Algebraic and probabilistic methods in Discrete Mathematics

Noga Alon *

Abstract

Combinatorics is an essential component of many mathematical areas, and its study has experienced an impressive growth in recent years. This survey contains a discussion of two of the main general techniques that played a crucial role in the development of modern combinatorics; algebraic methods and probabilistic methods. Both techniques are illustrated by examples, where the emphasis is on the basic ideas and the connection to other areas.

1 Introduction

Mathematical Research deals with ideas that can be meaningful to everybody and there is no doubt that it also lies behind most of the major advances in Science and Technology. Yet, mathematicians often tend to formulate their questions, results and thoughts in a way that is comprehensible only to their colleagues that work in a closely related area. One of the goals of the conference "Visions in Mathematics" was to try and present the main areas in mathematics in a way that can be interesting to a general mathematical audience, and possibly even to a general scientific audience. Although this is a difficult task, it is not impossible, and I believe that many of the lectures achieved this goal.

Following the spirit of the conference, this survey is also aimed to a general mathematical audience. I try to explain two of the main techniques that played a crucial role in the development of modern combinatorics: algebraic techniques and probabilistic methods. The focus is on basic ideas, rather than on technical details, and the techniques are illustrated by examples that demonstrate the connection between combinatorics and related mathematical areas.

My choice of topics and examples is inevitably influenced by my own personal taste, and hence it is somewhat arbitrary. Still, I believe that it provides some of the flavour of the techniques, problems and results in the area, which may hopefully be appealing to researchers in mathematics, even if their main interest is not Discrete Mathematics.

*School of Mathematics and Computer Science, Raymond and Beverly Sackler Faculty of Exact Sciences, Tel Aviv University, Tel Aviv, Israel. Email: noga@math.tau.ac.il. Research supported in part by a USA Israeli BSF grant, by a grant from the Israel Science Foundation and by the Hermann Minkowski Minerva Center for Geometry at Tel Aviv University.

2 Algebraic techniques

Various algebraic techniques have been used successfully in tackling problems in Discrete Mathematics over the years. These include several tools that I will not discuss here, like tools from Representation Theory applied extensively in enumeration problems, or spectral techniques used in the study of highly regular structures. In this section I describe mainly two representative algebraic tools. The first one may be called Combinatorial Nullstellensatz, is based on some basic properties of polynomials, and has applications in Combinatorial Number Theory, Graph Theory and Combinatorics. The second one may be called the dimension argument, and has had numerous applications over the years. The examples given here illustrate the basic ideas. More examples can be found in various survey articles and books including [25], [3], [11], [12].

2.1 Combinatorial Nullstellensatz

The classical Hilbert's Nullstellensatz (see, e.g., [45]) asserts that if F is an algebraically closed field, $f, g_1, \ldots, g_m$ are polynomials in the ring of polynomials $F[x_1, \ldots, x_n]$, and f vanishes over all common zeros of $g_1, \ldots, g_m$, then there is an integer k and polynomials $h_1, \ldots, h_m$ in $F[x_1, \ldots, x_n]$ so that

$$f^k = \sum_{i=1}^{n} h_i g_i.$$

In the special case $m = n$, where each g_i is a univariate polynomial of the form $\prod_{s \in S_i}(x_i - s)$, a stronger conclusion holds, as follows.

Theorem 2.1 *Let F be an arbitrary field, and let $f = f(x_1, \ldots, x_n)$ be a polynomial in $F[x_1, \ldots, x_n]$. Let $S_1, \ldots, S_n$ be nonempty subsets of F and define $g_i(x_i) = \prod_{s \in S_i}(x_i - s)$. If f vanishes over all the common zeros of $g_1, \ldots, g_n$ (that is; if $f(s_1, \ldots, s_n) = 0$ for all $s_i \in S_i$), then there are polynomials $h_1, \ldots, h_n \in F[x_1, \ldots, x_n]$ satisfying $deg(h_i) \leq deg(f) - deg(g_i)$ so that*

$$f = \sum_{i=1}^{n} h_i g_i.$$

As a consequence of the above one can prove the following,

Theorem 2.2 *Let F be an arbitrary field, and let $f = f(x_1, \ldots, x_n)$ be a polynomial in $F[x_1, \ldots, x_n]$. Suppose the degree $deg(f)$ of f is $\sum_{i=1}^{n} t_i$, where each t_i is a nonnegative integer, and suppose the coefficient of $\prod_{i=1}^{n} x_i^{t_i}$ in f is nonzero. Then, if $S_1, \ldots, S_n$ are subsets of F with $|S_i| > t_i$, there are $s_1 \in S_1, s_2 \in S_2, \ldots, s_n \in S_n$ so that*

$$f(s_1, \ldots, s_n) \neq 0.$$

These two results are proved in [5], where it is proposed to call them *Combinatorial Nullstellensatz*. The proofs are based on some simple properties of polynomials. It turns out that these results are related to some classical ones, and have many combinatorial applications.

One of the classical results that follow easily from Theorem 2.2 is the following theorem, conjectured by Artin in 1934, proved by Chevalley in 1935 and extended by Warning in 1935.

