Additive Combinatorics

with a view towards Computer Science and Cryptography

An Exposition

Khodakhast Bibak

Department of Combinatorics and Optimization
University of Waterloo
Waterloo, Ontario, Canada N2L 3G1
kbibak@uwaterloo.ca

July 30, 2012

Abstract

Recently, additive combinatorics has blossomed into a vibrant area in mathematical sciences. But it seems to be a difficult area to define – perhaps because of a blend of ideas and techniques from several seemingly unrelated contexts which are used there. One might say that additive combinatorics is a branch of mathematics concerning the study of combinatorial properties of algebraic objects, for instance, Abelian groups, rings, or fields. This emerging field has seen tremendous advances over the last few years, and has recently become a focus of attention among both mathematicians and computer scientists. This fascinating area has been enriched by its formidable links to combinatorics, number theory, harmonic analysis, ergodic theory, and some other branches; all deeply cross-fertilize each other, holding great promise for all of them! In this exposition, we attempt to provide an overview of some breakthroughs in this field, together with a number of seminal applications to sundry parts of mathematics and some other disciplines, with emphasis on computer science and cryptography.

1 Introduction

Additive combinatorics is a compelling and fast growing area of research in mathematical sciences, and the goal of this paper is to survey some of the recent developments and notable accomplishments of the field, focusing on both pure results and applications with a view towards computer science and cryptography. See [321] for a book on additive combinatorics, [237, 238] for two books on additive number theory, and [330, 339] for two surveys on additive

1

combinatorics. About additive combinatorics over finite fields and its applications, the reader is referred to the very recent and excellent survey by Shparlinski [291].

One might say that additive combinatorics studies combinatorial properties of algebraic objects, for example, Abelian groups, rings, or fields, and in fact, focuses on the interplay between combinatorics, number theory, harmonic analysis, ergodic theory, and some other branches. Green [151] describes additive combinatorics as the following: "additive combinatorics is the study of *approximate mathematical structures* such as approximate groups, rings, fields, polynomials and homomorphisms". *Approximate groups* can be viewed as finite subsets of a group with the property that they are *almost* closed under multiplication. Approximate groups and their applications (for example, to expander graphs, group theory, probability, model theory, and so on) form a very active and promising area of research in additive combinatorics; the papers [64, 65, 67, 68, 151, 190, 315] contain many developments on this area. Gowers [145] describes additive combinatorics as the following: "additive combinatorics focuses on three classes of theorems: *decomposition theorems*, *approximate structural theorems*, and *transference principles*". These descriptions seem to be mainly inspired by new directions of this area.

Techniques and approaches applied in additive combinatorics are often extremely sophisticated, and may have roots in several unexpected fields of mathematical sciences. For instance, Hamidoune [172], through ideas from connectivity properties of graphs, established the so-called *isoperimetric method*, which is a strong tool in additive combinatorics; see also [173, 174, 175] and the nice survey [278]. As another example, Nathanson [239] employed *König's infinity lemma* on the existence of infinite paths in certain infinite graphs, and introduced a new class of additive bases, and also a generalization of the Erdős-Turán conjecture about additive bases of the positive integers. In [245] the authors employed tools from coding theory to estimating Davenport constants. Also, in [15, 230, 231, 268, 319] information-theoretic techniques are used to study sumset inequalities. Very recently, Alon et al. [5, 6], using graph-theoretic methods, studied sum-free sets of order m in finite Abelian groups, and also, sum-free subsets of the set $[1, n]$. Additive combinatorics problems in matrix rings is another active area of research [53, 55, 67, 82, 83, 114, 125, 133, 134, 183, 184, 206, 298].

A celebrated result by Szemerédi, known as Szemerédi's theorem (see [11, 12, 29, 122, 143, 144, 158, 161, 236, 246, 255, 256, 259, 260, 304, 310, 311, 329] for different proofs of this theorem), states that every subset A of the integers with positive upper density, that is, $\limsup_{N \to \infty} |A \cap [1, N]|/N > 0$, has arbitrary long arithmetic progressions. A stunning breakthrough of Green and Tao [154] (that answers a long-standing and folkloric conjecture by Erdős on arithmetic progressions, in a special case: the primes) says that primes contain arbitrary long arithmetic progressions. The fusion of methods and ideas from combinatorics, number theory, harmonic analysis, and ergodic theory used in its proof is very impressive.

Additive combinatorics has recently found a great deal of remarkable applications to computer science and cryptography; for example, to expanders [20, 21, 38, 44, 52, 53, 54, 55, 62, 63, 66, 105, 106, 167, 206, 283, 342], extractors [19, 20, 26, 28, 38, 41, 103, 104, 107, 167, 182, 217, 346, 350], pseudorandomness [33, 223, 226, 227, 301] (also, [331, 334] are two surveys and [335] is a monograph on pseudorandomness), property testing [54, 176, 177, 181, 203, 204, 270, 281, 332] (see also [137]), complexity theory [27, 28, 30, 39, 244, 350], hardness amplification [301, 338, 340], probabilistic checkable proofs (PCPs) [271], information theory

[15, 230, 231, 268, 319], discrete logarithm based range protocols [77], non-interactive zero-knowledge (NIZK) proofs [220], compression functions [192], hidden shifted power problem [57], and Diffie-Hellman distributions [36, 37, 75, 121]. Additive combinatorics also has important applications in e-voting [77, 220]. Recently, Bourgain et al. [51] gave a new explicit construction of matrices satisfying the *Restricted Isometry Property* (RIP) using ideas from additive combinatorics. RIP is related to the matrices whose behavior is nearly orthonormal (at least when acting on sufficiently sparse vectors); it has several applications, in particular, in compressed sensing [71, 72, 73].

Methods from additive combinatorics provide strong techniques for studying the so-called *threshold phenomena*, which is itself of significant importance in combinatorics, computer science, discrete probability, statistical physics, and economics [2, 34, 60, 119, 120, 198]. There are also very strong connections between ideas of additive combinatorics and the theory of *random matrices* (see, e.g., [322, 323, 341] and the references therein); the latter themselves have several applications in many areas of number theory, combinatorics, computer science, mathematical and theoretical physics, chemistry, and so on [1, 69, 74, 141, 241, 265, 323, 324]. This area also has many applications to group theory, analysis, exponential sums, expanders, complexity theory, discrete geometry, dynamical systems, and various other scientific disciplines.

Additive combinatorics has seen very fast advancements in the wake of extremely deep work on Szemerédi's theorem, the proof of the existence of long APs in the primes by Green and Tao, and generalizations and applications of the sum-product problem, and continues to see significant progress (see [96] for a collection of open problems in this area). In the next section, we review Szemerédi's and Green-Tao theorems (and their generalizations), two cornerstone breakthroughs in additive combinatorics. In the third section, we will deal with the sum-product problem: yet another landmark achievement in additive combinatorics, and consider its generalizations and applications, especially to computer science and cryptography.

2 Szemerédi's and Green-Tao Theorems, and Their Generalizations

Ramsey theory is concerned with the phenomenon that if a sufficiently large structure (complete graphs, arithmetic progressions, flat varieties in vector spaces, etc.) is partitioned arbitrarily into finitely many substructures, then at least one substructure has necessarily a particular property, and so total disorder is impossible. In fact, Ramsey theory seeks general conditions to guarantee the existence of substructures with regular properties. This theory has many applications, for example, in number theory, algebra, geometry, topology, functional analysis (in particular, in Banach space theory), set theory, logic, ergodic theory, information theory, and theoretical computer science (see, e.g., [263] and the references therein). *Ramsey's theorem* says that in any edge coloring of a sufficiently large complete graph, one can find monochromatic complete subgraphs. A nice result of the same spirit is *van der Waerden's theorem*: For a given k and r, there exists a number $N = N(k, r)$ such that if the integers in $[1, N]$ are colored using r colors, then there is a nontrivial monochro-

matic k-term arithmetic progression (k-AP). Intuitively, this theorem asserts that in any finite coloring of a structure, one will find a substructure of the same type at least in one of the color classes. Note that the finitary and infinitary versions of the van der Waerden's theorem are equivalent, through a compactness argument.

One landmark result in Ramsey theory is the Hales-Jewett theorem [171], which was initially introduced as a tool for analyzing certain kinds of games. Before stating this theorem, we need to define the concept of combinatorial line. A *combinatorial line* is a k-subset in the n-dimensional grid $[1, k]^n$ yielded from some template in $([1, k] \cup \{*\})^n$ by replacing the symbol $*$ with $1, \ldots, k$ in turn. The Hales-Jewett theorem states that for every r and k there exists n such that every r-coloring of the n-dimensional grid $[1, k]^n$ contains a combinatorial line. Roughly speaking, it says that for every multidimensional grid whose faces are colored with a number of colors, there must necessarily be a line of faces of all the same color, if the dimension is sufficiently large (depending on the number of sides of the grid and the number of colors). Note that instead of seeking arithmetic progressions, the Hales-Jewett theorem seeks combinatorial lines. This theorem has many interesting consequences in Ramsey theory, two of which, are van der Waerden's theorem and its multidimensional version, i.e., the Gallai-Witt theorem (see, e.g., [132, 149, 197] for further information).

Erdős and Turán [113] proposed a very strong form of van der Waerden's theorem – the density version of van der Waerden's theorem. They conjectured that arbitrarily long APs appear not only in finite partitions but also in every sufficiently dense subset of positive integers. More precisely, the Erdős-Turán conjecture states that if δ and k are given, then there is a number $N = N(k, \delta)$ such that any set $A \subseteq [1, N]$ with $|A| \geq \delta N$ contains a non-trivial k-AP. Roth [264] employed methods from Fourier analysis (or more specifically, the *Hardy-Littlewood circle method*) to prove the $k = 3$ case of the Erdős-Turán conjecture (see also [32, 35, 43, 98, 110, 165, 213, 234, 242, 272, 274, 287, 296]). Szemerédi [303] verified the Erdős-Turán conjecture for arithmetic progressions of length four. Finally, Szemerédi [304] by a tour de force of sophisticated combinatorial arguments proved the conjecture, now known as *Szemerédi's theorem* – one of the milestones of combinatorics. Roughly speaking, this theorem states that long arithmetic progressions are very widespread and in fact it is not possible to completely get rid of them from a set of positive integers unless we can contract the set (sufficiently) to make it of density zero. Łaba and Pramanik [211] (also see [247]) proved that every compact set of reals with Lebesgue measure zero supporting a probabilistic measure satisfying appropriate dimensionality and Fourier decay conditions must contain non-trivial 3APs.

Conlon and Gowers [94] considered Szemerédi's theorem, and also several other combinatorial theorems such as Turán's theorem and Ramsey's theorem in sparse random sets. Also, Szemerédi-type problems in various structures other than integers have been a focus of significant amount of work. For instance, [150, 219] consider these kinds of problems in the finite field setting. Very recently, Bateman and Katz [22] (also see [23]) achieved new bounds for the *cap set problem*, which is basically Roth's problem, but in a vector space over finite fields (a set $A \subset \mathbb{F}_3^N$ is called a *cap set* if it contains no lines).

A salient ingredient in Szemerédi's proof (in addition to van der Waerden's theorem) is the *Szemerédi regularity lemma*. This lemma was conceived specifically for the purpose of this proof, but is now, by itself, one of the most powerful tools in extremal graph theory

(see, e.g., [205, 258], which are two surveys on this lemma and its applications). Roughly speaking, it asserts that the vertex set of every (large) graph can be partitioned into relatively few parts such that the subgraphs between the parts are random-like. Indeed, this result states that each large dense graph may be decomposed into a low-complexity part and a pseudorandom part (note that Szemerédi's regularity lemma is the archetypal example of the *dichotomy between structure and randomness* [312]). The lemma has found numerous applications not only in graph theory, but also in discrete geometry, additive combinatorics, and computer science. For example, as Trevisan [330] mentions, to solve a computational problem on a given graph, it might be easier to first construct a Szemerédi approximation – this resulted approximating graph has a simpler configuration and would be easier to treat. Note that the significance of Szemerédi's regularity lemma goes beyond graph theory: it can be reformulated as a result in information theory, approximation theory, as a compactness result on the completion of the space of finite graphs, etc. (see [222] and the references therein). Very recently, Tao and Green [158] established an *arithmetic regularity lemma* and a complementary *arithmetic counting lemma* that have several applications, in particular, an astonishing proof of Szemerédi's theorem.

