Non-constructive proofs in Combinatorics

Noga Alon
Department of Mathematics
Raymond and Beverly Sackler Faculty of Exact Sciences
Tel Aviv University, Tel Aviv, Israel
and IBM Almaden Research Center
San Jose, CA 95120, USA

One of the main reasons for the fast development of Combinatorics during the recent years is certainly the widely used application of combinatorial methods in the study and the development of efficient algorithms. It is therefore somewhat surprising that many results proved by applying some of the modern combinatorial techniques, including Topological methods, Algebraic methods, and Probabilistic methods, merely supply existence proofs and do not yield efficient (deterministic or randomized) algorithms for the corresponding problems.

We describe some representing non-constructive proofs of this type, demonstrating the applications of Topological, Algebraic and Probabilistic methods in Combinatorics, and discuss the related algorithmic problems.

1 Topological methods

The application of topological methods in the study of combinatorial objects like partially ordered sets, graphs, hypergraphs and their coloring have become in the last ten years part of the mathematical machinery commonly used in combinatorics. Many interesting examples appear in [12]. Some of the more recent results of this type deal with problems that are closely related to certain algorithmic problems. While the topological tools provide a powerful technique for proving the required results, they give us no clue on an efficient way for solving the corresponding algorithmic questions.

A typical result of this type is the following theorem, proved in [2].

Theorem 1.1 *Let N be an opened necklace with ka_i beads of color i, $1 \leq i \leq t$. Then one can cut N in $(k-1)t$ places and partition the resulting intervals into k collections, each containing precisely a_i beads of color i for all $1 \leq i \leq t$.*

The bound $(k-1)t$, conjectured in [17] (where it is proved for $k = 2$) is sharp. This can be seen by considering the necklace in which the beads of each type appear contiguously. The proof supplies no efficient procedure, which finds, given a necklace as above, a partition of it with the desired properties. By an efficient procedure we mean here, and in what follows, either a deterministic algorithm whose running time is polynomial (in the length of the input) or a randomized algorithm whose expected running time (on the worst-case input) is polynomial.

Here is a sketch of the proof of the above theorem. A similar method is used in [6]. First we need a continuous version of it. Let $I = [0, 1]$ be the (closed) unit interval. An *interval t-coloring* is a coloring of the points of I by t colors, such that for each i, $1 \leq i \leq t$, the set of points colored i is (Lebesgue) measurable. Given such a coloring, a *k-splitting of size r* is a sequence of numbers $0 = y_0 \leq y_1 \leq \ldots \leq y_r \leq y_{r+1} = 1$ and a partition of the family of $r + 1$ intervals $F = \{[y_i, y_{i+1}] : 0 \leq i \leq r\}$ into k pairwise disjoint subfamilies $F_1, \ldots, F_k$ whose union is F, such that for each j, $1 \leq j \leq k$, the union of all intervals in F_j captures precisely $1/k$ of the total measure of each of the t colors.

The following result is the continuous analogue of Theorem 1.1.

Proposition 1.2 *Every interval t-coloring has a k-splitting of size $(k-1)t$.*

We note that a similar statement can be proved for general continuous probability measures instead of those defined by the colors. This generalizes the Hobby-Rice Theorem on L_1-approximation [18]. It is also related to one of the cake-splitting problems of Steinhaus. It is easy to see that the classical theorem of Liapounoff [20] implies the existence of an even splitting in this more general setting, but unlike the above result does not supply any finite bound on the number of cuts required to form the splitting. For more details see [2].

It is not difficult to see that Proposition 1.2 implies Theorem 1.1. This is because any opened necklace with $\sum_{i=1}^{t} ka_i = kn$ beads as in the theorem can be converted into an interval t-coloring by

partitioning the interval I into kn segments of equal size and by coloring the j^{th} part by the color of the j^{th} bead of the necklace. By Proposition 1.2 there is a k splitting with $(k-1)t$ cuts. Of course, these cuts need not occur at the endpoints of the segments, but a simple induction argument can be used to show that the cuts may be shifted until they form a partition of the discrete necklace satisfying the assertion of Theorem 1.1. We omit the details.

Another simple observation, whose details we omit, is the fact that the validity of Proposition 1.2 for (t,k) and for (t,k') implies its validity for (t,kk'). Therefore, it suffices to prove the proposition for prime values of k. To do so we define, following [11], a CW-complex $Y = Y(k,m)$ as follows.

