On the PPA-completeness of the Combinatorial Nullstellensatz and the Chevalley-Warning Theorem

Miklos Santha

CNRS, Université Paris Diderot, France

joint work with

Alexander Belov	Gábor Ivanyos	Youming Qiao	Siyi Yang
U. of Latvia, Riga	SZTAKI, Budapest	U. Tech., Sydney	CQT, Singapore

Overview of the talk

1. The class PPA
2. CNSS and Chevalley-Warning Theorem
3. Arithmetic circuits and parse subcircuits
4. The problems PPA-Circuit Chevalley and PPA-Circuit CNSS
5. PPA-hardness and PPA-easiness

The class PPA

Functional NP (FNP)

NP-search problems are defined by binary relations

$$R \subseteq \{0,1\}^* \times \{0,1\}^* \text{ such that}$$

– $R \in P$,
– for some polynomial $p(n)$, $R(x,y) \implies |y| \le p(|x|)$.

SEARCH PROBLEM Π_R
Input: x
Output: A solution y such that $R(x,y)$ if there is any, or "failure"

Π_R is reducible to Π_S if there exist polynomial time computable functions f and g such that, for every positive x,

$$S(f(x),y) \implies R(x,g(x,y)).$$

Total Functional NP (TFNP) [MP'91]

An NP-search problem is total if for all x there exists a solution y.

Facts:

- If $\mathrm{FNP} \subseteq \mathrm{TFNP}$ then $\mathrm{NP} = \mathrm{coNP}$.
- If $\mathrm{TFNP} \subseteq \mathrm{P}$ then $\mathrm{P} = \mathrm{NP} \cap \mathrm{coNP}$.

TFNP is a semantic complexity class

Syntactical subclasses of TFNP:

- Polynomial Local Search PLS
  Examples: Local optima, pure equilibrium in potential games
- Polynomial Pigeonhole Principle PPP
  Examples: Pigeonhole SubsetSum, Discrete Logarithm
- Polynomial Parity Argument classes $\mathrm{PPA}, \mathrm{PPAD}$.

Polynomial Parity Argument [P'94]

Parity Principle: In a graph the number of odd vertices is even.

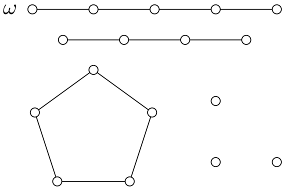
Definition: PPA is the set of total problems reducible to LEAF

LEAF

Input: (z, M, ω), where

- z is a binary string
- M is a polynomial TM that defines a graph $G_z = (V_z, E_z)$
- $V_z = \{0,1\}^{p(|z|)}$ for some polynomial p
- for $v \in V_z$, $M(z, v)$ is a set of at most two vertices
- $\{v, v'\} \in E_z$ if $v' \in M(z, v)$ and $v \in M(z, v')$
- $\omega \in V_z$ is a degree one vertex, the standard leaf

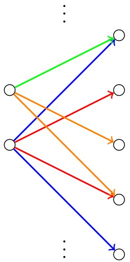
Output: A leaf different from ω.



PPA with edge recognition and pairing

Graphs $G_z = (V_z, E_z)$ of unbounded degree can be defined by two polynomial time algorithms ϵ and ϕ:

- Edge recognition: $\{v, v'\} \in E_z \Leftrightarrow \epsilon(v, v') = 1$
- Pairing: For every vertex v,
  - if $\deg(v)$ is even the function $\phi(v, \cdot)$ is a pairing between the vertices adjacent to v.
  - if $\deg(v)$ is odd then
    there exists exactly one neighbor w such that $\phi(v, w) = w$, and on the remaining neighbors $\phi(v, \cdot)$ is a pairing.



Fact: A problem defined in terms of ϵ and π is in PPA.

Proof: Let $G'_z = (V'_z, E'_z)$ be defined as

- $V'_z = E_z$
- $\{\{v, w\}, \{v, w'\}\} \in E'_z$
  if $\phi(w) = w'$.

Examples of problems in PPA

Few complete problems are known, mostly discretizations or combinatorial analogues of topological fixed point theorems:

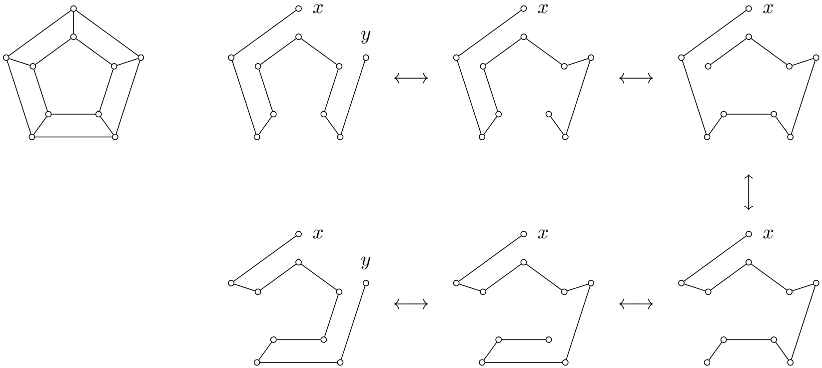
- 3-D Sperner in some non-orientable space [G'01]
- Locally 2-D Sperner [FISV'06]
- 2-D Tucker in the Euclidean space [ABB'15]
- Sperner and Tucker on the Möbius band [DEFLQX16]
- Octrahedral Tucker [DFK17]
- Consensus Halving [F-RG17]

