Polynomial calculus space and resolution width

Nicola Galesi[1] Leszek Kołodziejczyk[2] Neil Thapen[3]

[1]Sapienza University [2]University of Warsaw [3]Czech Academy of Sciences

Banff, January 2020

Resolution and Polynomial Calculus

- Resolution (Res) a refutational sound and complete propositional proof system for reasoning about CNFs

Lines:	$(\ell_1 \vee \ldots \vee \ell_k)$
Rule:	$\frac{C \vee x \quad \neg x \vee D}{C \vee D}$
Contradiction:	empty clause

- Polynomial Calculus with Resolution (PCR) extends Resolution to reason about polynomial equations.

Lines:	$p = 0$, p poly in $\mathbb{F}[x_1, \ldots, x_n, \bar{x}_1, \ldots, \bar{x}_n]$
Rules:	$\frac{}{x^2 - x}$, $\frac{}{x + \bar{x} - 1}$, $\frac{p \quad q}{ap + bq}$, $\frac{p}{xp}$
Contradiction:	1
CNF reasoning :	$x_1 \vee \neg x_2 \vee x_3 \quad \longmapsto \quad \bar{x}_1 x_2 \bar{x}_3$

Complexity measures: width and degree

Resolution width

Clause width: $\mathrm{w}(C) = \#$ literals in C
Proof width: $\mathrm{w}(\pi) = \max_{C \in \pi} \mathrm{w}(C)$

Given CNF F, $\mathrm{w}(F \vdash \bot) =$ minimal $\mathrm{w}(\pi)$ for π a Res proof of F.

PCR degree

Term degree: $\deg(t)$
Proof degree: $\deg(\pi) = \max_{t \in \pi} \deg(t)$

For CNF F, $\deg(F \vdash \bot) =$ minimal $\deg(\pi)$ for π a PCR proof of F.

Complexity measures: space

Memory configurations:

$$\mathbb{M}_i = \boxed{m_1}\boxed{m_2}\boxed{m_3} \quad \cdots \quad \boxed{}\boxed{m_{s_i}}$$

Each m_i is a clause in the case of Res, a term in the case of PCR.

Proofs are sequences $\mathbb{M}_1, \ldots \mathbb{M}_t$ of memory configurations such that: $\mathbb{M}_1 = \emptyset$, $\mathbb{M}_t = \{\bot\}$, and $\mathbb{M}_i \mapsto \mathbb{M}_{i+1}$ by one of:

- Axiom download: download a clause of F into $\mathbb{M}_{i+1}$,
- Inference: add conclusion of a rule applied to clauses/polys from $\mathbb{M}_i$,
- Deletion: delete a clause/poly appearing in $\mathbb{M}_i$.

The space of a proof π is the largest s_i for $\mathbb{M}_i \in \pi$.
The space needed to prove $F \vdash \bot$ in Res/PCR defined accordingly.

Relations between proof measures

Res space is lower-bounded by width [Atserias-Dalmau 08]:

$$F \text{ a } k\text{-CNF}, \quad \mathrm{Sp}_{\mathrm{Res}}(F \vdash \bot) \geq \mathrm{w}(F \vdash \bot) - k + 1,$$

Res total space is lower-bounded by width squared [Bonacina 16]:
(total space counts literals rather than just clauses in memory)

$$F \text{ a } k\text{-CNF}, \quad \mathrm{TSp}_{R}(F \vdash \bot) \geq \frac{1}{16}(\mathrm{w}(F \vdash) - k + 4)^2,$$

PCR space for $F([\oplus])$ is lower-bounded by Res width for F [FLMNV 13]:

$$F \text{ a } k\text{-CNF}, \quad \mathrm{Sp}_{\mathrm{PCR}}(F[\oplus] \vdash \bot) \geq (\mathrm{w}(F \vdash \bot) - k + 1)/4.$$

Our Contribution

Problem:

Is PCR space lower-bounded by degree, or even by Res width?

Our Contribution

Problem:

Is PCR space lower-bounded by degree, or even by Res width?

Theorem (Main)

Let F be a k-CNF. If F has a PCR *refutation in space s over some field $\mathbb{F}$, then F has a* Res *refutation of width $O(s^2) + k$.*

(In other words, $\mathsf{Sp}_{\mathsf{PCR}}(F \vdash \bot) \geq \Omega(\sqrt{\mathsf{w}(F \vdash \bot) - k})$.)