For two integers k and m, put $N = N(k,m) = (k-1)(m+1)$ and let $\Delta = \Delta^N$ denote the N-dimensional simplex; i.e., $\Delta = \{(x_0,\ldots,x_N) : \ x_i \geq 0, \sum_{i=0}^{N} x_i = 1\}$. The *support* of a point $x \in \Delta$, denoted by $Supp(x)$, is the minimal face of Δ that contains x. Define

$$Y = Y(k,m) = \{(y_1,\ldots,y_k) : \ y_1,\ldots,y_k \in \Delta, Supp(y_i) \cap Supp(y_j) = \emptyset \ for \ all \ 1 \leq i < j \leq k\}.$$

The cyclic group Z_k acts freely on Y by letting its generator ω cyclically shift the coordinates of each point $y \in Y$, i.e., $\omega(y_1,\ldots,y_k) = (y_2,\ldots,y_k,y_1)$.

The following lemma is proved in [11].

Lemma 1.3 *If k is a prime, $m \geq 1$, $N = N(k,m) = (k-1)(m+1)$ and $Y = Y(k,m)$ and ω are as in the preceding paragrapah, then Y is $N-k$ connected and hence for every continuous mapping $h : Y \mapsto R^m$ there is a whole orbit of the Z_k action on Y that is mapped by h into one point. I.e., there is a $y \in Y$ such that $h(y) = h(\omega(y)) = \ldots = h(\omega^{k-1}(y))$*

We can now prove Proposition 1.2 for primes k. Let c be an interval t-coloring. Define $N = N(k,t-1) = (k-1)t$, $Y = Y(k,t-1)$ and consider the continuous function $h : Y \mapsto R^{t-1}$ defined as follows.

Suppose $y = (y_1,\ldots,y_k) \in Y$. By the definition of Y, each y_i is a point of Δ^N, i.e., a real vector of length N with nonnegative coordinates whose sum is 1. Moreover, the supports of the points y_i are pairwise disjoint. Put $x = (x_0,\ldots,x_N) = \frac{1}{k}\sum_{i=1}^{k} y_i$, and define a partition of the $[0,1]$-interval I into $N+1$ intervals $I_0,\ldots,I_N$ by

$$I_0 = [0,x_0] \ \ and \ \ I_j = [\sum_{l=0}^{j-1} x_l, \sum_{l=0}^{j} x_l], \ (1 \leq j \leq N).$$

Observe that since the supports of the points y_i are pairwise disjoint, then for each interval I_j with a positive length there is a unique l such that the j^{th} coordinate of y_l is positive.

For each l, $1 \leq l \leq k$, let F_l be the family of all the intervals I_j such that the j^{th} coordinate of y_l is positive. Note that the sum of lengths of the intervals in each F_l is precisely $1/k$, and that $F_1, \ldots, F_l$ form a partition of all the intervals I_j whose lengths are positive. For each i, $1 \leq i \leq t-1$, define $h_i(y)$ to be the measure of the i^{th} color in the union of the intervals of F_1. The function $h(y)$ is now defined by $h(y) = (h_1(y), \ldots, h_{t-1}(y))$.

This function is clearly continuous. Also, for every $1 \leq l \leq k$ and $1 \leq i \leq t-1$, $h_i(\omega^{l-1}(y))$ is precisely the measure of the i^{th} color in the union of the intervals of F_l. By Lemma 1.3 there is a $y \in Y$ such that $h(y) = h(\omega(y)) = \ldots = h(\omega^{k-1}(y))$. This means that each of the k families F_l corresponding to this point y captures precisely $1/k$ of the measure of each of the first $t-1$ colors. Since the total measure of each F_l is $1/k$, it follows that the last color is evenly distributed between the families as well. This completes the proof for the case of prime k, and hence implies the validity of Proposition 1.2 and Theorem 1.1. $\Box$

The main topological tool in the above proof is the Borsuk-type theorem stated in Lemma 1.3. This proof does not seem to supply an efficient way of producing a partition whose existence is guaranteed by the theorem.