Many problems of various origins are in PPA:

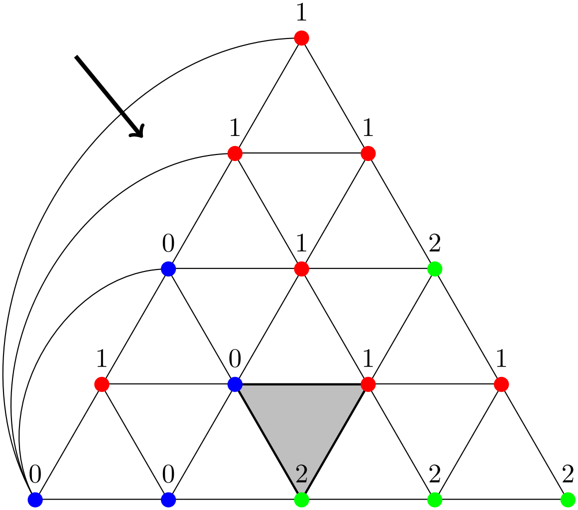
- Graph theory: Smith, Hamiltonian decomp. [P'94]
- Combinatorics: Necklace splitting and Discrete ham sandwich [P'94]
- Algebra: Explicit Chevalley [P'94]
- Number theory: Square root and Factoring [J'16]

Example: Smith

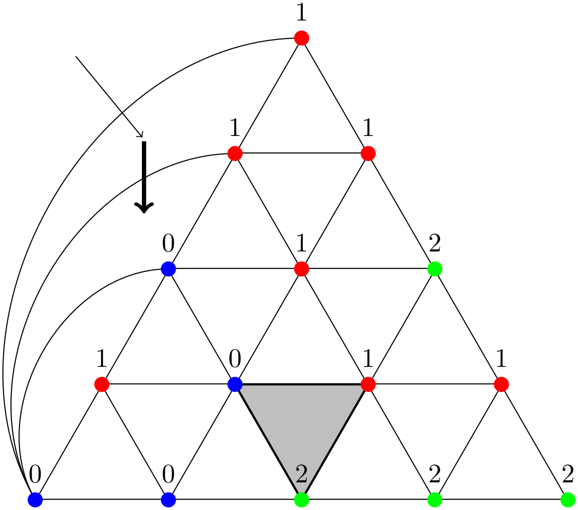
Theorem: In a cubic graph, for every edge, there is an even number of Hamiltonian cycles going trough the edge



