Incidence Theorems and Their Applications

Incidence Theorems and Their Applications

Zeev Dvir

Princeton University
Princeton, NJ 08540
USA
zdvir@princeton.edu

the essence of knowledge

Boston – Delft

Foundations and Trends® in Theoretical Computer Science

Published, sold and distributed by:
now Publishers Inc.
PO Box 1024
Hanover, MA 02339
USA
Tel. +1-781-985-4510
www.nowpublishers.com
sales@nowpublishers.com

Outside North America:
now Publishers Inc.
PO Box 179
2600 AD Delft
The Netherlands
Tel. +31-6-51115274

The preferred citation for this publication is Z. Dvir, Incidence Theorems and Their Applications, Foundation and Trends® in Theoretical Computer Science, vol 6, no 4, pp 257–393, 2010

ISBN: 978-1-60198-620-7

Foundations and Trends® in Theoretical Computer Science
Volume 6 Issue 4, 2010

Editorial Board

Editorial Scope

Foundations and Trends® in Theoretical Computer Science will publish survey and tutorial articles in the following topics:

- Algorithmic game theory
- Computational algebra
- Computational aspects of combinatorics and graph theory
- Computational aspects of communication
- Computational biology
- Computational complexity
- Computational geometry
- Computational learning
- Computational Models and Complexity
- Computational Number Theory
- Cryptography and information security
- Data structures
- Database theory
- Design and analysis of algorithms
- Distributed computing
- Information retrieval
- Operations Research
- Parallel algorithms
- Quantum Computation
- Randomness in Computation

Information for Librarians
Foundations and Trends® in Theoretical Computer Science, 2010, Volume 6, 4 issues. ISSN paper version 1551-305X. ISSN online version 1551-3068. Also available as a combined paper and online subscription.

Foundations and Trends® in
Theoretical Computer Science
Vol. 6, No. 4 (2010) 257–393

DOI: 10.1561/0400000056

now
the essence of knowledge

Incidence Theorems and Their Applications

Zeev Dvir

Princeton University, Mathematics and Computer Science Departments, Princeton, NJ 08540, USA, zdvir@princeton.edu

Abstract

We survey recent (and not so recent) results concerning arrangements of lines, points, and other geometric objects and the applications these results have in theoretical computer science and combinatorics. The three main types of problems we will discuss are:

(1) **Counting incidences:** Given a set (or several sets) of geometric objects (lines, points, etc.), what is the maximum number of incidences (or intersections) that can exist between elements in different sets? We will see several results of this type, such as the Szemeredi–Trotter theorem, over the reals and over finite fields and discuss their applications in combinatorics (e.g., in the recent solution of Guth and Katz to Erdos' distance problem) and in computer science (in explicit constructions of multisource extractors).

(2) **Kakeya type problems:** These problems deal with arrangements of lines that point in different directions. The goal is to try and understand to what extent these lines can overlap one another. We will discuss these questions both over the reals and over finite fields and see how they come up in the theory of randomness extractors.

(3) **Sylvester–Gallai type problems:** In this type of problems, one is presented with a configuration of points that contain many 'local' dependencies (e.g., three points on a line) and is asked to derive a bound on the dimension of the span of all points. We will discuss several recent results of this type, over various fields, and see their connection to the theory of locally correctable error-correcting codes.

Throughout the different parts of the survey, two types of techniques will make frequent appearance. One is the polynomial method, which uses polynomial interpolation to impose an algebraic structure on the problem at hand. The other recurrent techniques will come from the area of additive combinatorics.

Contents

1

Overview

Consider a finite set of points, P, in some vector space and another set L of lines. An *incidence* is a pair $(p, \ell) \in P \times L$ such that $p \in \ell$. There are many types of questions one can ask about the set of incidences and many different conditions one can impose on the corresponding set of points and lines. For example, the Szemeredi–Trotter theorem (which will be discussed at length below) gives an upper bound on the *number* of possible incidences. More generally, in this survey we will be interested in a variety of problems and theorems relating to arrangements of lines and points and the surprising applications these theorems have, in theoretical computer science and in combinatorics. The term 'incidence theorems' is used in a very broad sense and might include results that could fall under other categories. We will study questions about incidences between lines and points, lines and lines (where an incidence is a pair of intersecting lines), circles and points and more.

