PROOF COMPLEXITY AS A COMPUTATIONAL LENS
LECTURE 18

Last time: Total space $\gtrsim (\text{width})^2$ for resolution

THM [Bonacina '16]
If $W_R(F \vdash \bot) > w \geq 4 \cdot W(F)$, then
$TotSp_R(F \vdash \bot) > w^2/8$.

Developed notion of forcing

$\alpha \Vdash m = 0$ if $\exists \ell \in m$ s.t. $\alpha(\ell) = 0$
$\alpha \Vdash m = 1$ if no $\beta \supseteq \alpha$, $\beta \in \mathcal{A}$ sets $m = 0$

Relative to assignments in memory-w
Defendant strategy $\mathcal{A}$

$\forall \alpha \in \mathcal{A} \neq \emptyset$
(i) $|\mathrm{dom}(\alpha)| = |\alpha| \leq w$
(ii) If $\beta \subseteq \alpha$ then $\beta \in \mathcal{A}$
(iii) If $|\alpha| < w$ and $x \notin \mathrm{dom}(\alpha)$, then
$\exists \beta \supseteq \alpha$, $\beta \in \mathcal{A}$ s.t. $x \in \mathrm{dom}(\beta)$
(iv) $\forall C \in F$ $\alpha(C) \neq \bot$

Use forcing to prove

PCR monomial space $\gtrsim \sqrt{\text{resolution width}}$

Assumptions $\boxed{F \text{ k-CNF formula}}$

$\pi = (\mathbb{M}_0, \ldots, \mathbb{M}_\tau)$ functional monomial calculus refutation in $\boxed{\text{monomial space } s}$

Notation $\boxed{\pi[L, R]} = (\mathbb{M}_L, \mathbb{M}_{L+1}, \ldots, \mathbb{M}_{R-1}, \mathbb{M}_R)$

Assume w.l.o.g. $W(F) = k \geq 3$

Otherwise $W_R(F \vdash \bot) \leq k$

Let $\mathcal{A}$ memory-w Defendant strategy for F for w sufficiently large $w = 2s(s+1) + k$ for us today

DEFINITION (GUARANTEED NON-ZEROS)

For $\mathbb{M}$ and $\alpha \in \mathcal{A}$

$\boxed{Z(\mathbb{M}, \alpha)} = \{\text{monomials } m \in \mathbb{M} \mid \alpha \Vdash m = 0\}$

$\boxed{NZ(\mathbb{M}, \alpha)} = \{\text{monomials } m \in \mathbb{M} \mid \text{it does NOT hold that } \alpha \Vdash m = 0\}$

$\alpha \in \mathcal{A}$ $\boxed{\text{GUARANTEES } r \text{ non-zeros}}$ in $\mathbb{M}$ if

$\forall \beta \in \mathcal{A}, \beta \supseteq \alpha \quad |NZ(\mathbb{M}, \beta)| \geq r$

$\alpha \in \mathcal{A}$ guarantees r non-zeros in $\pi[L, R]$ if α guarantees r non-zeros for all $\mathbb{M}_t$, $t \in [L, R]$

OBSERVATION 12 If α guarantees r non-zeros in an interval and $\beta \supseteq \alpha$, $\beta \in \mathcal{A}$, then β also guarantees r non-zeros in this interval.

This notion plays nicely with forcing as follows

In main tech lemma

$\boxed{\text{LEMMA 13}}$ Suppose that $|NZ(\mathbb{M}, \alpha)| = r$ and that α guarantees r non-zeros in $\mathbb{M}$. Then α forces $\mathbb{M}$

Proof Let $NZ(\mathbb{M}, \alpha) = \{m_1, \ldots, m_r\}$
All other monomials in $\mathbb{M}$ forced to 0 by definition
Since α guarantees r non-zeros, no $\beta \supseteq \alpha$, $\beta \in \mathcal{A}$, can force any m_i to 0. Hence $\alpha \Vdash m_i = 1$
So α forces all monomials in $\mathbb{M}$, and hence also $\mathbb{M}$ $\boxtimes$