In the classification of algorithmic problems according to their complexity, it is customary to try and identify the problems that can be solved efficiently, and those that *probably* cannot be solved efficiently. A class of problems that can be solved efficiently is the class P of all problems for which there are deterministic algorithms whose running time is polynomial in the length of the input. A class of problems that probably cannot be solved efficiently are all the NP-complete problems. An extensive list of such problems appears in [16]. It is well known that if any of them can be solved efficiently, then so can all of them, since this would imply that the two complexity classes P and NP are equal.

It is not too difficult to show that the following problem is NP-complete: Given a necklace satisfying the assumptions of Theorem 1.1, decide if one can form an even k-splitting of it by using less than b cuts. On the other hand, we know that $(k-1)t$ cuts always suffice, so although the problem of finding the minimum possible number of cuts cannot be solved efficiently, unless $P = NP$, it is considerable and seems likely that the problem of finding an even k-splitting using

$(k-1)t$ cuts is much easier. We do not know any efficient algorithm for this problem.

Another result whose (simple) proof applies the Borsuk-Ulam theorem is the following fact, proved in [1]:

Theorem 1.4 *Let $A_1, \ldots, A_d$ be d pairwise disjoint subsets of R^d, each containing precisely n points, and suppose that no hyperplane contains $d+1$ of the points in the union of all the sets A_j. Then there is a partition of $\cup A_j$ into n pairwise disjoint sets $S_1, \ldots, S_n$, each containing precisely one point from each A_j, such that the n simplices $conv(S_1), \ldots, conv(S_n)$ are pairwise disjoint.*

Here, again, the proof does not supply an efficient way of finding the sets S_i if the sets A_j are given, (although the proof does provide an efficient way of doing it for each *fixed* dimension d.)

2 Algebraic methods

Many combinatorial proofs rely on methods from linear and multilinear algebra. Extensive survey of results of this type is given in [9]. These proofs rarely supply constructive procedures for the corresponding algorithmic problems. Here is a simple example, which is a special case of one of the results in [5].

Proposition 2.1 *Every (not necessarily simple) graph with maximum degree 5 and average degree greater than 4, contains a 3-regular subgraph.*

The proof relies on the classical theorem of Chevalley and Warning (see, e.g., [10]). This theorem, that deals with the number of solutions of a system of multi-variable polynomials over a finite field, is the following.

Theorem 2.2 *Let $P_j(x_1, \ldots, x_m)$, $(1 \leq j \leq n)$ be n polynomials over a finite field F of characteristic p. If the number of variables, m, is greater than the sum of the degrees of the polynomials then the number of common zeros of the polynomials (in F^m) is divisible by p. In particular, if there is one common zero then there is another one.*

The proof is extremely simple; If F has q elements, then the number N of common zeros satisfies

$$N \equiv \sum_{x_1,\ldots,x_m \in F} \prod_{j=1}^{n} (1 - P_j(x_1, \ldots, x_m)^{q-1}) \ (mod\ p).$$

By expanding the right hand side we get a linear combination of monomials of the form $\prod_{i=1}^{m} x_i^{k_i}$ and for each such monomial at least one of the exponents k_i is strictly smaller than $q-1$. This implies that in F, $\sum_{x_i \in F} x_i^{k_i} = 0$, showing that the contribution of each monomial to the sum expressing N is $0 (mod\ p)$ and completing the proof. □

We can now prove Proposition 2.1. Given a graph $G = (V, E)$ satisfying the assumptions of the proposition, let n denote the number of its vertices. For each edge $e \in E$ and for each vertex $v \in V$, let $a(v, e)$ be 0 if e is not incident with v, 1 if e is a non-loop incident with v, and 2 if e is a loop incident with v. For each $e \in E$ let x_e be a variable and consider the following system of polynomial equations over $GF(3)$:

$$\sum_{e \in E} a(v, e) x_e^2 = 0 \qquad (v \in V).$$

This is a system of n degree-2 polynomial equations with $|E| > 2n$ variables. Moreover, it clearly has the trivial solution $x_e = 0$ for all e. Hence there is, by Theorem 2.2, a non-trivial solution $(y_e : e \in E)$. Let H be the subgraph of G consisting of all edges e for which $y_e \neq 0$. By the equations above, the degree of every vertex of H is divisible by 3, and since the maximum degree in G is 5 it follows that H is 3-regular, completing the proof. □

It is known that the decision problem: "Given a graph G, decide if it contains a 3-regular subgraph", is NP-complete. By the proposition above in certain cases we know that the answer to the decision problem is "yes" and yet the proof does not yield an efficient procedure for finding such a subgraph.