Some of the results we will cover have direct and powerful applications to problems in theoretical computer sciences and combinatorics. One example in combinatorics is the recent solution of Erdos' distance problem by Guth and Katz [35]. The problem is to lower bound the

number of distinct distances defined by a set of points in the real plane and the solution (which is optimal up to logarithmic factors) uses a clever reduction to a problem on counting incidences of lines [27].

In theoretical computer science, incidence theorems (mainly over finite fields) have been used in recent years to construct *extractors*, which are procedures that transform *weak* sources of randomness (that is, distributions that have some amount of randomness but are not completely uniform) into completely uniform random bits. Extractors have many theoretical applications, ranging from cryptography to data structures to metric embedding (to name just a few) and the current state-of-the-art constructions all use incidence theorems in one way or another. The need to understand incidences comes from trying to analyze simple looking constructions that use basic algebraic operations. For example, how 'random' is $X \cdot Y + Z$, when X, Y, Z are three independent random variables each distributed uniformly over a large subset of $\mathbb{F}_p$.

We will see incidence problems over finite fields, over the reals, in low dimension and in high dimension. These changes in field/dimension are pretty drastic and, as a consequence, the ideas appearing in the proofs will be quite diverse. However, two main techniques will make frequent appearance. One is the 'polynomial method' which uses polynomial interpolation to try and 'force' an algebraic structure on the problem. The other recurrent techniques will come from additive combinatorics. These are general tools to argue about sets in Abelian groups and the way they behave under certain group operations. These two techniques are surprisingly flexible and can be applied in many different scenarios and over different fields.

The monograph is divided into four chapters, following this overview chapter. The first chapter will be devoted to problems of counting incidences over the real numbers (Szemeredi–Trotter and others) and will contain applications mostly from combinatorics (including the Guth–Katz solution to Erdos' distance problem). The second chapter will be devoted to the Szemeredi–Trotter theorem over finite fields and its applications to the explicit constructions of multisource extractors. The third chapter will be devoted to *Kakeya* type problems which deal with arrangements of lines pointing in different directions (over finite and

infinite fields). The applications in this chapter will be to the construction of another variant of extractors–seeded extractors. The fourth and final chapter will deal with arrangements of points with many collinear triples. These are related to questions in theoretical computer science having to do with *locally correctable* error-correcting codes. More details and definitions relating to each of the aforementioned chapters are given in the next four subsections of this overview which serves as a road map to the various sections.

This survey is aimed at both mathematicians and computer scientists and could serve as a basis for a one semester course. Ideally, each chapter should be read from start to end (the different chapters are mostly independent of each other). We only assume familiarity with undergraduate level algebra, including the basics of finite fields and polynomials.

Notations: We will use $\lesssim, \gtrsim$ and $\sim$ to denote (in)equality up to multiplicative absolute constants. That is, $X \lesssim Y$ means 'there exists an absolute constant C such that $X \leq CY$'. In some places, we opt to use instead the computer science notations of $O(\cdot), \Omega(\cdot)$, and $\theta(\cdot)$ to make some expressions more readable. So $X = O(Y)$ is the same as $X \lesssim Y$, $X = \Omega(Y)$ is the same as $X \gtrsim Y$, and $X = \theta(Y)$ is the same as $X \sim Y$. This allows us to write, for example, $X = 2^{\Omega(Y)}$ to mean: 'there exists an absolute constant C such that $x \geq 2^{CY}$'.

Sources: Aside from research papers there were two main sources that were used in the preparation of this monograph. The first is a sequence of posts on Terry Tao's blog which cover a large portion of Section 2 (see e.g., [67]). Ben Green's lecture notes on additive combinatorics [32] were the main source in preparing Section 3. Both of these sources were indispensable in preparing this monograph and I am grateful to both authors.

