Constructive and Non-Constructive Combinatorics

Noga Alon, Princeton and Tel Aviv

CSR 2018, Moscow, June 2018
I Constructive vs Non-constructive Combinatorics

Purely combinatorial proofs often provide efficient procedures for solving the corresponding algorithmic problems, even when dealing with NP-hard invariants.

Examples: Dirac’s Theorem: every graph with \( n \geq 3 \) vertices and minimum degree \( \geq n/2 \) is Hamiltonian.

Turán’s Theorem: every graph with degrees \( d_i \) contains an independent set of size at least \( \sum_i 1/(d_i +1) \)
Modern combinatorial techniques include topological, algebraic, geometric and probabilistic methods.

Proofs obtained using these methods (especially the first three) are often non-constructive, that is, provide no efficient algorithms for the corresponding problems.
II Topologoical methods: applying fixed point theorems

Thm (Lovász, 78): In any coloring $f$ of the $k$-subsets of an $n$-set by $n-2k+1$ colors, there are two disjoint $k$-subsets with the same color.

The shortest known proof (Greene 03) defines, using $f$, a coloring $g$ of the sphere $S^t$ with $t=n-2k$ by $t+1$ colors, applies the Borsuk-Ulam Theorem to get two nearly antipodal points with the same color, and concludes, using the definition of $g$ from $f$, that two disjoint $k$-sets have the same color.
Thm (Schrijver (78)): Given a cycle C of length n, for any coloring of the independent sets of size k of C by n-2k+1 colors, there are two disjoint independent sets with the same color.
The Necklace Thm [A (87)]: Any open necklace with $ka_i$ beads of type $i$ ($1 \leq i \leq t$) can be partitioned into intervals using at most $(k-1)t$ cuts, so that the resulting intervals can be partitioned into $k$ collections, each containing exactly $a_i$ beads of type $i$, for all $1 \leq i \leq t$.

This is tight for all $k$ and $t$. 
Steps of proofs:

Show that the validity of the statement for $k_1$ and $k_2$ implies its validity for $k=k_1k_2$

Consider a continuous version of the problem, in which the necklace is an interval colored by $t$ colors

Apply a fixed-point theorem (Bárány, Shlosman, Szűcs (81)) to prove the statement for prime $k$. 
Open: Can we find the \((k-1)t\) cuts efficiently, for a given input necklace?
The cycle+triangles conjecture (Du, Hsu, Hwang (90)):

Let \( G = (V, E) \) be a graph on \( 3n \) vertices whose edges are the union of a Hamilton cycle (of length \( 3n \)) and \( n \) pairwise vertex disjoint triangles. Then \( G \) contains an independent set of size \( n \).
A stronger conjecture (Erdös (91)): Any such $G$ is $3$-colorable

Thm (Fleischner and Stiebitz (92)): Any such $G$ is $3$-choosable: for any assignment of a list of $3$ colors to each vertex, there is a proper vertex coloring assigning to each vertex a color from its list.

The proof is based on the algebraic approach of A-Tarsi (92).
A new proof of the cycle + triangles original conjecture, based on Schrijver’s Theorem (whose proof is based on the Borsuk-Ulam Theorem). [Extensions appear in Aharaoni, A, Berger, Chudnovsky, Kotlar, Loebl, Ziv(17)]

**Schrijver(78):** Any coloring of the independent sets of size $k$ in a cycle of length $m$ by $m-2k+1$ colors contains two disjoint independent sets of the same color.
Assume, for contradiction, that there is a graph $G=(V,E)$ on a set $V$ of $3n$ vertices whose edges are a Hamilton cycle $C$ and $n$ disjoint triangles, with no independent set of size $n$.

Color the independent sets of size $n$ in $C$ as follows: each set $I$ is colored by the index of the first triangle that contains at least 2 points of $I$.

