Algebraic Combinatorics and the Parity Argument

PPA membership of Combinatorial Nullstellensatz and related problems

László Varga

ESRC Workshop on Algorithmic Game Theory, London
17-18 October 2013

Institute of Mathematics, Eötvös Loránd University, Budapest
LVarga@cs.elte.hu

Contents

Alon's Combinatorial Nullstellensatz

In 1999, Alon presented a general algebraic technique and its numerous applications in Combinatorial Number Theory, in Graph Theory and in Combinatorics.

Alon's Combinatorial Nullstellensatz

In 1999, Alon presented a general algebraic technique and its numerous applications in Combinatorial Number Theory, in Graph Theory and in Combinatorics.

Theorem (Combinatorial Nullstellensatz, Alon)

Let $\mathbb{F}$ be an arbitrary field, and let $f \in \mathbb{F}[x_1, \ldots x_m]$ be an m-variable polynomial. Suppose that the degree of f is $\sum_{j=1}^{n} t_j$, where each t_j is a nonnegative integer, and that the coefficient of $\prod_{j=1}^{m} x_j^{t_j}$ is nonzero. Then, if $S_1, S_2, \ldots, S_m$ are subsets of $\mathbb{F}$ with $|S_j| > t_j$ for all $j = 1, \ldots, m$, then there exists an $(s_1, s_2, \ldots, s_m) \in S_1 \times S_2 \times \cdots \times S_m$ such that $f(s_1, s_2, \ldots, s_m) \neq 0$.

Alon's Combinatorial Nullstellensatz

In 1999, Alon presented a general algebraic technique and its numerous applications in Combinatorial Number Theory, in Graph Theory and in Combinatorics.

Theorem (Combinatorial Nullstellensatz, Alon)

Let $\mathbb{F}$ be an arbitrary field, and let $f \in \mathbb{F}[x_1, \dots x_m]$ be an m-variable polynomial. Suppose that the degree of f is $\sum_{j=1}^{n} t_j$, where each t_j is a nonnegative integer, and that the coefficient of $\prod_{j=1}^{m} x_j^{t_j}$ is nonzero. Then, if $S_1, S_2, \dots, S_m$ are subsets of $\mathbb{F}$ with $|S_j| > t_j$ for all $j = 1, \dots, m$, then there exists an $(s_1, s_2, \dots, s_m) \in S_1 \times S_2 \times \cdots \times S_m$ such that $f(s_1, s_2, \dots, s_m) \neq 0$.

Alon's Combinatorial Nullstellensatz

In 1999, Alon presented a general algebraic technique and its numerous applications in Combinatorial Number Theory, in Graph Theory and in Combinatorics.

Theorem (Combinatorial Nullstellensatz, Alon)

Let $\mathbb{F}$ be an arbitrary field, and let $f \in \mathbb{F}[x_1, \dots x_m]$ be an m-variable polynomial. Suppose that the degree of f is $\sum_{j=1}^{n} t_j$, where each t_j is a nonnegative integer, and that the coefficient of $\prod_{j=1}^{m} x_j^{t_j}$ is nonzero. Then, if $S_1, S_2, \dots, S_m$ are subsets of $\mathbb{F}$ with $|S_j| > t_j$ for all $j = 1, \dots, m$, then there exists an $(s_1, s_2, \dots, s_m) \in S_1 \times S_2 \times \dots \times S_m$ such that $f(s_1, s_2, \dots, s_m) \neq 0$.

The proofs of its applications are algebraic, and hence non-constructive in the sense that they supply no efficient algorithm for solving the corresponding algorithmic problems.

Combinatorial Nullstellensatz MOD 2

Theorem (Combinatorial Nullstellensatz MOD 2)

Let $f \in \mathbb{F}_2[x_1, \ldots x_m]$ be an m-variable polynomial. Suppose that the degree of f is m and that the coefficient of $x_1 x_2 \ldots x_m$ is nonzero. Then, there exists an $(s_1, s_2, \ldots, s_m) \in \{0, 1\}^m$ such that $f(s_1, s_2, \ldots, s_m) \neq 0$.

Combinatorial Nullstellensatz MOD 2

Theorem (Combinatorial Nullstellensatz MOD 2)

Let $f \in \mathbb{F}_2[x_1, \ldots x_m]$ be an m-variable polynomial. Suppose that the degree of f is m and that the coefficient of $x_1 x_2 \ldots x_m$ is nonzero. Then, there exists an $(s_1, s_2, \ldots, s_m) \in \{0,1\}^m$ such that $f(s_1, s_2, \ldots, s_m) \neq 0$.

Combinatorial Nullstellensatz MOD 2

Theorem (Combinatorial Nullstellensatz MOD 2)

Let $f \in \mathbb{F}_2[x_1, \dots x_m]$ be an m-variable polynomial. Suppose that the degree of f is m and that the coefficient of $x_1 x_2 \dots x_m$ is nonzero. Then, there exists an $(s_1, s_2, \dots, s_m) \in \{0,1\}^m$ such that $f(s_1, s_2, \dots, s_m) \neq 0$.

For example, if $f(x_1, x_2, x_3) = x_1x_2x_3 + x_1x_2 + x_2x_3$,

Combinatorial Nullstellensatz MOD 2

Theorem (Combinatorial Nullstellensatz MOD 2)

Let $f \in \mathbb{F}_2[x_1, \ldots x_m]$ be an m-variable polynomial. Suppose that the degree of f is m and that the coefficient of $x_1 x_2 \ldots x_m$ is nonzero. Then, there exists an $(s_1, s_2, \ldots, s_m) \in \{0,1\}^m$ such that $f(s_1, s_2, \ldots, s_m) \neq 0$.

For example, if $f(x_1, x_2, x_3) = x_1 x_2 x_3 + x_1 x_2 + x_2 x_3$, $f(1,1,1) = 1$.

p-divisible subgraphs

A nonempty subset of edges is called *p-divisible subgraph* such that the number of edges incident to every vertex is divisible by p.

What does it mean in the case $p = 2$?

p-divisible subgraphs

A nonempty subset of edges is called *p-divisible subgraph* such that the number of edges incident to every vertex is divisible by p.

What does it mean in the case $p = 2$? a cycle,

p-divisible subgraphs

A nonempty subset of edges is called *p-divisible subgraph* such that the number of edges incident to every vertex is divisible by p.

