Some subsystems of constant depth Frege with parity

Leszek Kołodziejczyk
University of Warsaw

(based on joint work with Michal Garlík)

Proof Complexity Workshop
St Petersburg, May 2016

Constant depth Frege with parity

$\mathrm{PK}_\oplus$ has unbounded-fanin $\bigwedge, \bigvee, \oplus^0, \oplus^1$, plus negations of literals. Lines are cedents. Most rules roughly standard. Rules for $\oplus$:

$$\frac{\Gamma, \oplus^a \Phi \qquad \Gamma, \oplus^b \Psi}{\Gamma, \oplus^{a+b}(\Phi, \Psi)}\ \text{(Add)} \qquad \frac{\Gamma, \oplus^a(\Phi, \Psi) \qquad \Gamma, \oplus^b \Psi}{\Gamma, \oplus^{a-b}\Phi}\ \text{(Subtract)}$$

$$\frac{\Gamma, \overline{\varphi}, \oplus^{b-1}\Psi \qquad \Gamma, \varphi, \oplus^b \Psi}{\Gamma, \oplus^b(\Psi, \varphi)}\ \text{(MOD)}$$

Constant depth Frege with parity (a.k.a. $\mathrm{AC}^0[2]$-Frege): a (family of) subsystem(s) of $\mathrm{PK}_\oplus$ where formulas must have constant depth (= no. of alternations of $\bigwedge, \bigvee, \oplus$).

Context

Major open problem:

Prove a superpolynomial (or better) lower bound
on the size of $AC^0[2]$-Frege proofs of some family of tautologies.

Known strong lower bounds for:

- proof size in AC^0-Frege (constant depth proofs with no parities),
- size of $AC^0[2]$-circuits,
- proof size in polynomial Polynomial Calculus: refutation system where lines are polynomials (roughly $\oplus$'s of $\bigwedge$'s of literals).

Context (2)

Theorem (Buss-K-Zdanowski 2012/15)

$\mathrm{AC}^0[2]$-*Frege is quasipolynomially simulated by its fragment operating only with (cedents of)* $\bigwedge$*'s of* $\oplus$*'s of log-sized* $\wedge$*'s.*

But the result actually is:

Theorem

$\mathrm{AC}^0[2]$-*Frege is quasipolynomially simulated by (roughly) PC with an axiom corresponding to the surjective weak pigeonhole principle for functions whose graphs are defined by formulas involving* $\oplus$.

(sWPHP for a function f and size parameter $n > 1$ says:
f is not a surjective map from n onto n^2.)

Aim of our work (1)

Problem:

Understand the relationship between $AC^0[2]$-Frege and subsystems combining full AC^0-Frege with limited parity reasoning.

Examples of such systems:

- Constant depth Frege with parity axioms,
- The treelike and daglike versions of a system defined by Krajíček 1997.

Aim of our work (2)

Problem:

Understand the relationship between $AC^0[2]$-Frege and subsystems combining full AC^0-Frege with limited parity reasoning.

Why study this?

- Strong lower bounds for such systems known.
- AC^0-Frege has quasipolynomial-size proofs of sWPHP (for functions defined in constant depth without parity).
- BKZ tells us that the "hard part" of $AC^0[2]$-Frege is sWPHP.
- So, if these systems are "close enough" to $AC^0[2]$-Frege for formulas without parity, then we would actually have a lower bound for $AC^0[2]$-Frege.

Constant depth Frege with parity axioms

To AC^0-Frege, we add as axioms all instances of the principle Count_2, saying that there is no perfect matching on an odd-sized set:

$$\bigvee_{1\le i\le 2n+1} \bigwedge_{e\subseteq[2n+1]^2,\, i\in e} \neg\psi_e \vee \bigwedge_{e,f\subseteq[2n+1]^2,\, e\perp f} (\psi_e \wedge \psi_f),$$

where the ψ_e's are constant-depth formulas.

- Count_2 requires exponential-size proofs in AC^0-Frege.
- PHP_n^{n+1}, in the form "there is no injection from $n+1$ into n", requires exp-size proofs in AC^0-Frege plus parity axioms.

Krajíček's systems

(Systems from MFCS '97 paper, reformulated and given new name).

Jan_d^c: the fragment of $\mathrm{PK}_\oplus$ where (1) formulas have depth $\leq d$, (2) no $\oplus$'s are in the scope of $\bigwedge$, $\bigvee$, (3) there are $\leq c$ $\oplus$'s per line. E.g. ($c = 3$):

$$\varphi_1, \ldots, \varphi_n, \oplus(\Psi_1), \oplus(\Psi_2), \oplus(\Psi_3).$$

Two versions: daglike (normal) and treelike (each line used at most once as premise). We think of them as refutation systems.

- treelike $\mathrm{Jan}_{O(1)}^3$ p-simulates AC^0-Frege with counting axioms.
- PHP_n^{n+1} requires exp-size proofs in treelike Jan_d^c (Krajíček '97).
- Count_3 requires exp-size proofs in daglike Jan_d^c (Krajíček '97 + PC degree lower bounds from Buss et al. '99).

