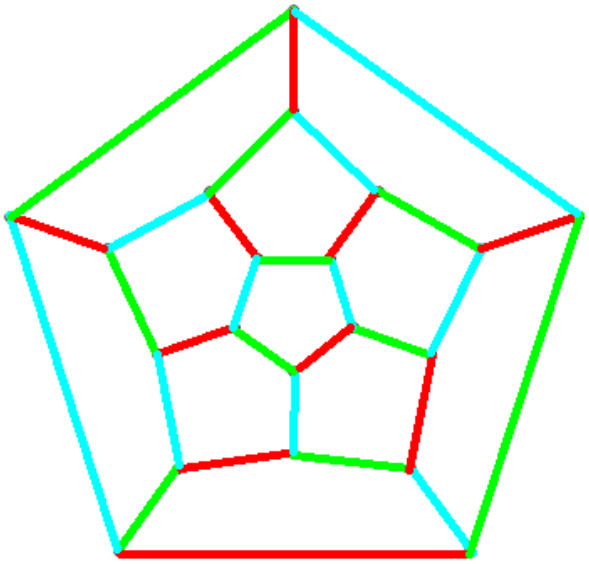
Combinatorial Nullstellensatz and its Algorithmic Aspects

Noga Alon, Tel Aviv U.



Hebrew U. Dec. 2016

I Nullstellensatz

Hilbert's Nullstellensatz (1893):

If F is an algebraically closed field, f, g_1 , …,g_m polynomials in $F[x_1,x_2,\ldots,x_n]$ 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

$$f = \sum_i h_i g_i$$

Combinatorial Nullstellensatz [CN2] (A-99):

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

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 $a_1,..,a_k \in Z_p$ (not necessarily distinct) and every subset B of Z_p , |B|=k, there is 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).

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

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

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 , … , a_k and a subset B of Z_p of cardinality k, can one find efficiently a numbering b_1 , b_2 , … ,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.

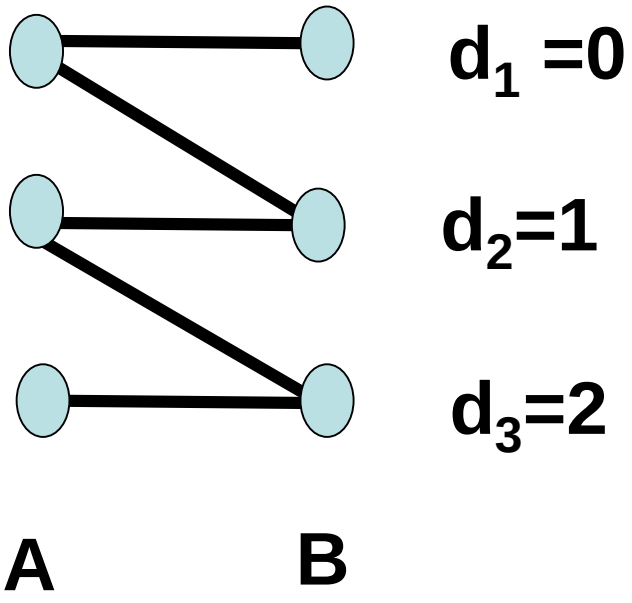
Proof: Apply CN2 to

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

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

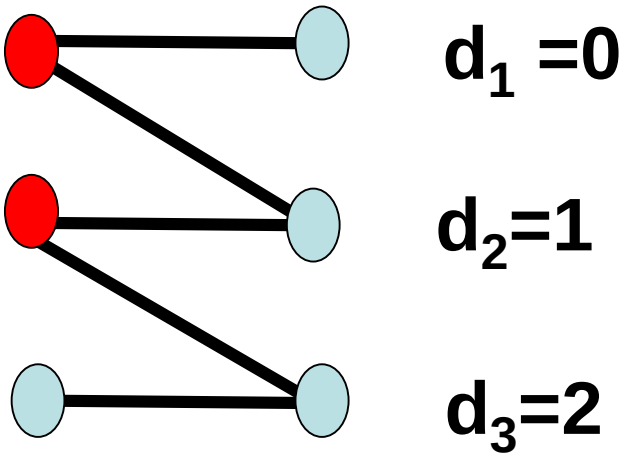
Corollary: If G is a bipartite graph with classes of vertices A,B, $|A|=|B|=n$, $B=\{b_1,b_2,\ldots,b_n\}$ which contains a perfect matching, then for any integers $d_1,\ldots,d_n$ there is a subset X of A so that for each i the number of neighbors of b_i in X is not d_i

