Jop Briët
Centrum Wiskunde & Informatica (CWI)
Amsterdam
J.Briet@cwi.nl

De oplossing The solution

On the resolution of Marton's conjecture from additive combinatorics

In this article, Briët delves into the history and scope of Marton's conjecture, which is also known as the polynomial Freĭman-Ruzsa conjecture. This conjecture concerns set coverings by cosets of subgroups in case of small doubling in finite-field setting.

Already in 1927, Van der Waerden published an article about arithmetic progressions (APs) in this magazine. Via the conjecture by Erdős en Turán, an ergodic version by Furstenberg and proofs constructed via Fourier-analytic techniques and ergodic theory, Briët arrives at the proof of Marton's conjecture by Gowers, Green, Manners and Tao in 2023. This proof was achieved using information-theoretic tools, in particular, the entropic Ruzsa distance. Briët concludes with the importance of equivalent formulations for various fields and a brief outline.

Breakthroughs are supposed to be rare. Not so, it seems, for the relatively young field of additive combinatorics lately. Additive combinatorics is sometimes said to have its origins in a 1927 paper of van der Waerden published in this very journal [44]. Van der Waerden's theorem asserts that for any coloring of the integers $1, \ldots, n$ with r colors, there will be a k-term arithmetic progression (k-AP) whose terms all have the same color, provided n is big enough in terms of k and r.

The pigeonhole principle implies that one of the color classes has at least a $\frac{1}{r}$-fraction of $1, \ldots, n$. It was conjectured by Erdős and Turán [6] that this fact alone is sufficient, in other words, that dense sets of the integers always contain long arithmetic progressions. Erdős went even further and conjectured that any set $A \subseteq \mathbb{N}$ satisfying $\sum_{n \in A} \frac{1}{n} = \infty$ contains arithmetic progressions of arbitrary length. Perhaps the most important example of such a set is formed by the prime numbers.

The first progress towards the Erdős-Turán conjecture was made by Roth in 1953, who used Fourier analysis over $\mathbb{Z}/n\mathbb{Z}$ to prove that any set of size roughly $\frac{n}{\log\log n}$ contains a 3-AP [36]. Roth's methods turned out hard to generalize to deal with longer progressions, however. The next advance came from Szemerédi in 1975, who reproved Roth's theorem with combinatorial methods – introducing the now famous regularity lemma from graph theory – which he could generalize to prove the conjecture for arbitrary progression lengths [41].

A downside of Szemerédi's proof was that it gave extremely poor quantitative upper bounds on $r_k(n)$, the maximal size of a k-AP-free set in $\{1, \cdots, n\}$. In particular, Roth's proof gave far superior bounds on $r_3(n)$. This fact, in addition to the elegance of Roth's proof, motivated Gowers in the late 90's to search for suitable adaptations of Fourier analysis over $\mathbb{Z}/n\mathbb{Z}$ to reprove Szemerédi's theorem – not for a second, but a third time [10, 11]. A surprising new proof had already been discovered in the late 70's by Furstenburg by translating the theorem to an equivalent statement in ergodic theory [9]. The new ergodic theory proof gave no quantitative bounds on $r_k(n)$ at all, however, although it did give rise to powerful generalizations of van der Waerden's theorem and Szemerédi's theorem, such as a density version of the Hales-Jewett theorem and Szemerédi's theorem with polynomial progressions [8, 2]. Quantitative combinatorial and Fourier-analytic proofs for these results were developed only relatively recently [34, 35, 31].

Gowers's new proof of Szemerédi's theorem involves ingenious innovations of Fourier-analytic techniques, intitiating the new field of higher-order Fourier analysis [15, 43]. Building on these ideas, Green and Tao famously managed to prove that the primes indeed contain arbitrarily long arithmetic progressions [19].

A key tool in the (higher-order) Fourier-analytic proof of Szemerédi's theorem comes from the theory of set addition developed by Freĭman [7]. A main goal in this theory is to understand the structure of a finite subset A of an abelian group whose *doubling*, $A + A = \{a + b \mid a, b \in A\}$, is not much bigger than A itself. Cosets of subgroups are extreme examples where such set addition leads to no growth at all. Marton's conjecture concerns an inverse theorem for sets in finite vector spaces, asserting that if such a set has small doubling, then it can be covered by a few cosets of

a relatively small subgroup. Her motivation for posing the conjecture did not have to do with questions from additive combinatorics but rather originated from an information-theoretic source-coding problem [25]. However, the relevance of the conjecture to higher-order Fourier analysis is the reason for most of the attention it received in the last couple of decades.

