Extremal and Probabilistic Combinatorics

N. Alon and M. Krivelevich **Revised, August 2006**

Sackler Faculty of Exact Sciences, Tel Aviv University, Tel Aviv, Israel 69978

1 Combinatorics – an introduction

1.1 Examples

It is hard to give a rigorous definition of Combinatorics, hence we start with a few examples illustrating the area. Testing friendship relations between children some fifty years ago, the Hungarian sociologist S. Szalai observed that any group of about twenty children he checked contained a set of four children any two of whom were friends, or a set of four no two of whom were friends. Despite the temptation to try and draw some behavioral consequences, Szalai realized this may well be a mathematical phenomenon, rather than a sociological one. Indeed, a brief discussion with the mathematicians P. Erdős, P. Turán and V. Sós convinced him this was the case. For every symmetric relation R on a set X of size 18 or more, there is a subset S of size 4 so that the relation R either contains all $\binom{4}{2} = 6$ pairs of distinct members of S or none of them. Here, the symmetric relation R consists of all pairs of friends among the group of children X. The above fact is a very special case of Ramsey Theorem proved by the economist and mathematician F. Ramsey in 1930. This result led to the development of Ramsey Theory, a branch of Extremal Combinatorics.

Motivated by the study of Fermat's Last Theorem, I. Schur proved in 1916 that for every integer k and every sufficiently large prime p, there are three integers, a, b, c, such that p divides the difference $a^k + b^k - c^k$, but does not divide any of the integers a, b and c. Although this is a result in Number Theory, its (simple) proof is purely combinatorial, and forms another example of the many applications of Graph Theory and Ramsey Theory.

When studying the number of real zeros of random polynomials, Littlewood and Offord investigated in 1943 the following problem. Given n (not necessarily distinct) complex numbers $z_1, z_2, \ldots, z_n$ of absolute value at least 1, what is the maximum possible number of sums $\sum_{i=1}^{n} \epsilon_i z_i$, with $(\epsilon_1, \epsilon_2, \ldots, \epsilon_n) \in \{-1, 1\}^n$, such that the difference between any two sums is of absolute value less than 2? Kleitman and Katona proved that the maximum is $\binom{n}{\lfloor n/2 \rfloor}$, by applying tools from Extremal Finite Set Theory, another area of Extremal Combinatorics.

Consider a school in which there are m teachers $T_1, T_2, \ldots, T_m$, and n classes $C_1, C_2, \ldots, C_n$. The teacher T_i has to teach the class C_j a specified number p_{ij} of periods. What is the minimum possible number of periods in a complete timetable? Let d_i denote the total number of periods the teacher T_i has to teach, and let c_j denote the total number of periods the class C_j has to be taught. Clearly, the number of periods required for a complete schedule is at least d – the maximum of all numbers d_i and c_j. It turns out that this obvious lower bound is also an upper bound; there is always a complete timetable consisting of that number of periods. This is a consequence of König's Theorem, a basic result in Graph Theory. Suppose, now, that the situation is not so simple; for every teacher T_i and class C_j, there is a specified set of d specific possible periods in which the teaching has to take place. Can we always find a feasible timetable, keeping these constraints? Recent results on a subject known as list coloring of graphs imply this is always possible.

Can the countries of any planar map be colored in at most four colors so that no two countries that share a common boundary have the same color? Here we assume that each country forms a connected region in the plane. Of course, at least four colors may be necessary – think of Belgium, France, Germany and Luxembourg, each having a common border with each other. The Four Color Theorem, proved by Appel and Haken in 1976, asserts that indeed four colors always suffice. The study of this problem led to numerous interesting questions and results about Graph Coloring.

Let S be an arbitrary subset of the lattice $\mathbb{Z}^2$. For any two finite subsets $A, B \subset Z$, let $d_S(A, B) = \frac{|S \cap A \times B|}{|A||B|}$ denote the density of S in the 'combinatorial rectangle' $A \times B$. Define $d(S) = \limsup_{k \to \infty} \{d_S(A, B) : |A| = |B| = k\}$. What are the possible values of $d(S)$? Basic results in Extremal Graph Theory imply that there are only

two possibilities: for every S, either $d(S) = 0$ or $d(S) = 1$.

Suppose that n basketball teams compete in a tournament and each two teams play one game. The organizers wish to award k prizes at the end of the tournament. They are, however, embarrassed to find out that no matter which k teams they pick as the winners of these prizes, there is always another team that won its games against each of these k winners. Is this indeed possible for any k, provided n is large enough? This problem can be easily solved by the so called Probabilistic Method, a powerful technique in Combinatorics. For any fixed k, and all sufficiently large n, a random tournament on n teams, in which the result of each game is chosen randomly, uniformly and independently has, with high probability, the property that for each k teams there is another one that beats all of them. Probabilistic Combinatorics, which is one of the most active areas in modern combinatorics, started with the realization that probabilistic reasoning often provides simple solutions to problems of this type, that may otherwise seem very hard.

If G is a finite group of n elements, and H is a subgroup of size k in G, then there are n/k left cosets and n/k right cosets of H. Is there always a set of n/k elements of G, containing a single representative of each right coset and a single representative of each left coset? Hall's theorem, a basic result in Graph Theory, implies that this is always the case. In fact, if H' is another subgroup of size k in G, then there is always a set of n/k elements of G, containing a single representative of each right coset of H, and a single representative of each left coset of H'. This may sound like a result in Group Theory, but it really is a (simple) result in Combinatorics.

1.2 Topics

The examples described in the previous subsection illustrate the main themes of Combinatorics. The subject, sometimes also called Discrete Mathematics, is a branch of mathematics focusing on the study of discrete objects and their properties. Although Combinatorics is probably as old as the human ability to count, the field has experienced tremendous growth during the last fifty years and has matured into a thriving area with its own set of problems, approaches and methodology.

The examples above suggest that Combinatorics is a basic mathematical discipline which plays a crucial role in the development of many other mathematical areas. In this essay we discuss some of the main aspects of this modern field, focusing on Extremal and Probabilistic Combinatorics. It is, of course, impossible to cover the area in such a short article. A detailed account of the subject can be found in [3]. Our main intention is to give a glimpse of the topics, methods and applications illustrated by representative examples. The topics we discuss include Extremal Graph Theory, Ramsey Theory, Extremal Finite Set Theory, Combinatorial Number Theory and Combinatorial Geometry, Random graphs and Probabilistic Combinatorics. The methods applied in the area include combinatorial techniques, probabilistic methods and tools from Linear Algebra, spectral techniques and topological methods. We also discuss the algorithmic aspects and some of the many fascinating open problems in the area.

