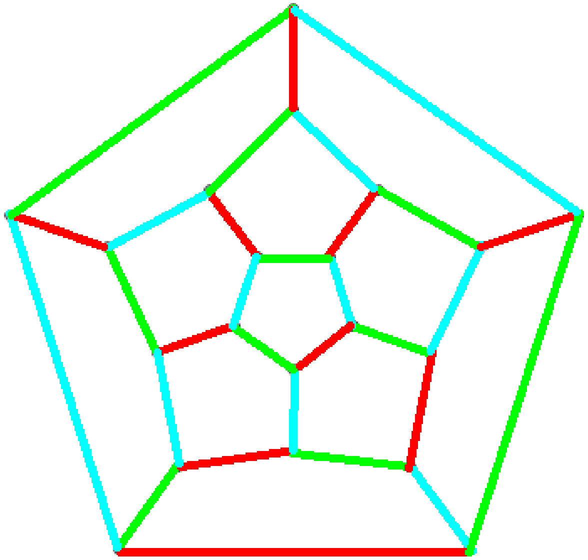
The Polynomial Method

Noga Alon, Princeton and Tel Aviv



FPSAC, Bar Ilan U., January 2022

I Nullstellensatz

Hilbert's Nullstellensatz (1893):

If F is an algebraically closed field, f, g_1 , …,g_m polynomials in F[x_1,x_2,…,x_n] and f vanishes whenever all g_i do, then there is k ≥ 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 $\deg(h_i) \le \deg(f) - \deg(g_i)$ and

$$f = \sum_i h_i g_i$$

Combinatorial Nullstellensatz [CN2] (A-99):

Let F be a field, $f(x_1, x_2, \ldots, x_n)$ a polynomial over F, and $t_1, t_2, \ldots, t_n$ non-negative 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.

Proofs of combinatorial statements obtained using this theorem are often non-constructive, that is, provide no efficient algorithms for the corresponding algorithmic problems.

II Distinct Sums

Thm [A (00), Dasgupta,Károlyi,Serra and Szegedy(01), Arsovski (11)]:
If p is a prime, and k<p then for every $a_1,..,a_k$ ϵ Z_p (not necessarily distinct) and every subset B of Z_p , |B|=k, there is a numbering $b_1,b_2, \dots ,b_k$ of the elements of B so that all sums a_i+b_i are distinct (in Z_p).

Pf: Apply CN2 to $f=f(x_1,x_2,\dots,x_k)=$

$$\prod_{1\le i<j\le k}(x_i-x_j)\prod_{1\le i<j\le k}(x_i+a_i-x_j-a_j)$$

with $F=Z_p$, $t_i=k-1$ and $S_i = B$ for all i.

Note: Here the coefficient of $\prod_{i=1}^{k} x_i^{k-1}$ is k! which is nonzero modulo p

Several extensions follow by the Dyson Conjecture. Related results: Karasev and Petrov (12).

Question: Given $a_1, a_2, \ldots, a_k$ and a subset B of Z_p of cardinality k, can one find efficiently a numbering $b_1, b_2, \ldots, b_k$ of the elements of B so that all sums a_i+b_i are distinct (in Z_p).

III The Permanent Lemma

If A is an n by n matrix over a field, Per(A)≠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.

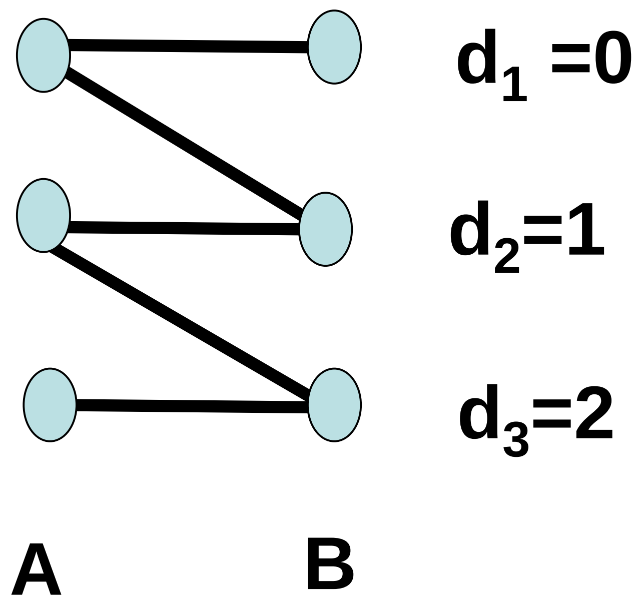
Proof: Apply CN2 to

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

with $t_1=t_2=\ldots=t_n=1$, $S_i=\{0,1\}$ for all i.