Finite-field models

The finite-field setting of Marton's conjecture comes about in a heuristic that is often considered in additive combinatorics where the integers are replaced by finite vector spaces. A variant of Roth's theorem was proved by Meshulam in 1995 and shows that any set $A \subseteq \mathbb{F}_3^n$ (the n-dimensional vector space over the field of three elements) of size about $\frac{3^n}{n}$ contains a 3-term arithmetic progression (or equivalently, an affine line) [30]. Meshulam's theorem can be proved in much the same way as Roth's theorem, now using Fourier analysis over $\mathbb{F}_3^n$. Remarkably, the resulting proof is much cleaner and yields comparatively better bounds. Such finite-field models have proved to be a valuable testing grounds for problems over the integers or cyclic groups [14, 45, 32]. The relevance of finite vector spaces in theoretical computer science, in particular $\mathbb{F}_2^n$, also led to an ever-continuing process of cross fertilization between disciplines [29].

Many prior spectacular results notwithstanding, recent years have witnessed a surprising number of major strides in additive combinatorics. These include for instance the resolution of the cap set conjecture by Ellenberg and Gijswijt, showing that $r_3(\mathbb{F}_3^n) \leq 3^{cn}$ for some absolute constant $c < 1$ [5]; a proof of the above-mentioned Erdős conjecture for 3-APs by Bloom and Sisask [4]; and a further strong quantitative improvement on $r_3(n)$ by Kelley and Meka [24], which gets tantalizingly close to a lower bound due to Behrend from 1946 [1]. In the words of mathematician and popular math-blogger Gil Kalai, the most recent breakthrough is due to a veritable A-Team of mathematics. In November of 2023, Tim Gowers, Ben Green, Freddie Manners and Terence Tao posted an arXiv preprint [12] in which they settled Marton's conjecture, widely known in the literature as the polynomial Freĭman-Ruzsa conjecture.

Marton's conjecture


Marton

Let G be an abelian group. For a pair of finite subsets $A,B \subseteq G$, define their sum and difference sets by $A \pm B = \{a \pm b \mid a \in A, b \in B\}$. The key quantity of interest is the *doubling parameter* of A, which is defined by $\sigma(A) = \frac{|A+A|}{|A|}$ This parameter is easily seen to be bounded by $1 \leq \sigma(A) \leq \frac{1}{2}(|A|+1)$. Sets that attain the upper bound, known as Sidon sets, have the property that all sums of pairs from A are distinct. A basic example of a Sidon set is the set of standard basis vectors in $\mathbb{F}_3^n$. Of interest to Marton's conjecture, however, is the lower end of the spectrum, where the doubling parameter turns out to be a proxy for algebraic structure. To see why, it is instructive to first consider the extreme case.

Cosets of subgroups are easily seen to have doubling parameter 1. It turns out that the converse also holds.

Proposition 1 Let $A \subseteq G$ be a finite subset with doubling 1. Then A is a coset of a subgroup of G.

Proof: We may suppose that A contains 0 because for any $b \in A$, the translate $A - b = \{a - b \mid a \in A\}$ contains zero and has doubling $\sigma(A)$. If A contains 0, then $A \subseteq A + A$ and in fact equality $A = A + A$ holds because $\sigma(A) = 1$. Hence, A is closed under addition. This implies that for each $x \in A$, we have that $x + A = A$ as these two sets have equal size. Since $0 \in A$, we thus have that $-x \in A$.

A natural question that arises from this characterization is what can be said about sets with "small" doubling. As an example, if $H \subseteq G$ is a coset of subgroup and $A \subseteq H$ is any set that occupies an ε-proportion of H, then A has doubling at most $\frac{1}{\varepsilon}$ since $|A+A| \leq |H+H| = |H| \leq \frac{1}{\varepsilon}|A|$. In 1973, Freĭman slightly moved the scale and showed that these are the only examples if the doubling is not too much larger than 1 [7].