Theorem 2.3 (cf., e.g., [41]) *Let p be a prime, and let*

$$P_1 = P_1(x_1, \ldots, x_n), P_2 = P_2(x_1, \ldots, x_n), \ldots, P_m = P_m(x_1, \ldots, x_n)$$

be m polynomials in the ring $Z_p[x_1, \ldots, x_n]$. If $n > \sum_{i=1}^{m} deg(P_i)$ and the polynomials P_i have a common zero $(c_1, \ldots, c_n)$, then they have another common zero.

The proof follows in a few lines by applying Theorem 2.2 to the polynomial

$$f = f(x_1, \ldots, x_n) = \prod_{i=1}^{m}(1 - P_i(x_1, \ldots, x_n)^{p-1}) - \delta \prod_{j=1}^{n} \prod_{c \in Z_p, c \neq c_j} (x_j - c),$$

where δ is chosen so that $f(c_1, \ldots, c_n) = 0$.

Another classical result that follows from a similar reasoning is the Cauchy-Davenport Theorem, which is one of the fundamental results in Additive Number Theory, see, e.g., [35]. This theorem asserts that if p is a prime, and A, B are two nonempty subsets of Z_p, then

$$|A + B| \geq min\{p, |A| + |B| - 1\}.$$

Cauchy proved this theorem in 1813, and applied it to give a new proof to a lemma of Lagrange in his well known 1770 paper that shows that any integer is a sum of four squares. Davenport formulated the theorem as a discrete analogue of a conjecture of Khintchine (proved a few years later) about the Schnirelman density of the sum of two sequences of integers. The original proofs of the theorem given by Cauchy and Davenport are purely combinatorial. As observed in [8], there is a different, algebraic proof, which extends easily and gives several related results. This proof is, again, a simple application of Theorem 2.2. It readily extends to provide bounds for restricted sums in finite fields. If $h = h(x_0, x_1, \ldots, x_k)$ is a polynomial over Z_p and $A_0, A_1, \ldots, A_k$ are subsets of Z_p, then the method provides a lower bound (which is often tight) for the cardinality of the set

$$\{a_0 + a_1 + \ldots + a_k : a_i \in A_i, \quad h(a_0, a_1, \ldots, a_k) \neq 0\}.$$

When h is the polynomial $\prod_{k \geq i > j \geq 0}(x_i - x_j)$ the above set corresponds to sums of disticnt elements. By applying Theorem 2.2 to an appropriate polynomial, and by observing that the relevant coefficient in this case can be computed from the known results about the Ballot problem (see, e.g.,

[32]), as well as from the known connection between this problem and the hook formula for the number of Young tableaux of a given shape, one can obtain a tight lower bound for the number of such sums. The very special case of this result in which $k = 1$, $A_0 = A$ and $A_1 = A - \{a\}$ for an arbitrary element $a \in A$, implies the following theorem, conjectured by Erdős and Heilbronn in 1964 (cf., e.g., [20]) and proved, after various partial results by several researchers, by Dias Da Silva and Hamidoune [16], using some tools from linear algebra and the representation theory of the symmetric group.

Theorem 2.4 ([16]) *If p is a prime, and A is a nonempty subset of Z_p, then*

$$|\{a + a' : a, a' \in A, a \neq a'\}| \geq min\{p, 2|A| - 3\}.$$

This special case can be proved directly by assuming it is false, taking C to be a set of cardinality $2|A| - 4$ containing all sums of distinct elements $a_1, a_2 \in A$, with $a_2 \neq a$ for some fixed $a \in A$, and then by applying Theorem 2.2 to the polynomial $f(x, y) = (x - y)\prod_{c \in C}(x + y - c)$ to get a contradiction.

Erdős, Ginzburg and Ziv [21] proved that every sequence of $2n - 1$ elements of the cyclic group Z_n contains a subsequence of exactly n terms whose sum (in Z_n) is 0. This is tight, as shown, for example, by the sequence consisting of $n - 1$ zeros and $n - 1$ ones. The main part of the proof of this statement is its proof for prime values of $n = p$, as the general case can then be easily obtained by induction. Kemnitz [29] conjectured that for every prime p, every sequence of $4p - 3$ elements of Z_p^2 contains a subsequence of exactly p terms whose sum (in Z_p^2) is zero. Rónyai has proved, very recently, that $4p - 2$ elements suffice. His proof can be described as an application of Theorem 2.2. This is done by first proving the following lemma.

Lemma 2.5 ([6]) *If $(a_1, b_1), \ldots, (a_{3p}, b_{3p}) \in Z_p^2$ and $\sum_{i=1}^{3p}(a_i, b_i) = 0$ (in Z_p^2), then there is an $I \subset \{1, 2, \ldots, 3p\}$, $|I| = p$, such that $\sum_{i \in I}(a_i, b_i) = 0$.*

To prove the lemma, consider the polynomial

$$f(x_1, x_2, \ldots, x_{3p-1}) = (1 - (\sum_{i=1}^{3p-1} a_i x_i)^{p-1})(1 - (\sum_{i=1}^{3p-1} b_i x_i)^{p-1})(1 - (\sum_{i=1}^{3p-1} x_i)^{p-1}) - \prod_{i=1}^{3p-1}(1 - x_i).$$

Then the coefficient of $\prod_{i=1}^{3p-1} x_i$ is nonzero, and hence, by Theorem 2.2 with $S_1 = S_2 \ldots = S_{3p-1} = \{0, 1\}$ there are $x_i \in \{0, 1\}$ such that $f(x_1, \ldots, x_{3p-1})$ is not zero. As $f(0, 0, \ldots, 0) = 0$, not all x_i are 0. If $\sum_{i=1}^{3p-1} x_i$ is not zero modulo p then $f(x_1, \ldots, x_{3p-1}) = 0$, hence this sum is either p or $2p$. In both cases we get the desired result, where in the second case we apply the fact that the sum of all $3p$ vectors is 0.