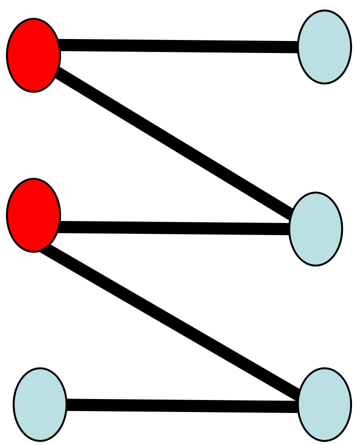
Corollary: If G is a **bipartite graph** with classes of vertices A,B, |A|=|B|=n, $B=\{b_1,b_2,\ldots,b_n\}$ which contains a **perfect matching**, then for any integers $d_1,\ldots,d_n$ there is a subset X of A so that for each i the number of neighbors of b_i in X is not d_i

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:



$d_1 = 0$

$d_2 = 1$

$d_3 = 2$

Problem: **Given a bipartite graph with a perfect matching on the vertex classes A and $B=\{b_1,..,b_n\}$, and given integers $d_1,..,d_n$, can one find efficiently a subset X of A so that the number of neighbors of each b_i in X is not d_i ?**

IV Graph Coloring

The list chromatic number $\chi_l(G)$ 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 Erdös, Rubin and Taylor (79).

Clearly $\chi_l(G) \geq \chi(G)$ 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,..,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

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

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

(Remark: This does not prove that NP=co-NP)

By CN2, if G has kn edges and the coefficient of $\prod x_i^{k}$ in f_G is nonzero, then $\chi_\ell(G) \le k+1$

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

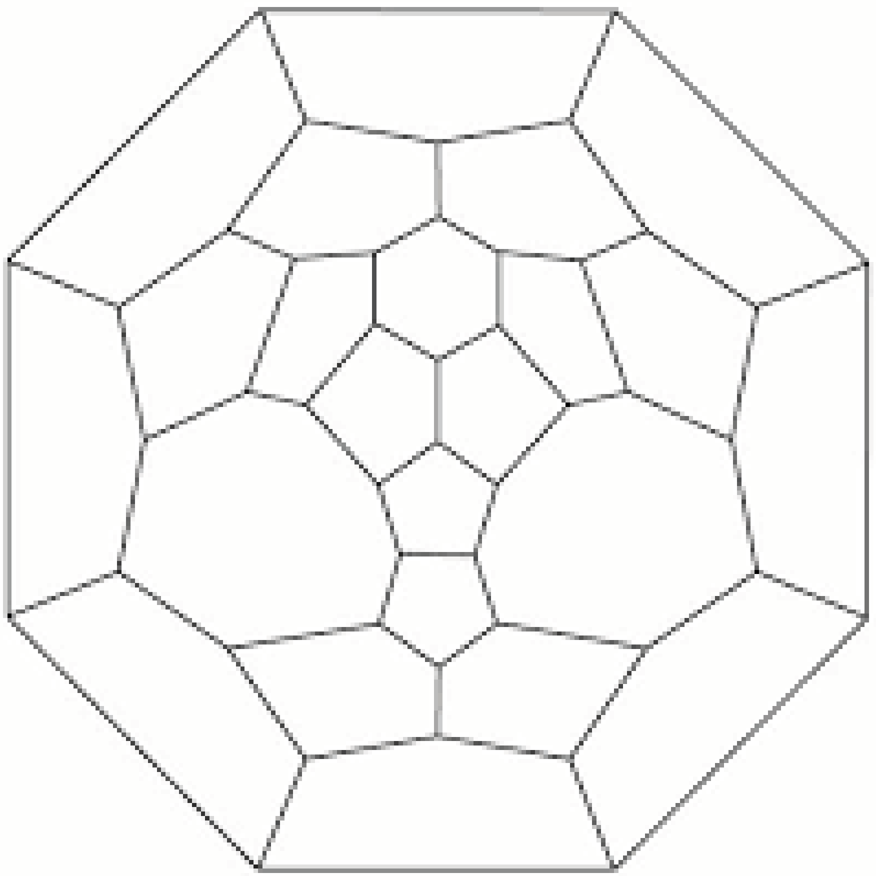
This can be used to prove a strengthening of the Four Color Theorem (4CT).