Theorem 2 (Freĭman) Let $A \subseteq G$ be a finite subset with doubling parameter at most $\frac{3}{2}$. Then $A - A$ is subgroup of G.

A result of Plünnecke implies that for any finite set $B \subseteq G$, the size of its difference set is related to its doubling parameter by $|B - B| \leq \sigma(B)^2 |B|$ [33]. Therefore, by translating $A - A$ by an arbitrary element of A, we ensure that it contains A and arrive at the following corollary.

Corollary 3 Let $A \subseteq G$ be a finite subset with doubling parameter at most $\frac{3}{2}$. Then, there is a subgroup $H \subseteq G$ and $x \in G$ such that $A \subseteq H + x$ and $|H| \leq \frac{9}{4}|A|$.

Does such a statement still hold if the scale is moved further? In the paper that first explicitly recorded Marton's conjecture, Ruzsa [7] proved that it does with the following finite-field analog of another celebrated result of Freĭman over the integers [17][46].

Theorem 4 (Freĭman–Ruzsa theorem) Let p be a prime number and let $A \subseteq \mathbb{F}_p^n$ be a set with doubling parameter K. Then, there is an affine subspace $H \subseteq \mathbb{F}_p^n$ of size $|H| \leq K^2 p^{K^4} |A|$ such that $A \subseteq H$.

Marton's conjecture concerns the dependence of the ratio $|H|/|A|$ on the doubling parameter K. An improvement on this dependence was obtained by Green and Ruzsa, who showed that the exponent K^4 could be reduced to $\lfloor 2K^2 - 2 \rfloor$ [17]. As stated, however, Theorem 4 cannot admit a better function than p^{K^c} for some constant $c > 0$, as the following example shows. Let $V \subseteq \mathbb{F}_2^n$ be the subspace spanned by the last $n - k$ standard basis vectors and let $A = \{e_1, \cdots, e_k\} + V$. Since A consists of k pairwise disjoint cosets of V, it has size $k2^{n-k}$. Due to the standard basis vectors, A has doubling about $k/2$ and any affine subspace containing A must have size at least $2^{n-1} = \frac{1}{k}2^{k-1}|A|$. In light of this, to what extent could one hope to improve on Theorem 4?

An important observation to make about the above example is that it contains a subspace V of size at most $|A|$ such that A is covered by only about K translates of V. Ruzsa attributed to Marton the conjecture that this fact points to a general economic description of small-doubling sets by subspaces. More precisely, Marton's conjecture, or polynomial Freĭman-Ruzsa conjecture, states that there is a subspace H of size at most $|A|$ such that A can be covered using K^c translates of H for some absolute constant $c > 0$ (see [37]).

Major progress towards this conjecture was obtained in 2012 by Sanders [39], who used sophisticated Fourier-analytic methods to show that a quasi-polynomial in K number of translates suffice. With similar methods, Konyagin shortly after showed a slightly better but still quasi-polynomial bound (see [40]). Remarkably, with only one more big leap the conjecture was recently settled in full [12].

Theorem 5 (Gowers, Green, Manners and Tao (2023)) If $A \subseteq \mathbb{F}_2^n$ has doubling parameter K, then there is a subspace H of size $|H| \leq |A|$ such that A can be covered by at most $2K^C$ translates of H, where $C > 0$ is an absolute constant.

The original proof gave the result with $C = 12$ but not long after it appeared this was improved to $C = 9$ by Liao [26]. Subsequently, it was shown by the same original authors that their result holds more generally over finite fields of larger characteristic [13]. A few words will be devoted to the ideas behind the proof of this result here, but it is worthwhile to first highlight a couple of intriguing equivalent formulations (for more formulations, see [23] and [12]). One example is of fundamental importance to the field of algebraic property testing [38].