To prove, next, that any sequence $(a_1, b_1), (a_2, b_2), \ldots, (a_{4p-2}, b_{4p-2})$ of elements of Z_p^2 contains a subsequence of precisely p terms whose sum is 0, apply Theorem 2.2 to the polynomial

$$f(x_1, x_2, \ldots, x_{4p-2})$$

$$= (1-(\sum_{i=1}^{4p-2} a_i x_i)^{p-1})(1-(\sum_{i=1}^{4p-2} b_i x_i)^{p-1})((1-(\sum_{i=1}^{4p-2} x_i)^{p-1})(2-\sum_{J\subset\{1,2,\ldots,4p-2\},|J|=p}\prod_{j\in J} x_j)-2\prod_{i=1}^{4p-2}(1-x_i),$$

with $S_1 = S_2 = \ldots = S_{4p-2} = \{0, 1\}$. As the coefficient of $\prod_i x_i$ is nonzero there are $x_i \in \{0, 1\}$ such that $f(x_1, \ldots, x_{4p-2}) \neq 0$. It is easy to check that not all x_i are zero. It also follows that $\sum_i x_i$ must be divisible by p; if it is p we are done, if it is $3p$ the desired result follows from the lemma, and the last ingredient is the fact that if it is $2p$ then the term

$$2 - \sum_{J\subset\{1,2,\ldots,4p-2\},|J|=p}\prod_{j\in J} x_j$$

is zero and hence so is f. This completes the proof.

Theorem 2.2 has various applications in Graph Theory, including ones in Graph Coloring, which is the most popular area of the subject. We sketch below the basic approach, following [10]. See also [33] for a related method.

A *vertex coloring* of a graph G is an assignment of a color to each vertex of G. The coloring is *proper* if adjacent vertices receive distinct colors. The *chromatic number* $\chi(G)$ of G is the minimum number of colors used in a proper vertex coloring of G. An *edge coloring* of G is, similarly, an assignment of a color to each edge of G. It is *proper* if adjacent edges receive distinct colors. The minimum number of colors in a proper edge-coloring of G is the *chromatic index* $\chi'(G)$ of G. This is equal to the chromatic number of the line graph of G.

A graph $G = (V, E)$ is *k-choosable* if for every assignment of sets of integers $S(v) \subset Z$, each of size k, to the vertices $v \in V$, there is a proper vertex coloring $c : V \mapsto Z$ so that $c(v) \in S(v)$ for all $v \in V$. The *choice number* of G, denoted $ch(G)$, is the minimum integer k so that G is k-choosable. Obviously, this number is at least the chromatic number $\chi(G)$ of G. The choice number of the line graph of G, denoted here by $ch'(G)$, is usually called the *list chromatic index* of G, and it is clearly at least the chromatic index $\chi'(G)$ of G.

The study of choice numbers was introduced, independently, by Vizing [47] and by Erdős, Rubin and Taylor [23]. There are many graphs G for which the choice number $ch(G)$ is strictly larger than the chromatic number $\chi(G)$ (a complete bipartite graph with 3 vertices in each color class is one such example). In view of this, the following conjecture, suggested independently by various researchers including Vizing, Albertson, Collins, Tucker and Gupta, which apparently appeared first in print in the paper of Bollobás and Harris ([13]), is somewhat surprising.

Conjecture 2.6 (The list coloring conjecture) *For every graph G, $ch'(G) = \chi'(G)$.*

This conjecture asserts that for *line graphs* there is no gap at all between the choice number and the chromatic number. Many of the most interesting results in the area are proofs of special cases of this conjecture, which is still wide open.

The *graph polynomial* $f_G = f_G(x_1, x_2, \ldots, x_n)$ of a graph $G = (V, E)$ on a set $V = \{1, \ldots, n\}$ of n vertices is defined by $f_G(x_1, x_2, \ldots, x_n) = \Pi\{(x_i - x_j) : i < j \ , \ ij \in E\}$. This polynomial has been studied by various researchers, starting already with Petersen [37] in 1891. Note that if $S_1, \ldots, S_n$ are sets of integers, then there is a proper coloring assigning to each vertex i a color from its list S_i, if and only if there are $s_i \in S_i$ such that $f_G(s_1, \ldots, s_n) \neq 0$. This condition is precisely the one appearing in the conclusion of Theorem 2.2, and it is therefore natural to expect that this theorem can be useful in tackling coloring problems. By applying it to line graphs of planar, cubic graphs, and by interpreting the appropriate coefficient of the corresponding polynomial combinatorially, it can be shown, using a known result of Vigneron [46] and the Four Color Theorem, that the list chromatic index of every 2-connected cubic planar graph is 3. This is a strengthening of the Four Color Theorem, which is well known to be equivalent to the fact that the chromatic index of any such graph is 3. An extension of this result appears in [18].
Additional results on graph coloring and choice numbers using the algebraic approach are described in the survey [2].