We can now argue about how to grow and shrink assignments in $\mathcal{A}$ that force configurations $\mathbb{M}$

In main tech lemma

LEMMA 14
Suppose $MSp(\mathbb{M}) \le s$ and that $\alpha \in \mathcal{A}$ guarantees r non-zeroes in $\mathbb{M}$. Then there is $\beta \supseteq \alpha$, $\beta \in \mathcal{A}$, such that β forces $\mathbb{M}$ and $|\beta| \le |\alpha| + s - r$.
Proof Use proof of Lemma 9, and observe that assignment is extended with $\{\ell \mapsto 0\}$ at most $s-r$ times $\boxtimes$

In main tech lemma

LEMMA 15
Suppose $MSp(\mathbb{M}) \le s$ and let $\alpha \in \mathcal{A}$.
Suppose $\exists \gamma \supseteq \alpha$, $\gamma \in \mathcal{A}$ such that $|NZ(\mathbb{M}, \gamma)| = r$
then $\exists \beta \in \mathcal{A}$, $\alpha \subseteq \beta \subseteq \gamma$ such that $|NZ(\mathbb{M}, \beta)| = r$ and $|\beta| \le |\alpha| + s - r$.
If α guarantees r non-zeroes in $\mathbb{M}$, then β forces $\mathbb{M}$, and β and γ both force $\mathbb{M}$ to either true or false.

Proof Let monomials in $\mathbb{M}$ be $m_1, \ldots, m_{s'}$, $s' \le s$
Write $NZ(\mathbb{M}, \gamma) = \{m_1, \ldots, m_r\}$
$Z(\mathbb{M}, \gamma) = \{m_{r+1}, \ldots, m_{s'}\}$ with $\ell_i \in m_i$ s.t. $\gamma(\ell_i) = 0$
Set $\beta = \alpha \cup \{ \ell_i \mapsto 0 \mid i \in [r+1, s'] \}$

$\beta \leq \gamma \in \mathcal{A}$, so $\beta \in \mathcal{A}$

$NZ(\mathbb{M}, \beta) = NZ(\mathbb{M}, \gamma)$ so $|NZ(\mathbb{M}, \beta)| = r$

$|\beta| \leq |\alpha| + s - r$ clear from construction

If α guarantees r non-zeroes, then so do β and γ, and by Lemma 13 they force $\mathbb{M}$. Since $\gamma \geq \beta$, they force $\mathbb{M}$ to same value (by Observation 4). $\boxed{/\!/}$

LEMMA 16 (MAIN TECHNICAL LEMMA)

Let $\pi = (\mathbb{M}_0, \ldots, \mathbb{M}_\tau)$ be an FMC refutation in monomial space s of the k-CNF formula F for $k \geq 2$. Let $\mathcal{A}$ be a memory-w Defendant strategy for F for $w \geq 2s(s+1) + k$. Then for each $r \leq s$ there is an $\alpha_r \in \mathcal{A}$ and a proof interval $[L_r, R_r]$ such that

(i) $\boxed{\alpha \Vdash \mathbb{M}_{L_r}}$ and $\boxed{\alpha \Vdash \neg \mathbb{M}_{R_r}}$

(ii) α guarantees r non-zeroes in $\pi[L_r, R_r]$

(iii) $|\alpha| \leq 4 \sum_{i=0}^{r-1} (s-i)$

Let us see how Theorem A' now follows.

$\boxed{\text{Proof of Theorem A'}}$ Towards contradiction, fix space-s FMC refutation $\pi = (\mathbb{M}_0, \ldots, \mathbb{M}_\tau)$ and suppose $W_R(F \vdash \bot) > 2s(s+1) + k = w$. Then $\exists$ memory-w Defendant strategy for F (even for $w+1$, but we don't have energy to carry this 1 around)

Apply Lemma 16 with $r = s$ to get $\alpha_r \in \mathcal{A}$ and $L \leq R$ such that

- $\boxed{\alpha_s \Vdash \mathbb{M}_L}$ and $\boxed{\alpha_s \Vdash \neg\mathbb{M}_R}$