2 Extremal Combinatorics

Extremal Combinatorics deals with the problem of determining or estimating the maximum or minimum possible cardinality of a collection of finite objects that satisfies certain requirements. Such problems are often related to other areas including Computer Science, Information Theory, Number Theory and Geometry. This branch of Combinatorics has developed spectacularly over the last few decades, see, e.g., [2], [6], and their many references.

2.1 Extremal Graph Theory

A graph is one of the very basic combinatorial structures, and can model, among other things, a communication network. It consists of a set of vertices, and a collection of pairs of vertices, called edges. It is common to denote a graph G by an ordered pair (V, E), where V is the set of its vertices, and E the set of its edges. If $\{u, v\}$ is an edge, we say that u and v are adjacent. The degree $d(v)$ of a vertex v is the number of vertices adjacent to it. A (simple) path of length k from u to v in G is a sequence of distinct vertices $u = v_0, v_1, \ldots, v_k = v$, where v_i and v_{i+1} are adjacent for all $i < k$. If

$v_0 = v_k$ (but all vertices v_i for $i < k$ are distinct), this is a cycle of length k, usually denoted by C_k. G is connected if for any two vertices u, v of G there is a path from u to v. A complete graph K_r is a graph on r vertices any two of which are adjacent. A subgraph of a graph G is a graph which contains some of the vertices of G and some of its edges. A clique in G is a subgraph of it which forms a complete graph, and the clique number of G is the maximum number of vertices in a clique in it. Similarly, an independent set in G is a set of vertices in it which spans no edges, and the independence number of G is the maximum size of an independent set in it. There are numerous notions and results dealing with graphs, see, for example, [3], Chapters 1-6.

Extremal Graph Theory deals with quantitative connections between various parameters of a graph such as its numbers of vertices and edges, its clique number or its independence number. In many cases a certain optimization problem involving these parameters has to be solved, and its optimal solutions are the extremal graphs for this problem.

2.1.1 Graph coloring

Let us return now to the map coloring example discussed in the introduction. We are mathematicians, and our (secret and powerful) language is symbols and numbers. We can thus describe the map coloring problem as a graph G, whose vertices correspond to the countries on the map; two vertices are connected by an edge in G if the corresponding countries share a common border. Instead of using red, blue and yellow, we are to assign positive integers to the vertices of G (countries of the map) so that neighboring vertices get different numbers. The Four Color Theorem states in this language that every graph obtained in this manner can be colored with just four colors.

Here is another illustrative example. Suppose we must schedule meetings of several parliament committees. We cannot assign two committees to the same time if some parliament member participates in both. How many sessions do we need?

We can model this situation by a graph G whose vertices are the committees, with two vertices adjacent if the corresponding committees share a member. A schedule is an assignment $f : V \to \{1, ..., k\}$ of time-slots 1 to k to the committees (vertices of G) so that two adjacent vertices get different numbers (time-slots). The question then becomes: what is the minimal value of k for which such a schedule exists? This leads to the notion of the chromatic number of G.

Here are the relevant formal definitions. Let $G = (V, E)$ be a graph with vertex set V and edge set E. A function $f : V \to \{1, \ldots, k\}$ is called a k-coloring of G if no edge of G is monochromatic under f, i.e., $f(u) \neq f(v)$ for every $e = \{u, v\} \in E$. This restriction can be put in the following equivalent form: for every $1 \leq i \leq k$, the set $f^{-1}(i) \subseteq V$ is an independent set. Thus, omitting the names of the colors we can say that a k-coloring is a partition of V into k independent sets. A graph is k-colorable if it admits a k-coloring. Finally, the chromatic number of G, denoted by $\chi(G)$, is the minimum k for which G is k-colorable.

Two simple examples are in order: if G is a complete graph K_n on n vertices then obviously in any coloring of G all vertices get distinct colors, and thus n colors are necessary. Of course, n colors are also sufficient, hence $\chi(K_n) = n$. If G is a cycle C_{2n+1} on $2n + 1$ vertices, then easy parity arguments show that at least three colors are needed, and three colors are enough – color the vertices along the cycle alternately by colors 1 and 2, and then color the last vertex by color 3. Thus, $\chi(C_{2n+1}) = 3$.

Clearly, $\chi(G) = 1$ if and only if G has no edges. It is not hard to prove that G is 2-colorable if and only if it does not contain a cycle of odd length; such graphs are usually called bipartite. The easy characterization ends here, and no simple criteria equivalent to k-colorability is available for $k \geq 3$. This is related to the fact that for each fixed $k \geq 3$ the computational problem of deciding whether a given graph is k-colorable is NP-hard, a notion treated in another chapter of this Companion.

Coloring is one of the most fundamental notions of Graph Theory, as a huge array of problems in this field and in related areas like Computer Science and Operations Research can be formulated in terms of graph coloring. Finding an optimal coloring of a graph is notoriously known to be a very hard task, both theoretically and practically.

There are two simple yet fundamental lower bounds on the chromatic number. First, as ev-

ery color class in a proper coloring of a graph G forms an independent set, its size is bounded by the independence number of G, denoted by $\alpha(G)$. Hence, at least $|V(G)|/\alpha(G)$ colors are necessary, implying that $\chi(G) \geq |V(G)|/\alpha(G)$. Second, if G contains a complete graph K_k on k vertices as a subgraph, then k colors are needed to color that subgraph alone, and thus $\chi(G) \geq k$. This implies that $\chi(G) \geq \omega(G)$, where $\omega(G)$ is the clique number of G.

What about upper bounds on the chromatic number? One of the simplest approaches to color a graph is to do it greedily: fix an order $\sigma = (v_1, \ldots, v_n)$ of the vertices of G, and then color them vertex by vertex in the order prescribed by σ. When a vertex v_i is to be colored, its color is the smallest color that has not been used on its neighbors colored already. While the greedy algorithm can be sometimes very inefficient (for example it can color bipartite graphs in an unbounded number of colors), it often works quite well. Observe that when applying the greedy algorithm, a color given to a vertex v is at most one more than the number of the neighbors of v preceding it in the chosen order, and is thus at most $d(v) + 1$, where $d(v)$ is the degree of v in G. It follows that the greedy algorithm uses at most $\Delta(G) + 1$ colors, where $\Delta(G)$ is the maximum degree of G. Therefore $\chi(G) \leq \Delta(G) + 1$. This bound is tight for complete graphs and odd cycles, and as shown by Brooks in 1941 those are the only cases: if G is a graph of maximum degree Δ, then $\chi(G) \leq \Delta$ unless G contains a clique $K_{\Delta+1}$, or $\Delta = 2$ and G contains an odd cycle.