What does it mean in the case $p = 2$? a cycle, an Eulerian subgraph.

p-divisible subgraphs

A nonempty subset of edges is called *p-divisible subgraph* such that the number of edges incident to every vertex is divisible by p.

What does it mean in the case $p = 2$? a cycle, an Eulerian subgraph.

Theorem (Alon)

For any prime p and any graph G on n vertices and m edges, if $m > n \cdot (p-1)$, *there exists a p-divisible subgraph.*

p-divisible subgraphs

A nonempty subset of edges is called *p-divisible subgraph* such that the number of edges incident to every vertex is divisible by p.

What does it mean in the case $p = 2$? a cycle, an Eulerian subgraph.

Theorem (Alon)

For any prime p and any graph G on n vertices and m edges, if $m > n \cdot (p-1)$, there exists a p-divisible subgraph.

p-divisible subgraphs

A nonempty subset of edges is called *p-divisible subgraph* such that the number of edges incident to every vertex is divisible by p.

What does it mean in the case $p = 2$? a cycle, an Eulerian subgraph.

Theorem (Alon)

For any prime p and any graph G on n vertices and m edges, if $m > n \cdot (p - 1)$, *there exists a p-divisible subgraph.*

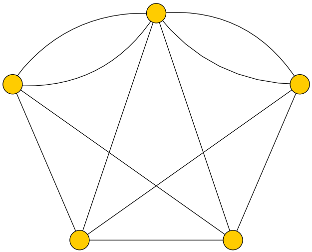
If $m > n$, of course, there exists a 2-divisible subgraph, e.g. a cycle.

p-divisible subgraphs

A nonempty subset of edges is called *p-divisible subgraph* such that the number of edges incident to every vertex is divisible by p.

Theorem (Alon)

For any prime p and any graph G on n vertices and m edges, if $m > n \cdot (p-1)$, there exists a p-divisible subgraph.

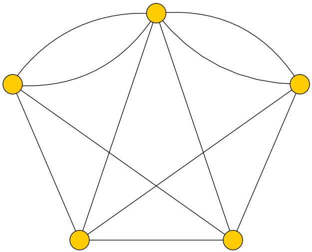


p-divisible subgraphs

A nonempty subset of edges is called *p-divisible subgraph* such that the number of edges incident to every vertex is divisible by p.

Theorem (Alon)

For any prime p and any graph G on n vertices and m edges, if $m > n \cdot (p-1)$, there exists a p-divisible subgraph.

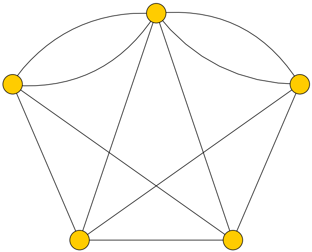


p-divisible subgraphs

A nonempty subset of edges is called *p-divisible subgraph* such that the number of edges incident to every vertex is divisible by p.

Theorem (Alon)

For any prime p and any graph G on n vertices and m edges, if $m > n \cdot (p-1)$, there exists a p-divisible subgraph.



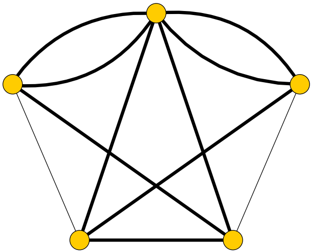
$n = 5$ vertices, $11 > 5 \cdot (3-1)$ edges $\Longrightarrow$ there exists a 3-divisible subgraph.

p-divisible subgraphs

A nonempty subset of edges is called *p-divisible subgraph* such that the number of edges incident to every vertex is divisible by p.

Theorem (Alon)

For any prime p and any graph G on n vertices and m edges, if $m > n \cdot (p-1)$, there exists a p-divisible subgraph.



$n = 5$ vertices, $11 > 5 \cdot (3-1)$ edges $\Longrightarrow$ there exists a 3-divisible subgraph.

Useful corollary of Combinatorial Nullstellensatz

Let p be an arbitrary prime. Let us be given some m-variable polynomials $f_1, f_2, \ldots, f_n$ over $\mathbb{F}_p$ with no constant terms. If

$$m > (p-1) \cdot \sum_{i=1}^{n} \deg(f_i),$$

then there exists a vector $\mathbf{0} \neq \mathbf{x} \in \{0,1\}^m$ such that $f_i(\mathbf{x}) = 0$ for all i.

$f_A(\mathbf{x}) = x_1 + x_2 + x_3 + x_4$

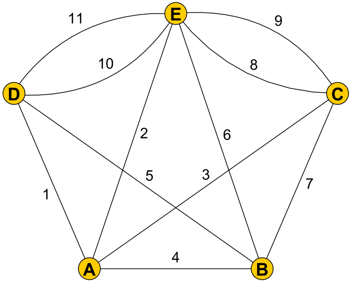
$f_B(\mathbf{x}) = x_4 + x_5 + x_6 + x_7$

$f_C(\mathbf{x}) = x_7 + x_3 + x_8 + x_9$

$f_D(\mathbf{x}) = x_1 + x_5 + x_{10} + x_{11}$

$f_E(\mathbf{x}) = x_{11} + x_{10} + x_2 + x_6 + x_8 + x_9$

$11 = m > 5 \cdot (3-1) \Rightarrow$
exists a vector $\mathbf{0} \neq \mathbf{x} : \ f_i(\mathbf{x}) = 0$.



Useful corollary of Combinatorial Nullstellensatz

Let p be an arbitrary prime. Let us be given some m-variable polynomials $f_1, f_2, \dots, f_n$ over $\mathbb{F}_p$ with no constant terms. If

$$m > (p-1) \cdot \sum_{i=1}^{n} \deg(f_i),$$

then there exists a vector $\mathbf{0} \neq \mathbf{x} \in \{0,1\}^m$ such that $f_i(\mathbf{x}) = 0$ for all i.