2.2 The dimension argument

In order to prove an upper bound for the cardinality of a set, it is sometimes possible to associate each member of the set with a vector in an appropriately defined vector space, and show that the set of vectors obtained in this manner is linearly independent. Thus, the cardinality of the set is at most the dimension of the vector space. This simple linear-algebra technique, which may be called the *dimension argument*, has many impressive combinatorial applications. In this subsection we describe a few representative examples.

Borsuk [15] asked if any set of points in R^d can be partitioned into at most $d + 1$ subsets of smaller diameter. Kahn and Kalai [30] gave an example showing that this is not the case, by applying a theorem of Frankl and Wilson [24]. Here is a sketch of a slightly modified version of this counterexample, following Nilli [36]. The main part of the proof uses the the dimension argument. Let $n = 4p$, where p is an odd prime, and let $\mathcal{F}$ be the set of all vectors $\mathbf{x} = (x_1, \ldots, x_n) \in \{-1, 1\}^n$, where $x_1 = 1$ and the number of negative coordinates of $\mathbf{x}$ is even.

Lemma 2.7 *If $\mathcal{G} \subset \mathcal{F}$ contains no two orthogonal vectors then $|\mathcal{G}| \leq \sum_{i=0}^{p-1} \binom{n-1}{i}$.*

To prove the lemma note, first, that the scalar product $\mathbf{a} \cdot \mathbf{b}$ of any two members of $\mathcal{F}$ is divisible by 4, and since there is no $\mathbf{a} \in \mathcal{F}$ for which $-\mathbf{a}$ is also in $\mathcal{F}$ the assumption implies that there are no distinct $\mathbf{a}$ and $\mathbf{b}$ in $\mathcal{G}$ so that $\mathbf{a} \cdot \mathbf{b} \equiv 0 \ (mod\ p)$. For each $\mathbf{a} \in \mathcal{G}$ define a polynomial over the finite field $GF(p)$ as follows: $P_{\mathbf{a}}(\mathbf{x}) = \prod_{i=1}^{p-1}(\mathbf{a} \cdot \mathbf{x} - i)$, where here $\mathbf{x} = (x_1, \ldots, x_n)$ is a vector of variables. Note that by the assumption
(i) $P_{\mathbf{a}}(\mathbf{b}) = 0$ (in $GF(p)$) for every two distinct members $\mathbf{a}$ and $\mathbf{b}$ of $\mathcal{G}$, and
(ii) $P_{\mathbf{a}}(\mathbf{a}) \neq 0$ for all $\mathbf{a} \in \mathcal{G}$.

Let $\overline{P}_{\mathbf{a}}$ be the multilinear polynomial obtained from the standard representation of $P_{\mathbf{a}}$ as a sum of monomials by using, repeatedly, the relations $x_i^2 = 1$. Since $\overline{P}_{\mathbf{a}}(\mathbf{x}) = P_{\mathbf{a}}(\mathbf{x})$ for every vector $\mathbf{x}$ with $\{-1, 1\}$ coordinates, the relations (i) and (ii) above hold with every P replaced by $\overline{P}$.

It is easy to see that this implies that the polynomials $\overline{P}_{\mathbf{a}}$ for $\mathbf{a} \in \mathcal{G}$ are linearly independent. Therefore, $|\mathcal{G}|$ is bounded by the dimension of the space of multilinear polynomials of degree at most $p-1$ in $n-1$ variables (since $x_1 = 1$) over $GF(p)$, which is $\sum_{i=0}^{p-1} \binom{n-1}{i}$, completing the proof of the lemma.
For any n-vector $\mathbf{x} = (x_1, \ldots, x_n)$, let $\mathbf{x} * \mathbf{x}$ denote the tensor product of $\mathbf{x}$ with itself, i.e., the vector of length n^2, $(x_{ij} : 1 \leq i, j \leq n)$, where $x_{ij} = x_i x_j$. Define $S = \{\mathbf{x} * \mathbf{x} : \mathbf{x} \in \mathcal{F}\}$, where $\mathcal{F}$ is as above. The norm of each vector in S is n and the scalar product between any two members of S is easily seen to be non-negative. Moreover, by Lemma 2.7 any set of more than $\sum_{i=0}^{p-1} \binom{n-1}{i}$ members of S contains an orthogonal pair, i.e., two points the distance between which is the diameter of S. It follows that S cannot be partitioned into less than $2^{n-2} / \sum_{i=0}^{p-1} \binom{n-1}{i}$ subsets of smaller diameter.

The vectors in S lie in an affine subspace of dimension $\binom{n}{2}$, and hence if

$$2^{n-2} / \sum_{i=0}^{p-1} \binom{n-1}{i} > \binom{n}{2} + 1,$$

the set S is a subset of R^d for $d = \binom{n}{2}$ that cannot be partitioned into at most $d+1$ subsets of smaller diameter. The smallest d for which this holds (with $n = 4p$, p an odd prime) is $d = 946 = \binom{44}{2}$ obtained by taking $p = 11$.

