Zhao mentions that the given definition of $e(X,Y)$ does not even equal the actual number of edges between X and Y unless those sets are disjoint. So the question is whether to **require** X and Y to be disjoint. Many authors do, although Zhao and Gowers do not. To see whether this omission was intentional, we examined the literature and easily found numerous sources of all kinds (lecture notes, preprints, slides and journal articles) requiring the sets to be disjoint. One specific example is Malliaris and Shelah [24]. As already mentioned in Section 1, Szemerédi originally proved his Regularity Lemma for bipartite graphs and then generalised it for arbitrary graphs: this may be the source of discrepancy with respect to disjointness. The question matters because it affects subsequent definitions, theorem statements and proofs. Ultimately we decided to omit the constraint provisionally and were never forced to reimpose it. In the video[3] of his MIT lecture, Zhao clarifies that we are in principle allowed to include pairs (V_i, V_j) with $i = j$ in the regular partition definition, Def. 4 (see around 12:45 in the video). This is what prompted us to omit the disjointness constraint both in the edge density within the regular pairs definition and in the regular partition definition, considering the more general case where $i = j$ is allowed everywhere.

The next problematic definition was that of an ϵ-regular pair, Def. 3. We call (X,Y) an ϵ-regular pair if a certain condition holds for all $A \subseteq X$ and $B \subseteq Y$. However, both Gowers and Zhao specified strict subsets, $A \subset X$ and $B \subset Y$. In this case, it seemed that there could be no doubt, because the Energy Boost Lemma requires strict subsets: it creates partitions $\{A, X \setminus A\}$ and $\{B, Y \setminus B\}$, and a component of a partition cannot be empty. This definition worked for the formalisation of Szemerédi's Regularity Lemma. Unfortunately, when we moved to the proof of Roth's Theorem, the version of the definition with strict subsets did not make sense. Proving the Triangle Counting Lemma, at the very start we "obtain a pair of subsets witnessing the irregularity of (X,Y)" and one of these so-called subsets is Y itself. With a little effort, we were able to show that the two definitions of regular pair, strict and non-strict, coincide provided both X and Y contained at least two elements. This extremely weak but necessary proviso unfortunately introduced a degenerate case in the Triangle Counting Lemma that we could not prove. Instead we changed the definition of ϵ-regular pair to involve non-strict subsets and redid the proof of the Regularity Lemma. The necessary correction to the Energy Boost Lemma introduced annoying but minor complications throughout the proof (in particular, the introduction of the function `P2` to deal with degenerate partitions, as mentioned in Section 2.3). Eventually we learned that in combinatorics, $\subset$ and $\subseteq$ might be used interchangeably even within the same context, with $\subsetneq$ reserved for the strict form.

Another issue in the formalisation was how to represent partitions. All informal expositions write a partition as a family of sets indexed by natural numbers: $\{V_1, \ldots, V_k\}$. The notation with indices looks natural and familiar. The indexing plays a prominent role in the proofs: sometimes we refer to (V_i, V_j) where $i < j$, so

[3] `https://www.youtube.com/watch?v=vcsxCFSLyP8&t=939s`

the order is also significant. But as we refine such a partition, further partitioning each of the V_i, the task of assigning correct indices to each set is irksome. So we—having completed the formalisation—redid it to formalise a partition as nothing but a set of sets. The reworking did not take long and resulted in a slightly shorter and definitely clearer proof. On the rare occasions when explicit indices were necessary, choosing an arbitrary ordering of the partition was sufficient.

On a related note, another difficulty was formalising the partition refinement step, the lemma Zhao calls *Energy Boost for an irregular partition* (Section 2.4). Here, a partition $\{V_1, \ldots, V_k\}$ of the vertex set is given and for all ϵ-irregular pairs (V_i, V_j), a further partition of both members is induced by the Energy Boost Lemma. The new partition must be a common, simultaneous refinement of all of those partitions. What must be done is fairly obvious but only to someone reasonably familiar with the material. (The latest drafts of Zhao's book cover these subtleties superbly.) The actual formalisation of the common refinement of a set of partitions (a set of set of sets) is the collection of all possible nonempty intersections involving a member of each of the partitions. The idea is obvious enough but the formalisation contains a few tricky elements.