Corollary 6 (Linearity testing) There are absolute constants $c, C > 0$ such that the following holds. Suppose $f: \mathbb{F}_2^m \to \mathbb{F}_2^n$ is a function such that if x, y are uniformly distributed over $\mathbb{F}_2^m$, we have

$$\Pr\big[f(x+y) = f(x) + f(y)\big] \geq \frac{1}{K}.$$

Then, there exists a linear map $g: \mathbb{F}_2^m \to \mathbb{F}_2^n$ such that

$$\Pr\big[f(x) = g(x)\big] \geq \frac{c}{K^C}$$

Another formulation lies at the heart of higher-order Fourier analysis and concerns inverse theorems for the Gowers uniformity norms.

Gowers Inverse Theorems

The uniformity norms measure how much a function behaves like a polynomial by looking at how much it oscillates after a certain derivative operation has been applied a number of times. Given a function $f: G \to \mathbb{C}$, its *multiplicative derivative* in direction $h \in G$ is given by the function $\Delta_h f: G \to \mathbb{C}$ defined by

$$\Delta_h f(x) = f(x+h)\overline{f(x)}.$$

An example to keep in mind to make sense of the terminology is a *polynomial phase function* $f(x) = \omega^{P(x)}$, where p is a prime, $\omega = e^{2\pi i/p}$ and $P(x) \in \mathbb{F}_p[x_1, \cdots, x_n]$ is an n-variate polynomial over $\mathbb{F}_p$. Then,

$$\Delta_h f(x) = \omega^{P(h+x)-P(x)}.$$

The exponent $P(h+x) - P(x)$ is the standard discrete derivative of $P(x)$ in direction h and if P has degree d, then this derivative has degree $d-1$. So, after applying the multiplicative derivative $d+1$ times to f, for any choice of directions, one is left with the constant-1 function, which exhibits no oscillation at all.

Definition 7 (Uniformity norms) For a finite abelian group G, positive integer k and $f: G \to \mathbb{C}$, the *Gowers k-uniformity norm* of f is defined by

$$\|f\|_{U^k} = \big(\mathbb{E}_{x, h_1, \ldots, h_k \in G} \Delta_{h_k} \cdots \Delta_{h_1} f(x)\big)^{\frac{1}{2^k}},$$

where the expectation is taken over independent uniformly distributed random elements from G.

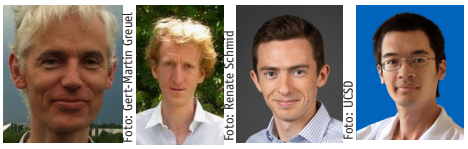
It is easily verified that the 1-uniformity norm is simply the absolute value of the average of f. This means that the 1-uniformity norm is in fact a semi-norm as it can be zero for nonzero f. For larger k, however, the uniformity norms are indeed norms.

To get some intuition for these norms, consider a linear phase function given by a character $\chi(x) = \omega^{\langle x, a \rangle}$ of $\mathbb{F}_p^n$ for a nonzero $a \in \mathbb{F}_p^n$. A single derivative in direction h turns this into the function $\chi(h)$, which is independent of x. Orthogonality of the characters implies that averaging over h causes such oscillation that the whole average cancels to zero. But a second derivative yields the constant-1 function. Linear phases thus attain the maximum-possible U^2-norm of 1. It is a routine exercise to show that these are the only such examples. Moreover, functions whose U^2-norm is bounded away from zero are closely related to linear phases. Using basic Fourier-analytic tools such as Parseval's identity and the Cauchy-Schwarz inequality, it is also not hard to show that if $\|f\|_{U^2} \geq \varepsilon$, then f correlates with some character χ, in the sense that

$$\big|\langle f, \chi \rangle\big| = \big|\mathbb{E}_{x \in \mathbb{F}_p^n} f(x)\,\overline{\chi(x)}\big| \geq \varepsilon^2.$$

This basic fact is a key step in a standard proof of Roth's theorem and Meshulam's version over finite vector spaces, as one can use the U^2-norm to count 3-APs in sets $A \subseteq G$. For a similar reason, Gowers introduced the U^k-norms to count $(k+1)$-APs.

