Some subsystems of constant-depth Frege with parity

Michal Garlík
Polytechnic University of Catalonia

(based on joint work with Leszek Kołodziejczyk)

Oxford Complexity Day - July 27, 2018

Proofs using a parity connective

PK($\oplus$) has unbounded fan-in $\bigwedge, \bigvee, \oplus^0, \oplus^1$, plus negations of literals. Lines are cedents (sequences of formulas, interpreted as disjunctions). Most rules roughly standard:

$$\frac{\Gamma}{\Gamma, \Delta}\ \text{Weakening} \qquad \frac{\Gamma, \varphi \qquad \Gamma, \overline{\varphi}}{\Gamma}\ \text{Cut}$$

$$\frac{\Gamma, \Delta}{\Gamma, \bigvee \Delta}\ \text{OR} \qquad \frac{\Gamma, \varphi_i \qquad \text{for all } i \in I}{\Gamma, \bigwedge_{i \in I} \varphi_i}\ \text{AND}$$

Proofs using a parity connective

PK($\oplus$) has unbounded fan-in $\bigwedge, \bigvee, \oplus^0, \oplus^1$, plus negations of literals. Lines are cedents (sequences of formulas, interpreted as disjunctions). Most rules roughly standard:

$$\frac{\Gamma}{\Gamma, \Delta}\ \text{Weakening} \qquad \frac{\Gamma, \varphi \qquad \Gamma, \overline{\varphi}}{\Gamma}\ \text{Cut}$$

$$\frac{\Gamma, \Delta}{\Gamma, \bigvee \Delta}\ \text{OR} \qquad \frac{\Gamma, \varphi_i \qquad \text{for all } i \in I}{\Gamma, \bigwedge_{i \in I} \varphi_i}\ \text{AND}$$

Rules for $\oplus^0, \oplus^1$ connectives:

$$\frac{}{\oplus^0 \emptyset}\ \text{Axiom} \qquad \frac{\Gamma, \overline{\varphi}, \oplus^{b-1}\Phi \qquad \Gamma, \varphi, \oplus^b \Phi}{\Gamma, \oplus^b(\Phi, \varphi)}\ \text{MOD}$$

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

for each $a, b \in \{0, 1\}$.

Constant depth Frege with parity

Constant depth Frege with parity (a.k.a. AC^0[2]-Frege): a (family of) subsystem(s) of $\mathrm{PK}(\oplus)$ where formulas must have constant depth ($=$ number of alternations of $\bigwedge, \bigvee, \oplus$).

Constant depth Frege with parity

Constant depth Frege with parity (a.k.a. AC^0[2]-Frege):
a (family of) subsystem(s) of $\mathrm{PK}(\oplus)$ where formulas must have constant depth (= number of alternations of $\bigwedge, \bigvee, \oplus$).

Major open problem:

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

Main reason of interest:

- Techniques for l.b. on size of AC^0 *circuits* useful in proving l.b. for AC^0-Frege *proofs* (without $\oplus$).
- L.b. on size of AC^0[2] *circuits* are known.

Theorem (Buss-Kołodziejczyk-Zdanowski 2012/15)

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.*

Aim of our work

Problem:

Understand the relationship between $\mathrm{AC}^0[2]$-Frege and its 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.

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:

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

where the ψ_e's are constant-depth formulas.

- Count_2 requires exponential-size proofs in AC^0-Frege. (BIKPRS '95)
- PHP_n^{n+1} (in the usual form "there is no injection from $n+1$ to n") requires exp-size proofs in AC^0-Frege w/ parity axioms. (Beame-Riis '98)

The system $\mathsf{PK}_d^c(\oplus)$

$\mathsf{PK}_d^c(\oplus)$ is a fragment of $\mathsf{PK}(\oplus)$ where

1. formulas have depth $\leq d$,
2. no $\oplus$'s are in the scope of $\bigvee, \bigwedge$,
3. there are $\leq c$ $\oplus$'s per line.