Another result proved by applying some extensions of the Chevalley- Warning Theorem is the following statement, proved in [7]. Recall that a *hypergraph* is a pair $(V, \mathcal{F})$ (sometimes denoted only by $\mathcal{F}$), where V is a finite set of vertices, and $\mathcal{F}$ is a finite set of subsets of V. The *degree* of a vertex is the number of edges that contain it.

Theorem 2.3 *Let q be a prime power, and let $\mathcal{F} = \{F_1, \ldots, F_{d(q-1)+1}\}$ be a hypergraph whose maximal degree is d. Then there exists $\emptyset \neq \mathcal{F}_0 \subset \mathcal{F}$, such that $|\bigcup_{F \in \mathcal{F}_0} F| \equiv 0 \pmod{q}$.*

Here, again, we do not know how to quickly find such a subset $\mathcal{F}_0$. Moreover, it can be shown that the problem of finding such an $\mathcal{F}_0$ is equivalent to the following problem: Given a polynomial h of degree at most d with $d(q-1)+1$ variables over $GF(q)$, suppose that $h(0) = 0$. Find another zero of $h(x)$ in which each variable is either 0 or 1.

3 Probabilistic methods

Probabilistic methods have been useful in combinatorics for almost fifty years. Many examples can be found in [14] and in [21].

In a typical application of the probabilistic method we try to prove the existence of a combinatorial structure (or a substructure of a given structure) with certain prescribed properties. To do so, we show that a randomly chosen element from an appropriately defined sample space satisfies all the required properties with positive probability. In most applications, this probability is not only positive, but is actually high and frequently tends to 1 as the parameters of the problem tend to ∞. In such cases, the proof usually supplies an efficient randomized algorithm for producing a structure of the desired type, and in many cases this algorithm can be derandomized and converted into an efficient deterministic one.

There are, however, certain examples, where one can prove the existence of the required combinatorial structure by probabilistic arguments that deal with rare events; events that hold with positive probability which is exponentially small in the size of the input. Such proofs usually yield neither randomized nor deterministic efficient procedures for the corresponding algorithmic problems.

A class of examples demonstrating this phenomenon is the class of results proved by applying the Local Lemma. This result, proved in [13] (see also, e.g., [21]), supplies a way of showing that certain events hold with positive probability, although this probability may be extremely small. The exact statement (for the symmetric case) is the following.

Lemma 3.1 *Let $A_1, \ldots, A_n$ be events in an arbitrary probability space. Suppose that the probability of each of the n events is at most p, and suppose that each event A_i is mutually independent of all but at most b of the other events A_j. If $ep(b+1) < 1$ then with positive probability none of the events A_i holds.*

One of the applications of this lemma, given already in the original paper [13], deals with *hypergraph coloring*. A hypergraph is *k-uniform* if each of its edges contains precisely k vertices. It is *k-regular* if each of its vertices is contained in precisely k edges. A hypergraph is 2-*colorable* if there is a two-coloring of the set of its vertices so that none of its edges is monochromatic. Erdös and Lovász proved the following result.

Proposition 3.2 *For each $k \geq 9$, every k-regular, k-uniform hypergraph is two colorable.*

The proof follows almost immediately from lemma 3.1. Let (V, E) be a k-uniform, k-regular hypergraph, and let $f : V \mapsto \{0, 1\}$ be a random 2-coloring obtained by choosing, for each $v \in V$ randomly and independently, $f(v) \in \{0, 1\}$ according to a unifrom distribution. For each $e \in E$ let A_e denote the event that f restricted to e is a constant, i.e., that e is monochromatic. It is obvious that $Prob(A_e) = 2^{-(k-1)}$ for every e, and that each event A_e is mutually independent of all the events A_f but those for which $f \cap e \neq \emptyset$. Since there are at most $k(k-1)$ edges f that intersect e we can substitute $b = k(k-1)$ and $p = 2^{-(k-1)}$ in Lemma 3.1 and conclude that for $k \geq 9$ with positive probability none of the events A_e holds, completing the proof. $\Box$

We note that a different, algebraic proof of the statement of the last proposition (that works for all $k \geq 8$) is given in [4]. Both proofs do not supply an efficient way of finding a proper two-coloring for a given hypergraph satisfying the assumptions of the proposition. Note that, in general, the problem of deciding whether a hypergraph is 2-colorable is NP-complete.