Corollary

PCR *refutations in space s can be transformed into* PCR *refutations of degree $O(s^2) + k$.*

An important tool

Definition (Atserias-Dalmau family)

Let F be a k-CNF. A *w-AD* family for F is a nonempty family $\mathcal{H}$ of partial assignments to the variables of F such that for each $\alpha \in \mathcal{H}$,

- $|\alpha| \leq w$,
- if $\beta \subseteq \alpha$ then $\beta \in \mathcal{H}$,
- if $|\alpha| < w$ and x a vble, then there is $\beta \supseteq \alpha$ in $\mathcal{H}$ with $x \in \mathrm{dom}(\beta)$,
- α does not falsify any clause of F.

Theorem (Atserias Dalmau 08)

If $\mathrm{w}(F \vdash \bot) \geq w$, *then there exists a* w-AD *family for* F.

Res space $\geq$ width, AD-style

- Assume that F has a Res refutation of space s: $\mathbb{M}_1, \ldots, \mathbb{M}_t$.
- Assume also that there is a $(s+k)$-AD family for F.
- Prove inductively that for each $i = 1, \ldots, t$,
  there is $\alpha_i \in \mathcal{H}$ with $|\alpha_i| \leq s$ satisfying each clause in $\mathbb{M}_i$.
- Induction goes through because no α in $\mathcal{H}$ falsifies F
  and because you only need s bits to satisfy s clauses.
- But $\mathbb{M}_t$ contains $\perp$: contradiction. □

In some other resolution lower bound proofs (esp. for width),
a dual approach is used: go up the refutation from the final clause,
finding small assignments that falsify a given clause.

Towards PCR space

From now on, fix:

- an unsatisfiable k-CNF F,
- which has a space s PCR refutation $\mathbb{M}_1, \ldots, \mathbb{M}_t$,
- but also has a w-AD family $\mathcal{H}$,
  (where w will turn out to be $4s^2 + k$.)

We would like to adapt the AD approach
to show that this situation cannot happen.

But there are difficulties...

A difficulty

Obvious problem:

It is no longer true that few bits suffice to satisfy a low-space configuration. The polynomial $1 - \prod_{i=1}^{n} x_i$ has space 2 but satisfying $1 - \prod_{i=1}^{n} x_i = 0$ requires setting n variables.

A difficulty

Obvious problem:

It is no longer true that few bits suffice to satisfy a low-space configuration. The polynomial $1 - \prod_{i=1}^{n} x_i$ has space 2 but satisfying $1 - \prod_{i=1}^{n} x_i = 0$ requires setting n variables.

Remedy:

Take seriously the idea (borrowed from forcing) that if no extension of α in $\mathcal{H}$ makes something true, then in a sense α makes it false.

Forcing with an AD-family

Definition ($\Vdash$, meaning "forces")

For an assignment $\alpha \in \mathcal{H}$ and a term t, we define

(i) $\alpha \Vdash t = 0$ if α sets some variable in t to 0,

(ii) $\alpha \Vdash t = 1$ if no $\beta \in \mathcal{H}$ with $\beta \supseteq \alpha$ sets any variable in t to 0.

Forcing with an AD-family

Definition ($\Vdash$, meaning "forces")

For an assignment $\alpha \in \mathcal{H}$ and a term t, we define

(i) $\alpha \Vdash t = 0$ if α sets some variable in t to 0,

(ii) $\alpha \Vdash t = 1$ if no $\beta \in \mathcal{H}$ with $\beta \supseteq \alpha$ sets any variable in t to 0.

This generalizes to polynomials and configurations:

- if $p = \sum_i a_i t_i$ with $a_i \in \mathbb{F}$, and α forces each t_i to a value $b_i \in \{0, 1\}$, then we say $\alpha \Vdash p = \sum_i a_i b_i$,
- $\alpha \Vdash \mathbb{M}$ if α forces each polynomial in $\mathbb{M}$ to 0,
- $\alpha \Vdash \neg\mathbb{M}$ if α forces each polynomial in $\mathbb{M}$ to a value, but at least one of those values is $\neq 0$.