There is an important class of graphs for which the chromatic number is always small; this is the class of planar graphs. A graph G is planar if it can be drawn in the plane with the vertices represented by points, and the edges forming straight lines between the corresponding vertices, such that no two edges cross each other. Such a drawing is called a plane graph. The plane plays a special role here, it is easy to see that every graph can be embedded in the three-dimensional space without intersecting edges. A way to obtain a planar graph from a planar map is by taking the regions of the map to be the vertices of the graph, and by connecting two regions by an edge if they have a common boundary. In fact, any connected planar graph can be obtained this way. F. Guthrie conjectured in 1852 that every planar graph can be colored in four colors. After a long series of efforts and several flawed proofs, this was finally verified by Appel and Haken in 1976 in a computer-assisted proof. This result is the celebrated Four Color Theorem, arguably the most famous graph theoretic result.

A different kind of coloring, where the colored objects are edges rather than vertices, is also of interest. Given a graph $G = (V, E)$, a function $f : E \to \{1, \ldots, k\}$ is called a k-edge coloring of G, if no two incident edges get the same color, i.e., $f(e) \neq f(e')$ for every pair of edges sharing a common end. The chromatic index of G, denoted by $\chi'(G)$, is the minimum k for which G admits a k-edge coloring. For example, one can prove that $\chi'(K_{2n}) = 2n - 1$ (ask the manager of your soccer league how to organize a round robin tournament of $2n$ teams in $2n - 1$ rounds – this is exactly the problem of edge coloring K_{2n}!), while $\chi'(K_{2n-1}) = 2n - 1$. Observe that in any proper edge coloring of G all edges of G containing v get distinct colors, and thus $\chi'(G) \geq \Delta(G)$. This bound is tight for bipartite graphs, as proved by König in 1931, and implies the existence of a complete timetable using d periods in the problem of teachers and classes discussed in the introduction.

For general graphs the fundamental theorem of Vizing from 1964 states that $\chi'(G) \leq \Delta(G) + 1$. Thus, the chromatic index of G is much easier to approximate than its chromatic number, as it is always either $\Delta(G)$ or $\Delta(G) + 1$.

2.1.2 Excluded subgraphs

How dense can a graph G on n vertices containing no copy of the triangle K_3 be ? Split the vertex set into two nearly equal parts A and B of sizes $\lfloor n/2 \rfloor$ and $\lceil n/2 \rceil$, respectively, and connect every vertex from A to every vertex from B by an edge. The obtained graph G is obviously triangle-free and is fairly dense – it has $\lfloor n^2/4 \rfloor$ edges. Moreover, adding any missing edge to G creates a triangle, and thus G is a triangle-free graph which is maximal with respect to inclusion. But is this indeed the densest triangle-free graph on n vertices? A one hundred year old theorem of Mantel answers this in the affirmative.

Let us generalize the above example and put it

onto a more formal footing. Let $n \geq 2$ be an integer and let H be a graph on at most n vertices with at least one edge. Denote by $ex(n, H)$ the maximum possible number of edges in a graph on n vertices not containing H as a subgraph ("ex" stands for "excluded"). The empty graph on n vertices does not contain H, while the complete graph K_n does, so the answer lies somewhere between 0 and $\binom{n}{2}-1$. The function $ex(n, H)$ is usually called the Turán number of H, and it is common to study its asymptotic behavior for fixed H, as n grows.

What kind of examples of graphs that do not contain H can we think of ? Assume that the chromatic number $\chi(H)$ of H is $r \geq 3$. Partition the n vertices into $r-1$ groups $V_1, \ldots, V_{r-1}$ and create a graph G by connecting, for all $1 \leq i \neq j \leq r-1$, every vertex $u \in V_i$ to every vertex $v \in V_j$. Such a graph is called a complete $(r-1)$-partite graph. Since $\chi(G) = r-1$, the target graph H cannot be embedded into G. This implies that $ex(n, H) \geq |E(G)|$. The graph G has the largest number of edges, when all of its parts are of nearly equal size, i.e., $||V_i| - |V_j|| \leq 1$. The graph satisfying this condition is the Turán graph $T_{r-1}(n)$ and its number of edges is denoted by $t_{r-1}(n)$. It follows that $ex(n, H) \geq t_{r-1}(n) \geq \left(1 - \frac{1}{r-1}\right)\binom{n}{2}$.

The most important case, when H is the complete graph K_r on r vertices, was resolved by Turán in 1941. He proved that in fact $ex(n, K_r) = t_{r-1}(n)$, and the only K_r-free graph on n vertices with $ex(n, K_r)$ edges is the Turán graph $T_{r-1}(n)$. Turán's paper is generally considered the starting point of Extremal Graph Theory.

Later, Erdős, Stone and Simonovits extended Turán's theorem by proving that the above simple lower bound for $ex(n, H)$ is asymptotically tight for any H with $\chi(H) \geq 3$. Formally, they proved that for every fixed H and large n

$$ex(n, H) = \left(1 - \frac{1}{\chi(H)-1}\right)\binom{n}{2} + o(n^2)\,.$$

The $o(n^2)$-term in this notation means that the limit, as n tends to infinity, of the ratio between the expression in the left hand side minus the main term in the right hand side, and n^2, is zero. In other words, the main term in the right hand side provides an asymptotic formula for $ex(n, H)$ for every graph H.

A moment's reflection shows, however, that this is not quite the case, as for bipartite graphs H (i.e., when $\chi(H) = 2$) the above only gives $ex(n, H) = o(n^2)$. The determination of the Turán numbers for bipartite graphs remains a challenging open problem with many unsettled questions. Partial results obtained so far use a variety of techniques from different fields including Probability Theory, Number Theory and Algebraic Geometry.

A question closely related to the latter problem is the so called Zarankiewicz problem, asking to determine $z(m, n; s, t)$, the maximum possible number of edges in a bipartite graph G with the first part of size m and the second of size n, not containing a copy of a complete bipartite graph with s vertices in the first part and t vertices in the second. Equivalently, this is the maximum possible number of ones in a binary m by n matrix containing no s by t submatrix of ones. In 1954 Kővari, Sós and Turán used a double counting argument to prove

$$m\binom{z/m}{t} \leq (s-1)\binom{n}{t}\,,$$

where $z = z(m, n; s, t)$. In particular, for $m = n$ and fixed $s = t$ the above bound shows that $z(n, n; t, t) = O(n^{2-1/t})$; this is known to be asymptotically tight for $t = 2, 3$, and implies that for any $S \subset \mathbb{Z}^2$ the quantity $d(S)$ defined in the introduction is either 0 or 1.

Interestingly, the Kővari-Sós-Turán bound for the first non-trivial case $z(n, n; 2, 2)$ is tight if and only if there exists a finite projective plane with n points.

2.1.3 Matchings and cycles

Given a graph G, a matching M in G is a collection of pairwise disjoint edges of G. A matching is called perfect if it covers all vertices of G. Of course, in order to have a perfect matching the number of vertices of G has to be even.