Another application of the Local Lemma, which appears in [8], is the following.

Proposition 3.3 *Every directed simple graph $D = (V, E)$ with minimum outdegree δ and maximum indegree Δ contains a directed (simple) cycle of length $0(mod\ k)$, provided $e(\Delta\delta + 1)(1 - \frac{1}{k})^{\delta} < 1$.*

The proof here first applies the Local Lemma to show that there exists a function $f : V \mapsto \{0, 1, \ldots, k\}$ such that for every $v \in V$ there is a vertex $u \in V$ such that (v, u) is a directed edge of D and $f(u) \equiv f(v) + 1(mod\ k)$.

Given such an f, the rest of the proof is very simple. We just choose, for every vertex $v \in V$, some vertex $p(v)$ such that $(v, p(v))$ is a directed edge and $f(p(v)) \equiv f(v) + 1(mod\ k)$. Suppose $v \in V$ and consider the sequence

$$v_0 = v, \quad v_1 = p(v_0), \quad v_2 = p(v_1), \ldots$$

Let j be the minimum index such that there is an $i < j$ with $v_i = v_j$. The cycle $v_i v_{i+1} \ldots v_{j-1} v_j = v_i$ is a directed cycle of length $0(mod\ k)$, as needed.

Here, again, the proof is not constructive in the sense that it does not provide an efficient way of finding such a cycle in a directed graph satisfying the assumptions. This is because the proof that a function f as above exists is non-constructive.

We note that it is not known if the related decision problem " Given a directed graph, decide if it contains a directed even cycle" is polynomial, but it is easy to deduce from the results of [15] that the similar problem " Given a directed graph and an edge e in it, decide if there is an even cycle containing e" is NP-complete.

The proof of the next result also relies on the Local Lemma, but contains several additional ingredients as well. The details appear in [3].

Theorem 3.4 *There is an absolute constant c with the following property: For any two graphs $G_1 = (V, E_1)$ and $G_2 = (V, E_2)$ on the same set of vertices, where G_1 has maximum degree at most d and G_2 is a vertex disjoint union of cliques of size cd each, the chromatic number of the graph $G = (V, E_1 \cup E_2)$ is precisely cd.*

The proof, again, does not supply an efficient (deterministic or randomized) algorithm for producing a proper cd-vertex coloring of G.

We close this section mentioning the following result of J. Spencer, whose proof, given in [22], which combines the probabilistic method with a counting argument, also fails to supply an efficient procedure for the corresponding algorithmic problem.

Theorem 3.5 *Let $v_1, \ldots, v_n$ be n real vectors of length n each, and suppose that the l_∞-norm of each v_i is at most 1. Then there are $\epsilon_1, \ldots, \epsilon_n \in \{-1, 1\}$, such that the l_∞-norm of the sum $\sum_{i=1}^{n} \epsilon_i v_i$ is at most $6\sqrt{n}$.*

4 Concluding remarks

We have seen several examples of combinatorial results proved by topological, algebraic or probabilistic methods. One natural question that arises is whether these methods are necessary. After all, we may tend to believe that simply stated combinatorial results should have simple combinatorial proofs. Although this sounds plausible, there are no known natural combinatorial proofs for any of the results mentioned here (as well as for various other known similar examples).

Another question that should be addressed is whether the proofs given here are really inherently non-constructive. Is it possible to modify them so that they yield efficient ways of solving the corresponding algorithmic problems? There are no known efficient algorithms for any of the

problems mentioned here. However, it seems very likely that such algorithms do exists. This is related to questions regarding the complexity of search problems that have been studied by several researchers. See, e.g., [19].

In the study of complexity classes like P and NP one usually considers only decision problems, i.e., problems for which the only two possible answers are "yes" or "no." However, the definitions extend easily to the so called "search" problems, which are problems where a more elaborate output is sought. The search problems corresponding to the complexity classes P and NP are sometimes denoted by FP and FNP.

