On Proof Complexity of Resolution over PC

Erfan Khaniki

Charles University

Institute of Math. of CAS

SAT Reunion, June 2022

- One of the ultimate goals of Proof Complexity is to Prove super poly LB for the length of proofs in any P.P.S.

- It is possible to introduce different P.P.S. based on the complexity of functions (in terms of definability) that apear in each line of a Proof.

Res	AC^0-Frege
CP	$AC^0[\oplus]$-Frege
PC	Frege

- One hope is that if we understand functions in a class Ω, then we can prove LB for Ω-Proofs

- Strong LB for $AC^0[\oplus]$ circuits are known (since 1986)
  but no LB is known for $AC^0[\oplus]$-Frege

- What about reasonable subsystems of $AC^0[\oplus]$-Frege or similar P.P.S that can work with some kind of limited counting?

NS	$Res(Lin_R)$
PC	$Res(PC_{d,R})$
AC^0-Frege + Count$_p$	

- $Res(\oplus)$ (Itsykson-Sokolov)
- R is a ring, $C := \bigvee_{i<\ell} f_i$ is a clause where $f_i \in R[\bar{x}]$
- C is true under a Boolean assignment $a \in \{0,1\}^n \iff \exists i<\ell : f_i(a)=0$
- $Res(PC_R)$: $(f, g \in R[\bar{x}],\ a, b \in R)$

Res. rule $\dfrac{C \vee f \quad D \vee g}{C \vee D \vee af+bg}$

Weak. rule $\dfrac{C}{C \vee f}$

Simp rule $\dfrac{C \vee a}{C}\ (a \neq 0)$

Mul. rule $\dfrac{C \vee f}{C \vee (g \cdot f)}$

Axioms

0

$x_i \vee x_i - 1$

- In a $Res(PC_{d,R})$-der every f has degree at most d
- Let $\pi = C_1, C_2 \cdots, C_\ell$ be a $Res(PC_{d,R})$-der, then $|\pi| = \ell$ is the size of π

- $S_{d,R}(F) := Min(|\pi|)$ over all $Res(PC_{d,R})$-ref π of F ($S^*_{d,R}$ for tree-like)

- Let $C = \bigvee_{i=1}^{\ell} f_i$, then $\omega(C) = \ell$
- For a $Res(PC_{d,R})$-der $\pi = C_1, C_2, \cdots, C_\ell$, $\omega(\pi) = \max_{1 \le i \le \ell}(\omega(C_i))$

- $W_{d,R}(F) := Min(\omega(\pi))$ over all $Res(PC_{d,R})$-ref π of F

- Known LB: tree-like $Res(PC_{1,\mathbb{F}_2})$ ($Res(lin_{\mathbb{F}_2})$, $Res(\oplus)$)

IS: $FPHP_n^m$, Lifted $TS_2(G)$, Lifted Peb_G

Kr: Hall n

GK: $Count_3^n$

Gr: $Ordering_n$, DLO_n

IR: $PMP_{K_{n+2,n}}$

Pa: $b \notin A(\{0,1\}^n)$

PT: $FPHP_n^m$, $TS_2(G,\sigma)$, Random k-CNF

$Res(PC_{L,Q})$

PT: Subset-sum Principle

Can Prover-Delayer

Communiction complexity

Lifting

Randomized FIP

size-width + PC

random restriction + PC

tree-like $Res(PC_{1,\mathbb{F}_{p^k}})$

tree-like $Res(PC_{d,\mathbb{F}_2})$

IR: BPHP

Thm. ([BW]) For any CNF $F \notin SAT$:

1. $w_{Res}(F) \leq \omega(F) + \lg\left(S_{Res^*}(F)\right)$
2. $w_{Res}(F) \leq \omega(F) + O\left(\sqrt{n \lg\left(S_{Res}(F)\right)}\right)$

Thm. (Size-width) Let R be a finite ring and $F \underset{CNF}{\notin} SAT$:

1. $\frac{w_{d,R}(F)}{|R|} - 1 \leq \max\{3, \omega(F)\} + \lg\left(3S^*_{d,R}(F)\right)$
2. $\frac{w_{d,R}(F)}{|R|} \leq \max\{3, \omega(F)\} + O\left(\sqrt{\left(n + S_{d,R}(F)\right) \lg\left(S_{d,R}\right)}\right)$

- For any $f \in \underset{\text{finite}}{R}[\bar{x}]$, q_f is an atomic variable
- $Q(f) = q_f$, $Q(C) = \bigvee_{i<\ell} q_{f_i}$ $(C = \bigvee_{i<\ell} f_i)$, $Q(\emptyset) = \emptyset$
- $$Q'(r) = \begin{cases} f & r = q_f \\ \bigvee_{a \in R \setminus \{0\}} (f - a) & r = \neg q_f \end{cases}$$

  , $Q'(C) = \bigvee_{i<\ell} Q'(r_i)$

  $C = \bigvee_{i<\ell} r_i$

  $Q'(\emptyset) = \emptyset$

- Let π be a $Res(PC_{d,R})$-ref of F.