The *triangle removal lemma* established by Ruzsa and Szemerédi [269] is one of the most notable applications of Szemerédi's regularity lemma. It asserts that each graph of order n with $o(n^3)$ triangles can be made triangle-free by removing $o(n^2)$ edges. In other words, if a graph has asymptotically few triangles then it is asymptotically close to being triangle-free. As a clever application of this lemma, Ruzsa and Szemerédi [269] obtained a new proof of Roth's theorem (see also [296], in which the author using the triangle removal lemma proves Roth type theorems in finite groups). Note that a generalization of the triangle removal lemma, known as *simplex removal lemma*, can be used to deduce Szemerédi's theorem (see [144, 259, 260, 311]). The triangle removal lemma was extended by Erdős, Frankl, and Rödl [111] to the *graph removal lemma*, which roughly speaking, asserts that if a given graph does not contain too many subgraphs of a given type, then all the subgraphs of this type can be removed by deleting a few edges. More precisely, given a fixed graph H of order k, any graph of order n with $o(n^k)$ copies of H can be made H-free by removing $o(n^2)$ edges. Fox [115] gave a proof of the graph removal lemma which avoids applying Szemerédi's regularity lemma and gives a better bound (also see [92]). The graph removal lemma has many applications in graph theory, additive combinatorics, discrete geometry, and theoretical computer science. One surprising application of this lemma is to the area of *property testing*, which is now a very dynamic area in computer science [7, 8, 9, 10, 13, 137, 138, 187, 254, 257, 261, 262, 270]. Property testing typically refers to the existence of sub-linear time probabilistic algorithms (called testers), which distinguish between objects G (e.g., a graph) having a given property P (e.g., bipartiteness) and those being far away (in an appropriate metric) from P. Property testing algorithms have been recently designed and utilized for many kinds of objects and properties, in particular, discrete properties (e.g., graph properties, discrete functions, and sets of integers), geometric properties, algebraic properties, etc.

There is a (growing) number of proofs of Szemerédi's theorem, arguably seventeen proofs to this date. One such elegant proof that uses ideas from model theory was given by Towsner [329]. For another model theory based perspective, see [232], in which the authors give stronger regularity lemmas for some classes of graphs.

In fact, one might claim that many of these proofs have themselves opened up a new field of research. Furstenberg [122] by rephrasing it as a problem in *dynamical systems*, and then applying several powerful techniques from ergodic theory achieved a nice proof of the Szemerédi's theorem. In fact, Furstenberg presented a correspondence between problems in the subsets of positive density in the integers and recurrence problems for sets of positive measure in a *probability measure preserving system*. This observation is now known as the *Furstenberg correspondence principle*. *Ergodic theory* is concerned with the long-term behavior in dynamical systems from a statistical point of view (see, e.g., [108]). This area and its formidable way of thinking have made many strong connections with several branches of mathematics, including combinatorics, number theory, coding theory, group theory, and harmonic analysis; see, for example, [207, 208, 209, 210] and the references therein for some connections between ergodic theory and additive combinatorics.

This ergodic-theoretic method is one of the most flexible known proofs, and has been very successful at reaching considerable generalizations of Szemerédi's theorem. Furstenberg and Katznelson [123] obtained the *multidimensional Szemerédi theorem*. Their proof relies on the concept of *multiple recurrence*, a powerful tool in the interaction between ergodic theory and additive combinatorics. A purely combinatorial proof of this theorem was obtained roughly in parallel by Gowers [144], and Nagle et al. [236, 255, 256, 259, 260], and subsequently by Tao [311], via establishing a *hypergraph removal lemma* (see also [257, 314]). Also, Austin [11] proved the theorem via both ergodic-theoretic and combinatorial approaches. The multidimensional Szemerédi theorem was significantly generalized by Furstenberg and Katznelson [124] (via ergodic-theoretic approaches), and Austin [12] (via both ergodic-theoretic and combinatorial approaches), to the *density Hales-Jewett theorem*. The density Hales-Jewett theorem states that for every $\delta > 0$ there is some $N_0 \geq 1$ such that whenever $A \subseteq [1, k]^N$ with $N \geq N_0$ and $|A| \geq \delta k^N$, A contains a combinatorial line. Recently, in a massively collaborative online project, namely *Polymath 1* (a project that originated in Gowers' blog), the Polymath team found a purely combinatorial proof of the density Hales-Jewett theorem, which is also the first one providing explicit bounds for how large n needs to be [246] (also see [240]). Such bounds could not be obtained through the ergodic-theoretic methods, since these proofs rely on the Axiom of Choice. It is worth mentioning that this project was selected as one of the TIME Magazine's Best Ideas of 2009.

Furstenberg's proof gave rise to the field of *ergodic Ramsey theory*, in which arithmetical, combinatorial, and geometrical configurations preserved in (sufficiently large) substructures of a structure, are treated via ideas and techniques from ergodic theory (or more specifically, multiple recurrence). Ergodic Ramsey theory has since produced a high number of combinatorial results, some of which have yet to be obtained by other means, and has also given a deeper understanding of the structure of measure preserving systems. In fact, ergodic theory has been used to solve problems in Ramsey theory, and reciprocally, Ramsey theory has led to the discovery of new phenomena in ergodic theory. However, the ergodic-theoretic methods and the infinitary nature of their techniques have some limitations. For example, these methods do not provide any effective bound, since, as we already mentioned, they rely on the Axiom of Choice. Also, despite van der Waerden's theorem is not directly used in Furstenberg's proof, probably any effort to make the proof quantitative would result in rapidly growing functions. Furthermore, the ergodic-theoretic methods, to this day, have the

limitation of only being able to deal with sets of positive density in the integers, although this density is allowed to be arbitrarily small. However, Green and Tao [154] discovered a *transference principle* which allowed one to reduce problems on structures in special sets of zero density (such as the primes) to problems on sets of positive density in the integers. It is worth mentioning that Conlon, Fox, and Zhao [93] established a *transference principle* extending several classical extremal graph theoretic results, including the removal lemmas for graphs and groups (the latter leads to an extension of Roth's theorem), the Erdős-Stone-Simonovits theorem and Ramsey's theorem, to sparse pseudorandom graphs.

Gowers [143] generalized the arguments previously studied in [142, 264], in a substantial way. In fact, he employed combinatorics, generalized Fourier analysis, and inverse arithmetic combinatorics (including multilinear versions of *Freiman's theorem* on sumsets, and the *Balog-Szemerédi theorem*) to reprove Szemerédi's theorem with explicit bounds. Note that Fourier analysis has a wide range of applications, in particular, to cryptography, hardness of approximation, signal processing, threshold phenomena for probabilistic models such as random graphs and percolations, and many other disciplines. Gowers' article introduced a kind of *higher degree Fourier analysis*, which has been further developed by Green and Tao. Indeed, Gowers initiated the study of a new measure of functions, now referred to as *Gowers (uniformity) norms*, that resulted in a better understanding of the notion of *pseudorandomness*.

The Gowers norm, which is an important special case of noise correlation (intuitively, the *noise correlation* between two functions f and g measures how much $f(x)$ and $g(y)$ correlate on random inputs x and y which are correlated), enjoys many properties and applications, and is now a very dynamic area of research in mathematical sciences; see [14, 153, 157, 159, 163, 164, 176, 181, 203, 221, 224, 226, 233, 270, 271] for more properties and applications of the Gowers norm. Also, the best known bounds for Szemerédi's theorem are obtained through the so-called *inverse theorems* for Gowers norms. Recently, Green and Tao [161] (see also [320]), using the density-increment strategy of Roth [264] and Gowers [142, 143], derived Szemerédi's theorem from the *inverse conjectures GI(s)* for the Gowers norms, which were recently established in [164].

To the best of my knowledge, there are two types of inverse theorems in additive combinatorics, namely the *inverse sumset theorems of Freiman type* (see, e.g., [78, 117, 118, 152, 155, 275, 299, 306, 307, 308, 318] and [116, 238]), and *inverse theorems for the Gowers norms* (see, e.g., [143, 146, 147, 148, 153, 162, 156, 159, 163, 164, 176, 181, 189, 203, 224, 233, 270, 326, 332]). It is interesting that the inverse conjecture leads to a finite field version of Szemerédi's theorem [320]: Let $\mathbb{F}_p$ be a finite field. Suppose that $\delta > 0$, and $A \subset \mathbb{F}_p^n$ with $|A| \geq \delta|\mathbb{F}_p^n|$. If n is sufficiently large depending on p and δ, then A contains an (affine) line $\{x, x + r, \ldots, x + (p-1)r\}$ for some $x, r \in \mathbb{F}_p^n$ with $r \neq 0$ (actually, A contains an affine k-dimensional subspace, $k \geq 1$).

Suppose $r_k(N)$ is the cardinality of the largest subset of $[1, N]$ containing no nontrivial k-APs. Giving asymptotic estimates on $r_k(N)$ is an important inverse problem in additive combinatorics. Behrend [24] proved that

$$r_3(N) = \Omega\left(\frac{N}{2^{2\sqrt{2}\sqrt{\log_2 N}} \cdot \log^{1/4} N}\right).$$

7

Rankin [249] generalized Behrend's construction to longer APs. Roth proved that $r_3(N) = o(N)$. In fact, he proved the first nontrivial upper bound

$$r_3(N) = O\left(\frac{N}{\log \log N}\right).$$

Bourgain [35, 43] improved Roth's bound. In fact, Bourgain [43] gave the upper bound

$$r_3(N) = O\left(\frac{N(\log \log N)^2}{\log^{2/3} N}\right).$$

Sanders [274] proved the following upper bound which is the state-of-the-art:

$$r_3(N) = O\left(\frac{N(\log \log N)^5}{\log N}\right).$$

Bloom [32] through the nice technique "translation of a proof in $\mathbb{F}_q[t]$ to one in $\mathbb{Z}/N\mathbb{Z}$", extends Sanders' proof to 4 and 5 variables. As Bloom mentions in his paper, many problems of additive combinatorics might be easier to attack via the approach "translating from $\mathbb{F}_p^N$ to $\mathbb{F}_q[t]$ and hence to $\mathbb{Z}/N\mathbb{Z}$".

Elkin [110] managed to improve Behrend's 62-year old lower bound by a factor of $\Theta(\log^{1/2} N)$. Actually, Elkin showed that

$$r_3(N) = \Omega\left(\frac{N}{2^{2\sqrt{2}\sqrt{\log_2 N}}} \cdot \log^{1/4} N\right).$$

See also [165] for a short proof of Elkin's result, and [242] for constructive lower bounds for $r_k(N)$. Schoen and Shkredov [277] using ideas from the paper of Sanders [273] and also the new probabilistic technique established by Croot and Sisask [98], obtained Behrend-type bounds for linear equations involving 6 or more variables. Thanks to this result, one may see that perhaps the Behrend-type constructions are not too far from being best-possible.

Almost all the known proofs of Szemerédi's theorem are based on a *dichotomy between structure and randomness* [312, 316], which allows many mathematical objects to be split into a 'structured part' (or 'low-complexity part') and a 'random part' (or 'discorrelated part'). Tao [310] best describes almost all known proofs of Szemerédi's theorem collectively as the following: "Start with the set A (or some other object which is a proxy for A, e.g., a graph, a hypergraph, or a measure-preserving system). For the object under consideration, define some concept of randomness (e.g., ε-regularity, uniformity, small Fourier coefficients, or weak mixing), and some concept of structure (e.g., a nested sequence of arithmetically structured sets such as progressions or Bohr sets, or a partition of a vertex set into a controlled number of pieces, a collection of large Fourier coefficients, a sequence of almost periodic functions, a tower of compact extensions of the trivial factors). Obtain some sort of structure theorem that splits the object into a structured component, plus an error which is random relative to that structured component. To prove Szemerédi's theorem (or a variant thereof), one then

needs to obtain some sort of *generalized von Neumann theorem* [154] to eliminate the random error, and then some sort of *structured recurrence theorem* for the structured component".

Erdős's famous conjecture on APs states that a set $A = \{a_1, a_2, \ldots, a_n, \ldots\}$ of positive integers, where $a_i < a_{i+1}$ for all i, with the divergent sum $\sum_{n \in \mathbb{Z}^+} \frac{1}{a_n}$, contains arbitrarily long APs. If true, the theorem includes both Szemerédi's and Green-Tao theorems as special cases. This conjecture seems to be too strong to hold, and in fact, might be very difficult to attack – it is not even known whether such a set must contain a 3-AP! So, let us mention an equivalent statement for Erdős's conjecture that may be helpful. Let N be a positive integer. For a positive integer k, define $a_k(N) := r_k(N)/N$ (note that Szemerédi's theorem asserts that $\lim_{N \to \infty} a_k(N) = 0$, for all k). It can be proved (see [286]) that Erdős's conjecture is true if and only if the series $\sum_{i=1}^{\infty} a_k 4^i$ converges for any integer $k \geq 3$. So, to prove Erdős's conjecture, it suffices to obtain the estimate $a_k(N) \ll 1/(\log N)^{1+\varepsilon}$, for any $k \geq 3$ and for some $\varepsilon > 0$.

Szemerédi's theorem plays an important role in the proof of the Green-Tao theorem [154]: The primes contain arithmetic progressions of arbitrarily large length (note that the same result is valid for every subset of the primes with positive relative upper density). Green and Tao [160] also proved that there is a k-AP of primes all of whose terms are bounded by

$$2^{2^{2^{2^{2^{2^{2^{2^{(100k)}}}}}}}},$$

which shows that how far out in the primes one must go to warrant finding a k-AP. A conjecture (see [207]) asserts that there is a k-AP in the primes all of whose terms are bounded by $k! + 1$.

There are three fundamental ingredients in the proof of the Green-Tao theorem (in fact, there are many similarities between Green and Tao's approach and the ergodic-theoretic method, see [188]). The first is Szemerédi's theorem itself. Since the primes do not have positive upper density, Szemerédi's theorem cannot be directly applied. The second major ingredient in the proof is a certain *transference principle* that allows one to use Szemerédi's theorem in a more general setting (a generalization of Szemerédi's theorem to the *pseudorandom sets*, which can have zero density). The last major ingredient is applying some notable features of the primes and their distribution through results of Goldston and Yildirim [139, 140], and proving the fact that this generalized Szemerédi theorem can be efficiently applied to the primes, and indeed, the set of primes will have the desired pseudorandom properties.