One of the best known theorems in Graph Theory is Hall's theorem that provides a necessary and sufficient condition for the existence of a perfect matching in a bipartite graph. What kind of condition can this be ? Let $G = (A \cup B, E)$ be a bipartite graph with sides A and B. For a set $S \subseteq A$, we denote by $N(S)$ its neighborhood in B, i.e., $N(S) = \{b \in B : b \text{ is connected by an edge to } S\}$.

We say that G satisfies the Hall condition for the side A if

$$|N(S)| \geq |S|$$

for every subset S of A. It is easy to see that if there is a matching covering all vertices of A, then G satisfies the above condition. Hall's theorem (1935) asserts that the Hall condition is also sufficient for the existence of such a matching. Observe that in case $|A| = |B|$ (which is the only case where a bipartite graph can have a perfect matching) a matching covering A is perfect.

Hall's theorem can be reformulated in the equally popular form of a system of distinct representatives (SDR). Let $\{S_i\}_{i\in I}$ be a finite collection of sets. Denote $U = \bigcup_{\imath\in I} S_i$. An ordered set $\{s_i\}_{i\in I}$ of distinct elements of U is called a system of distinct representatives if $s_i \in S_i$ for every $i \in I$. Then Hall's Theorem postulates that the family $\{S_i\}$ has an SDR if and only if $|\bigcup_{i\in J} S_i| \geq |J|$ for every subset of indices $J \subseteq I$. To see the equivalence of those two forms, define a bipartite graph G with sides I and U, where (i, u) is an edge if and only if $u \in S_i$. Then a matching covering A in G translates to an SDR for the family $\{S_i\}$.

Hall's theorem can be applied to solve the problem of finding a system of representatives for the right and left cosets of a subgroup H, mentioned in Section 1.1. Define a bipartite graph F, whose two sides (of size n/k each) are the left and the right cosets of H. A left coset g_1H is connected by an edge of F to a right coset Hg_2 if they share a common element. It is not difficult to show that F satisfies the Hall condition, and hence it has a perfect matching M. Choosing for each edge (g_iH, Hg_j) of M a common element of g_iH and Hg_j, we obtain the required family of representatives.

There is also a necessary and sufficient condition for the existence of a perfect matching in a general (not necessarily bipartite) graph G. This is a theorem of Tutte, which is not stated here.

Recall that C_k denotes a cycle of length k. A cycle is a very basic graph structure, and – as one might expect – there are many extremal results concerning cycles.

A graph without cycles is called a forest. A connected graph without cycles is a tree. Each tree on n vertices has exactly $n - 1$ edges. It follows that every graph G on n vertices with at least n edges has a cycle. In order to satisfy more elaborate requirements on cycles, more edges may be required. For example, the Turán theorem, applied for $r = 3$, asserts that a graph G with n vertices and more than $n^2/4$ edges contains a triangle $C_3 = K_3$. One can also prove that a graph $G = (V, E)$ with $|E| > \frac{k}{2}(|V| - 1)$ has a cycle of length longer than k, and this is tight.

A Hamilton cycle in a graph G is a cycle containing all of its vertices. This term originated in a game, invented by W. R. Hamilton in 1857, whose objective was to complete a Hamilton cycle in the graph of the dodecaherdon. A graph containing a Hamilton cycle is called Hamiltonian. This concept is strongly related to the well known Traveling Salesman problem (TSP) asking to find a Hamilton cycle of minimum total weight in a weighted graph. There are many sufficient criteria for a graph to be Hamiltonian, quite a few of which are based on the sequence of graph degrees. For example, Dirac proved in 1952 that a graph on $n \geq 3$ vertices all of whose degrees are at least $n/2$ is Hamiltonian.

2.2 Ramsey Theory

Ramsey theory studies quantitatively the following general phenomenon: every large structure, even if it looks totally chaotic, contains a rather large well-organized substructure. As succinctly put by the mathematician T. S. Motzkin, "Complete disorder is impossible". This phenomenon holds in great generality (though it is good to keep in mind that there are some structures for which it fails). It is natural to expect that the simple and very general form of this paradigm ensures it has many diverse manifestations in different mathematical areas, and this is indeed the case. The first and simplest Ramsey-type statement one usually encounters is the pigeonhole principle: every coloring of n objects in s colors contains a subset of at least n/s objects, all having the same color.

Although several Ramsey-type theorems had appeared before, the origin of Ramsey theory is usually credited to F. Ramsey, who in 1930 proved the following theorem. Let $k, l \geq 2$ be integers. Then there exists an integer n, such that every Red-Blue coloring of the edges of the complete graph K_n on n vertices contains either a Red complete graph on k vertices or a Blue complete graph on l vertices. Let $R(k, l)$ denote the minimum number n with

this property. In this language, the observation of Szalai, mentioned in the introduction, states that $R(4,4) \leq 20$ (in fact, $R(4,4) = 18$). Of course, one cannot guarantee a large complete graph of a specific color, but one of the two colors will do. Actually, Ramsey proved a more general theorem, allowing for an arbitrary but fixed number of colors and for coloring of r-tuples, and not just 2-tuples (pairs). As a side remark we note here that the exact computation of small Ramsey numbers is a notoriously difficult task, and even the value of $R(5,5)$ is unknown at present.

The second cornerstone of Ramsey theory was laid by P. Erdős and G. Szekeres, who in 1935 wrote a paper containing several important Ramsey-type results. In particular, they proved the recursion $R(k,l) \leq R(k-1,l) + R(k,l-1)$. Combined with the easy boundary conditions $R(2,l) = l$, $R(k,2) = k$, the recursion leads to the estimate $R(k,l) \leq \binom{k+l-2}{k-1}$. In particular, for the so called diagonal case $k = l$ we obtain $R(k,k) < 4^k$. No improvement in the exponent of the latter estimate has been found so far. The best known lower bound, discussed in Section 3.2 below, is roughly $R(k,k) \geq 2^{k/2}$, leaving a rather substantial gap.

Another Ramsey-type statement, proved by Erdős and Szekeres, is of geometric nature. They showed that for every $n \geq 3$ there exists a minimum $N = N(n)$, such that for any configuration of N points in the plane in general position (i.e., no three on a line), there are n that form a convex n-gon. (Try to prove that $N(4) = 5$ as an easy exercise!) There are several proofs of this theorem, some using the general Ramsey theorem. The conjectured value of N is $N(n) = 2^{n-2} + 1$.

The classic Erdős-Szekeres paper contains also the following Ramsey-type result: any sequence of $n^2 + 1$ distinct numbers contains a monotone (increasing or decreasing) subsequence of length $n+1$. This provides a quick lower bound of $\sqrt{n}$ for a well known problem of Ulam, asking for the typical length of a longest increasing subsequence of a random sequence of length n. A detailed description of the distribution of this length has recently been given by Baik, Deift and Johansson.