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 list chromatic number of the line graph of any cubic, bridgeless, planar graph is 3.

This is proved using CN2, by showing that the relevant coefficient of the graph polynomial is the number of 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 find efficiently a proper coloring of the edges assigning to each edge a color from its list ?



V Mixing Properties of Vertex Colorings of Z^d

A, Briceňo, Chandgotia, Magazinov and Spinka (21)

Let Z^d denote the (infinite) graph of the d-dimensional lattice

This is a bipartite 2d-regular graph

Motivation for considering proper vertex colorings of Z^d by q colors:

Statistical Physics: the vertices are atoms or molecules of a crystal. Each atom has a magnetic spin taking one of q values.

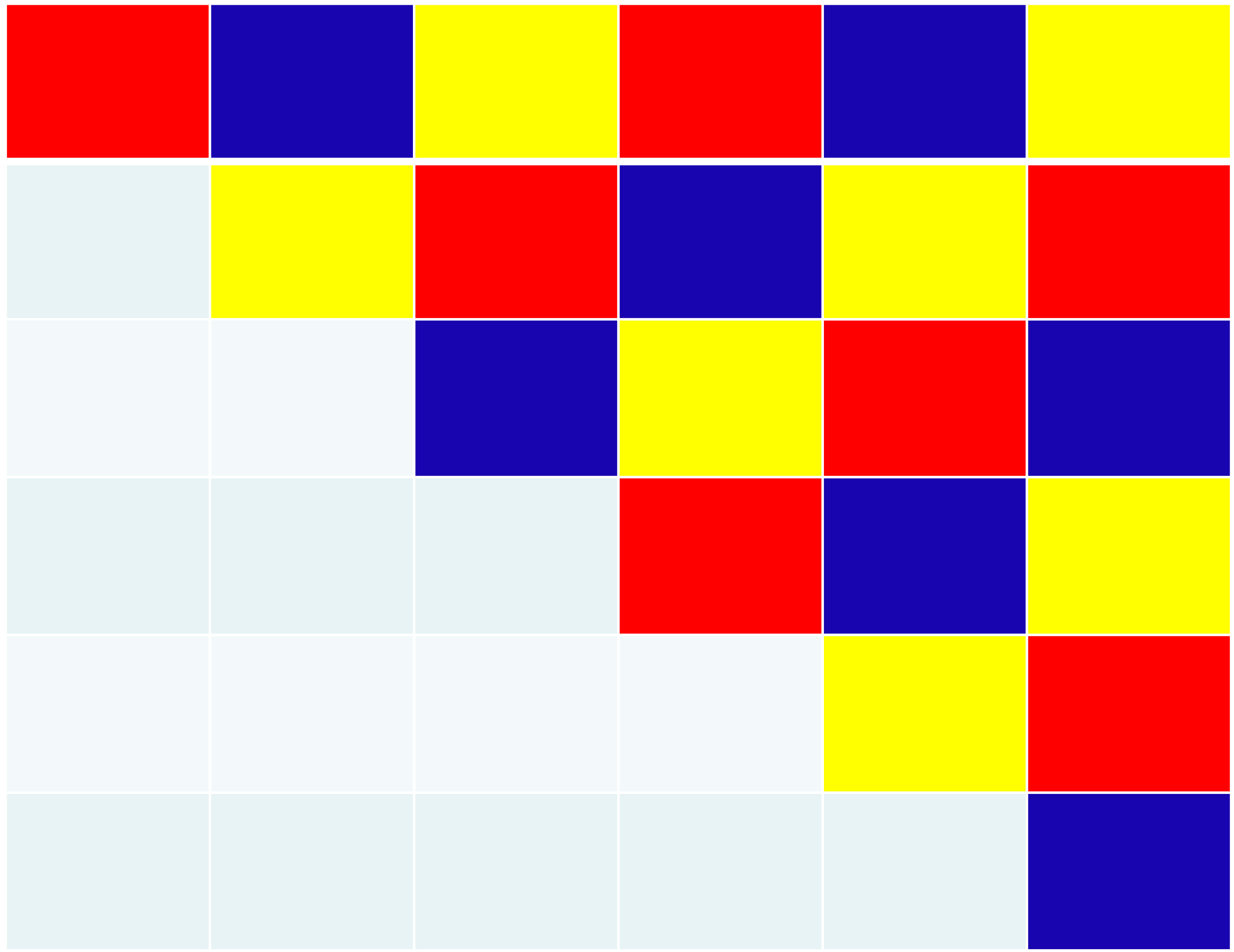
Antiferromagnetic material: adjacent spins tend to be different. This tendency becomes absolute in the zero-temperature limit