Section 2: Counting Incidences Over the Reals

Let P be a finite set of points and L a finite set of lines in $\mathbb{R}^2$. Let

$$I(P, L) = \{(p, \ell) \in P \times L \,|\, p \in \ell\}$$

denote the set of *incidences* between P and L. A basic question we will ask is how big can $I(P,L)$ be. The Szemeredi–Trotter (ST) theorem [65] gives the (tight) upper bound of

$$|I(P,L)| \lesssim (|L| \cdot |P|)^{2/3} + |L| + |P|.$$

We begin this section in Section 2.1 with two different proofs of this theorem. The first proof, presented in Section 2.1.1, is due to Tao [67] (based on [18] and similar to the original proof of [65]) and uses the method of cell partitions. The idea is to partition the two-dimensional plane into cells, each containing a bounded number of points/lines and to argue about each cell separately. This uses the special 'ordered' structure of the real numbers (this proof strategy is also the only one that generalizes to the complex numbers [68]). The second proof, presented in Section 2.1.2, is due to Szekely [64] ands uses the crossing number inequality for planar drawings of graphs and is perhaps the most elegant proof known for this theorem. This proof can also be adapted easily to handle intersections of more complex objects such as curves. We continue in Section 2.2 with some simple applications of the ST theorem to geometric and algebraic problems. These include proving sum-product estimates and counting distances between sets of points.

Sections 2.3–2.6 are devoted to the proof of the Guth–Katz theorem on Erdos' distance counting problem. This theorem, obtained in [35], says that a set of N points in the real plane define at least $\gtrsim N/\log N$ distinct distances. This gives an almost complete answer to an old question of Erdos (the upper bound has a factor of $\sqrt{\log N}$ instead of $\log N$). The tools used in the proof are developed over several sections which contain several other related results.

In Section 2.3 we discuss the Elekes–Sharir framework [27] which reduces distance counting to a question about incidences of a specific family of lines in $\mathbb{R}^3$, much in the spirit of the ST theorem. Sections 2.4 and 2.5 introduce the two main techniques used in the proof of the Guth–Katz theorem. In Section 2.4 we introduce for the first time one of the main characters of this survey — the polynomial method. As a first example to the power of this method, we show how it can be used to give a solution to another beautiful geometric conjecture — the joints conjecture [34]. Here, one has a set of lines in $\mathbb{R}^3$ and wants

to upper bound the number of *joints*, or noncoplanar intersections of three lines or more. In Section 2.5 we introduce the second ingredient in the Guth–Katz theorem — the polynomial ham sandwich theorem. This technique, introduced by Guth in [33], combines the polynomial method with the method of cell partitions. As an example of how this theorem is used we give a third proof of the ST theorem which was discovered recently [39].

Section 2.6, contains a relatively detailed sketch of the proof of the Guth–Katz theorem (omitting some of the more technical algebraic parts). The main result proved in this section is an incidence theorem upper bounding the number of pairwise intersections in a set of N lines in $\mathbb{R}^3$. If we don't assume anything, N lines can have $\gtrsim N^2$ intersections (an intersection is a pair of lines that intersect). An example is a set of $N/2$ horizontal lines and $N/2$ vertical lines, all lying in the same plane. If we assume, however, that the lines are 'truly' in three dimensions, in the sense that no large subset of them lies in two dimensions, we can get a better (and tight) bound of $\leq N^{1.5} \log N$. This theorem then implies the bound on distinct distances using the Elekes–Sharir framework.

In the last section of this section, Section 2.7, we see yet another beautiful application of the three-dimensional incidence theorem of Guth and Katz obtaining optimal bounds in the flavor of the sum-product theorem [38].

Section 3: Counting Incidences Over Finite Fields

This section deals with the analog of the Szemeredi–Trotter theorem over finite fields and its applications. When we replace the field $\mathbb{R}$ with a finite field $\mathbb{F}_q$ of q elements things become much more tricky and much less is known (in particular there are no tight bounds). Assuming nothing on the field, the best possible upper bound on the number of intersections between N lines and N points is $\sim N^{1.5}$, which is what one gets from only using the fact that two points determine a line (using a simple Cauchy–Schwarz calculation). However, if we assume that $\mathbb{F}_q$ does not contain large subfields (as is the case, for example, if q is prime) one can obtain a small improvement of the form $N^{1.5-\epsilon}$ for some positive ϵ, provided $N \ll p^2$. This was shown by Bourgain, Katz and

Tao as an application of the sum-product theorem over finite fields [14]. The sum-product theorem says that, under the same conditions on subfields, for every set $A \subset \mathbb{F}_q$ of size at most $q^{1-\alpha}$ we have $\max\{|A+A|, |A \cdot A|\} > |A|^{1+\alpha'}$, where α' depends only on α. The set $A+A$ is defined as the set of all elements of the form $a+a'$ with $a, a' \in A$ ($A \cdot A$ is defined in a similar way).