Finally, our sources differed on the maximum possible size of the partition of each V_i mentioned above. In the notes for Gowers's course [17] 2^{2k} is given, while according to the early version of the notes by Zhao [35] it is 2^k. We eventually discovered the updated version of Zhao's notes [36] with the correct (depending on details of definitions) figure of 2^{k+1} and a hint that one must exploit symmetry to avoid double counting (V_i, V_j) and (V_j, V_i) in order to fit within that bound. We have followed Zhao, who states that pairs where $i = j$ are also included; we say more about the treatment of the diagonal in Section 6 below. The inequality given is $k\,2^{k+1} \leq 2^{2^k}$, which in the final induction delivers the required stack of exponentials. Because in the notes for Gowers's course [17] a higher upper bound is given, this inequality is stated as $k\,2^{2k} \leq 2^{2^k}$, which however, is not true for $k = 2$ (and Isabelle reports this counterexample unprompted). All three different aforementioned bounds for this lemma lead, however, to the same tower of exponentials, which Gowers [15] proved to be tight.

In all these difficulties we have no one to blame but ourselves, since there were willing experts whom we could have consulted. Gowers works in a nearby department, and when we finally made contact with Zhao (having completed both formalisations) he was enthusiastic to help us clarify the ambiguity in the regular pair definition. And there is a further lesson: mathematicians expect the right methods to be used but are quite willing to overlook trivial details, while computer scientists expect everything to fit together perfectly. There is a difference in outlook that must somehow be bridged if the formalisation of mathematics is to become mainstream. At the same time, we see that formalising mathematics with a proof assistant like Isabelle can be helpful in clarifying minor details and edge cases. This is not only because the user is forced to examine every technical point while articulating a proof to a computer, but also because working with a formal proof can reveal delicate issues: for example, counterexample-finding tools implemented within Isabelle's automation may remind the user about missing assumptions and edge cases, or the users themselves may experiment to see where the proof breaks after minor modifications in the code.

6. Independent formalisation in Lean

As noted in Section 1, similar material was formalised in Lean by Yaël Dillies and Bhavik Mehta around the same time [5] and their formalisations[4] are pending full incorporation to mathlib, Lean's library of formalised mathematical proofs.

A notable difference between the two formalisations is that Dillies and Mehta treated the *equitable* version of Szemerédi's Regularity Lemma, which yields an equitable partition of the vertex set. A partition of a set of size n into k parts is equitable if every part has size $\lfloor n/k \rfloor$ or $\lceil n/k \rceil$. In particular, the equitable version of Szemerédi's Regularity Lemma states that

Theorem 6. *For every $\epsilon > 0$ and m_0, there exists a constant M such that every graph G has an ϵ-regular equitable partition of its vertex set into k parts with $m_0 \leq k \leq M$.*

The proof is similar to the proof of the non-equitable version, but at every stage when the partition is refined (by the Energy Boost Lemma), a further refinement step is done to keep the new partition equitable.

We earlier noted that our sources suggested three different upper bounds on the size of the partition obtained via the Energy Boost Lemma for an irregular partition. One of the three is numerically wrong, but the other two are both correct, depending on details of the definitions. To clarify, recall Definition 4: As we explained in the previous section, we removed the disjointness constraint both in the edge density within the regular pairs definition and in the regular partition definition, meaning that we considered the more general case where $i = j$ is allowed everywhere. Dillies and Mehta also allow for pairs (X, X) in the edge density definition, however in the regular partition definition, unlike us, they explicitly exclude the possibility $i = j$ (omitting the diagonal, explicitly ignoring all (V_i, V_i) pairs), that is, in their version of Definition 4 they instead consider the condition

$$\sum_{\substack{i \neq j \\ (i,j) \in [k]^2 \\ (V_i, V_j) \text{ not } \epsilon\text{-regular}}} |V_i||V_j| \leq \epsilon |V(G)|^2.$$

By omitting the diagonal pairs where $i = j$, the upper bound attained in the Lean development is 2^k rather than 2^{k+1} as in our case.

The diagonal pairs can safely be ignored in the development by Dillies and Mehta, since they formalise the equitable version of Szemerédi's Regularity Lemma, Theorem 6: if there are enough parts in the partition, then the proportion of pairs that are diagonal can be made small.

We are grateful to Timothy Gowers, who in a private email clarified this discrepancy between the two approaches. He moreover stated that he finds the non-equitable version that we formalised more mathematically natural: e.g. if the graph is quasirandom, partitioning it arbitrarily into enough parts to allow ignoring the diagonal contributions looks artificial when you can just take a single part. Gowers added that he is not aware of any practical applications where equitability would be required.