The intuition one should have for the higher-order uniformity norms is that if $|f| \leq 1$ and f has large U^k-norm, then f correlates with a polynomial phase of degree at most $k-1$. This intuition turns out to be approximately correct for functions on cyclic groups and finite vector spaces, as



From left to right: Gowers, Green, Manners and Tao

was established in a series of highly nontrivial works on inverse theorems for the uniformity norms [10, 38, 20, 3, 43, 22]. Quantitative aspects of these inverse theorems are important for their role in proofs of Szemerédi's theorem, where they are used to show that if a set deviates in the number of APs expected from a random set of equal size, then a balanced version of its indicator function must correlate with a structured function in the form of a polynomial phase. Such correlation can be leveraged to a density increment of the set in a large structured set such as an arithmetic progression or affine subspace. This argument can then be iterated in a so-called density increment strategy to show that AP-free sets of a given density only exist when the ambient group is not too big.

One of the main recent motivations for studying Marton's conjecture is due to its equivalence to the following polynomial version of the inverse theorem for the 3-uniformity norms over finite vector spaces [27, 21].

Corollary 8 (Polynomial inverse theorem for the U^3-norm) There exists an absolute constant $c > 0$ such that the following holds. For any function $f: \mathbb{F}_p^n \to [-1, 1]$, there exists a quadratic phase function $\phi: \mathbb{F}_p^n \to \mathbb{C}$ such that

$$\big|\langle f, \phi \rangle\big| \geq \|f\|_{U^3}^c.$$

Entropy version of PFR

We will only briefly touch upon some of the ideas behind the proof of Theorem 5. A streamlined and abridged version of it may also be found on Tao's blog [42]. The rough idea behind the proof of Theorem 5 is to follow a "doubling decrement" strategy. Given a set $A \subseteq \mathbb{F}_2^n$ with doubling K, the idea is to show that there is a set A' that is in some way related to A and that has doubling at most $K^{0.99}$. Iterating this process, one quickly ends up in the purview of Freĭman's $\frac{3}{2}$-theorem (Corollary 3), which gives an affine subgroup with which one might hope to cover A using only few translates. Due to certain difficulties of working with the doubling constant di-

rectly, Gowers et al. apply a strategy of this type instead to a smoother but equivalent information-theoretic setting where subsets are replaced by $\mathbb{F}_2^n$-valued random variables [16].

A subset A is then represented by a uniform random variable over A, denoted U_A. A key role is played by the *Shannon entropy* of finitely supported random variables X,

$$H[X] = -\mathbb{E}\big[\log_2(\Pr[X=x])\big].$$

The Shannon entropy serves as a measure of size, as $\mathrm{H}[\mathrm{U_A}] = \log_2|\mathrm{A}|$. For two finitely supported independent random variables X, Y taking values in an additive group G, define their *entropic Ruzsa distance* by

$$d[X;Y] = H[X-Y] - \tfrac{1}{2}H[X] - \tfrac{1}{2}H[Y].$$

This quantity is referred to as a distance, but it has the odd property that a random variable can have nonzero distance to itself. It is still useful in the context of doubling parameters, however, due to the fact that

$$\mathrm{d}[\mathrm{U_A}, \mathrm{U_A}] = \log_2 \mathrm{K}.$$

As one might expect in light of Proposition 1, it holds that $d[X,X] = 0$ if and only if X is uniformly distributed over an affine subspace. Another useful feature, also the main reason why this function is referred to as a distance, is that it obeys the triangle inequality.

Lemma 9 (Ruzsa triangle inequality) Let X, Y, Z be finitely supported random variables over an additive group G. Then,

$$d[X;Y] \le d[X;Z] + d[Y;Z].$$

This is a main tool in the entropic doubling decrement proof. It is used, very roughly speaking, to sequentially find certain improvements of the original distribution U_A to obtain distributions that are on the one hand closer to themselves in entropic Ruzsa distance (thereby moving towards a uniform distribution on an affine subspace), while on the other hand not moving too far away from U_A so as to still give an approximation of it. This results in the following version of Theorem 5.

Theorem 10 (The entropic polynomial Freĭman–Ruzsa theorem) Let X, Y be $\mathbb{F}_2^n$-valued random variables such that $d[X,Y] \le \varkappa$. Then, there is a subspace $H \subseteq \mathbb{F}_2^n$ such that

$$d[X;U_H] + d[Y;U_H] \le 11\varkappa,$$

When one replaces X and Y with U_A, then the resulting statement turns out to be equivalent to Theorem 5. In a large online collaboration, the proof of Theorem 10 was formalized in the automated proof assistant Lean4 (see https://teorth.github.io/pfr/).