In fact, Green and Tao's proof employs the techniques applied in several known proofs of Szemerédi's theorem and exploits a dichotomy between structure and randomness. This proof is based on ideas and results from several branches of mathematics, for example, combinatorics, analytical number theory, pseudorandomness, harmonic analysis, and ergodic theory. Reingold et al. [252], and Gowers [145], independently obtained a short proof for a fundamental ingredient of this proof.

Tao and Ziegler [325] (see also [252]), via a transference principle for polynomial configurations, extended the Green-Tao theorem to cover polynomial progressions: Let $A \subset \mathcal{P}$ be a set of primes of positive relative upper density in the primes, i.e., $\limsup_{N \to \infty} |A \cap$

9

$[1, N]|/|\mathcal{P} \cap [1, N]| > 0$. Then, given any integer-valued polynomials $P_1, \ldots, P_k$ in one unknown m with vanishing constant terms, the set A contains infinitely many progressions of the form $x + P_1(m), \ldots, x + P_k(m)$ with $m > 0$ (note that the special case when the polynomials are $m, 2m, \ldots, km$ implies the previous result that there are k-APs of primes). Tao [313] proved the analogue in the Gaussian integers. Green and Tao (in view of the parallelism between the integers and the polynomials over a finite field) thought that the analogue of their theorem should be held in the setting of function fields; a result that was proved by Lê [212]: Let $\mathbb{F}_q$ be a finite field over q elements. Then for any $k > 0$, one can find polynomials $f, g \in \mathbb{F}_q[t]$, $g \not\equiv 0$ such that the polynomials $f + Pg$ are all irreducible, where P runs over all polynomials $P \in \mathbb{F}_q[t]$ of degree less than k. Moreover, such structures can be found in every set of positive relative upper density among the irreducible polynomials. The proof of this interesting theorem follows the ideas of the proof of the Green-Tao theorem very closely.

3 Sum-Product Problem: Its Generalizations and Applications

The *sum-product problem* and its generalizations constitute another vibrant area in additive combinatorics, and have led to many seminal applications to number theory, Ramsey theory, computer science, and cryptography.

Let's start with the definition of sumset, product set, and some preliminaries. We will follow closely the presentation of Tao [316]. Let A be a finite nonempty set of elements of a ring R. We define the *sumset* $A + A = \{a + b : a, b \in A\}$, and the *product set* $A \cdot A = \{a \cdot b : a, b \in A\}$. Suppose that no $a \in A$ is a zero divisor (otherwise, $A \cdot A$ may become very small, which lead to degenerate cases). Then one can easily show that $A + A$ and $A \cdot A$ will be at least as large as A. The set A may be almost closed under addition, which, for example, occurs when A is an arithmetic progression or an additive subgroup in the ring R (e.g., if $A \subset \mathbb{R}$ is an AP, then $|A + A| = 2|A| - 1$, and $|A \cdot A| \geq c|A|^{2-\varepsilon}$), or it may be almost closed under multiplication, which, for example, occurs when A is a geometric progression or a multiplicative subgroup in the ring R (e.g., if $N \subset \mathbb{R}$ is an AP and $A = \{2^n : n \in N\}$, then $|A \cdot A| = 2|A| - 1$, and $|A + A| \approx |A|^2$). Note that even if A is a dense subset of an arithmetic progression or additive subgroup (or a dense subset of an geometric progression or multiplicative subgroup), then $A + A$ (or $A \cdot A$, respectively) is still comparable in size to A. But it is difficult for A to be almost closed under addition and multiplication simultaneously, unless it is very close to a subring. The *sum-product phenomenon* says that if a finite set A is not close to a subring, then either the sumset $A + A$ or the product set $A \cdot A$ must be considerably larger than A. The reader can refer to [276] and the references therein to see some lower bounds on $|C - C|$ and $|C + C|$, where C is a convex set (a set of reals $C = \{c_1, \ldots, c_n\}$ is called *convex* if $c_{i+1} - c_i > c_i - c_{i-1}$, for all i).

In the reals setting, does there exist an $A \subset \mathbb{R}$ for which $\max\{|A + A|, |A \cdot A|\}$ is 'small'? Erdős and Szemerédi [112] gave a negative answer to this question. Actually, they proved the inequality $\max\{|A + A|, |A \cdot A|\} \geq c|A|^{1+\varepsilon}$ for a small but positive ε, where A is a subset of the reals. They also conjectured that $\max\{|A + A|, |A \cdot A|\} \geq c|A|^{2-\delta}$, for any positive δ. Much efforts have been made towards the value of ε. Elekes [109] observed that

the sum-product problem has interesting connections to problems in incidence geometry. In particular, he applied the so-called *Szemerédi-Trotter theorem* and showed that $\varepsilon \geq 1/4$, if A is a finite set of real numbers. Elekes's result was extended to complex numbers in [292]. In the case of reals, the state-of-the-art is due to Solymosi [295]: one can take ε arbitrarily close to 1/3. For complex numbers, Solymosi [293], using the Szemerédi-Trotter theorem, proved that one can take ε arbitrarily close to 3/11. Very recently, Rudnev [267], again using the Szemerédi-Trotter theorem, obtained a bound which is the state-of-the-art in the case of complex numbers: one can take ε arbitrarily close to 19/69.

Solymosi and Vu [298] proved a sum-product estimate for a special finite set of square matrices with complex entries, where that set is *well-conditioned* (that is, its matrices are far from being singular). Note that If we remove the latter condition (i.e., well-conditioned!) then the theorem will not be true; see [298, Example 1.1].

Wolff [345] motivated by the 'finite field Kakeya conjecture', formulated the finite field version of sum-product problem. The *Kakeya conjecture* says that the Hausdorff dimension of any subset of $\mathbb{R}^n$ that contains a unit line segment in every direction is equal to n; it is open in dimensions at least three. The *finite field Kakeya conjecture* asks for the smallest subset of $\mathbb{F}_q^n$ that contains a line in each direction. This conjecture was proved by Dvir [102] using a clever application of the so-called *polynomial method*; see also [101] for a nice survey on this problem and its applications especially in the area of randomness extractors. The polynomial method, which has proved to be very useful in additive combinatorics, is roughly described as the following: Given a field $\mathbb{F}$ and a finite subset $S \subset \mathbb{F}^n$. Multivariate polynomials over $\mathbb{F}$ which vanish on all points of S, usually get some combinatorial properties about S. (This has some similarities with what we usually do in algebraic geometry!) See, e.g., [197, Chapter 16] for some basic facts about the polynomial method, [102, 168, 169, 170] for applications in additive combinatorics, and [107, 167, 300] for applications in computer science.

Actually, the finite field version (of sum-product problem) becomes more difficult, because we will encounter with some difficulties in applying the Szemerédi-Trotter incidence theorem in this setting. In fact, the *crossing lemma*, which is an important ingredient in the proof of Szemerédi-Trotter theorem [302], relies on *Euler's formula* (and so on the topology of the plane), and consequently does not work in finite fields. Note that the proof that Szemerédi and Trotter presented for their theorem was somewhat complicated, using a combinatorial technique known as *cell decomposition* [305].

When working with finite fields it is important to consider fields whose order is prime and not the power of a prime; because in the latter case we can take A to be a subring which leads to the degenerate case $|A| = |A + A| = |A \cdot A|$. A stunning result in the case finite field $\mathbb{F}_p$, with p prime, was proved by Bourgain, Katz and Tao [61]. They proved the following:

if $A \subset \mathbb{F}_p$, and $p^\delta \leq |A| \leq p^{1-\delta}$ for some $\delta > 0$, then there exists $\varepsilon = \varepsilon(\delta) > 0$ such that $\max\{|A + A|, |A \cdot A|\} \geq c|A|^{1+\varepsilon}$.

This result is now known as the *sum-product theorem* for $\mathbb{F}_p$. In fact, this theorem holds if A is not too close to be the whole field. The condition $|A| \geq p^\delta$ in this theorem was removed by Bourgain, Glibichuk, and Konyagin in [59]. Also, note that the condition $|A| \leq p^{1-\delta}$ is necessary (e.g., if we consider a set A consisting of all elements of the field except one, then $\max\{|A + A|, |A \cdot A|\} = |A| + 1$). The idea for the proof of this theorem is by contradiction;

11

assume that $|A + A|$ and $|A \cdot A|$ are close to $|A|$ and conclude that A is behaving very much like a subfield of $\mathbb{F}_p$. Sum-product estimates for rational functions (i.e., the results that one of $A + A$ or $f(A)$ is substantially larger than A, where f is a rational function) have also been treated (see, e.g., [19, 70]). Also, note that problems of the kind 'interaction of summation and addition' are very important in various contexts of additive combinatorics and have very interesting applications (see [16, 130, 135, 136, 170, 191, 243, 253]).

Garaev [126] proved the first quantitative sum-product estimate for fields of prime order: Let $A \subset \mathbb{F}_p$ such that $1 < |A| < p^{7/13} \log^{-4/13} p$. Then

$$\max\{|A + A|, |A \cdot A|\} \gg \frac{|A|^{15/14}}{\log^{2/7} |A|}.$$

Garaev's result was extended and improved by several authors. Rudnev [266] proved the following: Let $A \subset \mathbb{F}_p^*$ with $|A| < \sqrt{p}$ and p large. Then

$$\max\{|A + A|, |A \cdot A|\} \gg \frac{|A|^{12/11}}{\log^{4/11} |A|}.$$

Li and Roche-Newton [215] proved a sum-product estimate for subsets of a finite field whose order is not prime: Let $A \subset \mathbb{F}_{p^n}$ with $|A \cap cG| \leq |G|^{1/2}$ for any subfield G of $\mathbb{F}_{p^n}$ and any element $c \in \mathbb{F}_{p^n}$. Then

$$\max\{|A + A|, |A \cdot A|\} \gg \frac{|A|^{12/11}}{\log_2^{5/11} |A|}.$$

See also [56, 127, 128, 201, 202, 214, 282, 284] for other generalizations and improvements of Garaev's result. As an application, Shparlinski [290] using Rudnev's result [266], estimates the cardinality, $\#\Gamma_p(T)$, of the set

$$\Gamma_p(T) = \{\gamma \in \mathbb{F}_p \ : \ \mathrm{ord}\,\gamma \leq T \text{ and } \mathrm{ord}(\gamma + \gamma^{-1}) \leq T\},$$

where $\mathrm{ord}\,\gamma$ (multiplicative order of γ) is the smallest positive integer t with $\gamma^t = 1$.

Tóth [328] generalized the Szemerédi-Trotter theorem to complex points and lines in $\mathbb{C}^2$ (also see [347] for a different proof of this result, and a sharp result in the case of $\mathbb{R}^4$). As another application of the sum-product theorem, Bourgain, Katz and Tao [61] (also see [38]) derived an important Szemerédi-Trotter type theorem in prime finite fields (but did not quantify it):

If $\mathbb{F}_p$ is a prime field, and $\mathcal{P}$ and $\mathcal{L}$ are points and lines in the projective plane over $\mathbb{F}_p$ with cardinality $|\mathcal{P}|, |\mathcal{L}| \leq N < p^\alpha$ for some $0 < \alpha < 2$, then $\left|\{(p, l) \in \mathcal{P} \times \mathcal{L} \ : \ p \in l\}\right| \leq CN^{3/2-\varepsilon}$, for some $\varepsilon = \varepsilon(\alpha) > 0$.

Note that it is not difficult to generalize this theorem from prime finite fields to every finite field that does not contain a large subfield. The first quantitative Szemerédi-Trotter type theorem in prime finite fields was obtained by Helfgott and Rudnev [185]. They showed that $\varepsilon \geq 1/10678$, when $|\mathcal{P}| = |\mathcal{L}| < p$. (Note that this condition prevents P from being the entire plane $\mathbb{F}_p^2$.) This result was extended to general finite fields (with a slightly weaker exponent) by Jones [193]. Also, Jones [194, 196] improved the result of Helfgott and Rudnev [185] by replacing $1/10678$ with $1/806 - o(1)$, and $1/662 - o(1)$, respectively. A near-sharp

12

generalization of the Szemerédi-Trotter theorem to higher dimensional points and varieties was obtained in [297].

Using ideas from additive combinatorics (in fact, combining the techniques of cell decomposition and polynomial method in a novel way), Guth and Katz [170], achieved a near-optimal bound for the *Erdős distinct distance problem* in the plane. They proved that a set of N points in the plane has at least $c\frac{N}{\log N}$ distinct distances (see also [131] for some techniques and ideas related to this problem).

Hart, Iosevich, and Solymosi [179] obtained a new proof of the sum-product theorem based on incidence theorems for hyperbolas in finite fields which is achieved through some estimates on Kloosterman exponential sums. Some other results related to the incidence theorems can be found in [95, 178].