- Then $Ex(\pi)$ contains the following clauses:

I) $0 \in \pi \Rightarrow q_0 \in \bar{E}x(\pi)$

II) $x \vee x-1 \in \pi \Rightarrow q_x \vee q_{x-1} \in \bar{E}x(\pi)$

III) Res rule on f, g to der $af+bg \Rightarrow \neg q_f \vee \neg q_g \vee q_{af+bg} \in \bar{E}x(\pi)$

IV) Mult rule on f to der $g \cdot f \Rightarrow \neg q_f \vee q_{g \cdot f} \in \bar{E}x(\pi)$

V) Simp rule on $a \neq 0 \Rightarrow \neg q_a \in \bar{E}x(\pi)$

Lem. Let R be a finite ring, $F \notin SAt$ and π a $Res(PC_{d,r})$-ref. of F:

I) $\exists$ Res-ref π' of $Ex(\pi) \cup Q(F)$ s.t. $|\pi'| \leq 3|\pi|$. Moreover, if π is tree-like, then π' is also tree-like.

II) $\left| V(Ex(\pi) \cup Q(F)) \right| \leq 2n + 3|\pi|$

III) For every clause C' in $V\left(Ex(\pi) \cup Q(F)\right)$,

$$Ex(\pi) \cup Q(F) \vdash^{Res}_{w} C' \Rightarrow F \vdash^{Res(PC_{d,R}}_{|R|(w+1)} Q'(C')$$

- Proof of size-width relation for $Res(PC_{d,R})$:
- Let π be a $Res(PC_{d,R})$-ref of F s.t. $|\pi| = S_{d,R}(F)$

- By (I) $\Rightarrow$ $S_{Res}(Ex(\pi) \cup Q(F)) \leq 3 S_{d,R}(F)$
- By (II) $\Rightarrow$ $\frac{w_{d,R}(F)}{|R|} - 1 \leq w_{Res}(Ex(\pi) \cup Q(F))$

$\Big\}$ $\cdot |V(Ex(\pi) \cup Q(F))| \leq 2n + 3 S_{d,R}(F)$

- $w(Ex(\pi) \cup Q(F)) = \max\{3, w(F)\}$
- BW $\Rightarrow$ Let $F' := Ex(\pi) \cup Q(F)$, then $w_{Res}(F') \leq w(F) + O\left(\sqrt{|V(F')| \lg S_{Res}(F')}\right)$
- $\frac{w_{d,R}(F)}{|R|} \leq \max\{3, w(F)\} + O\left(\sqrt{(n + S_{d,R}(F)) \lg S_{d,R}(F)}\right)$

∎

- For a clause $C = \bigvee_{i \in \ell} f_i$, $h_C := \prod_{i \in \ell} f_i$

Lem. Let F be a CNF and $H_F := \{h_C : C \in F\}$. Then for every finite field $\mathbb{F}$ and any clause C' in $V(F)$:

$$F \vdash^{\omega}_{\mathrm{Res}(\mathrm{PC}_{d,\mathbb{F}})} C' \Rightarrow H_F \vdash^{\mathrm{PC}_{\mathbb{F}}}_{O(wd)} h_{C'}$$

$\Rightarrow$ size-width for $\mathrm{Res}(\mathrm{PC}_{d,\mathbb{F}})$ + $\mathrm{PC}_{\mathbb{F}}$ degree LB for F $\Rightarrow$ $\mathrm{Res}(\mathrm{PC}_{d,R})$ LB for F

- Let $G=(V,E)$ be a directed d-regular graph. For every $(v,u)\in E$ we have a fixed var $x_{v,u}$. Let $\sigma: V \to \mathbb{F}_q \Rightarrow TS_q(G,\sigma)$ is a CNF encoding of the following equations for every $v \in V$:

$$\left(\sum_{(v,u)\in E} x_{v,u} - \sum_{(u,v)} x_{u,v}\right) \overset{q}{\equiv} \sigma(v)$$

Thm. ([AR]) For any field $\mathbb{F}$ and any prime $q \neq \mathrm{char}(\mathbb{F})$, $\exists\ d_q \in \mathbb{N}$ s.t. for any $d \geq d_q$ and G is a d-regular Ramanujan graph on n nodes (its edges have been oriented), then for any σ s.t. $TS_q(G,\sigma) \notin \mathrm{SAT} \Rightarrow$ $PC_{\mathbb{F}}$-refutation degree is $\Omega(dn)$.

$$\Rightarrow S_{d,\mathbb{F}}(TS_q(G,\sigma)) \geq n^{2-\frac{(\log q)^2}{\log n}}.$$

Thank you!