Proper q-colorings represent zero-temperature anti-ferromagnetic q-state Potts Model.

Let f_1 and f_2 be two proper vertex colorings of Z^d by q colors, and let A and B be two subsets of Z^d which are far from each other: the distance between A and B is at least some g(d).

Question: **can we ensure that there is a proper vertex coloring f of Z^d which agrees with f_1 on A and agrees with f_2 on B ?**

Answer [A, Briceňo, Chandgotia, Magazinov and Spinka (21)]: yes if q is at least d+2, no if q is at most d+1.



Partial 3-coloring with a unique extension

To show that when $q \geq d+2$ for any two q-colorings f_1 , f_2 there is one that agrees with the first on A and with the second on B it suffices to prove that any proper q-coloring of part of the boundary of a large box $[n]^d$ in Z^d can be extended to a proper q-coloring of the interior of the box.

Indeed, we can partition the grid into boxes as above, color the ones intersecting A according to f_1 and those intersecting B according to f_2 and complete the coloring box by box.

Thm (ABCMS(21)): **If $q \geq d+2$ and $n \geq d+2$ then any proper vertex coloring of (any part of) the boundary of $[n]^d$ by q colors can be extended to a proper q-coloring of the interior of the box.**

The proof proceeds by observing that this is a statement about list coloring: assign to each vertex in the interior of the box the set of all colors besides those that appear on its neighbours that are already colored.

The result can then be proved combining the polynomial method with Hall's Theorem that can provide the existence of an orientation that supplies the required nonzero coefficient.

VI A hat guessing game

The Rules(Butler, Hajiaghayi, Kleinberg, Leighton, Farnik):

After coordinating a strategy, each of n players occupies a different vertex of a graph G. Hats of q colors are placed on their heads. Each player sees the colors of the hats of the neighboring players. Simultaneously, each player guesses the color of his hat. The players win if at least one player guesses correctly.

Question: what is the maximum number of colors q=q(G) such that the players can always ensure a win ?

Claim: n players can win on a complete graph with n colors. **Strategy:** Player i assumes the total sum is i modulo n. In fact $q(K_n)=n$.

What about complete bipartite graphs $K_{n,n}$?

Clearly $q(K_{1,1})=q(K_2)=2$

Indeed, for x,y in GF(2) either

$L=x-y \quad =0 \quad$ or

$R=y-(x+1)=0.$

Szczechla (17): $q(K_{2,2})=q(C_4) =3$

Indeed, for x_1,x_2,y_1,y_2 in GF(3) either

$L_1= \quad x_1-(y_1+y_2) \quad =0 \quad$ or

$L_2= \quad x_2-(2y_1+y_2) \quad =0 \quad$ or

$R_1=L_1-L_2 = y_1 - (2x_1+x_2) =0 \quad$ or

$R_2=L_1+L_2 = y_2-(2x_1+2x_2)=0$

What about complete bipartite graphs $K_{n,n}$?

Clearly $q(K_{1,1})=2$

Szczechla (17): $q(K_{2,2})=3$

In both cases there are optimal linear guessing schemes: each guessing function is a linear function of the colors the player sees (where the colors are represented as elements of a finite field)

Thm (A, Ben-Eliezer, Shangguan, Tamo(20)):
for q=4 and every n, there are no linear winning guessing schemes for $K_{n,n}$.
However, with non-linear schemes

$$q(K_{n,n}) \geq n^{1/2-o(1)}$$

Theorem: For every n there is no linear guessing scheme over GF(4) that wins on $K_{n,n}$

Proof (sketch): Let $x_1, x_2, \ldots, x_n$ denote the colors of the players in one vertex class, $y_1, y_2, \ldots, y_n$ denote the colors of the players in the other class. (Here x_i , y_j are in GF(4)).