$f_A(\mathbf{x}) = x_1 + x_2 + x_3 + x_4$

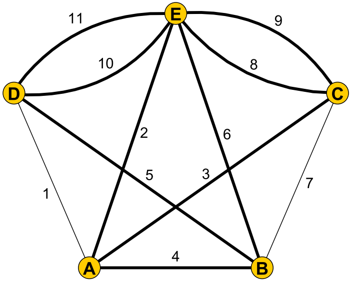
$f_B(\mathbf{x}) = x_4 + x_5 + x_6 + x_7$

$f_C(\mathbf{x}) = x_7 + x_3 + x_8 + x_9$

$f_D(\mathbf{x}) = x_1 + x_5 + x_{10} + x_{11}$

$f_E(\mathbf{x}) = x_{11} + x_{10} + x_2 + x_6 + x_8 + x_9$

$11 = m > 5 \cdot (3-1) \Rightarrow$
exists a vector $\mathbf{0} \neq \mathbf{x} : \ f_i(\mathbf{x}) = 0$.



p^d-divisible subgraphs

In a previous paper, Alon, Friedland and Kalai answered the analogous question modulo prime powers with no use of Combinatorial Nullstellensatz.

Theorem (Alon, Friedland and Kalai)

For any prime p and any graph G on n vertices and m edges, if $m > n \cdot (p^d - 1)$, there exist a p^d-divisible subgraph.

p^d-divisible subgraphs

In a previous paper, Alon, Friedland and Kalai answered the analogous question modulo prime powers with no use of Combinatorial Nullstellensatz.

Theorem (Alon, Friedland and Kalai)

For any prime p and any graph G on n vertices and m edges, if $m > n \cdot (p^d - 1)$, there exist a p^d-divisible subgraph.

p^d-divisble subgraphs

In a previous paper, Alon, Friedland and Kalai answered the analogous question modulo prime powers with no use of Combinatorial Nullstellensatz.

Theorem (Alon, Friedland and Kalai)

For any prime p and any graph G on n vertices and m edges, if $m > n \cdot (p^d - 1)$, there exist a p^d-divisible subgraph.

The analogous theorem about k-divisible subgraphs is not known, if k is not a prime power, but one can prove that if the graph has sufficiently large number of edges, there exists a k-divisible subgraph.

Our main results

New proofs via Combinatorial Nullstellensatz

We give a reduction of p^d-divisible subgraphs to Combinatorial Nullstellensatz.

Our main results

New proofs via Combinatorial Nullstellensatz

We give a reduction of p^d-divisible subgraphs to Combinatorial Nullstellensatz.

Theorem

Suppose that $f_1, f_2, \ldots, f_n$ are m-variable polynomials over $\mathbb{Z}$ without constant terms. Then, if

$$m > (p^d - 1) \cdot \sum_{i=1}^{n} \deg(f_i)$$

there exists a $\mathbf{0} \neq \mathbf{x} \in \{0,1\}^m$ such that $p^d | f_i(\mathbf{x})$ for all i.

Our main results

New proofs via Combinatorial Nullstellensatz

We give a reduction of p^d-divisible subgraphs to Combinatorial Nullstellensatz.

Theorem

Suppose that $f_1, f_2, \dots, f_n$ are m-variable polynomials over $\mathbb{Z}$ without constant terms. Then, if

$$m > (p^d - 1) \cdot \sum_{i=1}^{n} \deg(f_i)$$

there exists a $\mathbf{0} \neq \mathbf{x} \in \{0,1\}^m$ such that $p^d | f_i(\mathbf{x})$ for all i.

Theorem

Finding a 2^d-divisible subgraph and Combinatorial Nullstellensatz MOD 2 belong to PPA.

Conditions modulo p^d and conditions modulo p

p^d-divisible subgraphs – conditions modulo p^d.

Conditions modulo p^d and conditions modulo p

p^d-divisible subgraphs – conditions modulo p^d.

Combinatorial Nullstellensatz – conditions over a field, e.g. modulo p.

Conditions modulo p^d and conditions modulo p

p^d-divisible subgraphs – conditions modulo p^d.

Combinatorial Nullstellensatz – conditions over a field, e.g. modulo p.

How could you reduce conditions modulo p^d to conditions modulo p?

Conditions modulo p^d and conditions modulo p

p^d-divisible subgraphs – conditions modulo p^d.

Combinatorial Nullstellensatz – conditions over a field, e.g. modulo p.

How could you reduce conditions modulo p^d to conditions modulo p?

$$\sum x_j \equiv q \pmod{p^d} \quad \Longleftrightarrow \quad ??? \pmod{p}$$

Conditions modulo p^d and conditions modulo p

p^d-divisible subgraphs – conditions modulo p^d.

Combinatorial Nullstellensatz – conditions over a field, e.g. modulo p.

How could you reduce conditions modulo p^d to conditions modulo p?

$$\sum x_j \equiv q \pmod{p^d} \iff ??? \pmod{p}$$

$$f(\mathbf{x}) \equiv q \pmod{p^d} \iff ??? \pmod{p}$$

Key observation through an example

In our paper, a new algebraic technique is presented to describe conditions modulo p^d as conditions modulo p.

Key observation through an example

In our paper, a new algebraic technique is presented to describe conditions modulo p^d as conditions modulo p.

Example

If $(x_1, x_2, x_3) \in \{0,1\}^3$, then

$$x_1 + x_2 + x_3 \equiv 1 \pmod 4$$

is equivalent to the system

$$x_1 + x_2 + x_3 \equiv 1 \pmod 2$$

$$x_1x_2 + x_1x_3 + x_2x_3 \equiv 0 \pmod 2$$

Key observation through an example

In our paper, a new algebraic technique is presented to describe conditions modulo p^d as conditions modulo p.

Example

If $(x_1, x_2, x_3) \in \{0,1\}^3$, then

$$x_1 + x_2 + x_3 \equiv 1 \pmod 4$$

is equivalent to the system

$$x_1 + x_2 + x_3 \equiv 1 \pmod 2$$

$$x_1x_2 + x_1x_3 + x_2x_3 \equiv 0 \pmod 2$$

Key observation through an example

In our paper, a new algebraic technique is presented to describe conditions modulo p^d as conditions modulo p.

Example

If $(x_1, x_2, x_3) \in \{0,1\}^3$, then

$$x_1 + x_2 + x_3 \equiv 1 \pmod 4$$

is equivalent to the system

$$x_1 + x_2 + x_3 \equiv 1 \pmod 2$$

$$x_1x_2 + x_1x_3 + x_2x_3 \equiv 0 \pmod 2$$

This example can be extended to any polynomial f and prime power p^d.

Combinatorial Nullstellensatz MOD 2

In the rest of this presentation, we focus on PPA and the complexity of Combinatorial Nullstellensatz MOD 2.