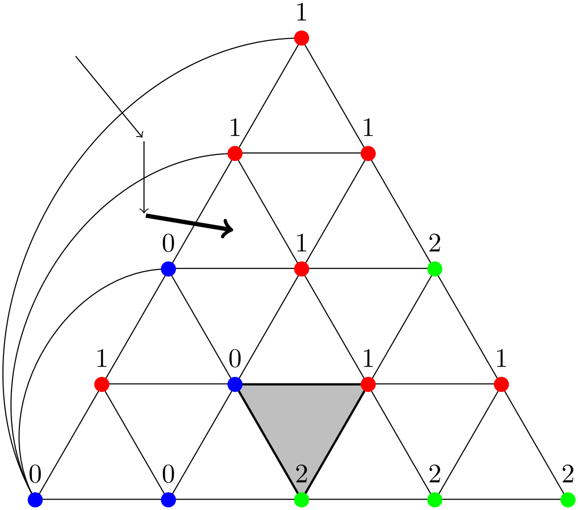
Example: SPERNER LEMMA



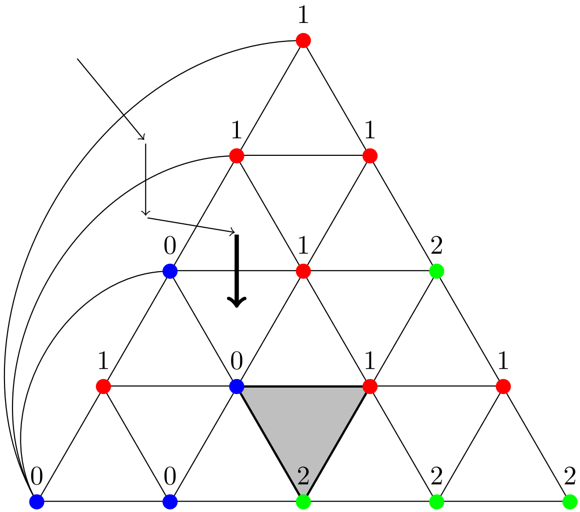
Example: Sperner Lemma



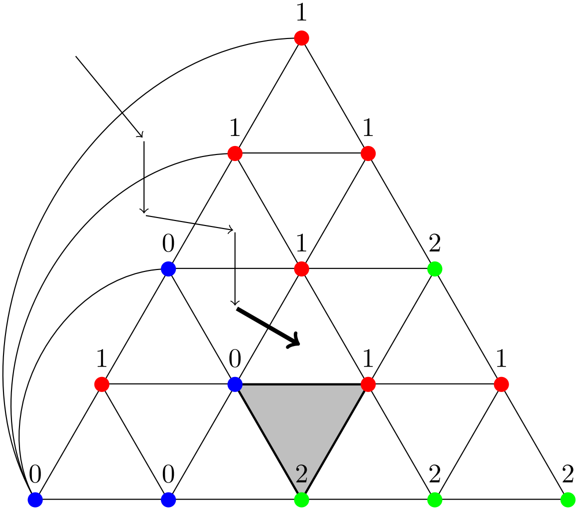
Example: Sperner Lemma



Example: Sperner Lemma



Example: Sperner Lemma



Combinatorial Nullstellensatz and Chevalley-Warning Theorem

Combinatorial Nullstellensatz

Theorem [Alon'99]: Let $\mathbb{F}$ be a field, let $d_1, \ldots, d_n$ be non-negative integers, and let $P \in \mathbb{F}[x_1, \ldots, x_n]$ be a polynomial. Suppose that

- $\deg(P) = \sum_{i=1}^{n} d_i$,
- the coefficient of $x_1^{d_1} \ldots x_n^{d_n}$ is non-zero.

Then for every subsets $S_1, \ldots, S_n$ of $\mathbb{F}$ with $|S_i| > d_i$, there exists $(s_1, \ldots s_n) \in S_1 \times \cdots \times S_n$ such that

$$P(s_1, \ldots, s_n) \neq 0.$$

Consequences in algebra, graph theory, combinatorics, additive number theory ...

Chevalley-Warning Theorem

Theorem [Chevalley'36, Warning'36]: Let $\mathbb{F}$ be a field of characteristic p, and let $P_1, \ldots, P_k \in \mathbb{F}[x_1, \ldots, x_n]$ be non-zero polynomials.

If $\sum_{i=1}^{k} \deg(P_i) < n$, then the number of common zeros of $P_1, \ldots, P_k$ is divisible by p.

In particular, if the polynomials have a common root, they also have another one.

The theorems over $\mathbb{F}_2$

Definition A multilinear polynomial over $\mathbb{F}_2$ is

$$M(x_1, \ldots, x_n) = \sum_{T \subseteq \{1,\ldots,n\}} c_T \prod_{i \in T} x_i, \quad \text{where} \quad c_T \in \mathbb{F}_2$$

Fact: For every P over $\mathbb{F}_2$, there exists a unique multilinear polynomial M_P such that P and M_P compute the same function.

Definition: The multilinear degree of P is $\mathrm{mdeg}(P) = \deg(M_P)$.

Theorem [Combinatorial Nullstellensatz over $\mathbb{F}_2$]: Let P be such that $\mathrm{mdeg}(P) = n$.
Then there exists $a \in \mathbb{F}_2^n$ such that $P(a) = 1$.

Theorem[Chevalley-Warning over $\mathbb{F}_2$]: Let P such that $\mathrm{mdeg}(P) < n$, and let $a \in \mathbb{F}_2^n$ such that $P(a) = 0$.
Then there exists $b \neq a$ such that $P(b) = 0$.

Theorem: $\mathrm{mdeg}(P) < n \iff$ the number of zeros is even

How to make them search problems?

Theorem[P'94]: The following problem is in PPA.

EXPLICIT CHEVALLEY

Input: Explicitly given polynomials $P_1, \ldots, P_k$ over $\mathbb{F}_2$ such that

$$\sum_{i=1}^{k} \deg(P_i) < n,$$

and a common root $a \in \mathbb{F}_2^n$.

Output: Another common root $a' \neq a$.

Remark: a is common root $\Leftrightarrow P(a) = 0$ where

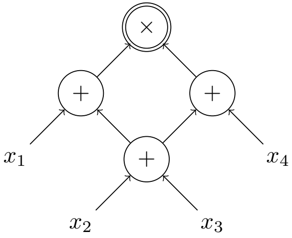
$$P = 1 + \prod_{i=1}^{k} (P_i + 1)$$

Could this be PPA-hard? Probably not. Two restrictions:

- P is given by an arithmetic circuit of specific form
- even the degree of P is less than n

Arithmetic circuits and parse subcircuits

Arithmetic circuits



C is a labeled, directed, acyclic graph.

Labels $= \{+, \times\}$,

$G^+ =$ sum gates, $G^\times =$ product gates.