By Schrijver, since $3n-2n+2>n$ there are two disjoint independent sets $I_1, I_2$ with the same color. This is impossible, as it means that the same triangle contains 2 points of each of them. ■
Open: Given a graph $G$ on $3n$ vertices whose edges are the union of a Hamilton cycle and $n$ disjoint triangles, can one find efficiently an independent set of size $n$ in $G$?
Hilbert’s Nullstellensatz (1893):

If $F$ is an algebraically closed field, $f, g_1, \ldots, g_m$ polynomials in $F[x_1, x_2, \ldots, x_n]$ and $f$ vanishes whenever all $g_i$ do, then there is $k \geq 1$ and polynomials $h_i$ so that

$$f^k = \sum_i h_i g_i$$
Combinatorial Nullstellensatz [CN1] (A-99):

Let $F$ be a field, $f(x_1, x_2, \ldots, x_n)$ a polynomial over $F$, let $S_1, S_2, \ldots, S_n$ be subsets of $F$, and put

$$g_i(x_i) = \prod_{s \in S_i} (x - s)$$

If $f$ vanishes whenever all $g_i$ do, then there are polynomials $h_i$ with $\deg(h_i) \leq \deg(f) - \deg(g_i)$ and

$$f = \sum_i h_i g_i$$

Let $F$ be a field, $f(x_1, x_2, \ldots, x_n)$ a polynomial over $F$, and $t_1, t_2, \ldots, t_n$ positive integers. If the degree of $f$ is $t_1 + t_2 + \ldots + t_n$, and the coefficient of

$$
\prod_{i=1}^{n} x_i^{t_i}
$$

in $f$ is nonzero, then for any subsets $S_1, \ldots, S_n$ of $F$, where $|S_i| \geq t_i + 1$ for all $i$, there are $s_i$ in $S_i$ so that $f(s_1, \ldots, s_n)$ is not 0.
The choice number $\text{ch}(G)$ (or list chromatic number) of a graph $G=(V,E)$ is the minimum $k$ so that for any assignment of a list $L_v$ of $k$ colors to each vertex $v$, there is a proper coloring $f$ of $G$ with $f(v)$ in $L_v$ for each $v$.

This was defined independently by Vizing (76) and by Erdős, Rubin and Taylor (79).

Clearly $\text{ch}(G) \geq \chi(G)$ for every $G$.

(Very) strict inequality is possible.
Sylvester (1878), Petersen (1891): The graph polynomial of a graph $G=(V,E)$ on the set of vertices $V=\{1,2,\ldots,n\}$ is

$$f_G(x_1, \ldots, x_n) = \prod_{ij \in E, i<j} (x_i - x_j)$$

If $S_1, S_2, \ldots, S_n$ are finite lists of colors (represented by real or complex numbers) then there are $s_i$ in $S_i$ so that $f_G(s_1, \ldots, s_n) \neq 0$ iff there is a proper coloring of $G$ assigning to each vertex $i$ a color from its list $S_i$. 


By **CN1**, a graph $G$ is not 3-colorable iff there are polynomials $h_i$ so that

$$f_G = \sum_i h_i (x_i^3 - 1)$$

**Exercise**: use this fact to prove that $K_4$ is not 3-colorable.

**Note**: this does not prove that $\text{NP}=\text{coNP}$
By CN2, if G has $kn$ edges and the coefficient of $\prod x_i^k$ in $f_G$ is nonzero, then $\text{ch}(G) \leq k+1$

In A-Tarsi(92) this coefficient is interpreted combinatorially in terms of Eulerian orientations of G.

Using this interpretation, Fleishner and Stiebitz(92) proved that the relevant coefficient is nonzero for any 4-regular graph G consisting of a Hamilton cycle+triangles, hence $\text{ch}(G) \leq 3$. 
**Open:** Given a graph $G$ on $3n$ vertices whose edges are the union of a Hamilton cycle and $n$ disjoint triangles, can one find efficiently an independent set of size $n$ in $G$?

Can we find efficiently a proper 3-coloring of the vertices?

Given lists of size 3 for the vertices, can we find efficiently a proper vertex coloring assigning to each vertex a color from its list?
A similar reasoning provides a strengthening of the **Four Color Theorem** (4CT).

By **Tait**, the 4CT (**Appel and Haken** (76), **Robertson, Sanders, Seymour** and **Thomas** (96)) is equivalent to the fact that the **chromatic number** of the line graph of any cubic, bridgeless **planar** graph is 3.