The sum-product theorem has a plethora of deep applications to various areas such as incidence geometry [30, 38, 61, 85, 86, 191, 195, 253, 309, 342, 343], analysis [79, 125, 180, 309], PDE [309], group theory [62, 67, 133, 134, 183, 184, 190, 206], exponential and character sums [18, 36, 37, 38, 39, 40, 42, 45, 46, 47, 48, 57, 58, 59, 81, 129], number theory [17, 18, 42, 46, 54, 55, 81, 84, 89, 90, 91, 243], combinatorics [20, 62, 53, 309], expanders [38, 52, 53, 54, 55, 62, 66, 206, 283, 342], extractors [19, 20, 38, 41, 88, 103, 182, 346], dispersers [20], complexity theory [39], pseudorandomness [33, 38, 227], property testing [137, 270], hardness amplification [338, 340], probabilistic checkable proofs (PCPs) [271], and cryptography [36, 37, 75, 121].

A sum-product problem associated with a graph was initiated by Erdős and Szemerédi [112]. Alon et al. [4] studied the sum-product theorems for sparse graphs, and obtained some nice results when the graph is a matching.

Let us ask does there exist any connection between the 'sum-product problem' and 'spectral graph theory'? Surprisingly, the answer is yes! In fact, the first paper that introduced and applied the spectral methods to estimate sum-product problems (and even more general problems) is the paper by Vu [342] (see also [180], in which Fourier analytic methods were used to generalize the results by Vu). In his elegant paper, Vu relates the sum-product bound to the expansion of certain graphs, and then via the relation of the spectrum (second eigenvalue) and expansion one can deduce a rather strong bound. Vinh [336] (also see [337]), using ideas from spectral graph theory, derived a Szemerédi-Trotter type theorem in finite fields, and from there obtained a different proof of Garaev's result [128] on sum-product estimate for large subsets of finite fields. Also, Solymosi [294] applied techniques from spectral graph theory and obtained estimates similar to those of Garaev [126] that already followed via tools from exponential sums and Fourier analysis. One important ingredient in Solymosi's method [294] is the well-known *Expander Mixing Lemma* (see, e.g., [186]), which roughly speaking, states that on graphs with good expansion, the edges of the graphs are well-distributed, and in fact, the number of edges between any two vertex subsets is about what one would expect for a random graph of that edge density.

The generalizations of the sum-product problem to polynomials, elliptic curves, and also the exponentiated versions of the problem in finite fields were obtained in [3, 19, 70, 97, 130, 285, 288, 289, 342]. Also, the problem in the commutative integral domain (with characteristic zero) setting was considered in [343]. Some other generalizations to algebraic division algebras and algebraic number fields were treated in [50, 80]. Tao [317] settled the

sum-product problem in arbitrary rings.

As we already mentioned, the sum-product theorem is certainly not true for matrices over $\mathbb{F}_p$. However, Helfgott [183] proves that the theorem is true for $A \subset SL_2(\mathbb{F}_p)$. In particular, the set $A \cdot A \cdot A$ is much larger than A (more precisely, $|A \cdot A \cdot A| > |A|^{1+\varepsilon}$, where $\varepsilon > 0$ is an absolute constant), unless A is contained in a proper subgroup. Helfgott's theorem has found several applications, for instance, in some nonlinear sieving problems [55], in the spectral theory of Hecke operators [125], and in constructing expanders via Cayley graphs [53]. Underlying this theorem is the sum-product theorem. Very recently, Kowalski [206] obtained explicit versions of Helfgott's growth theorem for SL_2. Helfgott [184] proves his result when $A \subset SL_3(\mathbb{F}_p)$, as well. Gill and Helfgott [133] generalized Helfgott's theorem to $SL_n(\mathbb{F}_p)$, when A is small, that is, $|A| \leq p^{n+1-\delta}$, for some $\delta > 0$. The study of growth inside solvable subgroups of $GL_r(\mathbb{F}_p)$ is done in [134]. Breuillard, Green, and Tao [67], and also Pyber and Szabó [248], independently and simultaneously, generalized Helfgott's theorem to $SL_n(\mathbb{F})$, (n arbitrary, $\mathbb{F}$ arbitrary finite field), and also to some other simple groups, as part of a more general result for groups of bounded Lie rank; see also [190].

Let us ask does there exist a 'sum-division theory'? Solymosi [295] using the concept of *multiplicative energy* proved the following: If A is a finite set of positive real numbers, then

$$|A + A|^2|A \cdot A| \geq \frac{|A|^4}{4\lceil \log_2 |A| \rceil}.$$

Solymosi's result also gives

$$|A + A|^2|A/A| \geq \frac{|A|^4}{4\lceil \log_2 |A| \rceil}.$$

Li and Shen [216] removed the term $\lceil \log_2 |A| \rceil$ in the denominator. In fact, they proved the following: If A is a finite set of positive real numbers, then

$$|A + A|^2|A/A| \geq \frac{|A|^4}{4},$$

which concludes that

$$\max\{|A + A|, |A/A|\} \geq \frac{|A|^{4/3}}{2}.$$

One may ask about a 'difference-product theory'. The work of Solymosi [293] considers this type, but the state-of-the-art not only for this type but also for all combinations of addition, multiplication, subtraction and division in the case of complex numbers is due to Rudnev [267].

As we already mentioned, Rudnev [266] proved

$$\max\{|A + A|, |A \cdot A|\} \gg \frac{|A|^{12/11}}{\log^{4/11} |A|},$$

where $A \subset \mathbb{F}_p^*$ with $|A| < \sqrt{p}$ and p large. In Remark 2 of his paper, Rudnev [266], mentions an interesting fact: "one can replace either one or both the product set $A \cdot A$ with the ratio

set A/A – in which case the logarithmic factor disappears – and the sumset $A + A$ with the difference set $A - A$"!

The sum-product problem can be applied efficiently to construct *randomness extractors* [19, 20, 38, 41, 88, 103, 182, 346]. Inspired by this fact, we are going to discuss some properties and applications of randomness extractors here. First, note that all cryptographic protocols and in fact, many problems that arise in cryptography, algorithm design, distributed computing, and so on, rely completely on randomness and indeed are impossible to solve without access to it.

A *randomness extractor* is a deterministic polynomial-time computable algorithm that computes a function $\mathsf{Ext} : \{0,1\}^n \to \{0,1\}^m$, with the property that for any defective source of randomness X satisfying minimal assumptions, $\mathsf{Ext}(X)$ is close to being uniformly distributed. In other words, a randomness extractor is an algorithm that transforms a weak random source into an almost uniformly random source. Randomness extractors are interesting in their own right as combinatorial objects that "appear random" in many strong ways. They fall into the class of "pseudorandom" objects. *Pseudorandomness* is the theory of efficiently generating objects that "appear random" even though they are constructed with little or no true randomness; see [331, 334, 335] (and also the surveys [279, 280]). Error correcting codes, hardness amplifiers, epsilon biased sets, pseudorandom generators, expander graphs, and Ramsey graphs are of other such objects. (Roughly speaking, an *expander* is a highly connected sparse finite graph, i.e., every subset of its vertices has a large set of neighbors. Expanders have a great deal of seminal applications in many disciplines such as computer science and cryptography; see [186, 229] for two excellent surveys on this area and its applications.) Actually, when studying large combinatorial objects in additive combinatorics, a helpful (and easier) procedure is to decompose them into a 'structured part' and a 'pseudorandom part'.

Constructions of randomness extractors have been used to get constructions of communication networks and good expander graphs [76, 344], error correcting codes [166, 327], cryptographic protocols [228, 333], data structures [235] and samplers [349]. Randomness extractors are widely used in cryptographic applications (see, e.g., [25, 87, 99, 100, 199, 200, 218, 348]). This includes applications in construction of pseudorandom generators from one-way functions, design of cryptographic functionalities from noisy and weak sources, construction of key derivation functions, and extracting many private bits even when the adversary knows all except $\log^{\Omega(1)} n$ of the n bits [251] (see also [250]). They also have remarkable applications to quantum cryptography, where photons are used by the randomness extractor to generate secure random bits [279].

Ramsey graphs (that is, graphs that have no large clique or independent set) have strong connections with extractors for two sources. Using this approach, Barak et al. [21] presented an explicit Ramsey graph that does not have cliques and independent sets of size $2^{\log^{o(1)} n}$, and ultimately beating the Frankl-Wilson construction!

Acknowledgements

References

[1] D. Achlioptas, Random matrices in data analysis, In *Proc. of ECML '04*, 2004, pp. 1–8.

[2] D. Achlioptas, A. Naor, and Y. Peres, Rigorous location of phase transitions in hard optimization problems, *Nature* 435 (2005), 759–764.

[3] O. Ahmadi and I. E. Shparlinski, Bilinear character sums and the sum-product problem on elliptic curves, *Proc. Edinburgh Math. Soc.* 53 (2010), 1–12.

[4] N. Alon, O. Angel, I. Benjamini, and E. Lubetzky, Sums and products along sparse graphs, *Israel J. Math.* 188 (2012), 353–384.

[5] N. Alon, J. Balogh, R. Morris, and W. Samotij, Counting sum-free sets in Abelian groups, arXiv/1201.6654, (2012).

[6] N. Alon, J. Balogh, R. Morris, and W. Samotij, A refinement of the Cameron-Erdős conjecture, arXiv/1202.5200, (2012).

[7] N. Alon, E. Fischer, I. Newman, and A. Shapira, A combinatorial characterization of the testable graph properties: It's all about regularity, *SIAM J. Comput.* 39(1) (2009), 143–167.

[8] N. Alon and A. Shapira, Homomorphisms in graph property testing - A survey, In Topics in Discrete Mathematics, volume 26 of Algorithms and Combinatorics, pp. 281–313. Springer, (2006).

[9] N. Alon and A. Shapira, A characterization of the (natural) graph properties testable with one-sided error, *SIAM J. Comput.* 37(6) (2008), 1703–1727.

[10] N. Alon and A. Shapira, Every monotone graph property is testable, *SIAM J. Comput.* 38(2) (2008), 505–522.

[11] T. Austin, Deducing the multidimensional Szemerédi theorem from an infinitary removal lemma, *J. Anal. Math.* 111 (2010), 131–150.

[12] T. Austin, Deducing the density Hales-Jewett theorem from an infinitary removal lemma, *J. Theoret. Probab.* 24(3) (2011), 615–633.

[13] T. Austin and T. Tao, Testability and repair of hereditary hypergraph properties, *Random Structures Algorithms* 36(4) (2010), 373–463.

[14] P. Austrin and E. Mossel, Noise correlation bounds for uniform low degree functions, *Ark. Mat.*, to appear.

[15] P. Balister and B. Bollobás, Projections, entropy and sumsets, *Combinatorica* 32(2) (2012), 125–141.

[16] A. Balog, Another sum-product estimate in finite fields, preprint, (2012).

[17] A. Balog, K. A. Broughan, and I. E. Shparlinski, On the number of solutions of exponential congruences, *Acta Arith.* 148(1) (2011), 93–103.

[18] A. Balog, K. A. Broughan, and I. E. Shparlinski, Sum-products estimates with several sets and applications, *Integers*, to appear.

[19] B. Barak, R. Impagliazzo, and A. Wigderson, Extracting randomness using few independent sources, *SIAM J. Comput.* 36(4) (2006), 1095–1118.

[20] B. Barak, G. Kindler, R. Shaltiel, B. Sudakov, and A. Wigderson, Simulating independence: new constructions of condensers, Ramsey graphs, dispersers, and extractors, *J. ACM* 57(4) (2010), Art. 20, 52 pp.

[21] B. Barak, A. Rao, R. Shaltiel, and A. Wigderson, 2-source dispersers for subpolynomial entropy and Ramsey graphs beating the Frankl-Wilson construction, In *Proc. 38th Annu. ACM Symp. Theory Comput (STOC '06)*, 2006, pp. 671–680.

[22] M. Bateman and N. H. Katz, New bounds on cap sets, *J. Amer. Math. Soc.* 25 (2012), 585–613.

[23] M. Bateman and N. H. Katz, Structure in additively nonsmoothing sets, arXiv/1104.2862, (2011).

[24] F. A. Behrend, On the sets of integers which contain no three in arithmetic progression, *Proc. Nat. Acad. Sci.* 23 (1946), 331–332.

[25] M. Bellare, S. Tessaro, and A. Vardy, A cryptographic treatment of the wiretap channel, arXiv/1201.2205, (2012).

[26] E. Ben-Sasson and S. Kopparty, Affine dispersers from subspace polynomials, In *Proc. 41st Annu. ACM Symp. Theory Comput (STOC '09)*, 2009, pp. 65–74.

[27] E. Ben-Sasson, S. Lovett, and N. Zewi, An additive combinatorics approach to the log-rank conjecture in communication complexity, arXiv/1111.5884, (2011).

[28] E. Ben-Sasson and N. Zewi, From affine to two-source extractors via approximate duality, In *Proc. 43rd Annu. ACM Symp. Theory Comput. (STOC '11)*, 2011, pp. 177–186.

[29] V. Bergelson, A. Leibman, and E. Lesigne, Intersective polynomials and the polynomial Szemerédi theorem, *Adv. Math.* 219 (2008), 369–388.

[30] A. Bhattacharyya, Z. Dvir, A. Shpilka, and S. Saraf, Tight lower bounds for 2-query LCCs over finite fields, In *Proc. 52nd Annu. IEEE Symp. Found. Comput. Sci. (FOCS '11)*, 2011, pp. 638–647.

[31] A. Bhattacharyya, E. Grigorescu, and A. Shapira, A unified framework for testing linear-invariant properties, In *Proc. 51st Annu. IEEE Symp. Found. Comput. Sci. (FOCS '10)*, 2010, pp. 478–487.