A linear guessing scheme is given by two n by n matrices A and B, and two vectors of length n, a and b, so that the polynomial over GF(4)

$$\prod_{i=1}^{n}\left(x_i - \sum_{j=1}^{n} a_{ij} y_j - a_i\right) \prod_{i=1}^{n}\left(y_i - \sum_{j=1}^{n} b_{ij} x_j - b_i\right)$$

vanishes for all x_i , y_j in GF(4).

The n linear forms $L_i = x_i - \sum_{j=1}^{n} a_{ij} y_j$ are linearly independent, and so are the n linear forms

$$M_i = y_i - \sum_{j=1}^{n} b_{ij} x_j$$

Let Z_1 , Z_2 , …,Z_r be a maximal set of linearly independent forms among { L_i , M_j } containing all the L_i and possibly some M_j , (the first ones, say), and let $C=(c_{ij})$ be the r by r nonsingular matrix so that

$$\sum_{j=1}^{r} c_{ij} Z_j = M_{r-n+i}$$

for $1 \le i \le 2n-r$.

Our objective is to show that there is an assignment for the variables Z_i over GF(4) so that

Z_i is not equal to a_i for $1 \le i \le n$

Z_i is not equal to b_{i-n} for $n+1 \le i \le r$, and

$$\sum_{j=1}^{r} c_{ij} Z_j \neq b_{r-n+i}$$

for $1 \le i \le 2n-r$.

This can be proved using the Combinatorial Nullstellensatz and the fact that over GF(4), The permanenet of a matrix is equal to its determinant.

Remark: A modified version works for every non-prime field. The statement for prime fields is closely related to a conjecture of A, Jaeger and Tarsi (89): If F is any field with at least 4 elements and C is a nonsigular square matrix over F, then there is a vector z so that both z and Cz have no zero entries.

Nagy and Pach (21): The AJT conjecture holds for all primes > 61 besides possibly 79.

Open: Given a linear guessing scheme over GF(4), find efficiently a hat configuration on which the scheme fails.

VII Hyperplane coverings

Thm (A and Füredi (93)): **Every collection of hyperplanes that covers all nonzero vertices of the discrete cube $\{0,1\}^n$ in R^n but does not cover the origin (0,0,..,0) contains at least n hyperplanes. This is tight as shown by $x_i=1$ for all $i \le n$.**

The proof follows easily using the CN.

Clifton and Huang (20): **What if every point is covered k times, and the origin is uncovered?**

Example: **The n hyperplanes $x_i=1$ together with k-j copies of $\sum_{i=1}^{n} x_i = j\,,\ 1 \le j < k$ show that $n + \binom{k}{2}$ hyperplanes suffice.**

Clifton and Huang (20): What if every point is covered k times, and the origin is uncovered?

Example: The n hyperplanes $x_i=1$ together with k-j copies of $\sum_{i=1}^{n} x_i = j$, $1 \leq j < k$ show that $n + \binom{k}{2}$ hyperplanes suffice.

Conjecture (CH (20)): For every fixed k and $n>n_0(k)$ this is tight

Thm (CH): This holds for k=2,3. For k ≥ 4 at least n+k+1 hyperplanes are needed

Thm (Sauermann and Wigderson (21)): For k≥2 and n≥2k-3, at least n+2k-3 hyperplans are needed.

The proofs are based on an extension of CN for polynomials that vanish to high order on most of the hypercube.

Extensions of this type also appear in
Ball and Serra (09)
Kós, Mészarós and Rónyai (11)
Kós and Ronyai (12)
Batzaya and Bayaramagnai (20)

VIII Hardness

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

Prop: The following algorithmic problem is at least as hard as inverting one-way permutations (e.g., computing discrete logarithm in 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 $f(s_1,\ldots,s_n) \neq 0$.

However, the problems discussed here (distinct sums, forbidden degrees, list-coloring, choice 4CT, hat-guessing, cube near-covering) and similar additional ones may be simpler.

Are they ?

Thank You