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

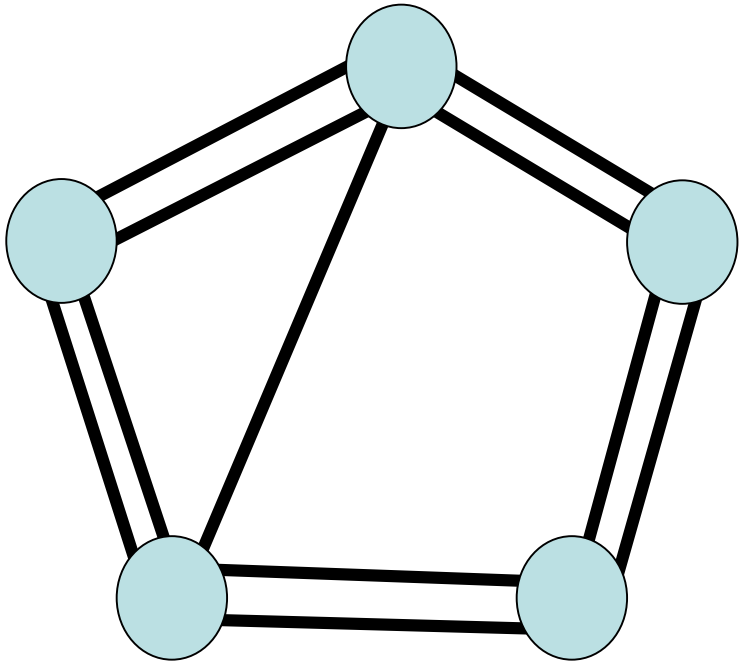
Example:



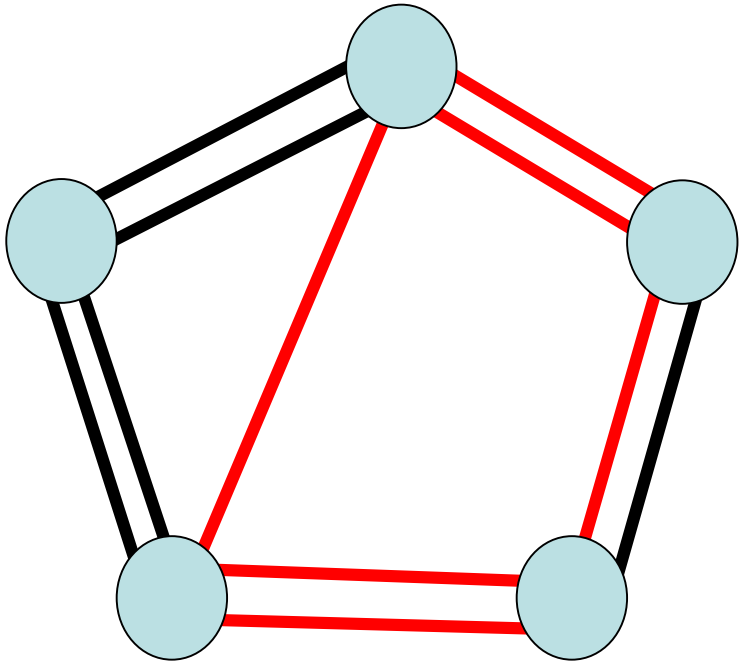
Problem: Given a bipartite graph with a perfect matching on the vertex classes A and $B=\{b_1,..,b_n\}$, and given integers $d_1,..,d_n$, can one find **efficiently** a subset X of A so that the number of neighbors of each b_i in X is not d_i ?