[32] T. Bloom, Translation invariant equations and the method of Sanders, arXiv/1107.1110, (2011).

[33] A. Bogdanov and E. Viola, Pseudorandom bits for polynomials, In *Proc. 48th Annu. IEEE Symp. Found. Comput. Sci. (FOCS '07)*, 2007, pp. 41–51.

[34] B. Bollobás and O. Riordan, The critical probability for random Voronoi percolation in the plane is 1/2, *Probab Theor Related Fields* 136 (2006), 417–468.

[35] J. Bourgain, On triples in arithmetic progression, *Geom. Funct. Anal.* 9 (1999), 968–984.

[36] J. Bourgain, New bounds on exponential sums related to the Diffie-Hellman distributions, *C. R. Math. Acad. Sci.* Paris 338(11) (2004), 825–830.

[37] J. Bourgain, Estimates on exponential sums related to the Diffie-Hellman distributions, *Geom. Funct. Anal.* 15 (2005), 1–34.

[38] J. Bourgain, More on sum-product phenomenon in prime fields and its applications, *Int. J. Number Theory* 1 (2005), 1–32.

[39] J. Bourgain, Estimation of certain exponential sums arising in complexity theory, *C. R. Math. Acad. Sci.* Paris 340(9) (2005), 627–631.

[40] J. Bourgain, Mordell's exponential sum estimate revisited, *J. Amer. Math. Soc.* 18(2) (2005), 477–499.

[41] J. Bourgain, On the construction of affine extractors, *Geom. Funct. Anal.* 17(1) (2007), 33–57.

[42] J. Bourgain, Some arithmetical applications of the sum-product theorems in finite fields, In Geometric aspects of functional analysis, Lecture Notes in Math., Springer, 2007, pp. 99–116.

[43] J. Bourgain, Roth's theorem on progressions revisited, *J. Anal. Math.*, 104 (2008), 155–192.

[44] J. Bourgain, Expanders and dimensional expansion, *C. R. Acad. Sci. Paris, Ser. I* 347 (2009), 357–362.

[45] J. Bourgain, Multilinear exponential sums in prime fields under optimal entropy condition on the sources, *Geom. Funct. Anal.* 18(5) (2009), 1477–1502.

[46] J. Bourgain, The sum-product phenomenon and some of its applications, In Analytic number theory, Cambridge Univ. Press, 2009, pp. 62–74.

[47] J. Bourgain, Sum-product theorems and applications, In Additive Number Theory, Springer, (2010), 9–38.

[48] J. Bourgain and M.-C. Chang, Sum-product theorem and exponential sum estimates, *C. R. Acad. Sci. Paris, Ser. I* 339 (2004), 463–466.

[49] J. Bourgain and M.-C. Chang, A Gauss sum estimate in arbitrary finite fields, *C.R. Math. Acad. Sci. Paris* 342(9) (2006), 643–646.

[50] J. Bourgain and M.-C. Chang, Sum-product theorems in algebraic number fields, *J. Anal. Math.* 109 (2009), 253–277.

[51] J. Bourgain, S. Dilworth, K. Ford, S. Konyagin, and D. Kutzarova, Explicit constructions of RIP matrices and related problems, *Duke Math. J.* 159(1) (2011), 145–185.

[52] J. Bourgain and A. Gamburd, New results on expanders, *Comptes Rendus Acad. Sci. Paris, Ser. I* 342 (2006), 717–721.

[53] J. Bourgain and A. Gamburd, Uniform expansion bounds for Cayley graphs of $SL_2(\mathbb{F}_p)$, *Ann. of Math.* 167(2) (2008), 625–642.

[54] J. Bourgain, A. Gamburd, and P. Sarnak, Sieving and expanders, *Comptes Rendus Acad. Sci.* Paris, Ser. I 343 (2006), 155–159.

[55] J. Bourgain, A. Gamburd, and P. Sarnak, Affine linear sieve, expanders, and sum-product, *Invent. Math.* 179(3) (2010), 559–644.

[56] J. Bourgain and M. Garaev, On a variant of sum-product estimates and exponential sum bounds in prime fields, *Math. Proc. Cambridge Philos. Soc.* 146 (2009), 1–21.

[57] J. Bourgain, M. Z. Garaev, S. V. Konyagin, and I. E. Shparlinski, On the hidden shifted power problem, arXiv/1110.0812, (2011).

[58] J. Bourgain, M. Z. Garaev, S. V. Konyagin, and I. E. Shparlinski, On congruences with products of variables from short intervals and applications, arXiv/1203.0017, (2012).

[59] J. Bourgain, A. A. Glibichuk, and S. V. Konyagin, Estimates for the number of sums and products and for exponential sums in fields of prime order, *J. London Math. Soc.* 73(2) (2006), 380–398.

[60] J. Bourgain and G. Kalai, Influences of variables and threshold intervals under group symmetries, *Geom. Funct. Anal.* 7 (1997), 438–461.

[61] J. Bourgain, N. Katz, and T. Tao, A sum-product estimate in finite fields, and applications, *Geom. Funct. Anal.* 14 (2004), 27–57.

[62] J. Bourgain and P. P. Varjú, Expansion in $SL_d(\mathbb{Z}/q\mathbb{Z})$, q arbitrary, *Invent. Math.* 188(1) (2012), 151–173.

[63] J. Bourgain and A. Yehudayoff, Monotone expansion, In *Proc. 44th Annu. ACM Symp. Theory Comput (STOC '12)*, 2012, pp. 1061–1078.

[64] E. Breuillard and B. Green, Approximate groups, I: The torsion-free nilpotent case, *J. Inst. Math. Jussieu* 10(1) (2011), 37–57.

[65] E. Breuillard and B. Green, Approximate groups, II: The solvable linear case, *Quart. J. Math.* 62(3) (2011), 513–521.

[66] E. Breuillard, B. Green, and T. Tao, Suzuki groups as expanders, *Groups Geom. Dyn.* 5 (2011), 281–299.

[67] E. Breuillard, B. Green, and T. Tao, Approximate subgroups of linear groups, *Geom. Funct. Anal.* 21(4) (2011), 774–819.

[68] E. Breuillard, B. Green, and T. Tao, The structure of approximate groups, arXiv/1110.5008, (2011).

[69] É. Brezin, V. Kazakov, D. Serban, P. Wiegmann, A. Zabrodin (eds.), Applications of random matrices in physics (NATO Sci. Ser. II Math. Phys. Chem.), 221, Springer, 2006.

[70] B. Bukh and J. Tsimerman, Sum-product estimates for rational functions, *Proc. Lond. Math. Soc.* 104(1) (2012), 1–26.

[71] E. J. Candès, The restricted isometry property and its implications for compressed sensing, *C. R. Math. Acad. Sci. Paris* 346 (2008), 589–592.

[72] E. J. Candès, J. K. Romberg, and T. Tao, Stable signal recovery from incomplete and inaccurate measurements, *Comm. Pure Appl. Math.* 59 (2006), 1207–1223.

[73] E. J. Candès and T. Tao, Decoding by linear programming, *IEEE Trans. Inform. Theory* 51 (2005), 4203–4215.

[74] E. Candès and T. Tao, Near-optimal signal recovery from random projections: universal encoding strategies?, *IEEE Trans. Inform. Theory* 52 (2006), 5406–5425.

[75] R. Canetti, J. Friedlander, S. Konyagin, M. Larsen, D. Lieman, and I. E. Shparlinski, On the statistical properties of Diffie-Hellman distributions, *Israel J. Math.* 120 (2000), part A, 23–46.

[76] M. Capalbo, O. Reingold, S. Vadhan, and A. Wigderson, Randomness conductors and constant-degree lossless expanders, In *Proc. 34th Annu. ACM Symp. Theory Comput (STOC '02)*, 2002, pp. 659–668.

[77] R. Chaabouni, H. Lipmaa, and A. Shelat, Additive combinatorics and discrete logarithm based range protocols, In *Proc. ACISP '10*, Sydney, Australia, July 5–7, 2010, Lecture Notes in Comput. Sci., Springer, 6168 (2010), pp. 336–351.

[78] M.-C. Chang, A polynomial bound in Freiman's theorem, *Duke Math. J.* 113(3) (2002), 399–419.

[79] M.-C. Chang, A sum-product theorem in semi-simple commutative Banach algebras, *J. Funct. Anal.* 212 (2004), 399–430.

[80] M.-C. Chang, A sum-product estimate in algebraic division algebras, *Israel J. Math.* 150 (2005), 369–380.

[81] M.-C. Chang, On sum-product representations in $\mathbb{Z}_q$, *J. Eur. Math. Soc. (JEMS)* 8(3) (2006), 435–463.

[82] M.-C. Chang, Additive and multiplicative structure in matrix spaces, *Combin. Probab. Comput.* 16(2) (2007), 219–238.

[83] M.-C. Chang, On a matrix product question in cryptography, preprint, (2012).

[84] M.-C. Chang, J. Cilleruelo, M. Z. Garaev, J. Hernández, I. E. Shparlinski, and A. Zumalacárregui, Points on curves in small boxes and applications, arXiv/1111.1543, (2011).

[85] M.-C. Chang and J. Solymosi, Sum-product theorems and incidence geometry, *J . Eur. Math. Soc. (JEMS)* 9(3) (2007), 545–560.

[86] J. Chapman, M. B. Erdoğan, D. Hart, A. Iosevich, and D. Koh, Pinned distance sets, k-simplices, Wolff's exponent in finite fields and sum-product estimates, *Math. Z.* 271(1-2) (2012), 63–93.

[87] C. Chevalier, P.-A. Fouque, D. Pointcheval, and S. Zimmer, Optimal randomness extraction from a Diffie-Hellman element, *Advances in Cryptology Proc. of Eurocrypt '09*, A. Joux Ed., Springer-Verlag, LNCS 5479, (2009), pp. 572–589.

[88] B. Chor and O. Goldreich, Unbiased bits from sources of weak randomness and probabilistic communication complexity, *SIAM J. Comput.* 17(2) (1988), 230–261.

[89] J. Cilleruelo and M. Z. Garaev, Concentration of points on two and three dimensional modular hyperbolas and applications, *Geom. Func. Anal.* 21 (2011), 892–904.

[90] J. Cilleruelo, M. Z. Garaev, A. Ostafe, and I. E. Shparlinski, On the concentration of points of polynomial maps and applications, *Math. Z.*, to appear.

[91] J. Cilleruelo, I. E. Shparlinski, and A. Zumalacárregui, Isomorphism classes of elliptic curves over a finite field in some thin families, *Math. Res. Letters*, to appear.

[92] D. Conlon and J. Fox, Bounds for graph regularity and removal lemmas, *Geom. Funct. Anal.*, to appear.

[93] D. Conlon, J. Fox, and Y. Zhao, Extremal results in sparse pseudorandom graphs, arXiv/1204.6645, (2012).

[94] D. Conlon and W. T. Gowers, Combinatorial theorems in sparse random sets, arXiv/1011.4310, (2010).

[95] D. Covert, D. Hart, A. Iosevich, D. Koh, and M. Rudnev, Generalized incidence theorems, homogeneous forms and sum-product estimates in finite fields, *European J. Combin.* 31(1) (2010), 306–319.

[96] E. Croot and V. F. Lev, Open problems in additive combinatorics, In Additive combinatorics, volume 43 of CRM Proc. Lecture Notes, Amer. Math. Soc., 2007, pp. 207–233.

[97] E. Croot and D. Hart, On sums and products in $\mathbb{C}[x]$, *Ramanujan J.* 22 (2010), 33–54.

[98] E. Croot and O. Sisask, A probabilistic technique for finding almost-periods of convolutions, *Geom. Funct. Anal.* 20 (2010), 1367–1396.

[99] D. Dachman-Soled, R. Gennaro, H. Krawczyk, and T. Malkin, Computational extractors and pseudorandomness, In *Proc. 9th Int. Conf. Theory Cryptogr. (TCC '12)*, 2012, pp. 383–403.

[100] Y. Dodis and D. Wichs, Non-malleable extractors and symmetric key cryptography from weak secrets, In *Proc. 41st Annu. ACM Symp. Theory Comput (STOC '09)*, 2009, pp. 601–610.

[101] Z. Dvir, From randomness extraction to rotating needles, *SIGACT News* 40(4) (2009), 46–61.

[102] Z. Dvir, On the size of Kakeya sets in finite fields, *J. Amer. Math. Soc.* 22(4) (2009), 1093–1097.

[103] Z. Dvir, A. Gabizon, and A. Wigderson, Extractors and rank extractors for polynomial sources, *Comput. Complex.* 18 (2009), 1–58.

[104] Z. Dvir, S. Kopparty, S. Saraf, and M. Sudan, Extensions to the method of multiplicities, with applications to kakeya sets and mergers, In *Proc. 50th Annu. IEEE Symp. Found. Comput. Sci. (FOCS '09)*, 2009, pp. 181–190.

[105] Z. Dvir and A. Shpilka, Towards dimension expanders over finite fields, *Combinatorica* 31(3) (2011), 305–320.

[106] Z. Dvir and A. Wigderson, Monotone expanders: Constructions and applications, *Theory Comput.* 6(1) (2010), 291–308.