**A-Jaeger-Tarsi** (same + extension by **Ellingham-Goddyn**): The **choice number** of the line graph of any cubic, bridgeless, planar graph is 3.
This is proved using \textbf{CN2}, by showing that the relevant coefficient of the graph polynomial is the number of \textit{proper 3 colorings} of this line graph, which is nonzero, by 4CT
Open: Given a cubic, bridgeless, planar graph with a list of 3 colors for every edge, can one fine **efficiently** a proper coloring of the edges assigning to each edge a color from its list?
An even older result:

**Thm (A-Friedland-Kalai (84)):** Any (multi)graph with average degree > 4 and maximum degree at most 5 contains a 3-regular subgraph.
An even older result:

**Thm (A-Friedland-Kalai (84)):** Any (multi)graph with average degree > 4 and maximum degree at most 5 contains a 3-regular subgraph.
Proof using **CN2**: Let $G=(V,E)$ be such a graph, and put $a_{v,e}=1$ if $v$ lies in $e$, 0 otherwise.

Apply **CN** to the following **polynomial** in the variables $x_e$ over $\mathbb{Z}_3$:

$$\prod_{v \in V} \left( 1 - \left( \sum_{e, v \in e} a_{v,e} x_e \right)^2 \right) - \prod_{e \in E} (1 - x_e)$$

with $S_e = \{0,1\}$ for all $e$.

The edges of the required subgraph are all $e$ with $x_e = 1$.
Open: Given a graph with average degree $> 4$ and maximum degree 5, can we find efficiently a 3-regular subgraph?
The Permanent Lemma

If $A$ is an $n$ by $n$ matrix over a field, $\text{Per}(A) \neq 0$ and $b$ is a vector in $F^n$ then there is a $0/1$ vector $x$ so that $(Ax)_i \neq b_i$ in all coordinates.

Proof: Apply CN2 to

$$f = \prod_{i=1}^{n} \left( \sum_{j=1}^{n} a_{ij}x_j - b_i \right)$$

with $t_1 = t_2 = \ldots = t_n = 1$, $S_i = \{0, 1\}$ for all $i$. 
Corollary: If $G$ is a bipartite graph with classes of vertices $A, B$, $|A| = |B| = n$, $B=\{b_1, b_2, \ldots, b_n\}$ which contains a perfect matching, then for any integers $d_1, \ldots, d_n$ there is a subset $X$ of $A$ so that for each $i$ the number of neighbors of $b_i$ in $X$ is not $d_i$

Example:
Corollary: If $G$ is a **bipartite graph** with classes of vertices $A,B$, $|A|=|B|=n$, $B=\{b_1,b_2,\ldots,b_n\}$ which contains a **perfect matching**, then for any integers $d_1,\ldots,d_n$ there is a subset $X$ of $A$ so that for each $i$ the number of neighbors of $b_i$ in $X$ is not $d_i$

Example:

![Diagram](image)

$d_1=0$

$d_2=1$

$d_3=2$
**Problem:** Given a bipartite graph with a perfect matching on the vertex classes A and B={b₁,...,bₙ}, and given integers d₁,...,dₙ, can one find **efficiently** a subset X of A so that the number of neighbors of each bᵢ in X is not dᵢ?
IV Hardness

Are these algorithmic problems complete for some natural complexity classes (like PPAD)?

Prop: The following algorithmic problem is at least as hard as inverting one-way permutations (e.g., computing discrete logarithm in $\mathbb{Z}_p^*$):

Given an arithmetic circuit computing an $f$ in $F[x_1, \ldots, x_n]$ with $\deg(f) = \sum_i t_i$ and coefficient of $\prod_i x_i^{t_i}$ being nonzero, and given $S_i$ in $F$ of size $t_i + 1$, find $s_i$ in $S_i$ with $f(s_1, \ldots, s_n) \neq 0$. 
The algorithmic versions of Borsuk-type fixed point theorems are also hard in general.

However, the problems discussed here (necklace, cycle+triangles, choice 4CT, 3-regular subgraph) and additional similar ones may be simpler. Are they?