For an undirected graph $G = (V, E)$, let G^n denote the graph whose vertex set is V^n in which two distinct vertices $(u_1, u_2, \ldots, u_n)$ and $(v_1, v_2, \ldots, v_n)$ are adjacent iff for all i between 1 and n either $u_i = v_i$ or $u_i v_i \in E$. The *Shannon capacity* $c(G)$ of G is the limit $\lim_{n\to\infty}(\alpha(G^n))^{1/n}$, where $\alpha(G^n)$ is the maximum size of an independent set of vertices in G^n. This limit exists, by super-multiplicativity, and it is always at least $\alpha(G)$.

The study of this parameter was introduced by Shannon in [40], motivated by a question in Information Theory. Indeed, if V is the set of all possible letters a channel can transmit in one

use, and two letters are adjacent if they may be confused, then $\alpha(G^n)$ is the maximum number of messages that can be transmitted in n uses of the channel with no danger of confusion. Thus $c(G)$ represents the number of distinct messages *per use* the channel can communicate with no error while used many times.

The *(disjoint) union* of two graphs G and H, denoted $G + H$, is the graph whose vertex set is the disjoint union of the vertex sets of G and of H and whose edge set is the (disjoint) union of the edge sets of G and H. If G and H are graphs of two channels, then their union represents the *sum* of the channels corresponding to the situation where either one of the two channels may be used, a new choice being made for each transmitted letter.

Shannon [40] proved that for every G and H, $c(G + H) \geq c(G) + c(H)$ and that equality holds if the vertex set of one of the graphs, say G, can be covered by $\alpha(G)$ cliques. He conjectured that in fact equality always holds. Counter examples are given in [4], where it is shown that there are graphs G and H satisfying $c(G) \leq k$ and $c(H) \leq k$, whereas $c(G + H) \geq k^{(1+o(1))\frac{\log k}{8 \log \log k}}$ and the $o(1)$-term tends to zero as k tends to infinity.

The construction is based on some of the ideas of Frankl and Wilson [24], together with a method for bounding the Shannon capacity of a graph using the dimension argument. This bound, described below, is strongly related to a bound of Haemers [27].

Let $G = (V, E)$ be a graph and let $\mathcal{F}$ be a subspace of the space of polynomials in r variables over a field F. A *representation* of G over $\mathcal{F}$ is an assignment of a polynomial f_v in $\mathcal{F}$ to each vertex $v \in V$ and an assignment of a point $c_v \in F^r$ to each $v \in V$ such that the following two conditions hold:

1. For each $v \in V$, $f_v(c_v) \neq 0$.
2. If u and v are distinct nonadjacent vertices of G then $f_v(c_u) = 0$.

In these notations, the following holds.

Proposition 2.8 *Let $G = (V, E)$ be a graph and let $\mathcal{F}$ be a subspace of the space of polynomials in r variables over a field F. If G has a representation over $\mathcal{F}$ then $c(G) \leq dim(\mathcal{F})$.*

This is proved by associating each vertex of an independent set of maximum cardinality in a given power of G, an appropriate polynomial in the corresponding tensor power of $\mathcal{F}$, and by showing that these polynomials are linearly independent. The details can be found in [4].

Many additional applications of the dimension argument appear in [12], [11], [25].

3 Probabilistic methods

The discovery, demonstrated in the early work of various researchers, that deterministic statements can be proved by probabilistic reasoning, led already more than fifty years ago to several striking results in Analysis, Number Theory, Combinatorics and Information Theory. These are demonstrated in early papers of Paley, Zygmund, Kac, Shannon, Turán and Szele, and even more so in the work of Paul Erdős. It soon became clear that the method, which is now called *the probabilistic method*, is a very powerful tool for proving results in Discrete Mathematics. The early results combined combinatorial arguments with fairly elementary probabilistic techniques, whereas the development of the method in recent years required the application of more sophisticated tools from probability theory. There is, by now, a huge amount of material on the topic, and it is hopeless to try and survey it in a comprehensive manner here. My intention in this section is therefore merely to illustrate the basic ideas with a few representative examples. More material can be found in the books [9], [42] and [28].

The *Ramsey number* $R(k,t)$ is the minimum number n such that every graph on n vertices contains either a clique of size k or an independent set of size t. By a special case of the celebrated theorem of Ramsey (cf., e.g., [26]), $R(k,t)$ is finite for every positive integers k and t, and in fact $R(k,t) \leq \binom{k+t-2}{k-1}$. In particular, $R(k,k) < 4^k$. The problem of determining or estimating the numbers $R(k,t)$ received a considerable amount of attention, and seems to be very difficult in general.

In one of the first applications of the probabilistic method in Combinatorics, Erdős [19] proved that if $\binom{n}{k}2^{1-\binom{k}{2}} < 1$ then $R(k,k) > n$. Therefore, $R(k,k) > \lfloor 2^{k/2} \rfloor$ for all $k > 2$. The proof is (by now) extremely simple; Let $G = G(n,1/2)$ be a *random graph* on the n vertices $\{1,2,\ldots,n\}$, obtained by picking each pair of distinct vertices, randomly and independently, to be connected with probability $1/2$. Every fixed set of k vertices of G forms a clique or an independent set with probability $2^{1-\binom{k}{2}}$. Thus $\binom{n}{k}2^{1-\binom{k}{2}}$ (< 1) is an upper bound for the probability that G contains a clique or an independent set of size k. It follows that with positive probability G is a graph without such cliques or independent sets, and hence such a graph exists !