E.g. $(c = 3)$:

$$\varphi_1, \ldots, \varphi_m, \oplus^0(\Psi_1), \oplus^0(\Psi_2), \oplus^1(\Psi_3).$$

The system $\mathsf{PK}_d^c(\oplus)$

$\mathsf{PK}_d^c(\oplus)$ is a fragment of $\mathsf{PK}(\oplus)$ where

1. formulas have depth $\leq d$,
2. no $\oplus$'s are in the scope of $\bigvee, \bigwedge$,
3. there are $\leq c$ $\oplus$'s per line.

E.g. ($c = 3$):

$$\varphi_1, \ldots, \varphi_m, \oplus^0(\Psi_1), \oplus^0(\Psi_2), \oplus^1(\Psi_3).$$

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

The system $\mathsf{PK}_d^c(\oplus)$

$\mathsf{PK}_d^c(\oplus)$ is a fragment of $\mathsf{PK}(\oplus)$ where

1. formulas have depth $\leq d$,
2. no $\oplus$'s are in the scope of $\bigvee, \bigwedge$,
3. there are $\leq c$ $\oplus$'s per line.

E.g. ($c = 3$):

$$\varphi_1, \ldots, \varphi_m, \oplus^0(\Psi_1), \oplus^0(\Psi_2), \oplus^1(\Psi_3).$$

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

- treelike $\mathsf{PK}^3_{O(1)}(\oplus)$ p-simulates AC^0-Frege with parity axioms.

The system $\mathrm{PK}_d^c(\oplus)$

$\mathrm{PK}_d^c(\oplus)$ is a fragment of $\mathrm{PK}(\oplus)$ where

1. formulas have depth $\leq d$,
2. no $\oplus$'s are in the scope of $\bigvee, \bigwedge$,
3. there are $\leq c$ $\oplus$'s per line.

E.g. ($c = 3$):

$$\varphi_1, \ldots, \varphi_m, \oplus^0(\Psi_1), \oplus^0(\Psi_2), \oplus^1(\Psi_3).$$

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

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

Some polynomial separations (all witnessed by families of CNFs) and a quasipolynomial simulation

$\mathrm{AC}^0[2]$-Frege

$\vee^{p}$?

daglike $\mathsf{PK}^{O(1)}_{O(1)}(\oplus)$

$\vee^{p}$?

treelike $\mathsf{PK}^{O(1)}_{O(1)}(\oplus)$

$\vee^{p}$ $|||^{qp}$

AC^0-Frege w/ parity axioms

$\mathsf{PK}_d^c(\oplus) <^p \mathrm{AC}^0[2]\text{-Frege}$

Theorem

There exist a family $\{\mathcal{A}_n\}_{n\in\omega}$ of unsatisfiable CNF's such that each $\mathcal{A}_n$ has a $\mathrm{poly}(n)$-size refutation in $\mathrm{AC}^0[2]$-Frege, but requires $n^{\omega(1)}$-size refutations in $\mathsf{PK}_d^c(\oplus)$ for any constants c, d.

$\mathsf{PK}_d^c(\oplus) <^p \mathrm{AC}^0[2]$-Frege

Theorem

There exist a family $\{\mathcal{A}_n\}_{n\in\omega}$ of unsatisfiable CNF's such that each $\mathcal{A}_n$ has a $\mathrm{poly}(n)$-size refutation in $\mathrm{AC}^0[2]$-Frege, but requires $n^{\omega(1)}$-size refutations in $\mathsf{PK}_d^c(\oplus)$ for any constants c, d.

- We use an Impagliazzo-Segerlind-style switching lemma to prove this.
- Switching turns $\mathsf{PK}_d^c(\oplus)$ for 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_n^{2n} (see next slide).