What's next?

The proof of Marton's conjecture settled a major open problem in the field of additive combinatorics. It shows that any set $A \subseteq \mathbb{F}_2^n$ with doubling K can be covered by at most $2K^9$ cosets of a subspace of size at most A. There is a close connection between this type of statement and results on containment of a large affine subspace in iterated sum sets of A. Indeed, Theorem 5 also has the following corollary [12].

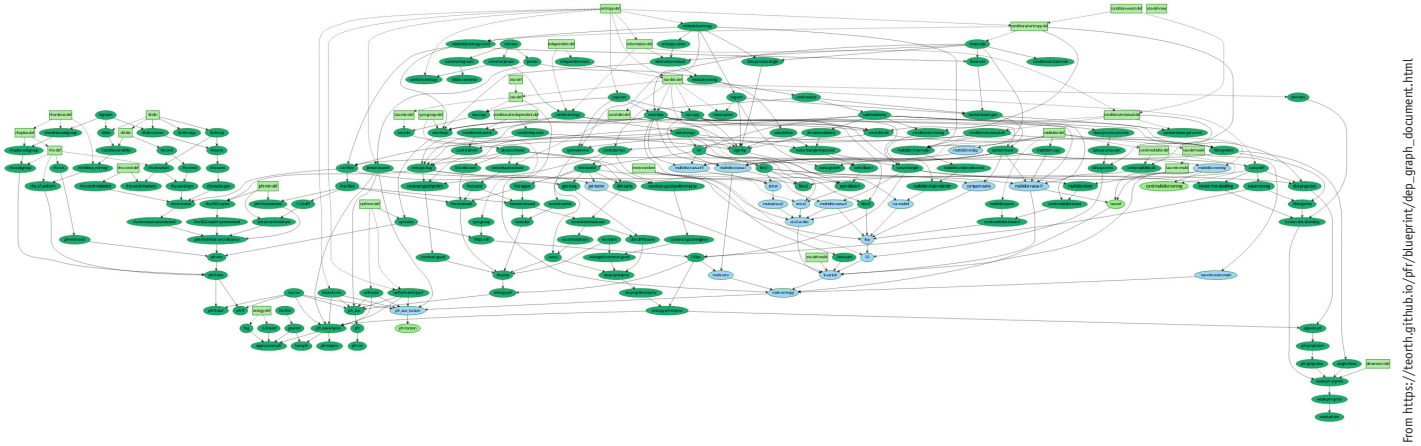
Corollary 11 There is an absolute constant $C > 0$ such that the following holds. Suppose $A \subseteq \mathbb{F}_2^n$ is a nonempty subset with doubling parameter K. Then, the m-fold iterated sum set $A + \cdots + A$ contains a subspace of size at least $K^{-C}|A|$ for some $m \le \log(K+2)^C$.

The relevance of this result is that it may be viewed as a weak version of the so-called *polynomial Bogulyubov conjecture*, posed by Lovett [28].

Conjecture 12 (Polynomial Bogulyubov conjecture) There is an absolute constant $C > 0$ such that the following holds. Suppose $A \subseteq \mathbb{F}_2^n$ is a nonempty subset with doubling parameter K. Then, $A + A + A + A$ contains a subspace of size at least $K^{-C}|A|$.

The best available result of this type, involving four-fold sum sets, is quasi-polynomial in K. It was proved by Sanders in the work that essentially established the previous best version of Theorem 5, showing that $4A$ contains a subspace of size at least $\exp\big(-\log(K+2)^C\big)|A|$ [39].

So while a major hurdle has just been overcome, a next milestone is already in clear view.



Bron: From https://teorth.github.io/pfr/blueprint/dep_graph_document.html

Figure 1 Dependency graph of the formalized proof of Marton's conjecture in proof assistant Lean4.

References and notes

1 F. A. Behrend. On sets of integers which contain no three terms in arithmetical progression. *Proc. Nat. Acad. Sci. U. S. A.*, 32:331–332, 1946.

2 V. Bergelson and A. Leibman. Polynomial extensions of van der Waerden's and Szemerédi's theorems. *J. Amer. Math. Soc.*, 9(3):725–753, 1996. doi:10. 1090/S0894-0347-96-00194-4.