A proper coloring of a graph is *acyclic* if there is no two-colored cycle. The *acyclic chromatic number* of a graph is the minimum number of colors in an acyclic coloring of it. The Four Color Theorem, which is the best known result in Discrete Mathematics, asserts that the chromatic number of every planar graph is at most 4. Answering a problem of Grünbaum and improving results of various authors, Borodin [14] showed that every planar graph has an acyclic 5-coloring. He conjectured that for any surface but the plane, the maximum possible chromatic number of a graph

embeddable on the surface, is equal to the maximum possible acyclic chromatic number of a graph embeddable on it. The Map Color Theorem proved in [39] determines precisely the maximum possible chromatic number of any graph embeddable on a surface of genus g. This maximum is the maximum number of vertices of a complete graph embeddable on such a surface, which turns out to be

$$\lfloor \frac{7+\sqrt{1+48g}}{2} \rfloor = \Theta(g^{1/2}).$$

The following result shows that the maximum possible acyclic chromatic number of a graph on such a surface is asymptotically different, thus disproving Borodin's conjecture.

Theorem 3.1 ([7]) *The acyclic chromatic number of any graph embeddable on a surface of genus g is at most $O(g^{4/7})$. Moreover, for every $g > 0$ there is a graph embeddable on a surface of genus g whose acyclic chromatic number is at least $\Omega(g^{4/7}/(\log g)^{1/7})$.*

The proof of the $O(g^{4/7})$ upper bound is probabilistic, and combines some combinatorial arguments with the Lovász Local Lemma. This Lemma, proved in [22], is a tool for proving that under suitable conditions, with positive probability, none of a large finite collection of nearly independent, low probability events in a probability space holds. This positive probability is often extremely small, and yet the Local Lemma can be used to show it is positive. The proof of the $\Omega(g^{4/7}/(\log g)^{1/7})$ lower bound is also probabilistic, and is based on an appropriate random construction. Note that the statement of the above theorem is purely deterministic, and yet its proof relies heavily on probabilistic arguments.

The final example in this section is a recent gem; it is based on a simple result in graph theory, whose proof is probabilistic. This result has several fascinating consequences in Combinatorial Geometry and Combinatorial Number Theory. Some weaker versions of these seemingly unrelated consequences have been proved before, in a far more complicated manner

An *embedding* of a graph $G = (V, E)$ in the plane is a a planar representation of it, where each vertex is represented by a point in the plane, and each edge uv is represented by a curve connecting the points corresponding to the vertices u and v. The *crossing number* of such an embedding is the number of pairs of intersecting curves that correspond to pairs of edges with no common endpoints. The *crossing number* $cr(G)$ of G is the minimum possible crossing number in an embedding of it in the plane. The following theorem was proved by Ajtai, Chvátal, Newborn and Szemerédi [1] and, independently, by Leighton [31].

Theorem 3.2 *The crossing number of any simple graph $G = (V, E)$ with $|E| \geq 4|V|$ is at least $\frac{|E|^3}{64|V|^2}$.*

The proof is by a simple probabilistic argument. By Euler's formula any simple planar graph with n vertices has at most $3n-6$ edges, implying that the crossing number of any simple graph with n vertices and m edges is at least $m-(3n-6) > m-3n$. Let $G=(V,E)$ be a graph with $|E| \geq 4|V|$ embedded in the plane with $t = cr(G)$ crossings. Let H be the random induced subgraph of G obtained by picking each vertex of G, randomly and independently, to be a vertex of H with probability p (where p will be chosen later). The expected number of vertices of H is $p|V|$, the expected number of its edges is $p^2|E|$, and the expected number of crossings in its given embedding is $p^4 t$, implying that the expected value of its crossing number is at most $p^4 t$. Therefore, $p^4 t \geq p^2|E| - 3p|V|$, implying that

$$cr(G) = t \geq \frac{|E|}{p^2} - 3\frac{|V|}{p^3}.$$

Without trying to optimize the constant factor, take $p = 4|V|/|E|$ (≤ 1), to get the desired result.

L. Székely [43] noticed that this result can be applied to obtain a surprisingly simple proof of a result of Szemerédi and Trotter in Combinatorial Geometry [44]. The original proof is far more complicated.

Theorem 3.3 *Let P be a set of n distinct points in the plane, and let L be a set of m distinct lines. Then, the number of incidences between the members of P and those of L (that is, the number of pairs (p,l) with $p \in P$, $l \in L$ and $p \in l$) is at most $c(m^{2/3}n^{2/3}+m+n)$, for some absolute constant c.*

Székely's proof is short and elegant: denote the number of incidences by I. Let $G=(V,E)$ be the graph whose vertices are all members of P, where two are adjacent if and only if they are consecutive points of P on some line in L. Clearly, $|V| = n$ and $|E| = I - m$. Note that G is already given embedded in the plane, where the edges are represented by segments of the corresponding lines in L. In this embedding, every crossing is an intersection point of two members of L, implying that $cr(G) \leq \binom{m}{2} \leq m^2/2$. By Theorem 3.2, either $I - m = |E| < 4|V| = 4n$, that is, $I \leq m + 4n$, or

$$\frac{m^2}{2} \geq cr(G) \geq \frac{(I-m)^3}{64n^2},$$

showing that $I \leq (32)^{1/3}m^{2/3}n^{2/3} + m$. In both cases $I \leq 4(m^{2/3}n^{2/3}+m+n)$, completing the proof.