Computational gates have indegree 2: left and right child

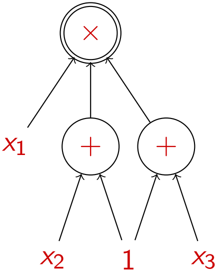
Polynomial computed by C

$$C(x) = (x_1 + x_2 + x_3) \times (x_2 + x_3 + x_4)$$
$$= x_1x_2 + x_1x_3 + x_1x_4 + x_2^2 + x_2x_4 + x_3^2 + x_3x_4$$

Lagrange-circuits

Circuits computing the Lagrange basis polynomials $L_a(x)$

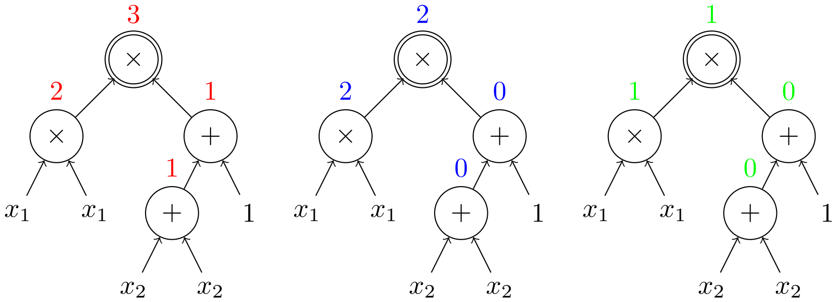
$$L_a(x) = 1 \iff x = a$$



Lagrange-circuit L_{100}

Degrees in a circuit

There are 3 types of degree



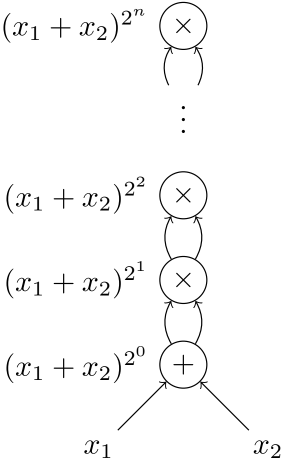
Formal degree = 3 Polynomial degree = 2 Multilinear degree =1

$2 = 0$ $x^2 = x$

easy to compute ??

We are interested in the multilinear degree

Multilinear degree and monomials



How can we certify $\mathrm{mdeg}(C(x)) = n$?

What is the the complexity of $\textsc{Mdeg} = \{C : \mathrm{mdeg}(C(x)) = n\}$?

We wish $\textsc{Mdeg} \in \mathrm{NP}$

A monomial m computed by C is maximal if $\mathrm{mdeg}(m) = n$

Fact: $\mathrm{mdeg}(C(x)) = n \iff$ odd number of maximal monomials

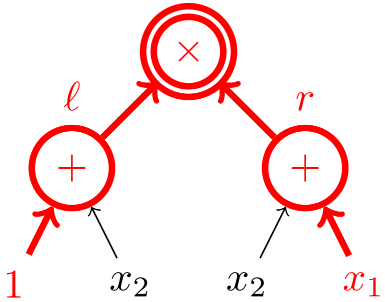
Difficulty: the number of monomials computed by C can be doubly exponential in the size of C

We can certainly say that $\textsc{Mdeg} \in \oplus\mathrm{EXP}$

Monomials in arithmetic formulae

Let F be an arithmetic formula

Monomials are computed by parse subtrees defined by the marking of appropriate sum gates: $S : G^{+} \to \{\ell, r, *\}$:



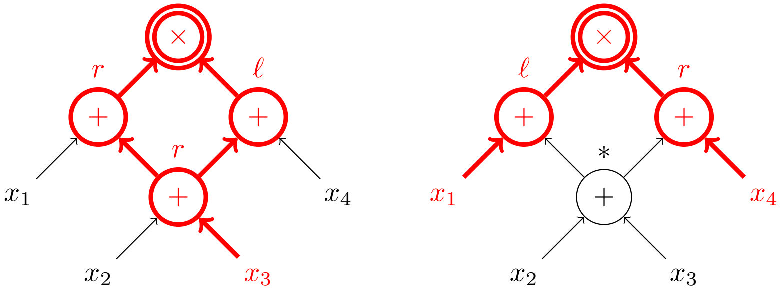
Parse subcircuits

C arithmetic circuit. A parse subcircuit is a partial marking

$$S : G^+ \to \{\ell, r, *\}$$

such that

marked vertices = accessible vertices



computes x_3^2 computes $x_1 x_4$

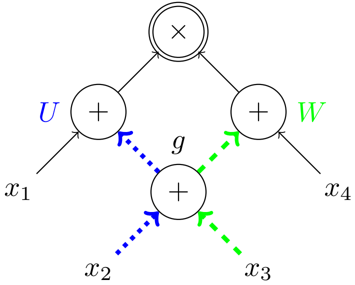
Parse subcircuits witness monomials

$\mathcal{S}(C) =$ set of parse subcircuits of C,

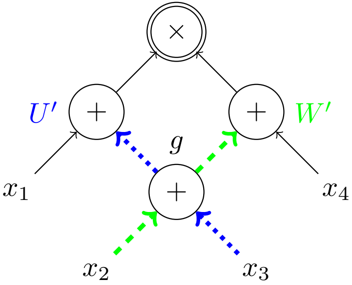
$m_S(x) =$ monomial computed by parse sub circuit S

Theorem: Let $\mathbb{F}$ be a field of characteristic 2. Then

$$C(x) = \sum_{S \in \mathcal{S}(C)} m_S(x).$$



$m_U m_W = x_2 x_3$



$m_{U'} m_{W'} = x_2 x_3$

Corollary: $\textsc{MDeg} \in \oplus\mathrm{P}$ Proposition: $\textsc{MDeg}$ is $\oplus\mathrm{P}$-hard.