Forcing: the bad and the good

Bad:

E.g.: if $|\alpha| = w$, $x \notin \mathrm{dom}(\alpha)$, then $\alpha \Vdash x + \bar{x} - 1 = -1$.
(Recall that we can derive $x + \bar{x} - 1$ from no premises at all!)

Good:

For α reasonably small ($|\alpha| \leq w - s - k$ generally suffices):

- it cannot happen that $\alpha \Vdash \mathbb{M}_i$ and $\alpha \Vdash \neg\mathbb{M}_i$,
- it cannot happen that $\alpha \Vdash \mathbb{M}_i$ and $\alpha \Vdash \neg\mathbb{M}_{i+1}$,
- for any i, there is always $\alpha \subseteq \beta_i \in \mathcal{H}$ with $|\beta_i| \leq |\alpha| + s$ such that $\beta_i \Vdash \mathbb{M}_i$ or $\beta_i \Vdash \neg\mathbb{M}_i$.

(So maybe we could go down the refutation like in A-D, maintaining small $\alpha_i \in \mathcal{H}$ such that $\alpha_i \Vdash \mathbb{M}_i$?)

Another difficulty

Slightly less obvious problem:

If $\alpha \Vdash \mathbb{M}_i$, and $\beta \supseteq \alpha$ with $\beta \Vdash \mathbb{M}_{i+1}$, there is no guarantee that we can find $\beta' \subseteq \beta$ with $\beta' \Vdash \mathbb{M}_{i+1}$ and $|\beta'| \leq s$.
(Deleting bits may cause terms to stop being forced to 1.)

Another difficulty

Slightly less obvious problem:

If $\alpha \Vdash \mathbb{M}_i$, and $\beta \supseteq \alpha$ with $\beta \Vdash \mathbb{M}_{i+1}$, there is no guarantee that we can find $\beta' \subseteq \beta$ with $\beta' \Vdash \mathbb{M}_{i+1}$ and $|\beta'| \leq s$.
(Deleting bits may cause terms to stop being forced to 1.)

Remedy:

Go down and up repeatedly in a number of steps $r = 1, \ldots, ?$:

- maintaning α_r that keeps increasing, but $|\alpha_r|$ is under control,
- finding $i_1 \leq i_2 \leq \ldots \leq i_r \leq \ldots \leq j_r \leq \ldots j_2 \leq j_1$ such that:
  - $\alpha \Vdash \mathbb{M}_{i_r}$ and $\alpha \Vdash \neg\mathbb{M}_{j_r}$,
  - α has increasingly "special" properties w.r.t. all configurations between $\mathbb{M}_{i_r}$ and $\mathbb{M}_{j_r}$.

The “special” property: non-zero terms

Definition

- $\mathrm{NZ}(\alpha, \mathbb{M}) = |\{t \in \mathbb{M} : \alpha \not\Vdash t = 0\}|$.
- α guarantees $\geq r$ NZ-terms in $\mathbb{M}$ if for each $\beta \in \mathcal{H}$
  $\beta \supseteq \alpha$ implies $\mathrm{NZ}(\beta, \mathbb{M}) \geq r$.

Some observations:

- Every α guarantees ≥ 0 NZ-terms in every $\mathbb{M}_i$.
- If α guarantees $\geq s$ NZ-terms in $\mathbb{M}_i$,
  then it forces each t in $\mathbb{M}_i$ to 1.
- If α guarantees $\geq r$ NZ-terms in $\mathbb{M}_i$,
  and $\gamma \supseteq \alpha$ with $\mathrm{NZ}(\alpha, \mathbb{M}_i) = r$ and $\gamma \Vdash (\neg)\mathbb{M}_i$,
  then there is $\beta \supseteq \alpha$ with $\beta \Vdash (\neg)\mathbb{M}_i$ and $|\beta| \leq |\alpha| + s$.

Main Lemma

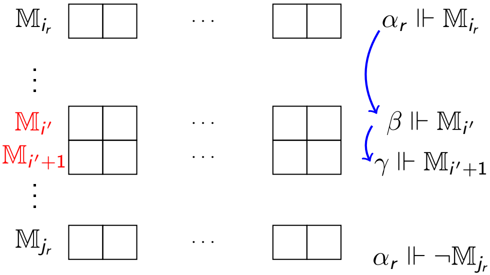
Lemma (Main)

For each $r \le s$, there are $\alpha_r \in H$ and $1 \le i_r < j_r \le t$ such that:

1. $\alpha_r \Vdash \mathbb{M}_{i_r}$ *and* $\alpha \Vdash \neg\mathbb{M}_{j_r}$,
2. α_r *guarantees* $\ge r$ NZ-*terms in each* $\mathbb{M}_\ell$ *for* $i_r \le \ell \le j_r$,
3. $|\alpha_r| \le 4rs$.