In 1927 van der Waerden proved what became known as van der Waerden's theorem: for all positive integers k and r there exists a minimum integer $W(k,r)$ so that for every coloring of the set of integers $\{1,\ldots,W(k,r)\}$ in r colors, one of the colors contains an arithmetic progression of length k. Van der Waerden's bounds for $W(k,r)$ are enormous – they grow like an Ackermann-type function. A new proof of his theorem was found by Shelah in 1987, and yet another proof was given by Gowers in 2000, while studying the (much deeper) density version of the theorem, described in Section 2.4. These recent proofs provided improved upper bounds for $W(k,r)$, but the best known lower bound for this number, which is only exponential in k for each fixed r, is much smaller.

Even before van der Waerden, Schur proved in 1916 that for any positive integer r there exists an integer $S(r)$ such that for every r-coloring of $\{1,\ldots,S(r)\}$ one of the colors contains a solution of the equation $x+y=z$. The proof can be derived rather easily from the general Ramsey theorem. Schur applied this statement to prove the following result, mentioned in Section 1.1: for every k and all sufficiently large primes p, the equation $a^k + b^k = c^k$ has a nontrivial solution in the integers modulo p. To prove this result, assume $p \geq S(k)$ and consider the field Z_p. Let $H = \{x^k : x \in Z_p^*\}$. Then H is a subgroup of the multiplicative group Z_p^* of index $r = gcd(k, p-1) \leq k$. The partition of Z_p^* into the cosets of H induces an r-coloring χ of Z_p^*. By Schur's theorem there exist $x,y,z \in \{1,\ldots,p-1\}$ with $\chi(x) = \chi(y) = \chi(z)$ and $x+y=z$. Thus, there exists a residue $d \in Z_p^*$ such that $x = da^k$, $y = db^k$, $z = dc^k$ and $da^k + db^k = dc^k$ modulo p. The desired result follows.

Many additional Ramsey-type results can be found in [4] or in [3], Chapter 25.

2.3 Extremal Finite Set Theory

The generic problem in Extremal Finite Set Theory is the problem of determining or estimating the maximum possible cardinality of a family $\mathcal{F}$ of distinct subsets of an n-element set that satisfies some given conditions. The first result of this form was proved by Sperner in 1928. He showed that the maximum possible number of subsets of an n-element set in which no subset contains another one is $\binom{n}{\lfloor n/2 \rfloor}$. The lower bound is given by the family of all subsets of cardinality $\lfloor n/2 \rfloor$. This result supplies a quick solution to the real analog

of the problem of Littlewood and Offord described in Section 1.1. If $x_1, x_2, \ldots, x_n$ are n not necessarily distinct real numbers of absolute value at least 1, then the number of sums $\sum_{i=1}^{n} \epsilon_i x_i$ with $(\epsilon_1, \epsilon_2, \ldots, \epsilon_n) \in \{-1, 1\}^n$, so that no two sums differ by at least 2, is at most $\binom{n}{\lfloor n/2 \rfloor}$. This bound is tight as shown by taking $x_i = 1$ for all i. To prove the bound observe, first, that we may assume that all x_i are positive, as we can always replace an element x_i by $-x_i$ and ϵ_i by $-\epsilon_i$ in all the sums. Given a set of sums as above, associate each sum $\sum_{i=1}^{n} \epsilon_i x_i$ with the subset of all indices i for which $\epsilon_i = 1$. Note that if the subset corresponding to one sum contains the subset corresponding to another one, then the two sums differ by at least twice the value of some a_i, that is, by at least 2, contradicting the assumption. The upper bound thus follows from Sperner's Theorem.

A family of sets is intersecting if any two members of the family intersect. What is the maximum possible size of an intersecting family of subsets of cardinality k of an n element set? We may assume that $n \geq 2k$ as otherwise the solution is trivial. Erdős, Ko and Rado proved that the maximum is $\binom{n-1}{k-1}$. Their proof uses a shifting technique, which proved to be very useful in tackling similar problems.

Let $n > 2k$ be two positive integers. What is the minimum possible number of colors t such that there is a coloring of all k-subsets of an n-element set $\{1, 2, \ldots, n\}$ by t colors, such that each color class forms an intersecting family? It is not difficult to see that $n - 2k + 2$ colors suffice. Indeed, one color class can be the family of all subsets of $\{1, 2, \ldots, 2k-1\}$, which is clearly intersecting. In addition, for each i satisfying $2k \leq i \leq n$, the family of all subsets whose largest element is i is also intersecting. These $n - 2k + 1$ families can thus form the remaining color classes.

Kneser conjectured in 1955, and Lovász proved in 1978 that this is tight; in any coloring of all k-subsets of an n-element set by less than $n-2k+2$ colors, there are two disjoint sets having the same color. Lovász' proof is topological, and relies on the Borsuk-Ulam Theorem. Several simpler proofs have been found during the years; all of them are based on the topological idea in the first proof, which played a crucial role in the development of topological tools in Combinatorics.

2.4 Combinatorial Number Theory

Combinatorial Number Theory deals with the arithmetic properties of "dense" sets of integers, with extremal problems dealing with addition of sets of integers or subsets of groups, as well as with some classical problems of number theory in which combinatorial methods proved useful. We describe below a few examples. Many more can be found in Chapter 20 of [3] and in [8].

The Cauchy-Davenport Theorem, which has numerous applications in Additive Number Theory, is the statement that if p is a prime, and A, B are two nonempty subsets of Z_p, then

$$|A + B| = |\{a + b : \ a \in A, b \in B\}|$$

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

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 every positive integer is a sum of four squares. Davenport formulated the theorem as a discrete analogue of a conjecture of Khintchine about the Schnirelman density of the sum of two sequences of integers. The proofs given by Cauchy and by Davenport are combinatorial, but there is also a more recent algebraic proof, based on some properties of roots of polynomials. Its advantage is that it provides many variants that do not seem to follow from the combinatorial approach. One variant is the fact that if p is a prime, A, B are two nonempty subsets of Z_p and $|A| \neq |B|$, then

$$|A \oplus B| = |\{a + b : \ a \in A, b \in B, \ a \neq b\}|$$

$$\geq min\{p, |A| + |B| - 2\}.$$

Additional extensions can be found in [8].