The proof of the finite field ST theorem is given in Sections 3.1–3.4. Section 3.1 describes the machinery called 'Ruzsa calculus' — a set of useful claims for working with sumsets. Section 3.2 proves a theorem about growth of subsets of $\mathbb{F}_p$ (we will only deal with prime fields) which is a main ingredient of the proof of the ST theorem. Section 3.3 proves the Balog–Szemeredi–Gowers theorem, a crucial tool in this proof and in many other results in additive combinatorics. Finally, Section 3.4 puts it all together and proves the final result. We note that, unlike previous expositions (and the original [14]), we opt to first prove the ST theorem and then derive the sum-product theorem from it as an application. This is not a crucial matter but it seems to simplify the proof of the ST theorem a bit.

As an application of these results over finite fields we will discuss, in Section 3.5, the theory of *multisource extractors* coming from theoretical computer science. We will see how to translate the finite field ST theorem into explicit mappings which transform 'weak' structured sources of randomness into purely random bits. More precisely, suppose you are given samples from several (at least two) independent random variables and want to use them to output uniform random bits. It is not hard to show that a random function will do the job, but finding *explicit* (that is, efficiently computable) constructions is a difficult task. Such constructions have applications in theoretical computer science, in particular in the area of de-randomization, which studies the power of randomized computation vs. deterministic computation.

We will discuss in some detail two representative results in this area: the extractors of Barak, Impagliazzo and Wigderson for several independent blocks [5], which were the first to introduce the tools of additive combinatorics to this area, and Bourgain's two-source extractor [12]. Both rely crucially on the finite field Szemeredi–Trotter theorem of [14].

Section 4: Packing Lines in Different Directions — Kakeya Sets

This section deals with a somewhat different types of theorems that describe the way lines in different directions can overlap. In Sections 4.1 and 4.2 we will discuss these questions over the real numbers and over finite fields, respectively. In Section 4.3 we will discuss applications of the finite field results to problems in theoretical computer science.

A Kakeya set $K \subset \mathbb{R}^n$ is a compact set containing a unit line segment in every direction. These sets can have measure zero. An important open problem is to understand the minimum Minkowski or Hausdorff dimension[1] of a Kakeya set. This question reduces in a natural way to a discrete incidence question involving a finite set of lines in many 'sufficiently separated' directions. The Kakeya conjecture states that Kakeya sets must have maximal dimension (i.e., have dimension n). The conjecture is open in dimensions $n \geq 3$ and was shown to have deep connections with other problems in Analysis, Number Theory, PDE's, and others (see [66]).

The most successful line of attack on this conjecture was initiated by Bourgain [11] and later developed by Katz and Tao [43] and uses tools from additive combinatorics. In Section 4.1 we will discuss Kakeya sets over the reals and prove a $\geq (4/7)n$ bound on the Minkowski dimension, which is very close to the best-known lower bound of $(0.596\ldots)n$. The underlying additive combinatorics problem that arises in this context is upper bounding the number of differences $a - b$, for pairs $(a, b) \in G \subset A \times B$ in some graph G as a function of the number of sums (or, more generally, weighted sums) on the same graph. We will not discuss the applications of the Euclidean Kakeya conjecture since they are out of scope for this survey (we are focusing on applications in discrete mathematics and computer science). Even though we will not directly use additive combinatorics results developed in Section 3, they will be in the background and will provide intuition as to what is going on.

Over a finite field $\mathbb{F}_q$ a Kakeya set is a set containing a line in every direction (a line will contain q points). It was conjectured by Wolff [69]

[1] For a definition see Section 4.1.

that the minimum size of a Kakeya set is at least $C_n \cdot q^n$ for some constant C_n depending only on n. We will see the proof of this conjecture (obtained by the author in [20]) which uses the polynomial method. An application of this result, described in Section 4.3, is a construction of *seeded extractors*, which are explicit mappings that transform a 'weak' random source into a close-to-uniform distribution with the aid of a short random 'seed' (since there is a single source, the extractor must use a seed). A specific question that arises in this setting is the following: Suppose Alice and Bob each pick a point $X, Y \in \mathbb{F}_q^n$ (X for Alice, Y for Bob). Consider the random variable Z computed by picking a random point on the line through X, Y. If both Alice and Bob pick their points independently at random then it is easy to see that Z will also be random. But what happens when Bob picks his points Y to be some function $Y = F(X)$? Using the connection to the Kakeya conjecture one can show that, in this case, Z is still sufficiently random in the sense that it cannot hit any small set with high probability. More formally, this requires proving a variant of the Kakeya conjecture over finite field with lines replaced by low degree curves.