Dillies and Mehta followed a different route than we did from Szemerédi's Regularity Lemma to Roth's Theorem: via the Corners Theorem. A *corner* in $\mathbb{Z}^2$ is a three-element set of the form

$$\{(x, y), (x + d, y), (x, y + d)\}$$

[4] `https://github.com/leanprover-community/mathlib/tree/szemeredi/src/combinatorics/szemeredi`

with $d > 0$. The Corners Theorem states that every corner-free subset of $[N]^2$ has size $o(N^2)$. It has a short proof using the Triangle Removal Lemma and leads fairly directly to Roth's Theorem. As already sketched above, we followed a route via the Diamond-Free Lemma, Corollary 1 (also referred to in the literature as a Ruzsa-Szemerédi bound).

Finally, it is worth mentioning that although the Isabelle/HOL type system is much simpler than Lean's (the latter uses dependent types), we never had to exercise any ingenuity in regard to types.

7. Conclusions

Szemerédi's Regularity Lemma and Roth's Theorem on Arithmetic Progressions are regarded as major results and our announcement of their formalisation was greeted enthusiastically [2]. And yet, the formalisation was almost straightforward, the main difficulties stemming from ambiguities in our sources compounded by our unwise refusal to consult available experts. The formalisations are relatively short: about 1000 lines for Szemerédi's Regularity Lemma and 1500 for Roth's Theorem. Zhao's exposition of the two theorems takes up about six pages for each. A rough calculation yields a de Bruijn factor (the ratio of the sizes of the formalised material over the original material) of about four for both developments. This sort of mathematics is clearly suitable for formalisation, and in view of the minor inaccuracies we discovered in standard presentations, there is some value in doing so.

Acknowledgements. Many thanks to Timothy Gowers and Yufei Zhao for valuable advice, and to Yaël Dillies and Bhavik Mehta for fruitful discussions. The referees scrutinised the manuscript with care and made numerous helpful suggestions.

Statements and declarations. The authors were supported by the ERC Advanced Grant ALEXANDRIA (Project 742178). Edmonds is jointly funded by the Cambridge Trust (Cambridge Australia Scholarship) and a Cambridge Department of Computer Science Premium Research Studentship.

The authors have no financial or proprietary interests in any material discussed in this article.

References

[1] S. Bell and W. Grodzicki. Using Szemerédi's regularity lemma to prove Roth's theorem, 2010. Lecture notes, University of Georgia.

[2] K. Buzzard. What is the point of computers? a question for pure mathematicians. In *Proceedings of the International Congress of Mathematicians (ICM 2022)*, 2022. In press. https://arxiv.org/abs/2112.11598v2.

[3] D. Conlon, J. Fox, and Y. Zhao. The Green–Tao theorem: an exposition. *EMS Surveys in Mathematical Sciences*, 1, 03 2014.

[4] R. Diestel. *Graph Theory*. Springer, 2017.

[5] Y. Dillies and B. Mehta. Formalizing Szemerédi's regularity lemma in Lean. In J. Andronick and L. de Moura, editors, *13th International Conference on Interactive Theorem Proving*. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2022. In press.

[6] M. Džamonja, A. Koutsoukou-Argyraki, and L. C. Paulson. Formalising ordinal partition relations using Isabelle/HOL. *Experimental Mathematics*, 31(2):383–400, 2022. Online at `https://doi.org/10.1080/10586458.2021.1980464`.

[7] C. Edmonds, A. Koutsoukou-Argyraki, and L. C. Paulson. Roth's theorem on arithmetic progressions. *Archive of Formal Proofs*, Dec. 2021. `https://isa-afp.org/entries/Roth_Arithmetic_Progressions.html`, Formal proof development.