The theorem of van der Waerden mentioned in Section 2.2 asserts that for any positive integer r, in any coloring of the integers by r colors there is a color class that contains arbitrarily long arithmetic progressions. Erdős and Turán conjectured in 1936 that this always holds for the "most popular" color class. More precisely, they conjectured that any set of positive integers with positive upper density contains arbitrarily long arithmetic progressions. This is equivalent, by compactness, to the following statement about finite sets of integers. For any positive integer k and for any real $\epsilon > 0$,

there is an $n_0 = n_0(k, \epsilon)$ such that if $n > n_0$, then any set of at least ϵn positive integers between 1 and n contains a k-term arithmetic progression. After several partial results, this conjecture was proved by Szemerédi in 1975. His deep proof is combinatorial, and applies techniques from Ramsey Theory and Extremal Graph Theory. Furstenberg gave another proof in 1977, based on techniques of Ergodic Theory. In 2000 Gowers gave a new proof, combining combinatorial arguments with tools from analytic number theory. This proof supplied a much better quantitative estimate. A related very recent spectacular result of Green and Tao asserts that there are arbitrarily long arithmetic progressions of prime numbers. Their proof combines number theoretic techniques with the ergodic theory approach. Erdős conjectured that any infinite sequence n_i for which the sum $\sum_i \frac{1}{n_i}$ diverges contains arbitrarily long arithmetic progressions. This conjecture, which implies the assertion of the Green-Tao result, is still open.

2.5 Discrete Geometry

Discrete Geometry investigates combinatorial properties of configurations of geometric objects. Many of the questions considered can be explained to a layman. Here are a few examples. What is the maximum possible number of incidences between m points and n lines in the plane ? What is the maximum possible number of unit distances determined by a set of n points in the plane ? Is there a finite number $h = h(p, q)$ so that for any finite family $\mathcal{F}$ of convex sets in the plane in which for any p of the sets there is a point lying in q of them, there is a set of h points that intersects each member of the family ? Problems and results of this type have been applied extensively in Computational Geometry and in Combinatorial Optimization during the last decades; two recent books on the subject are [9] and [7].

Let P be a set of points, and L a set of lines in the plane. The number of incidences between P and L, denoted by $I(P, L)$, is the number of ordered pairs (p, ℓ) with $p \in P, \ell \in L$ and $p \in \ell$. Let $I(m, n)$ denote the maximum possible value of $I(P, L)$, where the maximum is taken over all sets P of m distinct points and all sets L of n distinct lines. Szemerédi and Trotter determined the asymptotic behavior of this quantity, up to a constant factor, for all possible values of m and n. There are two absolute positive constants c_1, c_2 such that for all m, n,

$$c_1(m^{2/3}n^{2/3} + m + n) \leq I(m, n)$$

$$\leq c_2(m^{2/3}n^{2/3} + m + n).$$

The lower bound, in the non-trivial cases that m and n are not too far from each other, follows by taking the points to contain all points of a $\lfloor\sqrt{m}\rfloor$ by $\lfloor\sqrt{m}\rfloor$ grid, and by taking the n most popular lines determined by these grid points. The upper bound is more difficult. The most elegant proof of it is due to Székely, and is based on the fact that any embedding in the plane of a graph on m vertices and more than $4m$ edges has many pairs of crossing edges (a rather simple consequence of the famous Euler formula connecting the numbers of vertices, edges and regions in any planar drawing). To bound the number of incidences between a set of points P and a set of lines L in the plane, one considers the graph whose vertices are the points P, and whose edges are all segments between consecutive points along a line in L. The desired bound is obtained by observing that the number of crossings in this graph does not exceed the number of pairs of lines in L, and yet it should be large if there are many incidences.

Similar ideas can be used to bound the maximum possible number of unit distances between pairs of points in a set of n points in the plane. It is not surprising that the two problems are related; the number of these unit distances is simply the number of incidences between the given n points, and the n unit circles centered at these points. Here, however, there is a large gap between the resulting upper bound, which is $cn^{4/3}$ for some absolute constant c, and the best known lower bound, which is only $n^{1+c'/\log\log n}$, for an appropriate constant $c' > 0$.

A fundamental theorem of Helly asserts that if in a finite collection $\mathcal{F}$ of convex sets in $\mathbb{R}^d$ every $d+1$ sets or less intersect, then all sets have a common point. Suppose we only know that out of every p sets some $d + 1$ intersect, for some $p > d + 1$. Is there, in this case, a set of at most C points that intersects each member of $\mathcal{F}$, where C is bounded by a function of p, independent of the size of $\mathcal{F}$? This question was raised by Hadwiger and Debrunner

in 1957, and solved by Kleitman and the first author in 1992. The proof combines a fractional version of Helly's Theorem with the duality of linear programming and various additional geometric results. Unfortunately, it gives a very poor estimate for the number of points required C, and even in the case $p = 4$ in dimension 2 it is not known what the best possible value of C is.

2.6 Tools

While in the past many of the basic results in Extremal Combinatorics were obtained mainly by ingenuity and detailed reasoning, the modern theory has grown out of this early stage, and often relies on deep, well developed tools. In this subsection we include a very brief description of some of these tools.

The Regularity Lemma of Szemerédi is a result in Graph Theory that has numerous applications in various areas including combinatorial number theory, computational complexity and, mainly, extremal graph theory. The precise statement of the lemma, that can be found, for example, in [2], is somewhat technical. The rough statement, is, however, that every large graph can be partitioned into a constant number of pieces of nearly equal size, so that the bipartite graphs between most pairs behave like random bipartite graphs. The strength of this lemma is that it applies to any graph, providing a rough approximation of its structure which enables one to extract a lot of information about it. A typical application of the lemma is the fact that if one has to delete 'many' edges from a graph in order to destroy all triangles, then the graph must contain 'many' triangles. The formal statement is a bit technical, as follows. For any $\epsilon > 0$, there exist $n_0 = n_0(\epsilon)$ and $\delta = \delta(\epsilon) > 0$ so that the following holds. If $n > n_0$, and G is a graph on n vertices from which one has to delete at least ϵn^2 edges in order to get a graph containing no triangles, then G contains at least δn^3 triangles.

Tools from linear and multilinear algebra play an essential role in Extremal Combinatorics. The most fruitful technique of this kind, which is possibly also the simplest, is the so-called dimension argument. In its simplest form, the method can be described as follows. In order to bound the cardinality of a discrete structure A, one maps its elements to vectors in a linear space, and shows that the set A is mapped to a linearly independent set. It then follows that the cardinality of A is bounded by the dimension of the corresponding linear space. An early application of this argument was found by Larman, Rogers and Seidel in 1977. They showed that the maximum possible cardinality of a set of points in $\mathbb{R}^n$ that determines at most two distinct distances is at most $(n+1)(n+4)/2$ (and at least $n(n+1)/2$). The upper bound is proved by associating each point of such a set with a polynomial in n variables, and by showing that these polynomials are linearly independent and all lie in a space of dimension $(n+1)(n+4)/2$. This has been improved by Blokhuis to $(n+1)(n+2)/2$, by showing that one can add $n+1$ additional polynomials that lie in this space to those obtained from the two-distance set, keeping the augmented set linearly independent. More applications of the dimension argument can be found in [3], Chapter 31.