Parity axioms vs parity gates

Theorem (Impagliazzo-Segerlind 2001)

There is a family of DNFs requiring superpolynomially larger proofs in AC^0*-Frege with counting axioms than in* $\mathrm{AC}^0[2]$*-Frege.*

The tautologies implicitly say:
"if $\oplus^0(q_1^0,\ldots,q_m^0)$ and $\oplus^1(q_1^n,\ldots,q_m^n)$,
then for some $i<m$, $\oplus^0(q_1^i,\ldots,q_m^i)\wedge\oplus^1(q_1^{i+1},\ldots,q_m^{i+1})$".

But they have to say this without $\oplus$!
So, talk about matchings on the sets of q_j^i's and $q_j^i q_k^{i+1}$'s instead.

The proof combines a sophisticated switching lemma with more or less standard argument against AC^0-Frege with counting axioms.

Krajíček's systems vs parity gates

We can use an Impagliazzo-Segerlind-style switching lemma to prove:

Proposition

There is a family of DNFs requiring superpolynomially larger proofs in daglike $\mathrm{Jan}^c_O(1)$ *than in* $\mathrm{AC}^0[2]$*-Frege.*

- Switching turns $\mathrm{Jan}^c_{O(1)}$ proofs into low-degree PC refutations.
- So, we need tautology susceptible to IS-like switching lemma, with polysize proofs in $\mathrm{AC}^0[2]$-Frege, but not in low-degree PC.
- We use an obfuscated version of WPHP^{2n}_n (see next slide).

The separating tautology

Variables: p_{ijk} for $i \leq 2n, j \leq n, k \leq m$.
q_{ie} for $i \leq 2n$, $e \in [n \times m \cup \{*\}]^2$
$r_{\langle i_1, i_2, j\rangle, f}$ for $i \leq 2n, j \leq n, f \in [m \times m]^2$.

Idea: pigeon i goes to hole j iff $\oplus^1(p_{ij1}, \ldots, p_{ijm})$.

"for each i, the q's form a perfect matching
on $\{*\} \cup$ the set of p_{ijk}'s that are 1",

$\wedge$

for each $i_1 < i_2$ and j, the r's form a perfect matching
on the set of those $p_{i_1jk}p_{i_2jl}$'s in which both variables are 1".

Crucially, $m = 2^{\text{polylog(n)}}$, but it is not the case that $m = \text{poly}(n)$.

Some separations and a simulation

Generally,

$$\text{AC}^0\text{-Fr/count. ax.} <^p \text{tree-Jan}^c_{O(1)} <^p \text{dag-Jan}^c_{O(1)} <^p \text{AC}^0[2]\text{-Fr},$$

all witnessed by families of CNFs.

However...

Some separations and a simulation

Generally,

$$\text{AC}^0\text{-Fr/count. ax.} <^p \text{tree-Jan}^c_{O(1)} <^p \text{dag-Jan}^c_{O(1)} <^p \text{AC}^0[2]\text{-Fr},$$

all witnessed by families of CNFs.

However...

Theorem

AC^0-*Frege with counting axioms and treelike* $\text{Jan}^c_{O(1)}$
are quasipolynomially equivalent (w.r.t. the language without $\oplus$*).*

Remark

Inspired by "Counting axioms simulate Nullstellensatz"
(also Impagliazzo-Segerlind), but somewhat more complicated.

The simulation proof: structure

Theorem

AC^0-Frege with counting axioms and treelike $\mathrm{Jan}^c_{O(1)}$ are quasipolynomially equivalent (w.r.t. the language without $\oplus$).

Proof has four steps (given treelike $\mathrm{Jan}^c_{O(1)}$ refutation of size s):

1. Replace original refutation by treelike $\mathrm{Jan}^{O(\log s)}_{O(1)}$ refutation that is balanced (height $O(\log s)$).
2. Modify refutation so that each line contains exactly one $\oplus$.
3. Delay application of subtraction rules.
4. Simulate the single-parity system w/o subtraction.

We briefly discuss 2.-4.

Moving to single parities

Replace line

$$\varphi_1, \ldots, \varphi_k, \oplus^0(\psi_i^1 : i \in I_1), \ldots, \oplus^0(\psi_i^\ell : i \in I_\ell)$$

by

$$\varphi_1, \ldots, \varphi_k, \oplus^0(\psi_{i_1}^1 \wedge \ldots \wedge \psi_{i_\ell}^\ell : i_1 \in I_1, \ldots, i_\ell \in I_\ell).$$

This necessitates adding some new rules, such as

$$\frac{\Gamma, \oplus^0(\varphi_i : i \in I)}{\Gamma, \oplus^0(\varphi_i \wedge \psi_j : i \in I, j \in J)} \text{ (Mult)}$$

Delaying subtraction

Instead of

$$\frac{\oplus^0(\Phi,\Psi) \qquad \Gamma,\oplus^0\Psi}{\Gamma,\oplus^0\Phi}$$

do

$$\frac{\oplus^0(\Phi,\Psi) \qquad \Gamma,\oplus^0\Psi}{\Gamma,\oplus^0(\Phi,\Psi,\Phi)}$$

- This requires some adding some copies of φ,φ to $\oplus$'s so that premises of multipremise rules align.
- The size blowup is no worse that $(\text{size})^{O(\text{height})}$.
- The last line was $\oplus^0(1)$. Now it is $\oplus^0(1,\psi_1,\psi_1,\ldots,\psi_\ell,\psi_\ell)$.