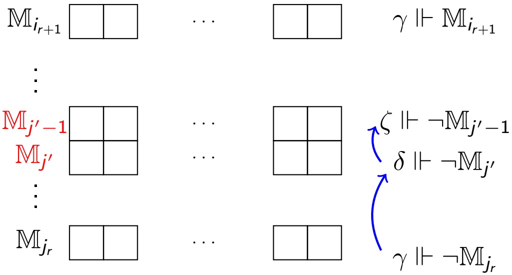
The proof is by induction on r.
The base case uses $\alpha_0 = \emptyset$, $i_0 = 1$, and $j_0 = t$.

Inductive step: downwards



- i' is greatest in $[i_r, j_r]$ s.t. there is $\beta \supseteq \alpha_r$ with $\beta \Vdash \mathbb{M}_{i'}$ and $\mathrm{NZ}(\beta, \mathbb{M}_{i'}) = r$; if none exists, $i' = i_r$. W.l.o.g. $|\beta| \leq |\alpha_r| + s$.
- Then exists $\gamma \supseteq \beta$ such that $\gamma \Vdash M_{i'+1}$. W.l.o.g. $|\gamma| \leq |\alpha_r| + 2s$. Necessarily $\mathrm{NZ}(\gamma, \mathbb{M}_{i'+1}) > r$.
- The number $i' + 1$ will be i_{r+1}.

Inductive step: upwards



- j' is smallest in $[i_{r+1}, j_r]$ s.t. there is $\delta \supseteq \gamma$ with $\mathrm{NZ}(\delta, \mathbb{M}_{j'}) = r$; if none exists, $j' = j_r$. W.l.o.g. $|\delta| \leq |\alpha| + 3s$. Necessarily, $\delta \Vdash \neg M_{j'}$.
- Then exists $\zeta \supseteq \delta$ such that $\zeta \Vdash \neg M_{j'-1}$. W.l.o.g. $|\zeta| \leq |\alpha| + 4s$. Necessarily $\mathrm{NZ}(\zeta, \mathbb{M}_{j'-1}) > r$.
- The number $j' - 1$ becomes j_{r+1}, and ζ becomes α_{r+1}.

Wrapping up the proof

- After s inductive steps we get $i_s < j_s$ and α_s with $|\alpha_s| \leq 4s^2$.
- We have $\alpha_s \Vdash \mathbb{M}_{i_s}$, $\alpha_s \Vdash \neg\mathbb{M}_{j_s}$.
- Moreover, $\mathrm{NZ}(\alpha_s, \mathbb{M}_\ell) = s$ for each ℓ in between.
  This means that $\alpha_s \Vdash \mathbb{M}_\ell$ or $\alpha_s \Vdash \neg\mathbb{M}_\ell$.
- By an easy induction, we get $\alpha_s \Vdash \mathbb{M}_\ell$ for each $\ell = i_s, i_s + 1, \ldots, j_s$. This contradicts $\alpha_s \Vdash \neg\mathbb{M}_{j_s}$. □

Improvements and consequences

- Argument works for wider class of "configurational proof systems" as long as each configuration is a boolean function of $\leq s$ terms.
- The bound on width is actually $\sim 2s^2 + k$, and for the special case of PCR it is $\sim s^2 + k$.
- A simple variant of our argument (once up, once down) reproves Bonacina's "Res total space $\geq$ (width)^2".
- We get $\Omega(\sqrt{n})$ PCR space lower bounds for GOP_n and FPHP_n.
- And n-variable formulas with $n^{O(1)}$-size, $O(1)$-degree PCR proofs but no $o(\sqrt{n})$-space PCR proofs independently of characteristic.

Open problem

Recall our main result:

Theorem

If a k-CNF F has a PCR *refutation in space s,*
then it has a Res *refutation of width $O(s^2) + k$.*

Problem

Is the square in our result needed?

(The intriguing option that it is needed for general systems but not for PCR has not been ruled out.)