Spectral techniques have been used extensively in Graph Theory. The adjacency matrix of a graph $G = (V, E)$ is the matrix $A = (a_{u,v})_{u,v \in V}$, in which $a_{u,v} = 1$ if $uv \in E$ and $a_{u,v} = 0$ otherwise. This is a symmetric matrix and hence has real eigenvalues and an orthonormal basis of eigenvectors. It turns out that there is a tight relation between the eigenvalues of A and several structural properties of the graph G, and these properties can often be useful in the study of various extremal problems. In particular, it can be shown that d-regular graphs in which the absolute value of every eigenvalue of the adjacency matrix besides the largest is much smaller than d, behave, in many ways, like random d-regular graphs. In particular, in such graphs on n vertices, every set of k vertices spans roughly $\frac{k^2 d}{2n}$ edges, and every set of vertices which is not too big has many neighbors outside the set. Graphs with the latter property are called expanders, and have numerous applications in Theoretical Computer Science. Constructing such graphs explicitly is not an easy matter, but there are several known constructions based on algebraic tools. See [1], Chapter 9 and its references for more details.

The application of topological methods in the study of combinatorial objects like partially ordered sets, graphs, hypergraphs and their coloring has already become part of the mathematical machinery commonly used in combinatorics. An

early example is Lovász' proof of Kneser's conjecture, mentioned in Section 2.3. Another example is the following result, proved by applying a Borsuk-type theorem: Every open necklace with ka_i beads of color i, $1 \leq i \leq t$, can be cut in at most $t(k-1)$ places so that the resulting segments can be partitioned into k piles, each containing exactly a_i beads of color i for all i. Many additional examples appear in [3], Chapter 34.

3 Probabilistic Combinatorics

The discovery, demonstrated in the early work of Paley, Zygmund, Erdős, Turán, Shannon and others, that deterministic statements can be proved by probabilistic reasoning, led already in the first half of the century to several striking results in Analysis, Number Theory, Combinatorics and Information Theory. 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. The book [1] is a recent text dealing with the subject.

The applications of probabilistic techniques in Discrete Mathematics, initiated by Paul Erdős who contributed to the development of the method more than anyone else, can be classified into three groups. The first one deals with the study of certain classes of random combinatorial objects, like random graphs or random matrices. The results here are essentially results in Probability Theory, although most of them are motivated by problems in Combinatorics. The second group consists of applications of probabilistic arguments in order to prove the existence of combinatorial structures which satisfy a list of prescribed properties. Existence proofs of this type often supply extremal examples to various questions in Discrete Mathematics. The third group, which contains some of the most striking examples, focuses on the application of probabilistic reasoning in the proofs of deterministic statements whose formulation often does not give any indication that randomness may be helpful in their study.

This section contains a brief description of several typical results in each of these three groups.

3.1 Random structures

The systematic study of Random Graphs was initiated by Erdős and Rényi in 1960. The most common model for a random graph is a slight variation of their model, and is denoted by $G(n,p)$. The term "the random graph $G(n,p)$" means a graph on a fixed set of n labeled vertices, where each pair of vertices forms an edge, randomly and independently, with probability p. Each graph property A is an event in this probability space, and one may study its probability $Pr[A]$, that is, the probability that the random graph $G(n,p)$ satisfies A.

One of the striking discoveries of Erdös and Rényi was the discovery of threshold functions. A graph property is monotone if it is closed under the addition of edges. Many interesting graph properties like hamiltonicity, non-planarity, or connectivity are monotone. For each of these three properties, when n is fixed and large, the probability of the random graph $G(n,p)$ to satisfy it changes very rapidly from nearly 0 to nearly 1 as p increases. Perhaps the most famous and illustrative example of this swift change is the sudden appearance of the so called giant component: if $p < c/n$ and $c < 1$, then a typical instance in the probability space $G(n,p)$ has all its connected components of size at most logarithmic in n; however, for every $c > 1$, $G(n,p)$ is likely to have one component of size linear in n (the giant component), while the rest are all of logarithmic size. This is related to the phase transition phenomenon in mathematical physics, which is treated in another chapter of this Companion. A recent result of Friedgut shows that the threshold for a graph property which is, in a sense that can be made precise, "global", is sharper than the one for a "local" property.

Another interesting early discovery in the study of Random Graphs was that of the fact that many interesting graph invariants are highly concentrated. A striking result of this type is the fact that for fixed values of p almost all graphs $G(n,p)$ have the same clique number. For every fixed positive value of $p < 1$ and every n, there is a real number $r_0 = r_0(n,p)$ which is roughly $2\log n/\log(1/p)$, such that the clique number of $G(n,p)$ is either $\lfloor r_0 \rfloor$ or $\lceil r_0 \rceil$ almost surely (that

is, with probability that tends to 1 as n tends to infinity). Moreover, $r_0(n,p)$ can be chosen to be an integer for most values of n and p. The proof of this result is based on the second moment method. One estimates the expectation and the variance of the number of cliques of a given size contained in $G(n,p)$, and applies the inequalities of Markov and Chebyshev.

The chromatic number of the random graph $G(n,p)$, whose typical behavior for values of p bounded away from 0 was determined by Bollobás, is also highly concentrated. This was proved by Shamir, Spencer, Łuczak and the authors of the present chapter. In particular, it can be shown that for every $\alpha < 1/2$ and every integer valued function $r(n) < n^\alpha$, there exists a function $p(n)$ such that the chromatic number of $G(n,p(n))$ is precisely $r(n)$ almost surely. Still, the determination of the concentration of the chromatic number of $G(n,p)$ for the most important case $p = 0.5$ (for which all labeled graphs on n vertices are equiprobable) remains an intriguing open problem.

Many additional results on random graphs can be found in [5].

3.2 Probabilistic constructions

The definition of the Ramsey number $R(k,k)$ is given in Section 2.2. In one of the first applications of the probabilistic method in Combinatorics, Erdős proved that if $\binom{n}{k}2^{1-\binom{k}{2}} < 1$ then $R(k,k) > n$, that is, there exists a graph on n vertices containing neither a clique of size k nor an independent set of size k. Note that $n = \lfloor 2^{k/2} \rfloor$ satisfies the above inequality for all $k \geq 3$, supplying an exponential lower bound for $R(k,k)$. The proof is simple: every fixed set of k vertices in the random graph $G(n,0.5)$ is 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 the random graph $G(n,0.5)$ contains a clique or an independent set of size k, and hence there is a graph without any such clique or independent set. Note that this proof is completely non-constructive, in the sense that it provides no efficient way to construct a graph with the above properties and merely proves its existence without giving any clue about an actual construction. This is a typical, intriguing phenomenon of probabilistic proofs.