Theorem (Combinatorial Nullstellensatz MOD 2)

Let $f \in \mathbb{F}_2[x_1, \ldots x_m]$ be an m-variable polynomial. Suppose that the degree of f is m and that the coefficient of $x_1 x_2 \ldots x_m$ is nonzero. Then, there exists an $(s_1, s_2, \ldots, s_m) \in \{0, 1\}^m$ such that $f(s_1, s_2, \ldots, s_m) \neq 0$.

The complexity of finding such a vector whose existence is guaranteed by the Combinatorial Nullstellensatz depends on the input form of the given polynomial.

The complexity of finding such a vector whose existence is guaranteed by the Combinatorial Nullstellensatz depends on the input form of the given polynomial.

If the polynomial is given explicitly, as the sum of monomials, e.g. $f(x_1, x_2, x_3) = x_1x_2x_3 + x_1x_2 + x_2x_3$

- one can trivially construct a polynomial time algorithm

The complexity of finding such a vector whose existence is guaranteed by the Combinatorial Nullstellensatz depends on the input form of the given polynomial.

If the polynomial is given explicitly, as the sum of monomials, e.g. $f(x_1, x_2, x_3) = x_1x_2x_3 + x_1x_2 + x_2x_3$

- one can trivially construct a polynomial time algorithm

The complexity of finding such a vector whose existence is guaranteed by the Combinatorial Nullstellensatz depends on the input form of the given polynomial.

If the polynomial is given explicitly, as the sum of monomials, e.g. $f(x_1, x_2, x_3) = x_1x_2x_3 + x_1x_2 + x_2x_3$

- one can trivially construct a polynomial time algorithm

If the polynomial is given as the sum of products of polynomials, e.g. $f(x_1, x_2, x_3) = (x_1 + x_2 + x_3)^3 + x_1x_2x_3$

- such as in the most of the applications

The complexity of finding such a vector whose existence is guaranteed by the Combinatorial Nullstellensatz depends on the input form of the given polynomial.

If the polynomial is given explicitly, as the sum of monomials, e.g. $f(x_1, x_2, x_3) = x_1x_2x_3 + x_1x_2 + x_2x_3$

- one can trivially construct a polynomial time algorithm

If the polynomial is given as the sum of products of polynomials, e.g. $f(x_1, x_2, x_3) = (x_1 + x_2 + x_3)^3 + x_1x_2x_3$

- such as in the most of the applications
- not known to be solvable in polynomial time

The complexity of finding such a vector whose existence is guaranteed by the Combinatorial Nullstellensatz depends on the input form of the given polynomial.

If the polynomial is given explicitly, as the sum of monomials, e.g. $f(x_1, x_2, x_3) = x_1x_2x_3 + x_1x_2 + x_2x_3$

- one can trivially construct a polynomial time algorithm

If the polynomial is given as the sum of products of polynomials, e.g. $f(x_1, x_2, x_3) = (x_1 + x_2 + x_3)^3 + x_1x_2x_3$

- such as in the most of the applications
- not known to be solvable in polynomial time
- an open question by Douglas West conjectures that the problem is in PPA

The complexity of finding such a vector whose existence is guaranteed by the Combinatorial Nullstellensatz depends on the input form of the given polynomial.

If the polynomial is given explicitly, as the sum of monomials, e.g. $f(x_1, x_2, x_3) = x_1x_2x_3 + x_1x_2 + x_2x_3$

- one can trivially construct a polynomial time algorithm

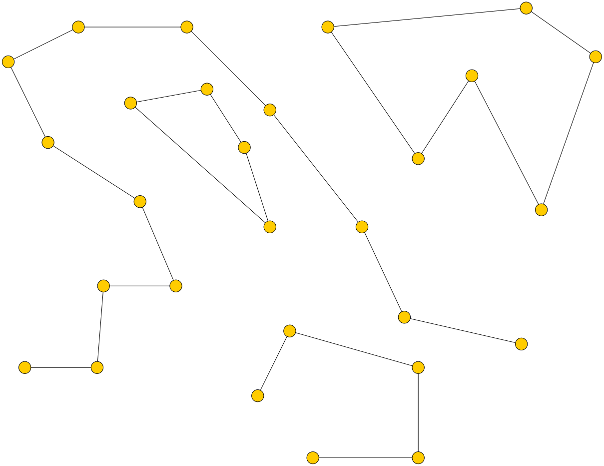
If the polynomial is given as the sum of products of polynomials, e.g. $f(x_1, x_2, x_3) = (x_1 + x_2 + x_3)^3 + x_1x_2x_3$

- such as in the most of the applications
- not known to be solvable in polynomial time
- an open question by Douglas West conjectures that the problem is in PPA
- we verify this conjecture

Reminder about Polynomial Parity Argument

In '94, Papadimitriou defined the complexity class Polynomial Parity Argument.

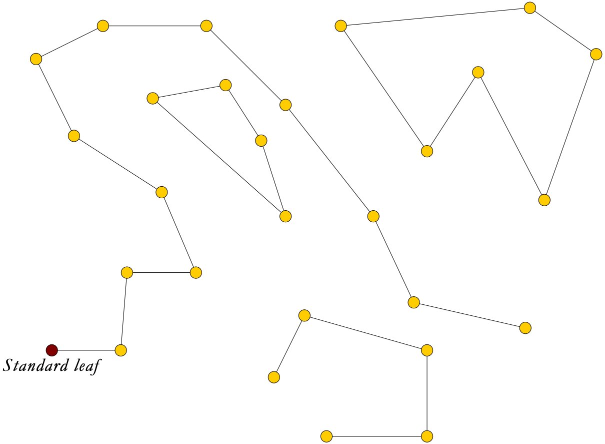
A problem is in PPA if and only if it is reducible to the End Of The Line.



Reminder about Polynomial Parity Argument

In '94, Papadimitriou defined the complexity class Polynomial Parity Argument.