Completing the simulation (1)

We build a quasipolynomial size constant depth formula that, for each line of the refutation, maintains a perfect matching on the true inputs to $\oplus^0$ (assuming part outside $\oplus^0$ is false).

E.g. (red = false):

$$\frac{\overline{\varphi}, \oplus^0(\psi_1, \psi_2, 1) \qquad \varphi, \oplus^0(\psi_1, \psi_2)}{\oplus^0(\psi_1, \psi_2, \varphi)}$$

or

$$\frac{\oplus_0(\varphi_1, \varphi_2)}{\oplus^0(\varphi_1 \wedge \psi_1, \varphi_2 \wedge \psi_1, \varphi_1 \wedge \psi_2, \varphi_2 \wedge \psi_2, \varphi_1 \wedge \psi_3, \varphi_2 \wedge \psi_3)}$$

Problem with subtraction:

$$\frac{\oplus^0(\varphi_1, \varphi_2, \varphi_3, \varphi_4, \psi_1, \psi_2) \qquad \oplus^0(\psi_1, \psi_2)}{\oplus^0(\varphi_1, \varphi_2, \varphi_3, \varphi_4)}$$

We match φ_3 to φ_4 because in the left premise they were matched to formulas that were matched to each other in the right premise.

Keeping track of this through the whole proof would blow up the formula size.

Completing the simulation (2)

Eventually, we get a perfect matching
on the true inputs to the end line $\oplus^0(1, \psi_1, \psi_1, \ldots, \psi_\ell, \psi_\ell)$.

But there is an obvious perfect matching
on all true inputs to $\oplus^0(1, \psi_1, \psi_1, \ldots, \psi_\ell, \psi_\ell)$ except 1.

AC^0-Frege with counting axioms knows this is a contradiction. □

This brings up...

Open problem:

Prove a superquasipolynomial separation between $\mathrm{AC}^0[2]$-Frege and a subsystem containing AC^0-Frege with counting axioms on a family of formulas without $\oplus$.

Remark:

For constant depth systems, superquasipolynomial separation seems to be the right notion of separation.

E.g., the BKZ collapse of $\mathrm{AC}^0[2]$-Frege is quasipolynomial and proved via a collapse in bounded arithmetic with $\exists, \forall, \oplus$ and the $n^{\log n}$ function. Using methods of Maciel-Nguyen-Pitassi, this fails without $n^{\log n}$ under complexity assumptions.

Separations with parity

If we consider formulas with $\oplus$, the difficulties with separating the systems disappear.

Theorem

In refuting families of polynomial equations of degree 2,
$\mathrm{AC}^0[2]$*-Frege is exponentially stronger than daglike* $\mathrm{Jan}^c_{O(1)}$*,*
which is in turn exponentially stronger than treelike $\mathrm{Jan}^c_{O(1)}$*.*

The separating families are, respectively:

- $\mathrm{WPHP}^{2n}_n[\oplus^1(p_{ij1},\ldots,p_{ijm})/p_{ij}]$,
- the housesitting principle, with p_{ij} replaced by $\oplus^1(p_{ij1},\ldots,p_{ijm})$.

A system of Itsykson and Sokolov

Itsykson and Sokolov (2014) proposed to study a subsystem of $\mathrm{PK}_{\oplus}$ where lines are cedents (= disjunctions) of linear equations mod 2.

They obtained an exponential lower bound for the treellike version, leaving the daglike as an open problem.

Theorem

A treelike system where lines are disjunctions of $\oplus$'s of constant depth formulas is quasipolynomially simulated by $\mathrm{Jan}^{c}_{\mathrm{polylog}}$
(and thus has no short proofs of Count_3*).*

Two suspicions

Suspicion 1:

A strong lower bound for the daglike Itsykson-Sokolov system is within reach.

Suspicion 2:

An analogue of daglike Itsykson-Sokolov where lines are $\bigvee$'s of polylog-degree equations (as opposed to linear equations) is quasipolynomially equivalent to $\mathrm{AC}^0[2]$-Frege.

Remark

The system in suspicion 2 proves (all reasonable versions of) WPHP for $\mathrm{FP}^{\oplus \mathrm{P}}$ functions, and can do some rudimentary approximate counting of sets defined in terms of $\oplus$.