[107] Z. Dvir and A. Wigderson, Kakeya sets, new mergers, and old extractors, *SIAM J. Comput.* 40(3) (2011), 778–792.

[108] M. Einsiedler and T. Ward, Ergodic theory: with a view towards number theory, Springer, (2010).

[109] G. Elekes, On the number of sums and products, *Acta Arith.* 81 (1997), 365–367.

[110] M. Elkin, An improved construction of progression-free sets, *Israel J. Math.* 184 (2011), 93–128.

[111] P. Erdős, P. Frankl, and V. Rödl, The asymptotic number of graphs not containing a fixed subgraph and a problem for hypergraphs having no exponent, *Graphs Combin.* 2 (1986), 113–121.

[112] P. Erdős and E. Szemerédi, On sums and products of integers, Studies in pure mathematics, Birkhäuser, (1983), pp. 213–218.

[113] P. Erdős and P. Turán, On some sequences of integers, *J. Lond. Math. Soc.* 11 (1936), 261–264.

[114] R. Ferguson, C. Hoffman, F. Luca, A. Ostafe, and I. E. Shparlinski, Some additive combinatorics problems in matrix rings, *Rev. Mat. Complut.* (2010), 1–13.

[115] J. Fox, A new proof of the graph removal lemma, *Ann. Math.* 174(1) (2011), 561–579.

[116] G. A. Freiman, *Foundations of a structural theory of set addition*, Translated from the Russian. Translations of Mathematical Monographs, Vol. 37, Amer. Math. Soc., Providence, RI, 1973.

[117] G. A. Freiman, D. Grynkiewicz, O. Serra, and Y. V. Stanchescu, Inverse additive problems for Minkowski sumsets I, *Collect. Math.*, to appear.

[118] G. A. Freiman, D. Grynkiewicz, O. Serra, and Y. V. Stanchescu, Inverse additive problems for Minkowski sumsets II, *J. Geom. Anal.*, to appear.

[119] E. Friedgut, Hunting for sharp thresholds, *Random Structures Algorithms* 26(1-2) (2005), 37–51.

[120] E. Friedgut, V. Rödl, A. Ruciński, and P. Tetali, A sharp threshold for random graphs with a monochromatic triangle in every edge coloring, *Mem. Amer. Math. Soc.* 179(845) (2006) vi+66 pp.

[121] J. B. Friedlander, S. Konyagin, and I. E. Shparlinski, Some doubly exponential sums over $\mathbb{Z}_m$, *Acta Arith.* 105(4) (2002), 349–370.

[122] H. Furstenberg, Ergodic behaviour of diagonal measures and a theorem of Szemerédi on arithmetic progressions, *J. Anal. Math.* 31 (1977), 204–256.

[123] H. Furstenberg and Y. Katznelson, An ergodic Szemerédi theorem for commuting transformations, *J. Anal. Math.* 34 (1978), 275–291.

[124] H. Furstenberg and Y. Katznelson, A density version of the Hales-Jewett theorem, *J. Anal. Math.* 57 (1991), 64–119.

[125] A. Gamburd, D. Jakobson, and P. Sarnak, Spectra of elements in the group ring of $SU(2)$, *J. Eur. Math. Soc.* 1 (1999), 51–85.

[126] M. Z. Garaev, An explicit sum-product estimate in $\mathbb{F}_p$, *Int. Math. Res. Not.* Vol. 2007 (2007), Article ID rnm035, 11 pages.

[127] M. Z. Garaev, A quantified version of Bourgain's sum-product estimate in $\mathbb{F}_p$ for subsets of incomparable sizes, *Electron. J. Combin.* 15 (2008), Article #R58.

[128] M. Z. Garaev, The sum-product estimate for large subsets of prime fields, *Proc. Amer. Math. Soc.* 136 (2008), 2735–2739.

[129] M. Z. Garaev, Sums and products of sets and estimates of rational trigonometric sums in fields of prime order, *Russ. Math. Surv.* 65(4) (2010), 599–658.

[130] M. Z. Garaev and C.-Y. Shen, On the size of the set $A(A + 1)$, *Math. Z.* 265 (2010), 125–132.

[131] J. Garibaldi, A. Iosevich, and S. Senger, *The Erdős distance problem*, Amer. Math. Soc., Providence, RI, 2011.

[132] W. Gasarch, C. Kruskal, and A Parrish, Purely combinatorial proofs of van der Waerden-type theorems, Draft book, (2010).

[133] N. Gill and H. Helfgott, Growth of small generating sets in $SL_n(\mathbb{Z}/p\mathbb{Z})$, *Int. Math. Res. Not.* Vol. 2010 (2010), Article ID rnq244, 26 pages.

[134] N. Gill and H. Helfgott, Growth in solvable subgroups of $GL_r(\mathbb{Z}/p\mathbb{Z})$, arXiv/1008.5264, (2010).

[135] A. A. Glibichuk, Sums of powers of subsets of an arbitrary finite field, *Izv. Math.* 75 (2) (2011), 253–285.

[136] A. A. Glibichuk and M. Rudnev, On additive properties of product sets in an arbitrary finite field, *J. Anal. Math.* 108 (2009), 159–170.

[137] O. Goldreich (Ed.), Property testing: current research and surveys, Lecture Notes in Comput. Sci., Springer, 6390 (2010).

[138] O. Goldreich, S. Goldwasser, and D. Ron, Property testing and its connection to learning and approximation, *J. ACM* 45(4) (1998), 653–750.

[139] D. A. Goldston and C. Y. Yildirim, Higher correlations of divisor sums related to primes I: Triple correlations, *Integers* 3 (2003), paper A5.

[140] D. A. Goldston and C. Y. Yildirim, Higher correlations of divisor sums related to primes III: small gaps between primes, *Proc. London Math. Soc.* 95(3) (2007), 653–686.

[141] G. Golub, M. Mahoney, P. Drineas, and L. H. Lim, Bridging the gap between numerical linear algebra, theoretical computer science, and data applications, *SIAM News* 9(8) (2006).

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

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

[144] W. T. Gowers, Hypergraph regularity and the multidimensional Szemerédi theorem, *Ann. Math.* (2) 166(3) (2007), 897–946.

[145] W. T. Gowers, Decompositions, approximate structure, transference, and the Hahn-Banach theorem, *Bull. London Math. Soc.* 42 (2010), 573–606.

[146] W. T. Gowers and J. Wolf, Linear forms and higher-degree uniformity for functions on $\mathbb{F}_p^n$, *Geom. Funct. Anal.* 21 (2011), 36–69.

[147] W. T. Gowers and J. Wolf, Linear forms and quadratic uniformity for functions on $\mathbb{F}_p^n$, *Mathematika* 57(2)(2012), 215–237.

[148] W. T. Gowers and J. Wolf, Linear forms and quadratic uniformity for functions on $\mathbb{Z}_N$, *J. Anal. Math.* 115 (2011), 121–186.

[149] R. L. Graham, B. L. Rothschild, and J. H. Spencer, Ramsey theory, 2nd Ed., John Wiley & Sons, (1990).

[150] B. Green, Finite field models in arithmetic combinatorics, In Surveys in combinatorics, London Math. Soc. Lecture Notes, 327 (2005), pp. 1–27.

[151] B. Green, Approximate groups and their applications: work of Bourgain, Gamburd, Helfgott and Sarnak, *Current Events Bulletin of the AMS*, 25 pp., 2010.

[152] B. Green and I. Ruzsa, Freiman's theorem in an arbitrary Abelian group, *J. Lond. Math. Soc.* 75 (2007), 163–175.

[153] B. Green and T. Tao, An inverse theorem for the Gowers U^3-norm, with applications, *Proc. Edinburgh Math. Soc.* 51(1) (2008), 73–153.

[154] B. Green and T. Tao, The primes contain arbitrarily long arithmetic progressions, *Ann. Math.* 167 (2008), 481–547.

[155] B. Green and T. Tao, Freiman's theorem in finite fields via extremal set theory, *Combin. Probab. Comput.* 18 (2009), 335–355.

[156] B. Green and T. Tao, New bounds for Szemerédi's theorem, II: a new bound for $r_4(N)$, In Analytic number theory: Essays in honour of Klaus Roth, Cambridge Univ. Press, 2009, pp. 180–204.

[157] B. Green and T. Tao, The distribution of polynomials over finite fields, with applications to the Gowers norms, *Contrib. Discrete Math.* 4(2) (2009), 1–36.

[158] B. Green and T. Tao, An arithmetic regularity lemma, associated counting lemma, and applications, In An irregular mind: Szemerédi is 70, Bolyai Soc. Math. Stud., 21 (2010), pp. 261–334.

[159] B. Green and T. Tao, An equivalence between inverse sumset theorems and inverse conjectures for the U^3-norm, *Math. Proc. Camb. Phil. Soc.* 149(1) (2010), 1–19.

[160] B. Green and T. Tao, Linear equations in primes, *Ann. Math.* 171(3) (2010), 1753–1850.

[161] B. Green and T. Tao, Yet another proof of Szemerédi's theorem, In An irregular mind: Szemerédi is 70, Bolyai Soc. Math. Stud., 21 (2010), pp. 335–342.

[162] B. Green and T. Tao, New bounds for Szemerédi's theorem, Ia: Progressions of length 4 in finite field geometries revisited, arXiv/1205.1330, (2012).

[163] B. Green, T. Tao, and T. Ziegler, An inverse theorem for the Gowers U^4-norm, *Glasgow Math. J.* 53 (2011), 1–50.

[164] B. Green, T. Tao, and T. Ziegler, An inverse theorem for the Gowers $U^{s+1}[N]$-norm, *Ann. Math.*, to appear.

[165] B. Green and J. Wolf, A note on Elkin's improvement of Behrend's construction, In Additive Number Theory, Springer, (2010), 141–144.

[166] V. Guruswami, Better extractors for better codes?, In *Proc. 36th Annu. ACM Symp. Theory Comput. (STOC '04)*, (2004), 436–444.

[167] V. Guruswami, C. Umans, and S. P. Vadhan, Unbalanced expanders and randomness extractors from Parvaresh-Vardy codes, *J. ACM* 56(4) (2009), 1–34.

[168] L. Guth, The endpoint case of the Bennett-Carbery-Tao multilinear Kakeya conjecture, *Acta Math.* 205(2) (2010), 263–286.

[169] L. Guth and N. H. Katz, Algebraic methods in discrete analogs of the Kakeya problem, *Adv. Math.* 225(5) (2010), 2828–2839.

[170] L. Guth and N. H. Katz, On the Erdős distinct distance problem in the plane, arXiv/1011.4105, (2010).

[171] A. W. Hales and R. I. Jewett, Regularity and positional games, *Trans. Amer. Math. Soc.* 106 (1963), 222–229.

[172] Y. O. Hamidoune, An isoperimetric method in additive theory, *J. Algebra* 179(2) (1996), 622–630.

[173] Y. O. Hamidoune, Some additive applications of the isoperimetric approach, *Ann. Inst. Fourier (Grenoble)* 58(6) (2008), 2007–2036.

[174] Y. O. Hamidoune, The isoperimetric method, In *Combinatorial number theory and additive group theory* Adv. Courses Math. CRM Barcelona, Birkhäuser, 2009, pp. 241–252.

[175] Y. O. Hamidoune, Topology of Cayley graphs applied to inverse additive problems, *Proc. 3rd Int. Workshop Optimal Netw. Topol. (IWONT 2010)*, Barcelona, 2011, pp. 265–283.

[176] E. Haramaty and A. Shpilka, On the structure of cubic and quartic polynomials, In *Proc. 42nd Annu. ACM Symp. Theory Comput (STOC '10)*, 2010, pp. 331–340.

[177] E. Haramaty, A. Shpilka, and M. Sudan, Optimal testing of multivariate polynomials over small prime fields, In *Proc. 52nd Annu. IEEE Symp. Found. Comput. Sci. (FOCS '11)*, 2011, pp. 629–637.

[178] D. Hart, A. Iosevich, D. Koh, and M. Rudnev, Averages over hyperplanes, sum-product theory in vector spaces over finite fields and the Erdős-Falconer distance conjecture, *Trans. Amer. Math. Soc.* 363 (2011), 3255–3275.

[179] D. Hart, A. Iosevich, and J. Solymosi, Sum-product estimates in finite fields via Kloosterman sums, *Int. Math. Res. Notices* Vol. 2007 (2007), Article ID rnm007, 14 pages.

[180] D. Hart, L. Li, and C.-Y. Shen, Fourier analysis and expanding phenomena in finite fields, *Proc. Amer. Math. Soc.*, to appear.

[181] H. Hatami and S. Lovett, Correlation testing for affine invariant properties on F_p^n in the high error regime, In *Proc. 43rd Annu. ACM Symp. Theory Comput (STOC '11)*, 2011, pp. 187–194.

[182] N. Hegyvári and F. Hennecart, Explicit constructions of extractors and expanders, *Acta Arith.* 140 (2009), 233–249.

[183] H. Helfgott, Growth and generation in $SL_2(\mathbb{Z}/p\mathbb{Z})$, *Ann. Math.* 167(2) (2008), 601–623.

[184] H. Helfgott, Growth in $SL_3(\mathbb{Z}/p\mathbb{Z})$, *J. Eur. Math. Soc.* 13(3) (2011), 761–851.