Consider, for example, the obvious algorithmic problem suggested by Theorem 1.1, namely, given a necklace satisfying the assumptions of the theorem, find a partition of it satisfying the conclusions of the theorem. This problem is in FNP, since it is a search problem, and given a proposed solution for it we can check in polynomial time that it is indeed a solution.

Notice that this problem always has a solution, by Theorem 1.1, and hence it seems plausible that finding one should not be a very difficult task. The situation is similar with all the other algorithmic problems corresponding to the various results mentioned here. Still, the problem of solving efficiently the corresponding search problems remains an intriguing open question.

References

[1] J. Akiyama and N. Alon, *Disjoint simplices and geometric hypergraphs*, in : Combinatorial Mathematics; Proc. of the Third International Conference , New York, NY 1985 (G. S. Blum, R. L. Graham and J. Malkevitch, eds.), Annals of the New York Academy of Sciences, Vol. 555 (1989), 1-3.

[2] N. Alon, *Splitting necklaces*, Advances in Mathematics 63 (1987), 247-253.

[3] N. Alon, *The strong chromatic number of a graph*, to appear.

[4] N. Alon and Z. Bregman, *Every* 8*-uniform,* 8*-regular hypergraph is* 2*-colorable*, Graphs and Combinatorics 4 (1988), 303-305.

[5] N. Alon, S. Friedland and G. Kalai, *Regular subgraphs of almost regular graphs*, J. Combinatorial Theory Ser. B 37(1984), 79-91.

[6] N. Alon, P. Frankl and L. Lovász, *The chromatic number of Kneser hypergraphs*, Trans. Amer. Math. Soc. 298(1986), 359-370.

[7] N. Alon, D. J. Kleitman, R. Lipton, R. Meshulam, M. O. Rabin and J. Spencer, *Set systems with no union of cardinality* 0 *modulo* m, to appear.

[8] N. Alon and N. Linial, *Cycles of length* 0 *modulo* k *in directed graphs*, J. Combinatorial Theory Ser. B 47 (1989), 114-119.

[9] L. Babai and P. Frankl, *Linear Algebra Methods in Combinatorics I*, preliminary version, Department of Computer Science, University of Chicago, 1988.

[10] Z. I. Borevich and I. R. Shafarevich, *Number Theory*, Academic Press, New York, 1966.

[11] I. Bárány, S. B. Shlosman and A. Szücz, *On a topological generalization of a theorem of Tverberg*, J. London Math. Soc. (2), 23 (1981), 158-164.

[12] A. Bjorner, *Topological Methods*, to appear in : "Handbook of Combinatorics", R.L. Graham, M. Grőtschel and L. Lovász eds., North Holland.

[13] P. Erdös and L. Lovász, *Problems and results on* 3*-chromatic hypergraphs and some related questions*, in:"Infinite and Finite Sets" (A. Hajnal et. al. eds), Colloq. Math. Soc. J. Bolyai 11, North Holland, Amsterdam, 1975, pp. 609-627.

[14] P. Erdös and J. Spencer, *Probabilistic Methods in Combinatorics*, Academic Press/Akademiai Kiado, New York-Budapest, 1974.

[15] S. Fortune, J.E.Hopcroft and J.Wyllie, The directed subgraph homeomorphism problem, Theoret. Comp. Sci. 10(1980),111-120.

[16] M. R. Garey and D. S. Johnson, *Computers and Intractability: A Guide to the Theory of* NP*-completeness*, Freeman, 1979.

[17] C. H. Goldberg and D. B. West, *Bisection of circle colorings*, SIAM J. Algeb. Discrete Methods 6 (1985), 93-106.

[18] C. R. Hobby and J. R. Rice, *A moment problem in L_1 approximation*, Proc. Amer. Math. Soc. 16 (1965), 665-670.

[19] D. S. Johnson, C. H. Papadimitriou and M. Yannakakis, *How easy is local serach?*, JCSS 37 (1988), 79-100.

[20] A. Liapounoff, *Sur les fonctions vecteurs completement additives*, Izv. Akad. Nauk SSSR 4 (1940), 465-478.

[21] J. Spencer, *Ten Lectures on the Probabilistic Method*, SIAM, Philadelphia, 1987.

[22] J. Spencer, *Six standard deviations suffice*, Trans. Amer. Math. Soc. 289 (1985), 679-706.