Section 5: From Local to Global — Sylvester–Gallai Type Theorems

The Sylvester–Gallai (SG) theorem says that, in a finite set of points in $\mathbb{R}^n$, not all on the same line, there exists a line intersecting exactly two of the points. In other words, if for every two points u, v in the set, the line through u, v contains a third point in the set, then all points are on the same line. Besides being a natural incidence theorem, one can also look at this theorem as converting local geometric information (collinear triples) into global upper bounds on the dimension (i.e., putting all points on a single line, which is one dimensional). We will see several generalizations of this theorem, obtained in [4], in various settings. For example, assume that for every point u in a set of N points there are at least $N/100$ other points v such that the line through u, v contains a third point. We will see in this case that the points all lie on an affine subspace of dimension bounded by a constant. The proof technique here is different than what we have seen so far and will rely

on convex optimization techniques among other things. These results will be described in Section 5.1 with the main technical tool, a rank lower bound for design matrices, proved in Section 5.2.

In Section 5.3 we will consider this type of question over a finite field and see how the bounds are weaker in this case. In particular, under the same assumption as above (with $N/100$) the best possible upper bound on the dimension will be $\lesssim \log_q(N))$, where q is the characteristic of the field [9]. Here, we will again rely on tools from additive combinatorics and will use results proved in Section 3.

In Section 5.4 we will see how this type of question arises naturally in computer science applications involving error-correcting codes which are 'locally correctable'. A (linear) *Locally Correctable Code* (LCC) is a (linear) error-correcting code in which each symbol of a possible corrupted codeword can be corrected by looking at only a few other locations (in the same corrupted codeword). Such codes are very different than 'regular' error-correcting codes (in which decoding is usually done in one shot for all symbols) and have interesting applications in complexity theory.[2]

[2] They are also very much related to Locally *Decodable* Codes (LDCs) which are discussed at length in the survey [71].

References

[1] M. Ajtai, V. Chvtal, M. Newborn, and E. Szemerdi, "Crossing-free subgraphs," in *Theory and Practice of Combinatorics a Collection of Articles Honoring Anton Kotzig on the Occasion of his Sixtieth Birthday*, (G. S. Peter, L. Hammer, A. Rosa, and J. Turgeon, eds.), pp. 9–12, North-Holland, 1982.

[2] N. Alon, "Perturbed identity matrices have high rank: Proof and applications," *Combinatorics of Probability & Computing*, vol. 18, no. 1–2, pp. 3–15, 2009.

[3] A. Balog and E. Szemerédi, "A statistical theorem of set addition," *Combinatorica*, vol. 14, no. 3, pp. 263–268, 1994.

[4] B. Barak, Z. Dvir, A. Yehudayoff, and A. Wigderson, "Rank bounds for design matrices with applications to combinatorial geometry and locally correctable codes," in *Proceedings of the Annual ACM Symposium on Theory of Computing (STOC '11)*, pp. 519–528, New York, NY, USA, 2011.

[5] B. Barak, R. Impagliazzo, and A. Wigderson, "Extracting randomness using few independent sources," *SIAM Journal on Computing*, vol. 36, no. 4, pp. 1095–1118, December 2006.

[6] B. Barak, G. Kindler, R. Shaltiel, B. Sudakov, and A. Wigderson, "Simulating independence: new constructions of condensers, Ramsey graphs, dispersers, and extractors," in *Proceedings of the Annual ACM Symposium on Theory of Computing (STOC '05)*, pp. 1–10, New York, NY, USA, 2005.

[7] J. Beck, "On the lattice property of the plane and some problems of Dirac, Motzkin and Erdos in combinatorial geometry," *Combinatorica*, vol. 3, pp. 281–297, 1983. 10.1007/BF02579184.