IV Regular subgraphs

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



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.

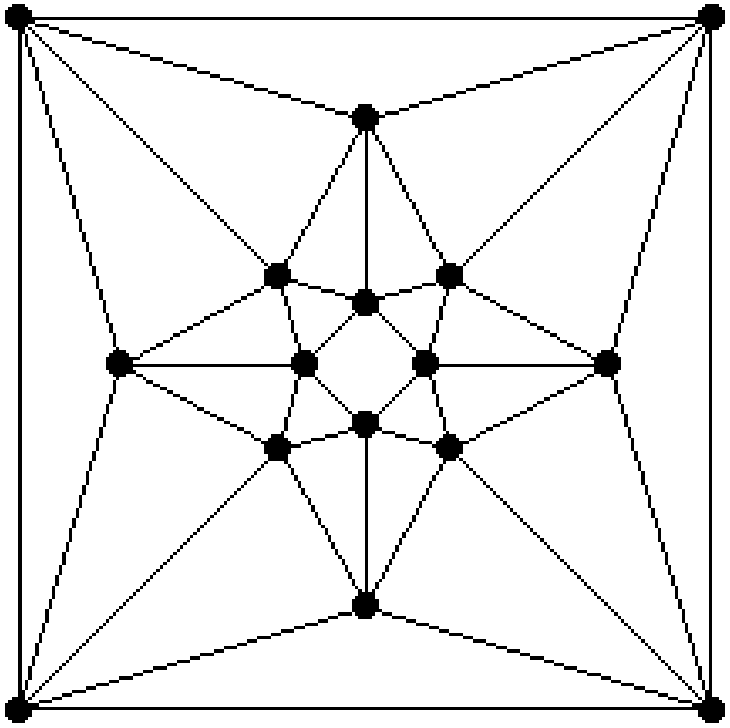
Apply **CN** to the following **polynomial** in the variables x_e over Z_3:

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

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 ?**



Thm (Pyber): **Any graph with n vertices and at least 100 n log n edges contains a 3-regular subgraph**

Proof is by showing that any such graph contains a subgraph with maximum degree 5 and average degree bigger than 4

Open: **given such a graph, can we find efficiently a 3-regular subgraph in it ?**

V Graph Coloring

The choice number 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 Erdös, Rubin and Taylor (79).

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

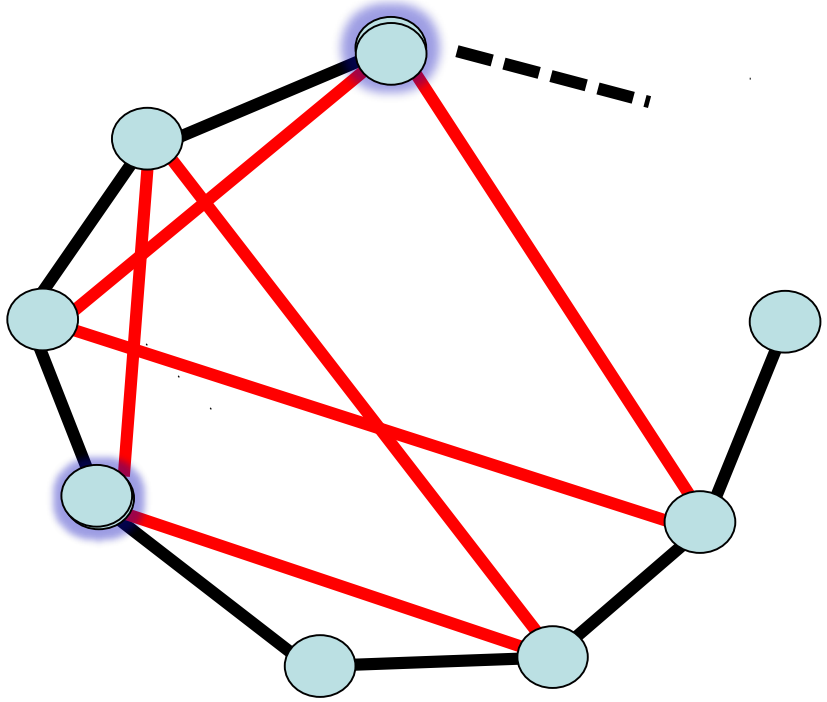
(Remark: This does not prove that NP=co-NP)

By CN2, if G has kn edges and the coefficient of $\prod x_i^k$ in f_G is nonzero, then ch(G) ≤ k+1

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

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.