The problems

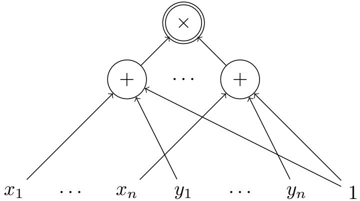
PPA-Circuit Chevalley

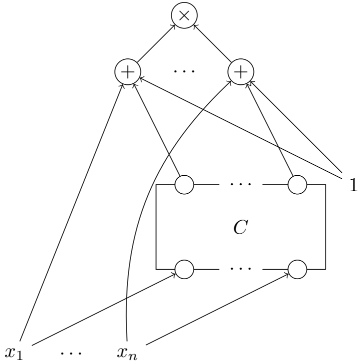
and PPA-Circuit CNSS

Towards PPA-circuits

We would like to characterize PPA with arithmetic circuits

Auxiliary circuits I and $I \diamond C$:





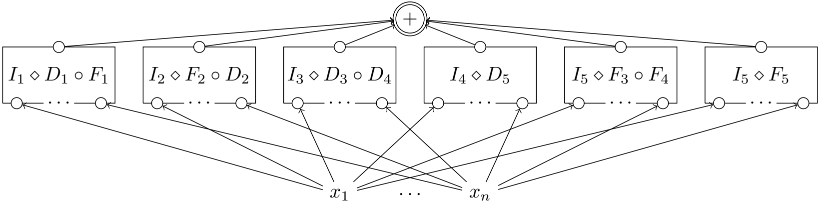
$$I(x_1, \ldots, x_n, y_1, \ldots, y_n) = \prod_{i=1}^{n}(x_i + y_i + 1)$$

$$I(x, y) = 1 \iff x = y$$

$$I \diamond C(x) = 1 \iff C(x) = x$$

PPA-circuits

Definition: A PPA-circuit is the PPA-composition $C_{D,F}$ of two n-variable, n-output arithmetic circuits D and F over $\mathbb{F}_2$



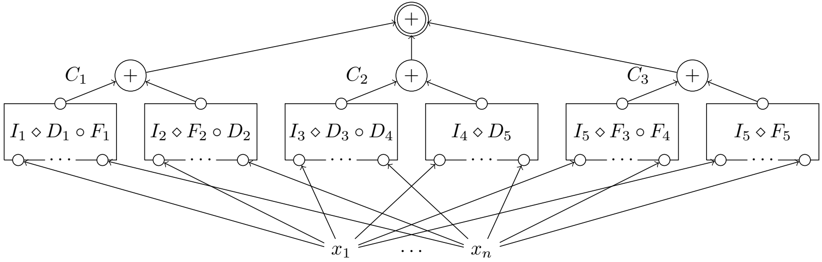
$C_{D,F}$

PPA-Circuit Matching Lemma:

If C is a PPA-circuit then in polynomial time a perfect matching μ can be computed between the maximal parse subcircuits of C.

PPA-Circuit Matching Lemma

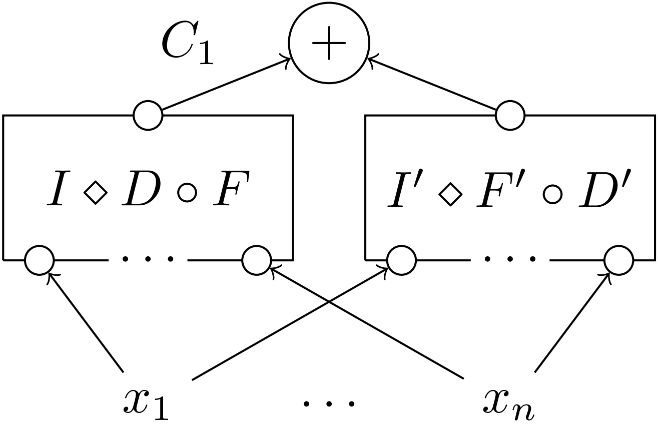
We want to define a polynomial time computable μ:
perfect matching on the maximal parse subcircuits of $C_{D,F}$