[8] C. Edmonds, A. Koutsoukou-Argyraki, and L. C. Paulson. Szemerédi's regularity lemma. *Archive of Formal Proofs*, Nov. 2021. `https://isa-afp.org/entries/Szemeredi_Regularity.html`, Formal proof development.
[9] C. Edmonds and L. C. Paulson. A modular first formalisation of combinatorial design theory. In F. Kamareddine and C. Sacerdoti Coen, editors, *Intelligent Computer Mathematics*, pages 3–18. Springer, 2021.
[10] C. Edmonds and L. C. Paulson. Fisher's inequality: Linear algebraic proof techniques for combinatorics. *Archive of Formal Proofs*, Apr. 2022. `https://isa-afp.org/entries/Fishers_Inequality.html`, Formal proof development.
[11] P. Erdős and P. Turán. On some sequences of integers. *Journal of the London Mathematical Society*, s1-11(4):261–264, 1936.
[12] P. Frankl and V. Rödl. Extremal problems on set systems. *Random Structures & Algorithms*, 20(2):131–164, 2002.
[13] H. Furstenberg. Ergodic behavior of diagonal measures and a theorem of Szemerédi on arithmetic progressions. *Journal d'Analyse Mathématique*, 31(1):204–256, 1977.
[14] S. Gouezel. Ergodic theory. *Archive of Formal Proofs*, Dec. 2015. `https://isa-afp.org/entries/Ergodic_Theory.html`, Formal proof development.
[15] W. T. Gowers. Lower bounds of tower type for Szemerédi's uniformity lemma. *Geometric & Functional Analysis GAFA*, 7(2):322–337, 1997.
[16] W. T. Gowers. A new proof of Szemerédi's theorem. *Geometric & Functional Analysis GAFA*, 11(3):465–588, 2001.
[17] W. T. Gowers. Topics in combinatorics. Online at `https://www.dpmms.cam.ac.uk/~par31/notes/tic.pdf`, 2004. Notes taken by Paul Russell.
[18] W. T. Gowers. Quasirandomness, counting and regularity for 3-uniform hypergraphs. *Combinatorics, Probability and Computing*, 15(1-2):143–184, Jan. 2006.
[19] W. T. Gowers. Hypergraph regularity and the multidimensional Szemerédi theorem. *Annals of Mathematics*, 166(3):897–946, 2007.
[20] W. T. Gowers. Erdős and arithmetic progressions. In L. Lovász, I. Z. Ruzsa, and V. T. Sós, editors, *Erdős Centennial*, pages 265–287. Springer, Berlin, 2013.
[21] R. L. Graham, B. L. Rothschild, and J. H. Spencer. *Ramsey Theory*. Wiley, 2nd edition, 1991.
[22] B. Green and T. Tao. The primes contain arbitrarily long arithmetic progressions. *Annals of Mathematics*, 167(2):481–547, 2008.
[23] K. Kreuzer and M. Eberl. Van der Waerden's theorem. *Archive of Formal Proofs*, June 2021. `https://isa-afp.org/entries/Van_der_Waerden.html`, Formal proof development.
[24] M. Malliaris and S. Shelah. Regularity lemmas for stable graphs. *Transactions of the American Mathematical Society*, 366(3):1551–1585, 2014.
[25] B. Nagle, V. Rödl, and M. Schacht. The counting lemma for regular k-uniform hypergraphs. *Random Structures & Algorithms*, 28(2):113–179, 2006.
[26] T. Nipkow, L. C. Paulson, and M. Wenzel. *Isabelle/HOL: A Proof Assistant for Higher-Order Logic*. Springer, 2002. Online at `http://isabelle.in.tum.de/dist/Isabelle/doc/tutorial.pdf`.
[27] L. Noschinski. A probabilistic proof of the girth-chromatic number theorem. *Archive of Formal Proofs*, Feb. 2012. `https://isa-afp.org/entries/Girth_Chromatic.html`, Formal proof development.
[28] L. Noschinski. A Graph Library for Isabelle. *Mathematics in Computer Science*, 9(1):23–39, Mar. 2015.
[29] M. Raussen and C. Skau. Interview with Endre Szemerédi. *Notices of the AMS*, 60(2):221–231, Feb. 2013.
[30] V. Rödl and J. Skokan. Regularity lemma for k-uniform hypergraphs. *Random Structures & Algorithms*, 25(1):1–42, 2004.
[31] K. F. Roth. On certain sets of integers. *Journal of the London Mathematical Society*, s1-28(1):104–109, 1953.
[32] E. Szemerédi. On sets of integers containing k elements in arithmetic progression. *Acta Arithmetica*, 27:199–245, 1975.
[33] E. Szemerédi. Regular partitions of graphs. Technical Report STAN-CS-75-489, Stanford University Computer Science Department, Apr. 1975.
[34] T. Tao. Szemerédi's regularity lemma revisited. *Contributions to Discrete Mathematics*, 1(1):8–28, 2006.
[35] Y. Zhao. Graph theory and additive combinatorics. Online at `https://yufeizhao.com/gtac/gtac17.pdf`, 2017.
[36] Y. Zhao. Graph theory and additive combinatorics. Online at `https://yufeizhao.com/gtacbook/`, 2022. book draft.

Email address, Chelsea Edmonds: cle47@cam.ac.uk
Email address, Angeliki Koutsoukou-Argyraki: ak2110@cam.ac.uk
Email address, Lawrence C. Paulson: lp15@cam.ac.uk