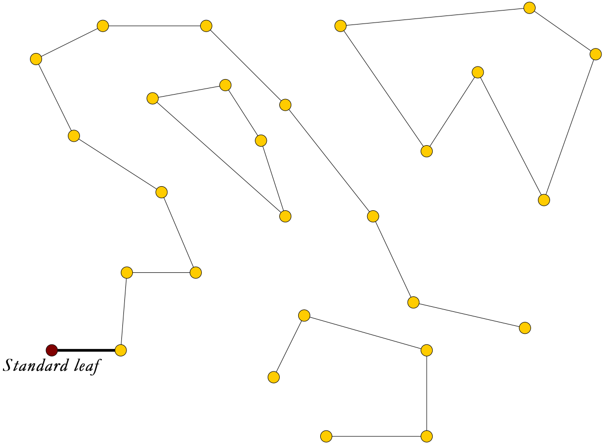
A problem is in PPA if and only if it is reducible to the End Of The Line.



Reminder about Polynomial Parity Argument

In '94, Papadimitriou defined the complexity class Polynomial Parity Argument.

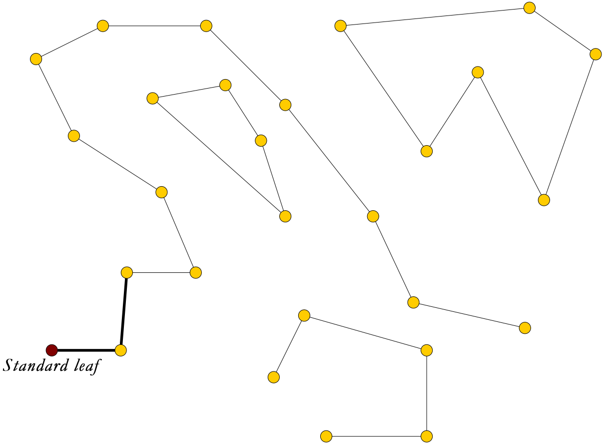
A problem is in PPA if and only if it is reducible to the End Of The Line.



Reminder about Polynomial Parity Argument

In '94, Papadimitriou defined the complexity class Polynomial Parity Argument.

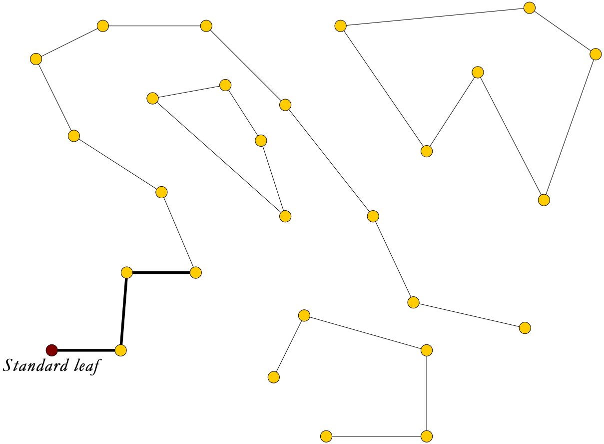
A problem is in PPA if and only if it is reducible to the End Of The Line.



Reminder about Polynomial Parity Argument

In '94, Papadimitriou defined the complexity class Polynomial Parity Argument.

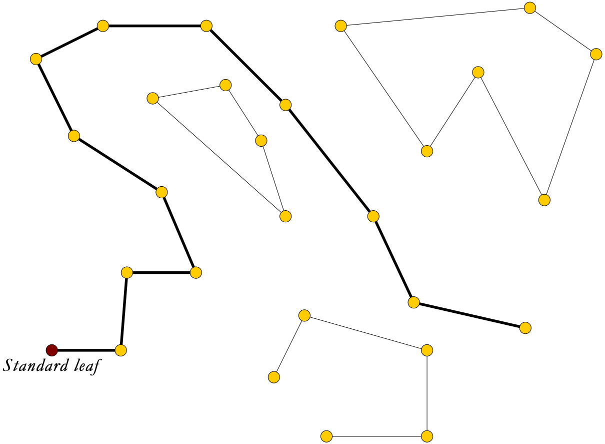
A problem is in PPA if and only if it is reducible to the End Of The Line.



Reminder about Polynomial Parity Argument

In '94, Papadimitriou defined the complexity class Polynomial Parity Argument.

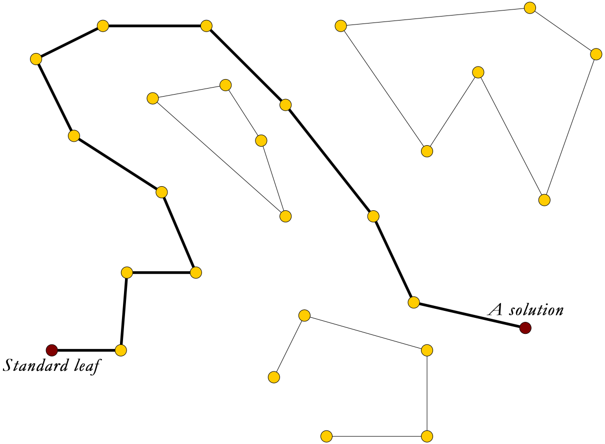
A problem is in PPA if and only if it is reducible to the End Of The Line.



Reminder about Polynomial Parity Argument

In '94, Papadimitriou defined the complexity class Polynomial Parity Argument.

A problem is in PPA if and only if it is reducible to the End Of The Line.



The pairing function

Papadimitriou shows that this problem is equivalent to the problem in which the nodes may have more (e.g. exponentially many) neighbours and a polynomial time pairing function is given.

The pairing function

Papadimitriou shows that this problem is equivalent to the problem in which the nodes may have more (e.g. exponentially many) neighbours and a polynomial time pairing function is given.

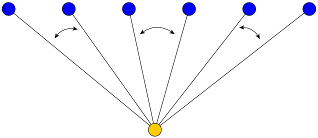
Pairing function ϕ for an input node v pairs up its neighbours.

The pairing function

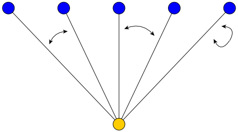
Papadimitriou shows that this problem is equivalent to the problem in which the nodes may have more (e.g. exponentially many) neighbours and a polynomial time pairing function is given.

Pairing function ϕ for an input node v pairs up its neighbours.

For an even-degree node:



For an odd-degree node:



PPA membership of Chévalley's theorem

Theorem (Chévalley)

Let $p_1, p_2, \ldots, p_n$ be polynomials in m variables over $\{0, 1\}$. Suppose that $\sum_{i=1}^{n} \deg(p_i) < m$. Then, the number of common solutions of the polynomial equation system $p_i(x_1, \ldots, x_m) = 0$ $(i = 1 \ldots n)$ is even. In particular, if there is a solution, there exists another.