[8] A. Besicovitch, "On Kakeya's problem and a similar one," *Mathematische Zeitschrift*, no. 27, pp. 312–320, 1928.

[9] A. Bhattacharyya, Z. Dvir, A. Shpilka, and S. Saraf, "Tight lower bounds for 2-query lccs over finite fields," in *Proceedings of the Symposium on Foundations of Computer science (FOCS 2011)*, pp. 638–647, 2011.

[10] K. Borsuk, "Drei Stze ber die n-dimensionale Euklidische sphre," *Fundamenta Mathematicae*, no. 20, pp. 177–190, 1933.

[11] J. Bourgain, "On the dimension of Kakeya sets and related maximal inequalities," *Geometric and Functional Analysis*, vol. 9, no. 2, pp. 256–282, 1999.

[12] J. Bourgain, "More on the sum-product phenomenon in prime fields and its applications," *International Journal of Number Theory*, 2005.

[13] J. Bourgain, "Multilinear exponential sums in prime fields under optimal entropy condition on the sources," *Geometric And Functional Analysis*, vol. 18, pp. 1477–1502, 2009. 10.1007/s00039-008-0691-6.

[14] J. Bourgain, N. Katz, and T. Tao, "A sum-product estimate in finite fields, and applications," *Geometric And Functional Analysis*, vol. 14, pp. 27–57, 2004. 10.1007/s00039-004-0451-1.

[15] I. Brny and D. G. Larman, "The convex hull of the integer points in a large ball," *Mathematische Annalen*, vol. 312, pp. 167–181, 1998. 10.1007/s002080050217.

[16] B. Chazelle, H. Edelsbrunner, L. J. Guibas, R. Pollack, R. Seidel, M. Sharir, and J. Snoeyink, "Counting and cutting cycles of lines and rods in space," in *Proceedings of the Annual Symposium on Foundations of Computer Science (SFCS '90)* , vol. 1, pp. 242–251, Washington, DC, USA, 1990.

[17] B. Chor and O. Goldreich, "Unbiased bits from sources of weak randomness and probabilistic communication complexity," *SIAM Journal on Computing*, vol. 17, no. 2, pp. 230–261, April 1988.

[18] K. L. Clarkson, H. Edelsbrunner, L. J. Guibas, M. Sharir, and E. Welzl, "Combinatorial complexity bounds for arrangement of curves and spheres," *Discrete & Computational Geometry*, vol. 5, pp. 99–160, 1990.

[19] R. O. Davies, "Some remarks on the Kakeya problem," *Mathematical Proceedings of the Cambridge Philosophical Society*, vol. 69, no. 03, pp. 417–421, 1971.

[20] Z. Dvir, "On the size of Kakeya sets in finite fields," *Journal of the American Mathematical Society*, 2008.

[21] Z. Dvir, S. Kopparty, S. Saraf, and M. Sudan, "Extensions to the method of multiplicities, with applications to Kakeya sets and mergers," in *Proceedings of the 2009 Annual Symposium on Foundations of Computer Science (FOCS 09)*, 2009. (to appear).

[22] Z. Dvir, S. Saraf, and A. Wigderson. Manuscript (in preparation), 2012.

[23] Z. Dvir and A. Shpilka, "Locally decodable codes with 2 queries and polynomial identity testing for depth 3 circuits," *SIAM Journal on Computing*, vol. 36, no. 5, pp. 1404–1434, 2006.

[24] Z. Dvir and A. Wigderson, "Kakeya sets, new mergers and old extractors," in *Proceedings of the 2008 Annual IEEE Symposium on Foundations of Computer Science (FOCS '08)*, pp. 625–633, Washington, DC, USA, 2008.

[25] G. Elekes, "On the number of sums and products," *Acta Arithmetica*, no. 81, pp. 365–367, 1997.