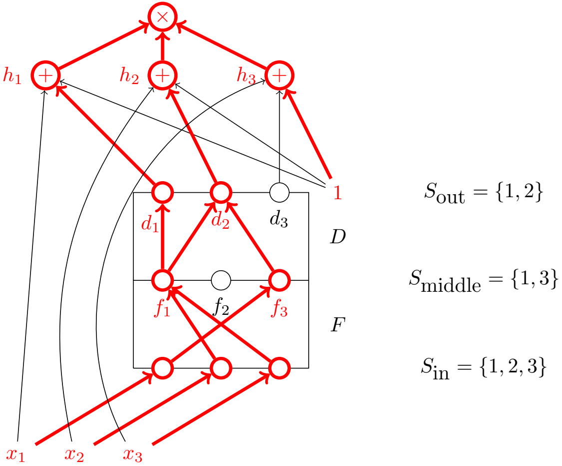
$$C_{D,F} = C_1 + C_2 + C_3$$

μ is defined inside C_1, inside C_2 and inside C_3

The matching μ inside C_1



The matching μ inside C_1



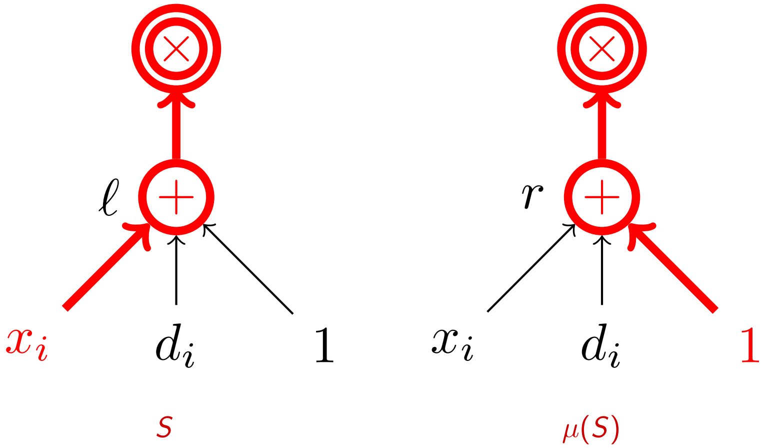
$i \in S_{\text{out}}$ if the edge from the d_i to h_i belongs to S
$i \in S_{\text{middle}}$ if there exists an edge in S from f_i to a gate in D
$i \in S_{\text{in}}$ if there exists an edge in S from x_i to a gate in F

Claim: $S_{\text{out}} \subseteq S_{\text{in}}$

The matching μ inside C_1

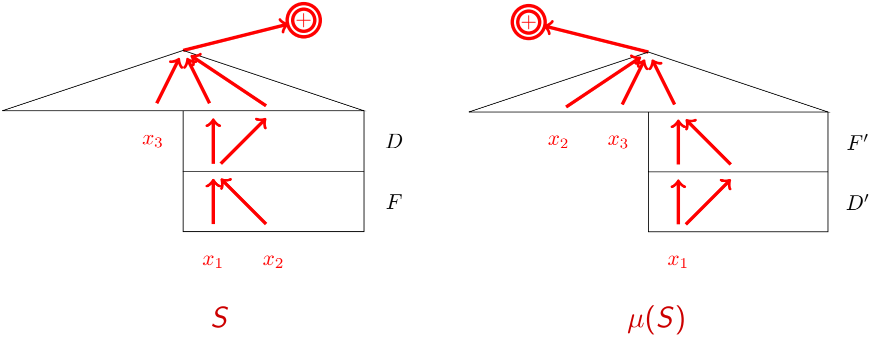
Case 1: $S_{\text{out}} \subset S_{\text{in}}$

Let i be the smallest index in $S_{\text{in}} \setminus S_{\text{out}}$

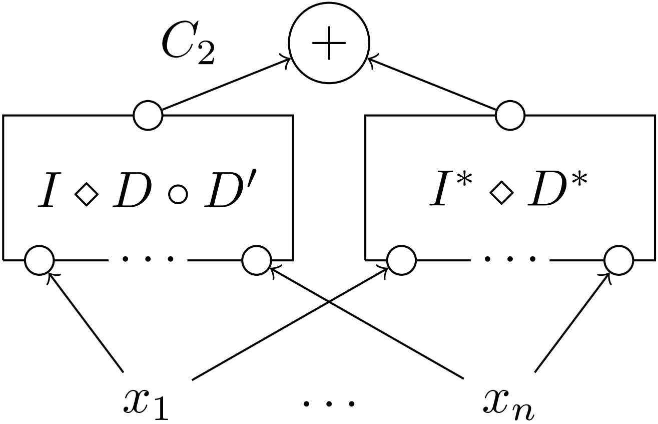


The matching μ inside C_1

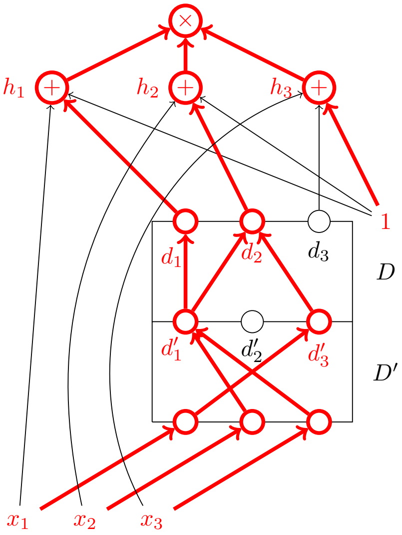
Case 2: $S_{\text{out}} = S_{\text{in}}$