PPA membership of Chévalley's theorem

Theorem (Chévalley)

Let $p_1, p_2, \ldots, p_n$ be polynomials in m variables over $\{0,1\}$. Suppose that $\sum_{i=1}^n \deg(p_i) < m$. Then, the number of common solutions of the polynomial equation system $p_i(x_1, \ldots, x_m) = 0$ $(i = 1 \ldots n)$ is even. In particular, if there is a solution, there exists another.

Chévalley MOD 2

Input: polynomials $p_1, p_2, \ldots, p_n$ over $\{0,1\}$ such that $\sum_{i=1}^n \deg(p_i) < m$. Also, we are given a root $(c_1, c_2, \ldots, c_m) \in \{0,1\}^m$ of the equation system $p_i(\mathbf{x}) = 0$ $(i = 1, \ldots, n)$

Find: another root of the equation system $p_i(\mathbf{x}) = 0$ $(i = 1, \ldots, n)$.

PPA membership of Chévalley's theorem

Theorem (Chévalley)

Let $p_1, p_2, \ldots, p_n$ be polynomials in m variables over $\{0, 1\}$. Suppose that $\sum_{i=1}^n \deg(p_i) < m$. Then, the number of common solutions of the polynomial equation system $p_i(x_1, \ldots, x_m) = 0$ $(i = 1 \ldots n)$ is even. In particular, if there is a solution, there exists another.

Chévalley MOD 2

Input: polynomials $p_1, p_2, \ldots, p_n$ over $\{0, 1\}$ such that $\sum_{i=1}^n \deg(p_i) < m$. Also, we are given a root $(c_1, c_2, \ldots, c_m) \in \{0, 1\}^m$ of the equation system $p_i(\mathbf{x}) = 0$ $(i = 1, \ldots, n)$

Find: another root of the equation system $p_i(\mathbf{x}) = 0$ $(i = 1, \ldots, n)$.

PPA membership of Chévalley's theorem

Theorem (Chévalley)

Let $p_1, p_2, \ldots, p_n$ be polynomials in m variables over $\{0,1\}$. Suppose that $\sum_{i=1}^n \deg(p_i) < m$. Then, the number of common solutions of the polynomial equation system $p_i(x_1, \ldots, x_m) = 0$ $(i = 1 \ldots n)$ is even. In particular, if there is a solution, there exists another.

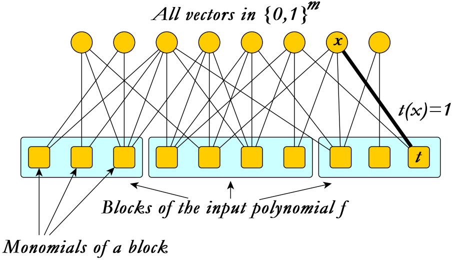
Chévalley MOD 2

Input: polynomials $p_1, p_2, \ldots, p_n$ over $\{0,1\}$ such that $\sum_{i=1}^n \deg(p_i) < m$. Also, we are given a root $(c_1, c_2, \ldots, c_m) \in \{0,1\}^m$ of the equation system $p_i(\mathbf{x}) = 0$ $(i = 1, \ldots, n)$

Find: another root of the equation system $p_i(\mathbf{x}) = 0$ $(i = 1, \ldots, n)$.

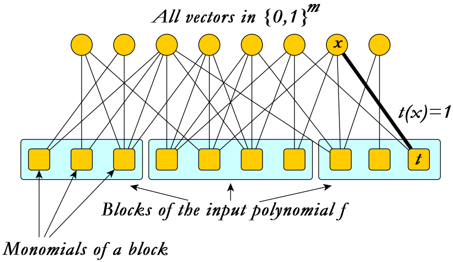
Papadimitriou showed that Chévalley MOD 2 belongs to PPA. Our following proof about Combinatorial Nullstellensatz is based on his proof but it requires trickier pairing function.

The construction of End Of The Line graph



The input polynomial: $f = \sum_{i=1}^{k} \left(\prod_{j=1}^{m_i} p_{ij} \right)$.

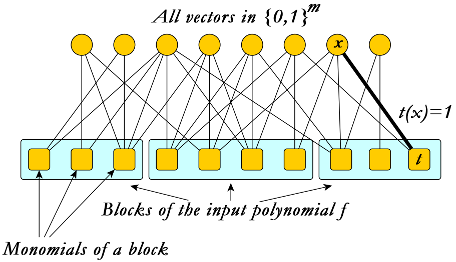
The construction of End Of The Line graph



The input polynomial: $f = \sum_{i=1}^{k} \left(\prod_{j=1}^{m_i} p_{ij} \right)$.

It has k blocks: $\prod_{j=1}^{m_1} p_{1j}, \prod_{j=1}^{m_2} p_{2j}, \ldots, \prod_{j=1}^{m_k} p_{kj}$.

The construction of End Of The Line graph



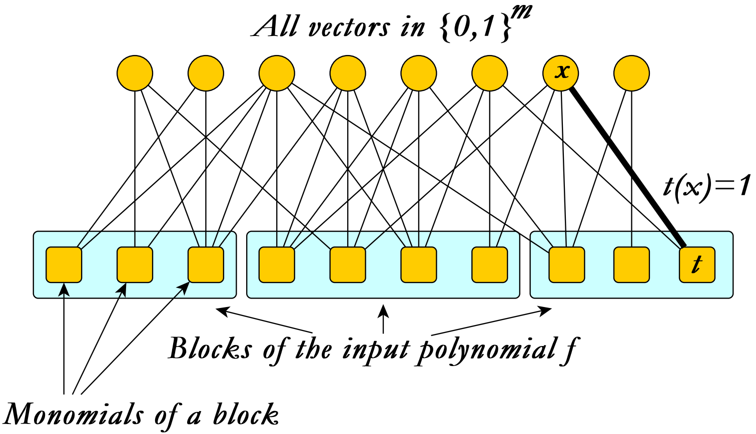
The input polynomial: $f = \sum_{i=1}^{k} \left(\prod_{j=1}^{m_i} p_{ij} \right)$.

It has k blocks: $\prod_{j=1}^{m_1} p_{1j}, \prod_{j=1}^{m_2} p_{2j}, \ldots, \prod_{j=1}^{m_k} p_{kj}$.