[26] G. Elekes, H. Kaplan, and M. Sharir, "On lines, joints, and incidences in three dimensions," *Journal of Combinatorial Theory, Series A*, vol. 118, no. 3, pp. 962–977, 2011.
[27] G. Elekes and M. Sharir, "Incidences in three dimensions and distinct distances in the plane," in *Proceedings of the 2010 Annual Symposium on Computational Geometry*, pp. 413–422, New York, NY, USA, 2010.
[28] P. Erdos, "On sets of distances of n points," *The American Mathematical Monthly*, vol. 53, no. 5, pp. 248–250, 1946.
[29] P. Erdos and E. Szemerdi, "On sums and products of integers," *Studies in pure mathematics*, pp. 213–218, 1983.
[30] O. Goldreich, H. Karloff, L. Schulman, and L. Trevisan, "Lower bounds for locally decodable codes and private information retrieval," in *IEEE Computational Complexity Conference (CCC)*, pp. 175–183, 2002.
[31] W. T. Gowers, "A new proof of Szemeredi's theorem for arithmetic progressions of length four," *Geometric and Functional Analysis*, vol. 17, no. 2, pp. 230–261, 1998.
[32] B. Green, "Additive Combinatorics," Cambridge lecture notes, http://www.dpmms.cam.ac.uk/ bjg23/add-combinatorics.html, 2009.
[33] L. Guth, "The endpoint case of the Bennett-Carbery-Tao multilinear Kakeya conjecture," arXiv/0811.2251, 2008.
[34] L. Guth and N. H. Katz, "Algebraic methods in discrete analogs of the Kakeya problem," *Advances in Mathematics*, vol. 225, no. 5, pp. 2828–2839, 2010.
[35] L. Guth and N. H. Katz, "On the Erdos distinct distance problem in the plane," arXiv/1011.4105, 2010.
[36] A. J. W. Hilton, "On double diagonal and cross Latin squares," *Journal of the London Mathematical Society*, vol. s2-6, no. 4, pp. 679–689, 1973.
[37] A. Iosevich Fourier analysis and geometric combinatorics. To appear in the Birkhauser volume dedicated to the annual Padova lectures in analysis, 2004.
[38] A. Iosevich, O. Roche-Newton, and M. Rudnev, "On an application of Guth-Katz theorem," arXiv/1103.1354, 2011.
[39] H. Kaplan, J. Matouvsek, and M. Sharir, "Simple proofs of classical theorems in discrete geometry via the guth–katz polynomial partitioning technique," arXiv/1102.5391, 2011.
[40] H. Kaplan, M. Sharir, and E. Shustin, "On lines and joints," *Discrete & Computational Geometry*, vol. 44, pp. 838–843, 2010. 10.1007/s00454-010-9246-3.
[41] J. Katz and L. Trevisan, "On the efficiency of local decoding procedures for error-correcting codes," in *ACM Symposium on Theory of Computing (STOC)*, pp. 80–86, 2000.
[42] N. Katz and T. Tao, "Bounds on arithmetic projections, and applications to the Kakeya conjecture," *Mathematical Research Letters*, vol. 6, pp. 625–630, 1999.
[43] N. Katz and T. Tao, "New bounds for Kakeya problems," *Journal d'Analyse de Jerusalem*, vol. 87, pp. 231–263, 2002.
[44] L. M. Kelly, "A Resolution of the Sylvester — Gallai Problem of J.-P. Serre," *Discrete & Computational Geometry*, vol. 1, pp. 101–104, 1986.

[45] J. Kollr, "Sharp effective Nullstellensatz," *Journal of the American Mathematical Society*, vol. 1, pp. 963–975, 1988.

[46] S. Kopparty and S. Saraf, "Local list-decoding and testing of random linear codes from high error," in *Proceedings of the ACM Symposium on Theory of Computing*, pp. 417–426, New York, NY, USA, 2010.

[47] F. T. Leighton, "New lower bound techniques for VLSI," in *Proceedings of the Annual Symposium on Foundations of Computer Science (SFCS '81)*, pp. 1–12, Washington, DC, USA, 1981.

[48] N. Linial, A. Samorodnitsky, and A. Wigderson, "A deterministic strongly polynomial algorithm for matrix scaling and approximate permanents," *Combinatorica*, vol. 20, no. 4, pp. 545–568, 2000.

[49] C. Lu, O. Reingold, S. Vadhan, and A. Wigderson, "Extractors: Optimal up to constant factors," in *Proceedings of the Annual ACM Symposium on Theory of Computing (FOCS 03)*, 2003.