The matching μ inside C_2



The matching μ inside C_2



$S_{\text{out}} = \{1, 2\}$

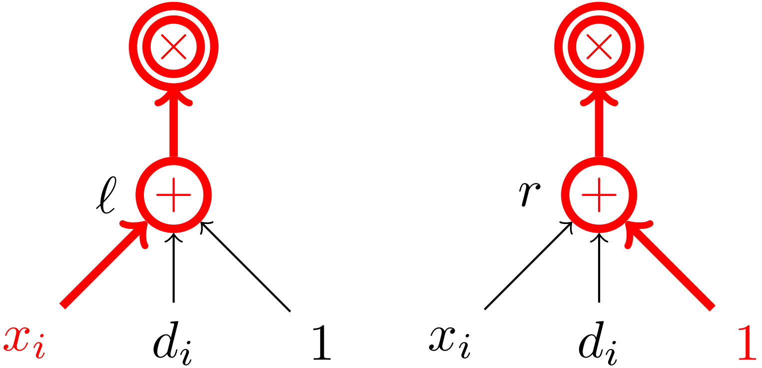
$S_{\text{middle}} = \{1, 3\}$

$S_{\text{in}} = \{1, 2, 3\}$

The matching μ inside C_2

Case 1: $S_{\text{out}} \subset S_{\text{in}}$

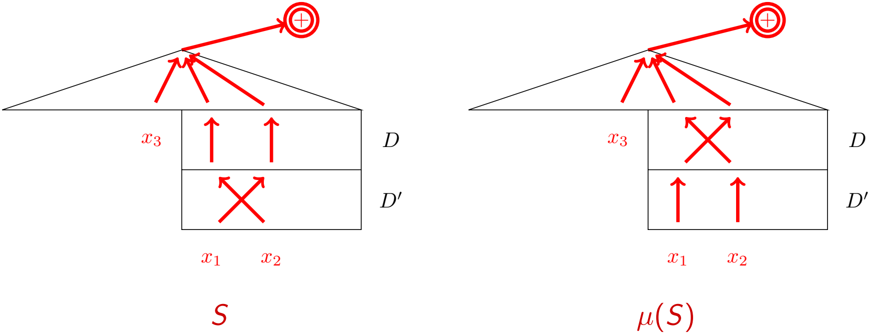
Let i be the smallest index in $S_{\text{in}} \setminus S_{\text{out}}$



S $\mu(S)$

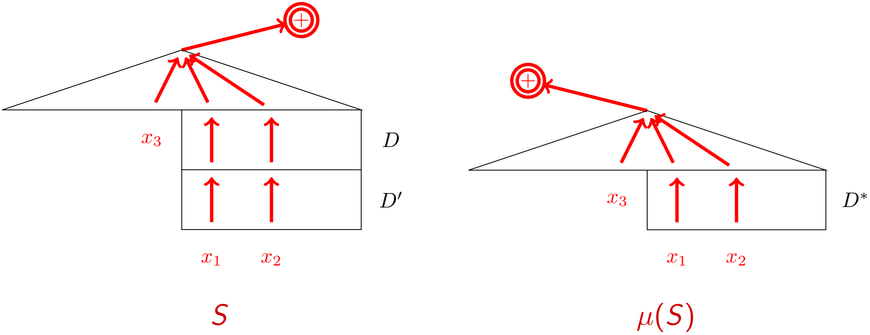
The matching μ inside C_2

Case 2: $S_{\text{out}} = S_{\text{in}}$ and $S(g) \neq S(g')$ for some sum gate in D



The matching μ inside C_2

Case 3: $S_{\text{out}} = S_{\text{in}}$ and $S(g) = S(g')$ for all sum gate in D



The computational problems

PPA-CIRCUIT CHEVALLEY

Input: (C, a), where
C: an n-variable PPA-circuit over $\mathbb{F}_2$,
a: a root of C.

Output: Another root $b \neq a$ of C.

PPA-CIRCUIT CNSS

Input: (C', a), where
C: an n-variable PPA-circuit over $\mathbb{F}_2$,
a: an element of $\mathbb{F}_2^n$.

Output: An element $b \in \mathbb{F}_2^n$ satisfying $C = C' \oplus L_a$.

The result

Main Theorem: PPA-Circuit Chevalley
and PPA-Circuit-CNSS are PPA-complete.

The proof contains three parts:

Proposition: PPA-Circuit Chevalley
and PPA-Circuit CNSS are polynomially equivalent.

Hardness Theorem: PPA-Circuit Chevalley is PPA-hard.

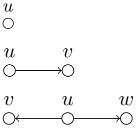
Easiness Theorem: PPA-Circuit CNSS is in PPA.

PPA-hardness and PPA-easiness

PPA-hardness

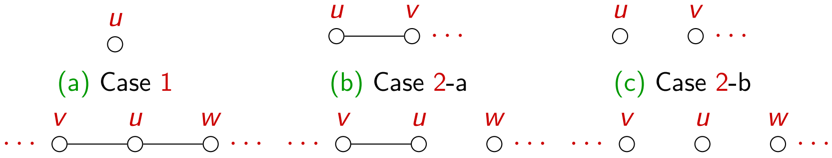
Theorem: PPA-Circuit Chevalley is PPA-hard.