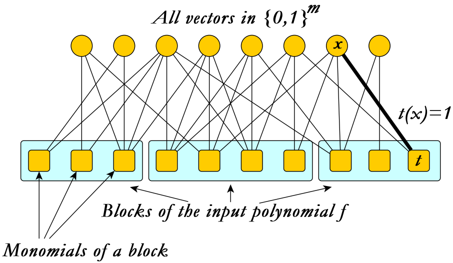
A monomial (term) in the ith block can be represented by an $(m_i + 1)$-tuple of integers: $(i, a_{i,1}, \ldots, a_{i,m_i})$. $a_{i,j}$ shows that the term is the product of $a_{i,j}$th monomials of p_{ij}.

E.g. in $(1 + x_1)(1 + x_2)$ $(i, 1, 1) \sim 1, (i, 1, 2) \sim x_2, (i, 2, 1) \sim x_1, (i, 2, 2) \sim x_1 x_2$.

The construction of End Of The Line graph



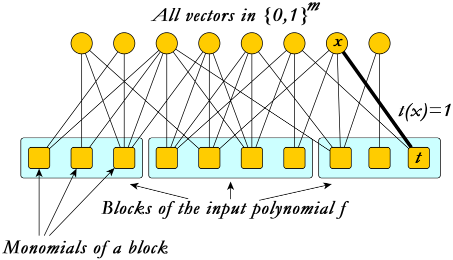
The construction of End Of The Line graph



Edges:

A vector x is connected to a term t if and only if the value of t is 1 at x.

The construction of End Of The Line graph



For a vector $(s_1, s_2, \ldots, s_m)$, $f(s_1, s_2, \ldots, s_m) \neq 0$ holds if and only if in the constructed graph its degree is odd.

The degree of a term $t(\mathbf{x}) \neq x_1 \ldots x_m$ is even because there exists a variable x_i not appearing in t. The degree of term term $x_1 \ldots x_m$ is odd because it is connected only to the vector $(1, 1, \ldots, 1)$.

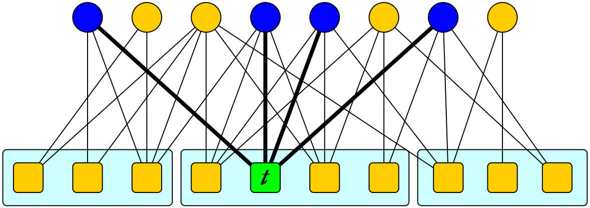
The standard leaf is the term $x_1 \ldots x_m$. Another leaf is a solution.

Pairing for a term t

However, the nodes of this graph have exponentially large degrees, and therefore we must exhibit a pairing function between the edges out of a node.

Pairing for a term t

However, the nodes of this graph have exponentially large degrees, and therefore we must exhibit a pairing function between the edges out of a node.

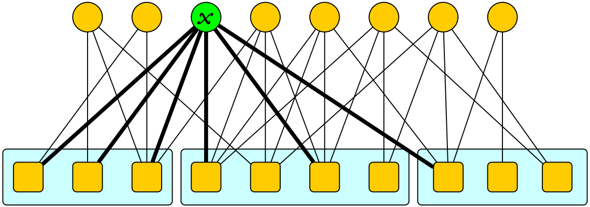


For a term t

For a node corresponding to the term $t(\mathbf{x}) \neq x_1 x_2 \ldots x_m$, we pair up the vector $\mathbf{x}$ via the variable x_l is such that does not appear in t.

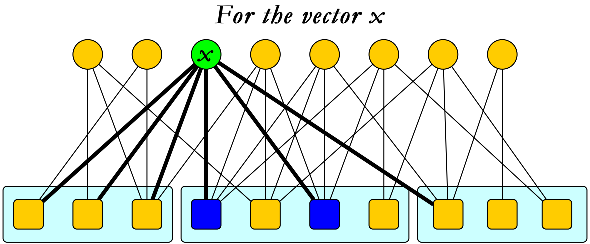
Pairing at a vector x

For the vector x

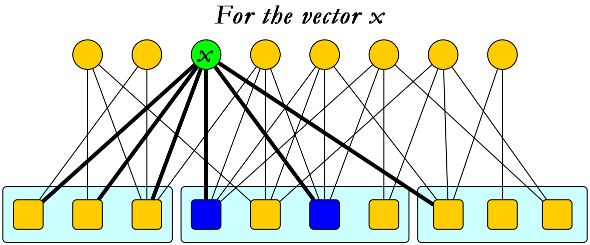


Suppose that $f(\mathbf{x}) = 0$. The case $f(\mathbf{x}) = 1$ can be checked similarly.

Pairing at a vector x



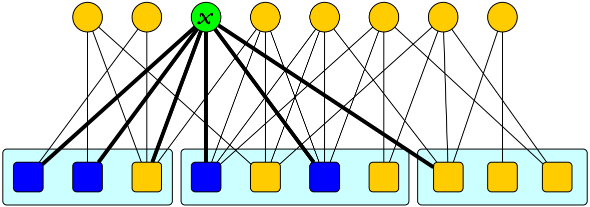
Pairing at a vector x



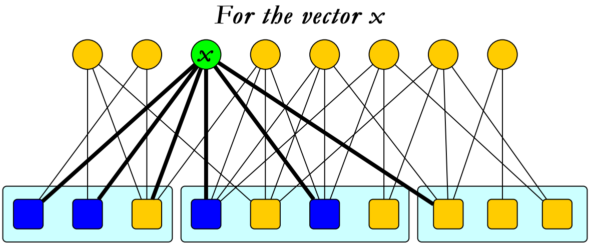
For a block $g = \prod_{j=1}^{m_i} p_{ij}$ such that $g(\mathbf{x}) = 0$, then there is an index j such that $p_{ij}(\mathbf{x}) = 0$. Pick the smallest such j. There is an even number of monomials of p_{ij} such that $p_{ij}(\mathbf{x}) = 1$. We pair these monomials by a pairing function ϕ_i. Then the mate of term $(i, a_{i1}, \ldots, a_{ij}, \ldots, a_{i,m_i})$ is $(i, a_{i1}, \ldots, \phi_i(a_{ij}), \ldots, a_{i,m_i})$.