[50] J. Matousek, *Using the Borsuk-Ulam Theorem: Lectures on Topological Methods in Combinatorics and Geometry*. Springer Publishing Company, Incorporated, 2007.

[51] G. Mockenhaupt and T. Tao, "Restriction and Kakeya phenomena for finite fields," *Duke Mathematical Journal*, vol. 121, pp. 35–74, 2004.

[52] D. E. Muller, "Application of boolean algebra to switching circuit design and to error detection," *IEEE Transactions on Computers*, vol. 3, pp. 6–12, 1954.

[53] J. Pach and M. Sharir, "On the number of incidences between points and curves," *Combinatorics Probability & Computing*, vol. 7, no. 1, pp. 121–127, March 1998.

[54] L. M. Pretorius, N. D. Elkies, and K. J. Swanepoel, "Sylvester-gallai theorems for complex numbers and quaternions," *Discrete and Computational Geometry*, vol. 35, no. 3, pp. 361–373, 2006.

[55] I. S. Reed, "A class of multiple-error-correcting codes and the decoding scheme," *IEEE Transactions on Information Theory*, vol. 4, pp. 38–49, 1954.

[56] U. Rothblum and H. Schneider, "Scaling of matrices which have prespecified row sums and column sums via optimization," *Linear Algebra and Its Applications*, vol. 114–115, pp. 737–764, 1989.

[57] I. Ruzsa, "Sums of finite sets," in *Number Theory: New York Seminar*, (D. V. Chudnovsky, G. V. Chudnovsky, and M. B. Nathanson, eds.), Springer Verlag, 1996.

[58] I. Z. Ruzsa, "Sums of finite sets," *Number theory (New York, 1991–1995)*, pp. 281–293, 1996.

[59] S. Saraf and M. Sudan, "Improved lower bound on the size of Kakeya sets over finite fields," *Analysis and PDE*, vol. 1, no. 3, pp. 375–379, 2008.

[60] R. Shaltiel, B. Barak, A. Rao, and A. Wigderson, "2-source dispersers for subpolynomial entropy and Ramsey graphs beating the Frankl-Wilson construction," in *Proceedings of Annual ACM Symposium on Theory of Computing*, pp. 671–680, 2006.

[61] R. Sinkhorn, "A relationship between arbitrary positive matrices and doubly stochastic matrices," *The Annals of Mathematical Statististics*, vol. 35, pp. 876–879, 1964.

[62] J. Solymosi, "On the number of sums and products," *Bulletin of the London Mathematical Society*, vol. 37, no. 4, pp. 491–494, 2005.

[63] A. H. Stone and J. W. Tukey, "Generalized sandwich theorems," *Duke Mathematical Journal*, no. 9, pp. 356–359, 1942.

[64] L. A. Székely, "Crossing numbers and hard Erdos problems in discrete geometry," *Combinatorics Probability and Computing*, vol. 6, no. 3, pp. 353–358, September 1997.

[65] E. Szemerédi and W. T. Trotter, "Extremal problems in discrete geometry," *Combinatorica*, vol. 3, no. 3, pp. 381–392, 1983.

[66] T. Tao, "From rotating needles to stability of waves: emerging connections between combinatorics, analysis, and PDE," *Notices of the American Mathematical Society*, vol. 48, no. 3, pp. 294–303, 2001.

[67] T. Tao, "The Szemerdi–Trotter theorem and the cell decomposition," *Blog: What's new*, 12 June 2009. http://terrytao.wordpress.com/2009/06/12/the-szemeredi-trotter-theorem-and-the-cell-decomposition/.

[68] C. Toth, "The Szemeredi–Trotter theorem in the complex plane," *arXiv:math/0305283v4*, 2003.

[69] T. Wolff, "Recent work connected with the Kakeya problem," *Prospects in mathematics (Princeton, NJ, 1996)*, pp. 129–162, 1999.

[70] D. Woodruff, "New lower bounds for general locally decodable codes," in *Electronic Colloquium on Computational Complexity (ECCC)*, 2007.

[71] S. Yekhanin, "Locally Decodable Codes," *Foundations and Trends in Theoretical Computer Science*, 2011. To appear. Preliminary version available for download at http://research.microsoft.com/en-us/um/people/yekhanin/Papers/LDC now.pdf.