[185] H. Helfgott and M. Rudnev, An explicit incidence theorem in $\mathbb{F}_p$, *Mathematika* 57(1) (2011), 135–145.

[186] S. Hoory, N. Linial, and A. Wigderson, Expander graphs and their applications, *Bull. Amer. Math. Soc.* 43 (2006), 439–561.

[187] C. Hoppen, Y. Kohayakawa, C. G. Moreira, and R. M. Sampaio, Property testing and parameter testing for permutations, In *Proc. 21th Annu. ACM-SIAM Symp. Discrete Algorithms*, 2010, pp. 66–75.

[188] B. Host and B. Kra, Nonconventional ergodic averages and nilmanifolds, *Ann. Math.* (2) 161(1) (2005), 397–488.

[189] B. Host and B. Kra, A point of view on Gowers uniformity norms, *New York J. Math.* 18 (2012), 213–248.

[190] E. Hrushovski, Stable group theory and approximate subgroups, *J. Amer. Math. Soc.* 25 (2012), 189–243.

[191] A. Iosevich, O. Roche-Newton, and M. Rudnev, On an application of Guth-Katz theorem, *Math. Res. Lett.* 18(4) (2011), 1–7.

[192] D. Jetchev, O. Özen, and M. Stam, Collisions are not incidental: a compression function exploiting discrete geometry, In *Proc. 9th Int. Conf. Theory Cryptogr. (TCC '12)*, 2012, pp. 303–320.

[193] T. Jones, Explicit incidence bounds over general finite fields, *Acta Arith.* 150 (2011), 241–262.

[194] T. Jones, An improved incidence bound for fields of prime order, arXiv/1110.4752, (2011).

[195] T. Jones, New results for the growth of sets of real numbers, arXiv/1202.4972, (2012).

[196] T. Jones, Further improvements to incidence and Beck-type bounds over prime finite fields, arXiv/1206.4517, (2012).

[197] S. Jukna, Extremal combinatorics: with applications in computer science, second ed., Springer, 2011.

[198] G. Kalai and S. Safra, Threshold phenomena and infl uence: perspectives from mathematics, computer science, and economics, In Computational complexity and statistical physics, Oxford Univ. Press (2006), pp. 25–60.

[199] Y. T. Kalai, X. Li, and A. Rao, 2-Source extractors under computational assumptions and cryptography with defective randomness, In *Proc. 50th Annu. IEEE Symp. Found. Comput. Sci. (FOCS '09)*, 2009, pp. 617–626.

[200] J. Kamp, A. Rao, S. Vadhan, and D. Zuckerman, Deterministic extractors for small-space sources, *J. Comput. System Sci.* 77 (2011), 191–220.

[201] N. Katz and C.-Y. Shen, A slight improvement to garaevs sum product estimate, *Proc. Amer. Math. Soc.* 136(7) (2008), 2499–2504.

[202] N. Katz and C.-Y. Shen, Garaev's inequality in finite fields not of prime order, *Online J. Anal. Comb.* 3(3) (2008), 6 pp.

[203] T. Kaufman and S. Lovett, Worst case to average case reductions for polynomials, In *Proc. 49th Annu. IEEE Symp. Found. Comput. Sci. (FOCS '08)*, 2008, pp. 166–175.

[204] T. Kaufman and S. Lovett, New extension of the Weil bound for character sums with applications to coding, In *Proc. 52nd Annu. IEEE Symp. Found. Comput. Sci. (FOCS '11)*, 2011, pp. 788–796.

[205] J. Komlós and M. Simonovits, Szemerédi's regularity lemma and its applications in graph theory, In Combinatorics, Paul Erdős is eighty (Vol. 2), Bolyai Soc. Math. Stud. 2 (1996), pp. 295–352.

[206] E. Kowalski, Explicit growth and expansion for SL_2, arXiv/1201.1139, (2012).

[207] B. Kra, The Green-Tao Theorem on arithmetic progressions in the primes: an ergodic point of view, *Bull. Amer. Math. Soc.* 43(1) (2005), 3–23.

[208] B. Kra, From combinatorics to ergodic theory and back again, *Proc. Int. Congr. Math.*, Madrid 2006, volume III, pp. 57–76.

[209] B. Kra, Ergodic methods in additive combinatorics, In *Additive combinatorics*, CRM Proc. Lecture Notes 43, Amer. Math. Soc., (2007), pp. 103–144.

[210] B. Kra, Poincaré recurrence and number theory: thirty years later, *Bull. Amer. Math. Soc.* 48 (2011), 497–501.

[211] I. Łaba and M. Pramanik, Arithmetic progressions in sets of fractional dimension, *Geom. Funct. Anal.* 19(2) (2009), 429–456.

[212] T. H. Lê, Green-Tao theorem in function fields, *Acta Arith.* 147(2) (2011), 129–152.

[213] V. F. Lev, Character-free approach to progression-free sets, *Finite Fields Appl.* 18(2) (2012), 378–383.

[214] L. Li, Slightly improved sum-product estimates in fields of prime order, *Acta Arith.* 147(2) (2011), 153–160.

[215] L. Li and O. Roche-Newton, An improved sum-product estimate for general finite fields, *SIAM J. Discrete Math.* 25(3) (2011), 1285–1296.

[216] L. Li and J. Shen, A sum-division estimate of reals, *Proc. Amer. Math. Soc.* 138(1) (2010), 101–104.

[217] X. Li, A new approach to affine extractors and dispersers, In *Proc. 2011 IEEE 26th Annu. Conf. Comput. Complexity (CCC '11)*, 2011, pp. 137–147.

[218] X. Li, Non-malleable extractors, two-source extractors and privacy amplification, In *Proc. 53rd Annu. IEEE Symp. Found. Comput. Sci. (FOCS '12)*, 2012, to appear.

[219] Y. Lin and J. Wolf, On subsets of $\mathbb{F}_q^n$ containing no k-term progressions, *European J. Combin.* 31(5)(2010), 1398–1403.

[220] H. Lipmaa, Progression-free sets and sublinear pairing-based non-interactive zero-knowledge arguments, In *Proc. 9th Int. Conf. Theory Cryptogr. (TCC '12)*, 2012, pp. 169–189.

[221] H. Liu, Gowers uniformity norm and pseudorandom measures of the pseudorandom binary sequences, *Int. J. Number Theory* 7(5) (2011), 1279–1302.

[222] L. Lovász and B. Szegedy, Regularity partitions and the topology on graphons, in An irregular mind: Szemeredi is 70, Bolyai Soc. Math. Stud., 21 (2010), pp. 415–446.

[223] S. Lovett, Unconditional pseudorandom generators for low degree polynomials, *Theory Comput.* 5(1) (2009), 69–82.

[224] S. Lovett, Equivalence of polynomial conjectures in additive combinatorics, *Combinatorica*, to appear.

[225] S. Lovett, R. Meshulam, and A. Samorodnitsky, Inverse conjecture for the Gowers norm is false, In *Proc. 40th Annu. ACM Symp. Theory Comput. (STOC '08)*, 2008, pp. 547–556.

[226] S. Lovett, P. Mukhopadhyay, and A. Shpilka, Pseudorandom generators for $CC_0[p]$ and the Fourier spectrum of low-degree polynomials over finite fields, In *Proc. 51st Annu. IEEE Symp. Found. Comput. Sci. (FOCS '10)*, 2010, pp. 695–704.

[227] S. Lovett, O. Reingold, L. Trevisan, and S. Vadhan, Pseudorandom bit generators that fool modular sums, In *Proc. APPROX '09 / RANDOM '09* , LNCS 5687, pp. 615–630, (2009).

[228] C. J. Lu, Encryption against storage-bounded adversaries from on-line strong extractors, *J. Cryptology* 17(1) (2004), 27–42.

[229] A. Lubotzky, Expander graphs in pure and applied mathematics, *Bull. Amer. Math. Soc.* 49 (2012), 113–162.

[230] M. Madiman, A. Marcus, and P. Tetali, Information-theoretic inequalities in additive combinatorics In *Proc. of the 2010 IEEE Information Theory Workshop*, 2010, pp. 1–4.

[231] M. Madiman, A. Marcus, and P. Tetali, Entropy and set cardinality inequalities for partition-determined functions, *Random Structures Algorithms* 40(4) (2012), 399–424.

[232] M. Malliaris and S. Shelah, Regularity lemmas for stable graphs, *Trans. Amer. Math. Soc.*, to appear.

[233] L. Matthiesen, Linear correlations amongst numbers represented by positive definite binary quadratic forms, *Acta Arith.*, to appear.

[234] R. Meshulam, On subsets of finite Abelian groups with no 3-term arithmetic progressions, *J. Combin. Theory, Ser. A* 71(1) (1995), 168–172.

[235] P. Miltersen, N. Nisan, S. Safra, and A. Wigderson, On data structures and asymmetric communication complexity, *J. Comput. Syst. Sci.* 57(1) (1998), 37–49.

[236] B. Nagle, V. Rödl, and M. Schacht, The counting lemma for regular k-uniform hypergraphs, *Random Structures Algorithms* 28 (2006), 113–179.

[237] M. B. Nathanson, Additive number theory: The classical bases, Springer, 164 (1996).

[238] M. B. Nathanson, Additive number theory: Inverse problems and the geometry of sumsets, Springer, 165 (1996).

[239] M. B. Nathanson, Generalized additive bases, König's lemma, and the Erdős-Turán conjecture, *J. Number Theory* 106(1) (2004), 70–78.

[240] M. A. Nielsen, Introduction to the Polymath project and "density Hales-Jewett and Moser numbers", In An irregular mind: Szemerédi is 70, Bolyai Soc. Math. Stud., 21 (2010), pp. 651–657.

[241] J. I. Novak, Topics in combinatorics and random matrix theory, PhD thesis, Queen's University, 2009.

[242] K. O'Bryant, Sets of integers that do not contain long arithmetic progressions, *Electron. J. Combin.* 18 (2011), Article #P59.

[243] A. Ostafe and I. E. Shparlinski, On the Waring problem with Dickson polynomials in finite fields, *Proc. Amer. Math. Soc.* 139 (2011), 3815–3820.

[244] A. Plagne, On threshold properties of k-SAT: An additive viewpoint, *European J. Combin.* 27 (2006), 1186–1198.

[245] A. Plagne and W. A. Schmid, An application of coding theory to estimating Davenport constants, *Des. Codes Cryptogr.* 61 (2011), 105–118.

[246] D. H. J. Polymath, A new proof of the density Hales-Jewett theorem, *Ann. Math.* 175(3) (2012), 1283–1327.

[247] P. Potgieter, Arithmetic progressions in Salem-type subsets of the integers, *J. Fourier Anal. Appl.* 17 (2011), 1138–1151.

[248] L. Pyber and E. Szabó, Growth in finite simple groups of Lie type of bounded rank, arXiv/1005.1858, (2010).

[249] R. A. Rankin, Sets of integers containing not more than a given number of terms in arithmetical progression, *Proc. Roy. Soc. Edinburgh Sect. A* 65 (1962), 332–344.

[250] A. Rao, Extractors for a constant number of polynomially small min-entropy independent sources, *SIAM J. Comput.* 39(1) (2009), 168–194.

[251] A. Rao, Extractors for low-weight affine sources, In *Proc. 24th Annu. IEEE Conf. Comput. Complexity (CCC '09)*, 2009, pp. 95–101.

[252] O. Reingold, L. Trevisan, M. Tulsiani, and S. Vadhan, Dense subsets of pseudorandom sets, *Electron. Colloq. Comput. Complexity (ECCC)*, Technical Report TR08-045, (2008).

[253] O. Roche-Newton and M. Rudnev, Areas of rectangles and product sets of sum sets, arXiv/1203.6237, (2012).

[254] V. Rödl and M. Schacht, Property testing in hypergraphs and the removal lemma, In *Proc. 39th Annu. ACM Symp. Theory Comput. (STOC '07)*, 2007, pp. 488–495.

[255] V. Rödl and M. Schacht, Regular partitions of hypergraphs: Regularity lemmas, *Combin. Probab. Comput.* 16(6) (2007), 833–885.

[256] V. Rödl and M. Schacht, Regular partitions of hypergraphs: Counting lemmas, *Combin. Probab. Comput.* 16(6) (2007), 887–901.

[257] V. Rödl and M. Schacht, Generalizations of the removal lemma, *Combinatorica* 29(4) (2009), 467–501.

[258] V. Rödl and M. Schacht, Regularity lemmas for graphs, In Fete of combinatorics and computer science, Bolyai Soc. Math. Stud., 20 (2010), pp. 287–325.

[259] V. Rödl and J. Skokan, Regularity lemma for k-uniform hypergraphs, *Random Structures Algorithms* 25 (2004), 1–42.

[260] V. Rödl and J. Skokan, Applications of the regularity lemma for uniform hypergraphs, *Random Structures Algorithms* 28 (2006), 180–194.

[261] D. Ron, Property testing: A learning theory perspective, *Found. Trends Mach. Learn.* 1(3) (2008), pp 307–402.

[262] D. Ron, Algorithmic and analysis techniques in property testing, *Found. Trends Theor. Comput. Sci.* 5(2) (2009), pp 73–205.

[263] V. Rosta, Ramsey theory applications, *Electron. J. Combin.* (2004), Article #DS13.