3 Vitaly Bergelson, Terence Tao, and Tamar Ziegler. An inverse theorem for the uniformity seminorms associated with the action of F∞ p . *Geom. Funct. Anal.*, 19(6):1539–1596, 2010. doi:10.1007/s00039-010-0051-1.

4 Thomas F Bloom and Olof Sisask. Breaking the logarithmic barrier in Roth's theorem on arithmetic progressions. *arXiv preprint arXiv:2007.03528, 2020*.

5 Jordan S Ellenberg and Dion Gijswijt. On large subsets of with no three-term arithmetic progression. *Annals of Mathematics*, pages 339–343, 2017.

6 Paul Erdős and Paul Turán. On some sequences of integers. *Journal of the London Mathematical Society*, s1-11(4):261–264, 1936.

7 Grigory A. Freĭman. Foundations of a structural theory of set addition. *American Mathematical Society*, 1973.

8 H. Furstenberg and Y. Katznelson. A density version of the Hales-Jewett theorem. *J. Anal. Math.*, 57:64–119, 1991. doi:10.1007/BF03041066.

9 Harry Furstenberg. Ergodic behavior of diagonal measures and a theorem of Szemerédi on arithmetic progressions. *J. Analyse Math.*, 31:204–256, 1977.

10 W. T. Gowers. A new proof of Szemerédi's theorem for arithmetic progressions of length four. *Geom. Funct. Anal.*, 8(3):529–551, 1998.

11 W. T. Gowers. A new proof of Szemerédi's theorem. *Geom. Funct. Anal.*, 11(3):465–588, 2001.

12 W. T. Gowers, Ben Green, Freddie Manners, and Terence Tao. On a conjecture of Marton, 2023. arXiv:2311.05762.

13 W. T. Gowers, Ben Green, Freddie Manners, and Terence Tao. Marton's con- jecture in abelian groups with bounded torsion, 2024. arXiv:2404.02244.

14 Ben Green. Finite field models in additive combinatorics. In Surveys in combi- natorics 2005, volume 327 of London Math. Soc. Lecture Note Ser., pages 1–27. Cambridge Univ. Press, Cambridge, 2005. doi:10.1017/CBO9780511734885. 002.

15 Ben Green. Montréal notes on quadratic Fourier analysis. In Additive combi- natorics, volume 43 of CRM Proc. Lecture Notes, pages 69–102. *Amer. Math. Soc.*, Providence, RI, 2007.

16 Ben Green, Freddie Manners, and Terence Tao. Sumsets and entropy revisited, 2023. URL: https://arxiv.org/abs/2306.13403, arXiv:2306.13403.

17 Ben Green and Imre Z. Ruzsa. Sets with small sumset and rectification. Bull. *London Math. Soc.*, 38(1):43–52, 2006. doi:10.1112/S0024609305018102.

18 Ben Green and Imre Z. Ruzsa. Freiman's theorem in an arbitrary abelian group. *J. Lond. Math. Soc.* (2), 75(1):163–175, 2007. doi:10.1112/jlms/ jdl021.

19 Ben Green and Terence Tao. The primes contain arbitrarily long arithmetic progressions. *Ann. of Math.* (2), 167(2):481–547, 2008. doi:10.4007/annals. 2008.167.481.

20 Ben Green and Terence Tao. The distribution of polynomials over finite fields, with applications to the Gowers norms. Contrib. *Discrete Math.*, 4(2):1–36, 2009.

21 Ben Green and Terence Tao. An equivalence between inverse sumset theorems and inverse conjectures for the U 3 norm. *Math. Proc. Cambridge Philos. Soc.*, 149(1):1–19, 2010. doi:10.1017/S0305004110000186.

22 Ben Green, Terence Tao, and Tamar Ziegler. An inverse theorem for the Gowers U s+1[N]-norm. *Ann. of Math.* (2), 176(2):1231–1372, 2012. doi: 10.4007/annals.2012.176.2.11.

23 Benjamin J. Green. Notes on the Polynomial Freĭman- Ruzsa Conjecture. expository note. Available at http://people.maths.ox.ac.uk/greenbj/papers/PFR.pdf.