G. Elekes found several applications of the last theorem to Additive Number Theory. Here, too, the proofs are amazingly simple. Here is a representative result. A related one appears in [17].

Theorem 3.4 *For any three sets A,B and C of s real numbers each,*

$$|A \cdot B + C| = |\{ab + c : \ a \in A, b \in B, c \in C\}| \geq \Omega(s^{3/2}).$$

To prove this result, define $R = A \cdot B + C$, $|R| = r$ and put

$$P = \{(a, t) : a \in A, t \in R\}, \quad L = \{y = bx + c : b \in B, c \in C\}.$$

Thus P is a set of $n = sr$ points in the plane, L is a set of $m = s^2$ lines in the plane, and each line $y = bx + c$ in L is incident with s points of P, that is, with all the points $\{(a, ab + c) : a \in A\}$. Therefore, by Theorem 3.3, $s^3 \leq 4(s^{4/3}(sr)^{2/3} + sr + s^2)$, implying that $r \geq \Omega(s^{3/2})$, as needed.

4 The algorithmic aspects

The rapid development of theoretical Computer Science and its tight connection to Discrete Mathematics motivated the study of the algorithmic aspects of algebraic and probabilistic techniques. Can a combinatorial structure, or a substructure of a given one, whose existence is proved by algebraic or probabilistic means, be constructed *explicitly* (that is, by an efficient deterministic algorithm)? Can the algorithmic problems corresponding to existence proofs be solved by efficient procedures? The investigation of these questions are often related to other branches of mathematics. Here we merely mention a few open problems motivated by these questions.

As mentioned in the last paragraph of subsection 2.1, the list chromatic index of any planar cubic 2-connected graph is 3. Can the corresponding algorithmic problem be solved efficiently? That is, can we color properly the edges of any given planar cubic 2-connected graph using given lists of three colors per edge, in polynomial time ?

This problem, as well as several similar applications of Theorem 2.2, are widely open. Note that any efficient procedure that finds, for a given input polynomial that satisfies the assumptions of Theorem 2.2, a point $(s_1, s_2, \ldots, s_n)$ satisfying its conclusion, would provide efficient algorithms for all these algorithmic problems. It would thus be interesting to find such an efficient procedure.

Probabilistic proofs also suggest the study of the corresponding algorithmic problems. This is related to the study of randomized algorithms, a topic which has been developed tremendously during the last decade. See, e.g., [34] and its many references. Even the simple proof of Erdős, described in Section 3, that there are graphs on more than $\lfloor 2^{k/2} \rfloor$ vertices containing neither a clique nor an independent set of size k leads to an open problem which seems very difficult. Can we construct, explicitly, a graph on $n \geq (1 + \epsilon)^k$ vertices with neither a clique nor an independent set of size k, in time which is polynomial in n, where $\epsilon > 0$ is any positive absolute constant ?

The above problems, as well as many related ones, could be viewed as a victory of algebraic and probabilistic techniques. They illustrate the fact that these methods often supply solutions to problems that we cannot solve constructively. I am convinced that the study of algebraic and

probabilistic methods, as well as the related search for more constructive proofs, will keep playing a major role in the future development of Discrete Mathematics.

References

[1] M. Ajtai, V. Chvátal, M. M. Newborn and E. Szemerédi, *Crossing-free subgraphs*, in *Theory and Practice of Combinatorics*, 9–12, North-Holland Math. Stud., 60, North-Holland, Amsterdam and New York, 1982.

[2] N. Alon, *Restricted colorings of graphs*, in *Surveys in Combinatorics*, Proc. 14^{th} British Combinatorial Conference, London Mathematical Society Lecture Notes Series 187, edited by K. Walker, Cambridge University Press, 1993, 1-33.

[3] N. Alon, *Tools from higher algebra*, in: *Handbook of Combinatorics*, (edited by R. Graham, M. Grötschel and L. Lovász), Elseveir and MIT Press (1995), 1749-1783.

[4] N. Alon, *The Shannon Capacity of a union*, Combinatorica 18 (1998), 301-310.

[5] N. Alon, *Combinatorial Nullstellensatz*, Combinatorics, Probability and Computing 8 (1999), 7-29.

[6] N. Alon and M. Dubiner, *Zero-sum sets of prescribed size,* in *Combinatorics, Paul Erdős is Eighty*, János Bolyai Math. Soc., Budapest, 1993, 33–50.

[7] N. Alon, B. Mohar and D. P. Sanders, *On acyclic colorings of graphs on surfaces*, Israel J. Math. 94 (1996), 273-283.

[8] N. Alon, M. B. Nathanson and I. Z. Ruzsa, *The polynomial method and restricted sums of congruence classes*, J. Number Theory 56 (1996), 404-417.

[9] N. Alon and J. H. Spencer, **The Probabilistic Method**, Wiley, New York, 1992. (The second edition will be published in 2000).

[10] N. Alon and M. Tarsi, *Colorings and orientations of graphs*, Combinatorica 12 (1992), 125-134.

[11] L. Babai and P. Frankl, **Linear Algebra Methods in Combinatorics**, to appear.