Pairing at a vector x

For the vector x

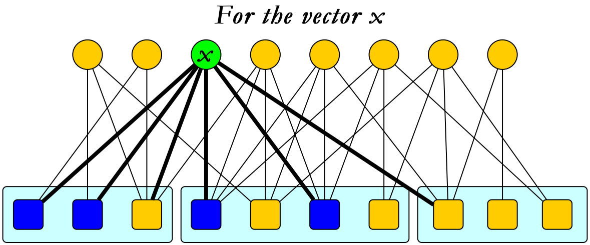


Pairing at a vector x



For a block $g = \prod_{j=1}^{m_i} p_{ij}$ such that $g(\mathbf{x}) = 1$, then for all index j, that $p_{ij}(\mathbf{x}) = 1$ holds. We can pair all but one monomials of p_{ij} with $p_{ij}(\mathbf{x}) = 1$ by a pairing function ϕ_{ij}. One of them does not have a mate, denote its index by ω_{ij}.

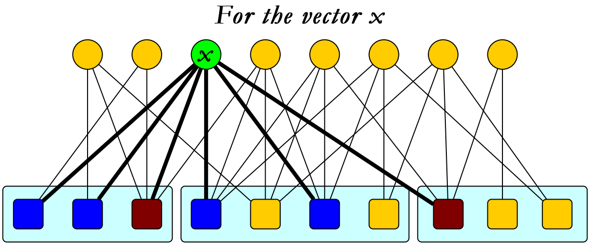
Pairing at a vector x



For a block $g = \prod_{j=1}^{m_i} p_{ij}$ such that $g(\mathbf{x}) = 1$, then for all index j, that $p_{ij}(\mathbf{x}) = 1$ holds. We can pair all but one monomials of p_{ij} with $p_{ij}(\mathbf{x}) = 1$ by a pairing function ϕ_{ij}. One of them does not have a mate, denote its index by ω_{ij}.

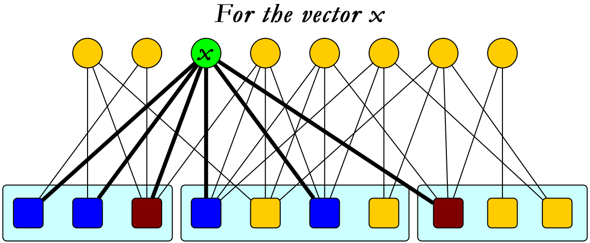
If there exists an index j such that $a_{ij} \neq \omega_{ij}$, pick the smallest such j. Then the mate of $(i, a_{i1}, \ldots, a_{i,m_i})$ is $(i, a_{i1}, \ldots, \phi_{ij}(a_{ij}), \ldots, a_{i,m_i})$.

Pairing at a vector x



What about the term t if it is represented by $(i, \omega_{i1}, \ldots, \omega_{i,m_i})$?

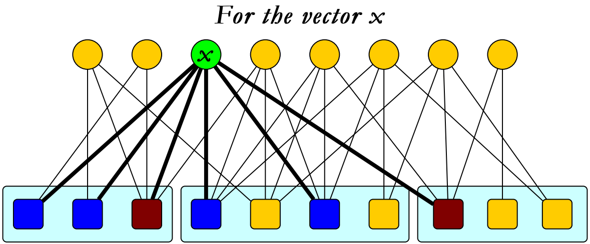
Pairing at a vector x



What about the term t if it is represented by $(i, \omega_{i1}, \ldots, \omega_{i,m_i})$?

Since $f(\mathbf{x}) = 0$, there is an even number of blocks that are 1 at $\mathbf{x}$. We pair these blocks by a pairing function ϕ.

Pairing at a vector x

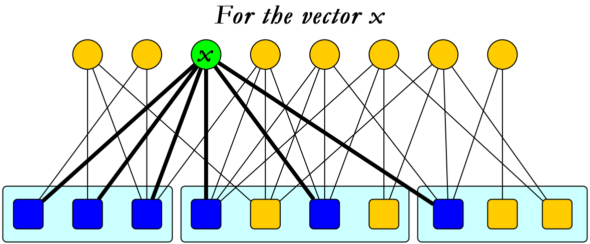


What about the term t if it is represented by $(i, \omega_{i1}, \ldots, \omega_{i,m_i})$?

Since $f(\mathbf{x}) = 0$, there is an even number of blocks that are 1 at $\mathbf{x}$. We pair these blocks by a pairing function ϕ.

Then, the mate of $(i, \omega_{i1}, \ldots, \omega_{i,m_i})$ is $(\phi(i), \omega_{\phi(i),1}, \ldots, \omega_{\phi(i),m_{\phi(i)}})$.

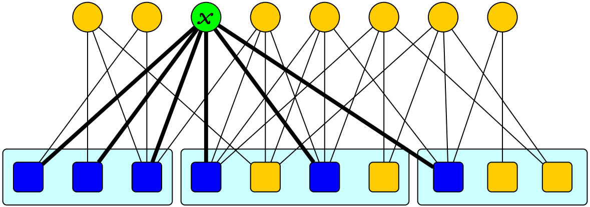
Pairing at a vector x



The key idea is this upper-level pairing function which pair up such blocks.

Pairing at a vector x

For the vector x



The key idea is this upper-level pairing function which pair up such blocks.

So, we presented a polynomial algorithm that computes the mate of an edge out of a node, and therefore we reduced Combinatorial Nullstellensatz MOD 2 to the End Of The Line, so the proof is complete.

2^d-divisible subgraph.

Input: a positive integer d and a graph $G = (V, E)$, where $|V| = n$, $|E| = m$ and $m > n \cdot (2^d - 1) - 2^{d-1}$.

Find: a 2^d-divisible subgraph, that is, an $\emptyset \neq F \subseteq E$ such that for every $v \in V$, the number of incident edges of F is divisible by 2^d.

2^d-divisible subgraph.

Input: a positive integer d and a graph $G = (V, E)$, where $|V| = n$, $|E| = m$ and $m > n \cdot (2^d - 1) - 2^{d-1}$.

Find: a 2^d-divisible subgraph, that is, an $\emptyset \neq F \subseteq E$ such that for every $v \in V$, the number of incident edges of F is divisible by 2^d.

Theorem

Finding a 2^d-divisible subgraph is polynomially reducible to Combinatorial Nullstellensatz, hence it belongs to PPA.

Thank you for your attention!

Thank you for your attention!

László Varga
Institute of Mathematics, Eötvös Loránd University, Budapest
LVarga@cs.elte.hu