A similar computation yields a solution for the tournament problem mentioned in Section 1.1. Let k and n be two integers, and suppose that

$$\binom{n}{k}\left(1-\frac{1}{2^k}\right)^{n-k} < 1.$$

Then there is a tournament on n teams, in which for every set of k teams, there is another one who beats them all. If n is larger than about $k^2 2^k \ln 2$ the above inequality holds.

Probabilistic constructions proved to be very powerful in supplying lower bounds for Ramsey numbers. Besides the bound for $R(k,k)$ mentioned above, there is a subtle probabilistic proof, due to Kim, that $R(3,k) \geq ck^2/\log k$, for some $c > 0$. This is known to be tight up to a constant factor, as proved by Ajtai, Komlós and Szemerédi, who also used probabilistic methods.

3.3 Proving deterministic theorems

Straus conjectured, and Erdős and Lovász proved, that for every k there is some $m = m(k)$, so that for every set S of m integers there is a coloring of the set of all integers by k colors, such that every translate of S intersects all color classes. The proof is probabilistic, and applies (besides some standard combinatorial arguments) the Lovaśz Local Lemma, a lemma that enables one to show that certain events hold with positive probability, even when this probability is extremely small. The assertion of this lemma, which has numerous additional applications, is, roughly, that for any finite collection of 'nearly independent' low probability events, there is a positive probability that none of the events holds. Note that the statement of Straus' conjecture has nothing to do with probability, and yet its proof relies on probabilistic arguments.

The choice number $ch(G)$ of a graph $G = (V,E)$ is the minimum number k so that for any assignment of a list of k colors for each vertex, there is a vertex coloring of G assigning to each vertex a color from its list, such that adjacent vertices get distinct colors. It is easy to see that for any graph G, $ch(G) \geq \chi(G)$. This inequality may be strict. In fact, it can be proved that for any c there is C so that any graph $G = (V,E)$ for which

$|E|/|V| \geq C$ satisfies $ch(G) \geq c$. In other words, every graph with large average degree has a large choice number. Somewhat surprisingly, the proof is probabilistic. This result can be used to show that the choice number of the graph whose vertices are all points of the plane where two are adjacent if their distance is 1, is infinite (though its chromatic number is known to be between 4 and 7).

Probabilistic arguments have proven extremely useful in numerous problems related to discrepancy or irregularities of distribution. For example, Erdős and Spencer proved that in any Red-Blue coloring of the edges of the complete graph K_n there is a subset V_0 of vertices so that the number of red edges it spans deviates from the number of blue edges it spans by at least $cn^{3/2}$, for some absolute constant $c > 0$. This problem is a convincing manifestation of the power of probabilistic methods – the result can be shown to be tight up to a constant factor by using, again, probabilistic considerations. Additional examples of such results can be found in [1].

4 Algorithmic aspects and future challenges

The rapid development of theoretical Computer Science and its tight connection to Discrete Mathematics motivated the study of the algorithmic aspects of combinatorial results.

The study of the algorithmic problems corresponding to probabilistic proofs is related to the investigation of randomized algorithms, a topic which has been developed tremendously during the last decade. In particular, it is interesting to find explicit constructions of combinatorial structures whose existence is proved by probabilistic arguments. "Explicit" here means that there is an efficient algorithm that constructs the desired structure in time polynomial in its size. Constructions of this type, besides being interesting in their own, have applications in other areas. Thus, for example, explicit constructions of error correcting codes that are as good as the random ones are of major interest in coding and information theory, and explicit constructions of certain Ramsey type colorings may have applications in derandomization – the process of converting randomized algorithms into deterministic ones.

It turns out, however, that the problem of finding a good explicit construction is often very difficult. Even the simple proof of Erdős, described in Section 3.2, that there are graphs on $\lfloor 2^{k/2} \rfloor$ 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, such a graph on $n \geq (1+\epsilon)^k$ vertices, in time which is polynomial in n, where $\epsilon > 0$ is any positive absolute constant? This problem is still wide open, despite a considerable amount of efforts.

The application of other advanced tools such as algebraic and analytic techniques, spectral methods and topological proofs, also tend to lead in many cases to non-constructive proofs. The conversion of these to algorithmic ones may well be one of the main future challenges of the area. Another interesting recent development is the increased appearance of computer aided proofs in Combinatorics, starting with the proof of the Four Color Theorem. A successful incorporation of such proofs in the area, without losing its special beauty and appeal, is another challenge. These challenges, the fundamental nature of the area, its tight connection to other disciplines, and the many fascinating open problems studied in it, ensure that Combinatorics will keep playing an essential role in the general development of Science in the future as well.

Bibliography

1. N. Alon and J. H. Spencer, *The Probabilistic Method*, Second Edition, Wiley, 2000.
2. B. Bollobás, *Extremal Graph Theory*, Academic Press, London, 1978.
3. R. L. Graham, M. Grötschel and L. Lovász, Editors, *Handbook of Combinatorics*, North Holland, Amsterdam, 1995.
4. R. L. Graham, B. L. Rothschild and J. H. Spencer, *Ramsey Theory*, Second Edition, Wiley, New York, 1990.
5. S. Janson, T. Łuczak and A. Ruciński, *Random Graphs*, Wiley, New York, 2000.
6. S. Jukna, *Extremal Combinatorics*, Springer-Verlag, Berlin, 2001.
7. J. Matoušek, Lectures on Discrete Geometry, Springer Verlag, 2002.
8. M. B. Nathanson, *Additive Number Theory: Inverse Theorems and the Geometry of Sumsets*, Springer-Verlag, New York, 1996.
9. J. Pach and P. Agarwal, *Combinatorial Geometry*, Wiley, 1995.

Biography of contributors

Noga Alon is a Baumritter Professor of Mathematics and Computer Science at Tel Aviv University, Israel. His research interests are Combinatorics and theoretical Computer Science. He is a member of the Israel National Academy of Sciences and received the Erdős prize, the Feher prize, the Pólya Prize, the Bruno Memorial Award, the Landau Prize and the Gödel Prize.

Michael Krivelevich is a Professor of Mathematics at Tel Aviv University, Israel. He got his PhD there and then spent a year at the Institute for Advanced Study in Princeton and another year at DIMACS Center, Rutgers University, before returning to Tel Aviv. His field of interest is Combinatorics and its applications.

Keywords
Extremal Graph Theory, Ramsey Theory, Extremal Set Theory, Combinatorial Number Theory, Discrete Geometry, Random Graphs, The Probabilistic Method.