Proof: Reduce Leaf to PPA-Circuit Chevalley
Express the ≤ 2 neighbours $M(u)$ of u via $D(u)$ and $F(u)$:



- Case 1: then $D(u) = F(u) = u$,
- Case 2: then $D(u) = v$ and $F(u) = u$,
- Case 3: then $D(u) = v$ and $F(u) = w$

Claim: Parity of $\deg(u)$ = Parity of satisfied components of $C_{D,F}$



(a) Case 1 (b) Case 2-a (c) Case 2-b

(d) Case 3-a (e) Case 3-b (f) Case 3-c

PPA-easiness

We prove something stronger

MATCHED-CIRCUIT CNSS

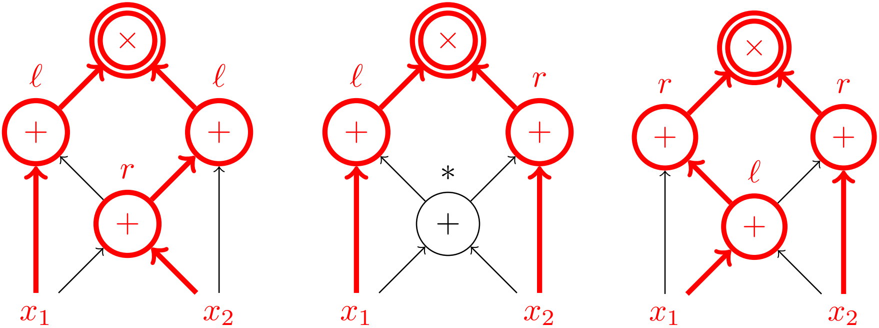
Input: (C, T, μ), where
C: an n-variable arithmetic circuit over $\mathbb{F}_2$,
T: maximal parse subcircuit
μ: polynomial time perfect matching for the maximal parse subcircuits in C but T.

Output: An element $b \in \mathbb{F}_2^n$ satisfying C.

Theorem: MATCHED-CIRCUIT CNSS is in PPA

An instance of Matched-Circuit CNSS

Input: $N = (C, T, \mu)$ Remark: $C(x) = x_1 x_2$

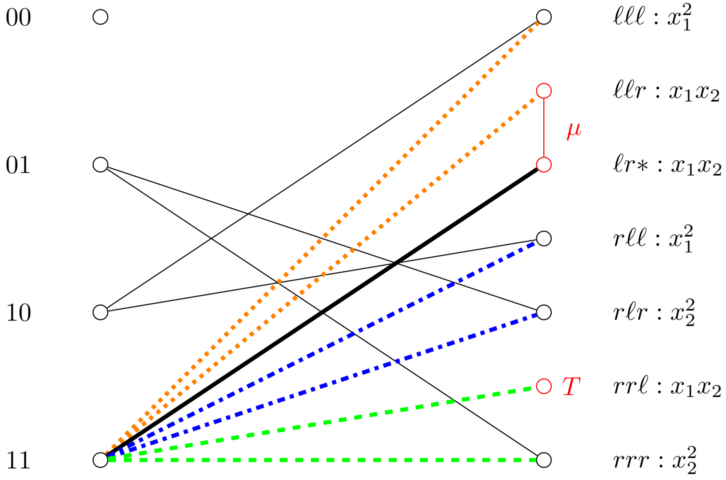


μ matches $\ell\ell r$ and $\ell r*$ unmatched $T = rr\ell$

PPA-easiness

Theorem: MATCHED-CIRCUIT CNSS is in PPA

Proof: We reduce MATCHED-CIRCUIT CNSS to LEAF.

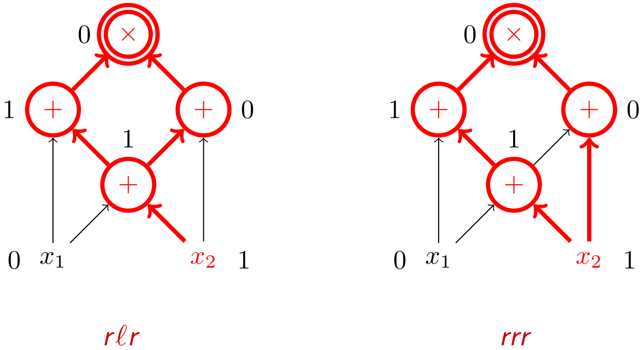


G_N resulting from the CIRCUIT-CNSS instance $N = (C, \mu, T)$

The pairing on the left hand side

Vertex 01 of even degree:

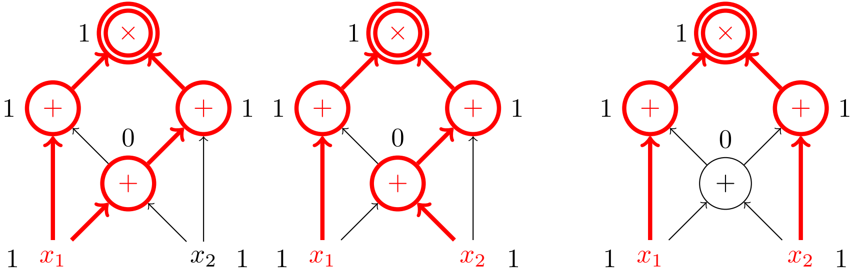
For all parse subcircuit S, $m_S(a) = 1$, $\exists$ sum gate g with $P_g(a) = 0$



The pairing on the left hand side

Vertex 11 of odd degree:

There exists a unique S, $m_S(a) = 1$, such that $P_g(a) = 1$ for all sum gate g



$\ell\ell\ell$ $\ell\ell r$ unique unmatched parse subcircuit

Thank you