[12] A. Blokhuis, *Polynomials in Finite Geometries and Combinatorics*, in *Surveys in Combinatorics*, Proc. 14^{th} British Combinatorial Conference, London Mathematical Society Lecture Notes Series 187, edited by K. Walker, Cambridge University Press, 1993, 35-52.

[13] B. Bollobás and A. J. Harris, *List colorings of graphs*, Graphs and Combinatorics 1 (1985), 115-127.

[14] O.V. Borodin, *On acyclic colorings of planar graphs,* Discrete Math. 25 (1979), 211-236.

[15] K. Borsuk, *Drei Sätze über die n-dimensionale euklidische Sphäre*, Fundamenta Math. 20 (1933), 177-190.

[16] J. A. Dias da Silva and Y. O. Hamidoune, *Cyclic spaces for Grassmann derivatives and additive theory*, Bull. London Math. Soc. 26 (1994), 140-146.

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

[18] M. N. Ellingham and L. Goddyn, *List edge colourings of some* 1*-factorable multigraphs*, Combinatorica 16 (1996), 343–352.

[19] P. Erdős, *Some remarks on the theory of graphs*, Bulletin of the Amer. Math. Soc. 53 (1947), 292-294.

[20] P. Erdős and R. L. Graham, **Old and New Problems and Results in Combinatorial Number Theory**, L'Enseignement Mathématique, Geneva, 1980.

[21] P. Erdős, A. Ginzburg and A. Ziv, *Theorem in the additive number theory,* Bull. Research Council Israel, **10F** (1961), 41–43.

[22] P. Erdős and L. Lovász, *Problems and results on* 3*-chromatic hypergraphs and some related questions*, in *Infinite and Finite Sets*, A. Hajnal et. al. eds, North Holland (1975), 609-628.

[23] P. Erdős, A. L. Rubin and H. Taylor, *Choosability in graphs*, Proc. West Coast Conf. on Combinatorics, Graph Theory and Computing, Congressus Numerantium XXVI, 1979, 125-157.

[24] P. Frankl and R. Wilson, *Intersection theorems with geometric consequences*, Combinatorica 1 (1981), 259-286.

[25] C. Godsil, *Tools from linear algebra*, in: *Handbook of Combinatorics*, (edited by R. Graham, M. Grötschel and L. Lovász), Elseveir and MIT Press (1995), 1705-1748.

[26] R. L. Graham, B. L. Rothschild and J. H. Spencer, **Ramsey Theory**, Second Edition, Wiley, New York, 1990.

[27] W. Haemers, *On some problems of Lovász concerning the Shannon capacity of a graph*, IEEE Trans. Inform. Theory **25** (1979), 231–232.

[28] S. Janson, T. Łuczak and A. Ruciński, **Random Graphs**, Wiley, New York, 2000.

[29] A. Kemnitz, *On a lattice point problem*, *Ars Combinatoria* 16b, (1983), 151–160.

[30] J. Kahn and G. Kalai, *A counterexample to Borsuk's conjecture*, Bulletin of the AMS 29 (1993), 60-62.

[31] F. T. Leighton, **Complexity issues in VLSI**, MIT Press (1983).

[32] M. P. A. Macmahon, **Combinatory Analysis**, Chelsea Publishing Company, 1915, Chapter V.

[33] Y. Matiyasevich, A criterion for colorability of vertices of a graph stated in terms of edge orientations (in Russian), Discrete Analysis (Novosibirsk) 26 (1974), 65-71.

[34] R. Motwani and P. Raghavan, **Randomized Algorithms**, Cambridge University Press, New York, 1995.

[35] M. B. Nathanson, **Additive Number Theory: Inverse Theorems and the Geometry of Sumsets**, Springer-Verlag, New York, 1996.

[36] A. Nilli, *On Borsuk's problem*, Contemporary Mathematics, Vol. 178 (1994), AMS, 209-210.

[37] J. Petersen, *Die Theorie der regulären Graphs*, Acta Math. 15 (1891), 193-220.

[38] L. Rónyai, *On a conjecture of Kemnitz*, to appear.

[39] G. Ringel and J. W. T. Youngs, *Solution of the Heawood map coloring problem,* Proc. Nat. Acad. Sci. U.S.A. 60 (1968), 438-445.

[40] C. E. Shannon, *The zero–error capacity of a noisy channel*, IRE Trans. Inform. Theory **2** (1956), 8–19.

[41] W. Schmidt, **Equations over Finite Fields, an Elementary Approach**, Lecture Notes in Mathematics, Vol. 536, Springer, Berlin, 1976.

[42] J. H. Spencer, **Ten lectures on the Probabilistic Method**, Second Edition, SIAM, Philadelphia, 1994.

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

[44] E. Szemerédi and W. T. Trotter, *Extremal problems in discrete geometry*, Combinatorica 3 (1983), no. 3-4, 381–392.

[45] B. L. van der Waerden, **Modern Algebra**, Julius Springer, Berlin, 1931.

[46] L. Vigneron, *Remarques sur les réseaux cubiques de classe* 3 *associés au probléme des quatre couleurs*, C. R. Acad. Sc. Paris, t. 223 (1946), 770-772.

[47] V. G. Vizing, *Coloring the vertices of a graph in prescribed colors* (in Russian), Diskret. Analiz. No. 29, Metody Diskret. Anal. v. Teorii Kodov i Shem 101 (1976), 3-10.