Take m s.t. $n = 2^{\mathrm{polylog(m)}}$ and WPHP:

$$1 + \sum_{j \in [m]} x_{ij}, \qquad i \in [2m],$$

$$x_{i_1 j} \cdot x_{i_2 j}, \qquad i_1 < i_2 \in [2m], j \in [m]$$

Replace each x_{ij} by a sum of n variables $x_{ijk}, k \in [n]$ and expand.

$$\oplus^1 \left(\{x_{ijk} : j \in [m], k \in [n]\}\right), \qquad i \in [2m], \tag{1}$$

$$\oplus^0 \left(\{x_{i_1 jk} \wedge x_{i_2 j\ell} : k, \ell \in [n]\}\right), \qquad i_1 < i_2 \in [2m], j \in [m] \tag{2}$$

Take m s.t. $n = 2^{\mathrm{polylog(m)}}$ and WPHP:

$$1 + \sum_{j \in [m]} x_{ij}, \qquad i \in [2m],$$

$$x_{i_1 j} \cdot x_{i_2 j}, \qquad i_1 < i_2 \in [2m], j \in [m]$$

Replace each x_{ij} by a sum of n variables $x_{ijk}, k \in [n]$ and expand.

$$\oplus^1 (\{x_{ijk} : j \in [m], k \in [n]\}), \qquad i \in [2m], \qquad (1)$$

$$\oplus^0 (\{x_{i_1 jk} \wedge x_{i_2 j\ell} : k, \ell \in [n]\}), \qquad i_1 < i_2 \in [2m], j \in [m] \qquad (2)$$

- For each i, introduce $nm + 1$ "type-1 extra points", and reexpress (1) using new variables by saying that there is a perfect matching on the union of the set of type-1 extra points and the set of x_{ijk}'s with value 1.
- For each triple (i_1, i_2, j), introduce a set of n^2 "type-2 extra points", and reexpress (2) using new variables by saying that there is a perfect matching on the union of the set of type-2 extra points and the set of pairs (k, ℓ) s.t. both $x_{i_1 jk}$ and $x_{i_2 j\ell}$ evaluate to 1.

The simulation

Theorem

AC^0-Frege with parity axioms and treelike $\mathsf{PK}^{O(1)}_{O(1)}(\oplus)$ are quasipolynomially equivalent (w.r.t. the language without $\oplus$).

Inspired by "Counting axioms simulate Nullstellensatz" (Impagliazzo-Segerlind '06), but somewhat more complicated.

The simulation

Theorem

AC^0*-Frege with parity axioms and treelike* $\mathsf{PK}^{O(1)}_{O(1)}(\oplus)$ *are quasipolynomially equivalent (w.r.t. the language without* $\oplus$*).*

Inspired by "Counting axioms simulate Nullstellensatz" (Impagliazzo-Segerlind '06), but somewhat more complicated.

Proof

has four steps (given treelike $\mathsf{PK}^{c}_{O(1)}(\oplus)$ refutation of size s):

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

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

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

This leads to an auxiliary proof system, which we call one-parity system.

Simulation - the main idea

- Given: a derivation P in the one-parity system from some set of axioms $\mathcal{A}$ that don't contain $\oplus$.
- Consider a line $C := \varphi_1, \ldots, \varphi_\ell, \oplus^0(\xi_1, \ldots, \xi_k)$.
- We want to write down a constant-depth formula γ^C which says: "If all φ's are false, there exists a perfect matching on the set of satisfied ξ's."
- To this end, for each $e \in \binom{[k]}{2}$, we introduce a formula μ_e^C (in the variables of P) with meaning: "the two formulas ξ_i, ξ_j with $e = \{i, j\}$ are matched to one another".
- We need to make sure that γ^C has AC^0-Frege (*without* parity axioms) derivation of a small size from the non-logical axioms $\mathcal{A}$.

Propagating the matchings

The matching formulas μ_e^C are constructed inductively, depending on how C was derived in P.
E.g. Multiply by (ψ_1, ψ_2, ψ_3):
(red = false)

$$\frac{\bigoplus_0(\boxed{\varphi_1, \varphi_2})}{\bigoplus^0(\boxed{\varphi_1 \wedge \psi_1, \varphi_2 \wedge \psi_1}, \boxed{\varphi_1 \wedge \psi_2, \varphi_2 \wedge \psi_2}, \varphi_1 \wedge \psi_3, \varphi_2 \wedge \psi_3)}$$

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.

Delaying subtraction

Instead of

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

do

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

- The size blowup is no worse that $(\mathrm{size})^{O(\mathrm{height})}$.
- 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

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 parity axioms knows this is a contradiction. $\square$

Open problem:

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