To prove it they show that the relevant coefficient (expressed in terms of Eulerian orientations) is nonzero.

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 ?

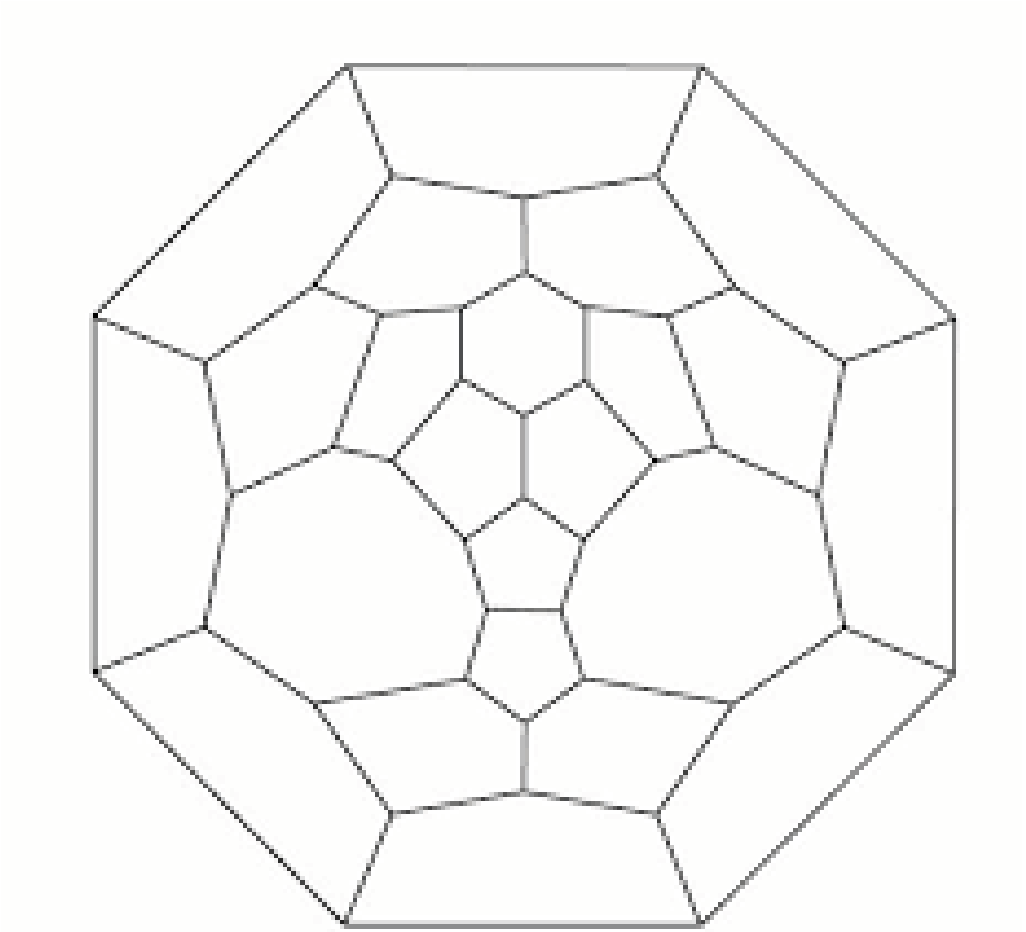
A similar reasoning provides a strengthening of the Four Color Theorem (4CT).

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 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 ?



VI 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 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, 3-regular subgraphs, cycle+triangles, choice 4CT) and similar additional ones may be simpler.

Are they ?