[264] K. F. Roth, On certain sets of integers, *J. Lond. Math. Soc.* 28 (1953), 104–109.

[265] M. Rudelson and R. Vershynin, Non-asymptotic theory of random matrices: extreme singular values, In *Proc. Internat. Congr. Math.*, Volume III, Hindustan Book Agency, New Delhi, (2011), 1576–1602.

[266] M. Rudnev, An improved sum-product inequality in fields of prime order, *Int. Math. Res. Not.*, to appear.

[267] M. Rudnev, On new sum-product type estimates, arXiv/1111.4977, (2011).

[268] I. Z. Ruzsa, Sumsets and Entropy, *Random Structures Algorithms* 34(1) (2009), 1–10.

[269] I. Z. Ruzsa and E. Szemerédi, Triple systems with no six points carrying three triangles, in Combinatorics, Colloq. Math. Soc. J. Bolyai 18 (1978), 939–945.

[270] A. Samorodnitsky, Low-degree tests at large distances, In *Proc. 39th Annu. ACM Symp. Theory Comput. (STOC '07)*, 2007, pp. 506–515.

[271] A. Samorodnitsky and L. Trevisan, Gowers uniformity, influence of variables, and PCPs, *SIAM J. Comput.* 39(1) (2009), 323–360.

[272] T. Sanders, Appendix to 'Roth's theorem on progressions revisited,' by J. Bourgain, *J. Anal. Math.*, 104 (2008), 193–206.

[273] T. Sanders, On the Bogolyubov-Ruzsa lemma, arXiv/1011.0107v1, (2010).

[274] T. Sanders, On Roth's theorem on progressions, *Ann. Math.* 174(1) (2011), 619–636.

[275] T. Schoen, Near optimal bounds in Freiman's theorem, *Duke Math. J.* 158(1) (2011), 1–12.

[276] T. Schoen and I. D. Shkredov, On sumsets of convex sets, *Combin. Probab. Comput.*, 20 (2011), 793–798.

[277] T. Schoen and I. D. Shkredov, Roth's theorem in many variables, arXiv/1106.1601, (2011).

[278] O. Serra, An isoperimetric method for the small sumset problem, In *Surveys in combinatorics*, London Math. Soc. Lecture Note Ser., 327 (2005), pp. 119–152.

[279] R. Shaltiel, Recent developments in explicit construction of extractors, *Bull. Eur. Assoc. Theoret. Comput. Sci.* 77 (2002), 67–95.

[280] R. Shaltiel, An introduction to randomness extractors, In L. Aceto, M. Henzinger, and J. Sgall (Eds.): ICALP 2011, Part II, LNCS 6756, pp. 21–41, (2011).

[281] A. Shapira, Green's conjecture and testing linear-invariant properties, In *Proc. 41st Annu. ACM Symp. Theory Comput (STOC '09)*, 2009, pp. 159–166.

[282] C.-Y. Shen, An extension of Bourgain and Garaev's sum-product estimates, *Acta Arith.* 135(4) (2008), 351–356.

[283] C.-Y. Shen, On the sum product estimates and two variables expanders, *Publ. Mat.* 54(1) (2010), 149–157.

[284] C.-Y. Shen, Sum-product phenomenon in finite fields not of prime order, *Rocky Mountain J. Math.* 41(3) (2011), 941–948.

[285] C.-Y. Shen, Algebraic methods in sum-product phenomena, *Israel J. Math.* 188(1) (2012), 123–130.

[286] I. D. Shkredov, Szemerédi's theorem and problems on arithmetic progressions, *Russian Math. Surveys* 61(6) (2006), 1101–1166.

[287] I. D. Shkredov, On a two-dimensional analogue of Szemerédi's theorem in Abelian groups, *Izv. Math.* 73(5) (2009), 1033–1075.

[288] I. E. Shparlinski, On the elliptic curve analogue of the sum-product problem, *Finite Fields and Their Appl.* 14 (2008), 721–726.

[289] I. E. Shparlinski, On the exponential sum-product problem, *Indag. Math.* 19 (2009), 325–331.

[290] I. E. Shparlinski, Sum-product estimates and multiplicative orders of γ and $\gamma + \gamma^{-1}$ in finite fields, *Bull. Aust. Math. Soc.* 85 (2012), 505–508

[291] I. E. Shparlinski, Additive combinatorics over finite fields: New results and applications, In *Proc. RICAM-Workshop on Finite Fields and Their Applications: Character Sums and Polynomials*, De Gruyter, to appear.

[292] J. Solymosi, On sum-sets and product-sets of complex numbers, *J. Théor. Nombres Bordeaux* 17 (2005), 921–924.

[293] J. Solymosi, On the number of sums and products, *Bull. Lond. Math. Soc.* 37 (2005), 491–494.

[294] J. Solymosi, Incidences and the spectra of graphs, In Building bridges: between mathematics and computer science, Bolyai Soc. Math. Stud., 19 (2008), pp. 499–513.

[295] J. Solymosi, Bounding multiplicative energy by the sumset, *Adv. Math.* 222(2) (2009), 402–408.

[296] J. Solymosi, Roth type theorems in finite groups, arXiv/1201.3670, (2012).

[297] J. Solymosi and T. Tao, An incidence theorem in higher dimensions, *Discrete Comput. Geom.*, to appear.

[298] J. Solymosi and V. Vu, Sum-product estimates for well-conditioned matrices, *Bull. London Math. Soc.* 41 (2009), 817–822.

[299] B. Sudakov, E. Szemerédi, and V. Vu, On a question of Erdős and Moser, *Duke Math. J.* 129 (2005), 129–155.

[300] M. Sudan, Decoding of Reed-Solomon codes beyond the errorcorrection bound, *J. Complexity* 13(1) (1997), 180–193.

[301] M. Sudan, L. Trevisan, and S. P. Vadhan, Pseudorandom generators without the XOR lemma, *J. Comput. Syst. Sci.* 62(2) (2001), 236–266.

[302] L. Székely, Crossing numbers and hard Erdős problems in discrete geometry, *Combin. Probab. Comput.* 6 (1997), 353–358.

[303] E. Szemerédi, On sets of integers containing no four elements in arithmetic progression, *Acta Math. Acad. Sci. Hung.* 20 (1969), 89–104.

[304] E. Szemerédi, On sets of integers containing no k elements in arithmetic progression, *Acta Arith.* 27 (1975), 199–245.

[305] E. Szemerédi and W. T. Trotter Jr., Extremal problems in discrete geometry, *Combinatorica* 3 (1983), 381–392.

[306] E. Szemerédi and V. Vu, Long arithmetic progressions in sum-sets and the number of x-sum-free sets, *Proc. Lond. Math. Soc.* 90(2) (2005), 273–296.

[307] E. Szemerédi and V. Vu, Finite and infinite arithmetic progressions in sumsets, *Ann. Math. (2)* 163(1) (2006), 1–35.

[308] E. Szemerédi and V. Vu, Long arithmetic progressions in sumsets: Thresholds and bounds, *J. Amer. Math. Soc.* 19 (2006), 119–169.

[309] T. Tao, From rotating needles to stability of waves: emerging connections between combinatorics, analysis, and PDE, *Notices Amer. Math. Soc.* 48(3) (2001), 294–303.

[310] T. Tao, A quantitative ergodic theory proof of Szemerédi's theorem, *Electron. J. Combin.* 13 (2006), Article #R99.

[311] T. Tao, A variant of the hypergraph removal lemma, *J. Combin. Theory Ser. A* 113 (2006), 1257–1280.

[312] T. Tao, The dichotomy between structure and randomness, arithmetic progressions, and the primes, In *Proc. Int. Congr Math.*, Madrid, Spain, (2006), pp. 581–608.

[313] T. Tao, The Gaussian primes contain arbitrarily shaped constellations, *J. d'Analyse Math.* 99 (2006), 109–176.

[314] T. Tao, A correspondence principle between (hyper)graph theory and probability theory, and the (hyper)graph removal lemma, *J. Anal. Math.* 103 (2007), 1–45.

[315] T. Tao, Product set estimates in noncommutative groups, *Combinatorica* 28 (2008), 547–594.

[316] T. Tao, Structure and randomness: Pages from year one of a mathematical blog, Amer. Math. Soc., (2008).

[317] T. Tao, The sum-product phenomenon in arbitrary rings, *Contrib. Discrete Math.* 4(2) (2009), 59–82.

[318] T. Tao, Freiman's theorem for solvable groups, *Contrib. Discrete Math.* 5(2) (2010), 137–184.

[319] T. Tao, Sumset and inverse sumset theory for Shannon entropy, *Combin. Probab. Comput.* 19 (2010), 603–639.

[320] T. Tao, Higher order Fourier analysis, in preparation.

[321] T. Tao and V. Vu, Additive combinatorics, Cambridge Univ. Press, 105 (2006).

[322] T. Tao and V. Vu, Random Matrices: The circular Law, *Commun. Contemp. Math.* 10(2)(2008), 261–307.

[323] T. Tao and V. Vu, From the Littlewood-Offord problem to the circular law: universality of the spectral distribution of random matrices, *Bull. Amer. Math. Soc.* 46 (2009), 377–396.

[324] T. Tao and V. Vu, Random matrices: Universality of local eigenvalue statistics up to the edge, *Commun. Math. Phys.* 298(2)(2010), 549–572.

[325] T. Tao and T. Ziegler, The primes contain arbitrarily long polynomial progressions, *Acta Math.* 201 (2008), 213–305.

[326] T. Tao and T. Ziegler, The inverse conjecture for the Gowers norm over finite fields via the correspondence principle, *Analysis & PDE* 3(1) (2010), 1–20.

[327] A. Ta-Shma and D. Zuckerman, Extractor codes, *IEEE Trans. Inform. Theory* 50(12) (2004), 3015–3025.

[328] C. D. Tóth, The Szemerédi-Trotter theorem in the complex plane, arXiv/0305283, (2003).

[329] H. Towsner, A model theoretic proof of Szemerédi's theorem, arXiv/1002.4456, (2010).

[330] L. Trevisan, Additive combinatorics and theoretical computer science, *ACM SIGACT News* 40(2) (2009), 50–66.

[331] L. Trevisan, Pseudorandomness in computer science and in additive combinatorics, In An irregular mind: Szemerédi is 70, Bolyai Soc. Math. Stud., 21 (2010), pp. 619–650.

[332] M. Tulsiani and J. Wolf, Quadratic Goldreich-Levin theorems, In *Proc. 52th Annu. IEEE Symp. Found. Comput. Sci. (FOCS '11)*, 2011, pp. 619–628.

[333] S. P. Vadhan, Constructing locally computable extractors and cryptosystems in the bounded-storage model, *J. Cryptology* 17(1) (2004), 43–77.

[334] S. P. Vadhan, The unified theory of pseudorandomness, In *Proc. Internat. Congr. Math.*, Volume IV, Hindustan Book Agency, New Delhi, (2011), 2723–2745.

[335] S. P. Vadhan, Pseudorandomness, *Found. Trends Theor. Comput. Sci.*, to appear.

[336] L. A. Vinh, The Szemerédi-Trotter type theorem and the sum-product estimate in finite fields, *European J. Combin.* 32(8) (2011), 1177–1181.

[337] L. A. Vinh, Sum and shifted-product subsets of product-sets over finite rings, *Electron. J. Combin.* 19(2) (2012), Article #P33.

[338] E. Viola, New correlation bounds for $GF(2)$ polynomials using Gowers uniformity, *Electron. Colloq. Comput. Complexity (ECCC)*, Technical Report TR06–097, (2006).

[339] E. Viola, Selected results in additive combinatorics: An exposition, *Theory Comput. Library, Graduate Surveys*, 3 (2011), 1–15.

[340] E. Viola and A. Wigderson, Norms, XOR lemmas, and lower bounds for polynomials and protocols, *Theory Comput.* 4 (2008), 137–168.

[341] V. Vu, Random discrete matrices, In Horizons of combinatorics, Bolyai Soc. Math. Stud., 17 (2008), pp. 257–280.

[342] V. Vu, Sum-product estimates via directed expanders, *Math. Res. Lett.* 15(2) (2008), 375–388.

[343] V. Vu, M. M. Wood, and P. M. Wood, Mapping incidences, *J. Lond. Math. Soc.* 84(2) (2011), 433–445.

[344] A. Wigderson and D. Zuckerman, Expanders that beat the eigenvalue bound: Explicit construction and applications, *Combinatorica* 19(1) (1999), 125–138.

[345] T. Wolff, Recent work connected with the Kakeya problem, Prospects in Mathematics (Princeton, NJ, 1996), 129–162, Amer. Math. Soc., Providence, RI, 1999.

[346] A. Yehudayoff, Affine extractors over prime fields, *Combinatorica* 31(2) (2011), 245–256.

[347] J. Zahl, A Szemerédi-Trotter type theorem in $\mathbb{R}^4$, arXiv/1203.4600, (2012).

[348] M. Zimand, Simple extractors via constructions of cryptographic pseudorandom generators, *Theor. Comput. Sci.* 411 (2010), 1236–1250.

[349] D. Zuckerman, Randomness-optimal oblivious sampling, *Random Structures Algorithms* 11 (1997), 345–367.

[350] D. Zuckerman, Linear degree extractors and the inapproximability of max clique and chromatic number, *Theory Comput.* 3(1) (2007), 103–128.