24 Zander Kelley and Raghu Meka. Strong bounds for 3-progressions, 2024. arXiv:2302.05537.

25 J. Korner and K. Marton. How to encode the modulo-two sum of binary sources (corresp.). *IEEE Transactions on Information Theory*, 25(2):219–221, 1979. doi:10.1109/TIT.1979.1056022.

26 Jyun-Jie Liao. Improved exponent for Marton's conjecture in Fn 2, 2024. URL: https://arxiv.org/abs/2404.09639, arXiv:2404.09639.

27 Sachar Lovett. Equivalence of polynomial conjectures in additive combinatorics. *Combinatorica*, 32:607–618, 2012. doi:doi.org/10.1007/ s00493-012-2714-z.

28 Shachar Lovett. An Exposition of Sanders' Quasi-Polynomial Freiman-Ruzsa Theorem. Number 6 in Graduate Surveys. Theory of Computing Library, 2015. URL: http://www.theoryofcomputing.org/library.html, doi:10.4086/toc.gs.2015.006.

29 Shachar Lovett. Additive Combinatorics and its Applications in Theoretical Computer Science. Number 8 in Graduate Surveys. Theory of Computing Library, 2017. URL: http://www.theoryofcomputing.org/library.html, doi:10.4086/toc.gs.2017.008.

30 Roy Meshulam. On subsets of finite abelian groups with no 3-term arithmetic progressions. *Journal of Combinatorial Theory, Series A*, 71(1):168–172, 1995.

31 Sarah Peluse. On the polynomial Szemerédi theorem in finite fields. *Duke Math. J.*, 168(5):749–774, 2019. doi:10.1215/00127094-2018-0051.

32 Sarah Peluse. Finite field models in arithmetic combinatorics – twenty years on, 2023. URL: https://arxiv.org/abs/2312.08100, arXiv:2312.08100.

33 Helmut Plünnecke. Eigenschaften und Abschätzungen von Wirkungsfunktionen. Number 22. Gesellschaft für Mathematik und Datenverarbeitung, 1961.

34 DHJ Polymath. A new proof of the density Hales-Jewett theorem. *Annals of Mathematics*, pages 1283–1327, 2012.

35 Sean Prendiville. Quantitative bounds in the polynomial Szemerédi theorem: the homogeneous case. *Discrete Anal., pages* Paper No. 5, 34, 2017. doi: 10.19086/da.1282.

36 Klaus F Roth. On certain sets of integers. *Journal of the London Mathematical Society*, 1(1):104–109, 1953.

37 Imre Ruzsa. An analog of Freiman's theorem in groups. *Astérisque*, 258(199):323–326, 1999.

38 Alex Samorodnitsky. Low-degree tests at large distances. In STOC'07— *Proceedings of the 39th Annual ACM Symposium on Theory of Computing, pages 506–515. ACM, New York, 2007*. Available at arXiv: 0604353.

39 Tom Sanders. On the Bogolyubov-Ruzsa lemma. *Anal. PDE*, 5(3):627–655, 2012. doi:10.2140/apde.2012.5.627.

40 Tom Sanders. The structure theory of set addition revisited. *Bull. Amer. Math. Soc. (N.S.),* 50(1):93–127, 2013. doi:10.1090/S0273-0979-2012-01392-7.

41 Endre Szemerédi. On sets of integers containing no k elements in arithmetic progression. *Acta Arith*, 27(299-345):21, 1975.

42 Terence Tao. URL: https://terrytao.wordpress.com/2024/06/22/ an-abridged-proof-of-martons-conjecture/.

43 Terence Tao and Tamar Ziegler. The inverse conjecture for the Gowers norm over finite fields in low characteristic. *Annals of Combinatorics*, 16(1):121–188, 2012.

44 Bartel Leendert van der Waerden. Beweis einer Baudetschen vermutung. *Nieuw Archief voor Wiskunde*, 15:212–216, 1927.

45 J. Wolf. Finite field models in arithmetic combinatorics—ten years on. *Finite Fields* Appl., 32:233–274, 2015. doi:10.1016/j.ffa.2014.11.003.

46 Analogous results were proved for arbitrary abelian groups in [18].