- $\boxed{|\alpha_s|} \leq 4 \sum_{i=0}^{s-1} (s-i) = 4 \cdot \frac{s(s+1)}{2}$
  $= 2s(s+1) = \boxed{w-k}$
- α_s guarantees s non-zeroes in $\pi[L, R]$

By Lemma 13, α_s forces all $\mathbb{M}_t$, $t \in [L, R]$
Using Lemma 11, it follows by induction over $t \in [L, R]$ that $\alpha_s \Vdash \mathbb{M}_t$
But then $\alpha_s \Vdash \mathbb{M}_R$ and $\alpha_s \Vdash \neg \mathbb{M}_R$
which contradicts Observation 8 ↯ ☒

See picture on MSW XIII

Proof of Lemma 16 By induction over r.
For the base case $r = 0$, we take $\alpha_0 = \emptyset$, $L_0 = 0$, $R_0 = \tau$. $\emptyset \Vdash \mathbb{M}_0 \equiv \top$ and $\emptyset \Vdash \neg \mathbb{M}_\tau$ for $\mathbb{M}_\tau \equiv \bot$ since both FMC configurations have arity 0.
Conditions (ii) and (iii) are vacuously true.

For the inductive step, suppose that conditions (i)-(iii) hold for α_r and $\pi[L_r, R_r]$ for $r < s$
We will use that condition (iii) implies

$$|\alpha_r| + 4(s-r) \leq w - k$$

First consider "left end" of proof interval. Case analysis:
(a) $\exists t' \in [L_r, R_r]$ and $\beta' \supseteq \alpha_r$, $\beta' \in A$, such that $|NZ(\mathbb{M}_{t'}, \beta')| = r$ and $\beta' \Vdash \mathbb{M}_{t'}$
(b) No such t' exists

In case (b), α_r must guarantee $\geq r + 1$ non-zeros, so set $\alpha' := \alpha_r$ and $L' := L_r$

In case (a), fix maximal such t' and corresponding β'

By condition (i) and Observations 4 & 8, $t' < R_r$

By condition (ii) and Lemma 15 can choose β' such that

$$\boxed{|\beta'| \le |\alpha_r| + s - r}$$

By condition (ii) and Lemma 14 can extend β' to $\alpha' \supseteq \beta'$, $\alpha' \in \mathcal{A}$ such that

$$|\alpha'| \le |\beta'| + s - r \le |\alpha_r| + 2(s-r)$$

and α' forces $\mathbb{M}_{t'+1}$ (and also $\mathbb{M}_{t'}$ since already $\alpha' \supseteq \beta' \Vdash \mathbb{M}_{t'}$ by construction)

Since $|\alpha'| \le w - k$, Lemma 11 says that

$\boxed{\alpha' \Vdash \mathbb{M}_{t'+1}}$ Set $L' := t' + 1$

Now work on "right end" of proof interval

Again we have two cases:

(c) $\exists\, t'' \in [L', R_r]$ and $\beta'' \supseteq \alpha'$, $\beta \in \mathcal{A}$ such that $|NZ(\mathbb{M}_{t''}, \beta'')| = r$

(d) No such t'' exists

In case (d) set $\alpha_{r+1} := \alpha'$ and $R' := R_r$

In case (c) fix minimal such t'' and corresponding β''. By construction of α' and Lemma 15 can choose β'' such that

$$\boxed{|\beta''| \le |\alpha'| + s - r}$$

By condition (ii) and Lemma 13, β'' forces $\mathbb{M}_{t''}$. Therefore $\boxed{\beta'' \Vdash \neg \mathbb{M}_{t''}}$ since otherwise we would have picked this $t'' > t'$ in case (a)

Since $\beta'' \supseteq \alpha' \Vdash \mathbb{M}_{L'}$, $\boxed{t'' > L'}$

Appeal to Lemma 14 to get $\alpha'' \supseteq \beta''$, $\alpha'' \in \mathcal{A}$ such that

$$\boxed{|\alpha''|} \leq |\beta''| + (s-r) \leq |\alpha'| + 2(s-r) \leq W-k$$

and α'' forces $\mathbb{M}_{t''-1}$.

Since $\alpha'' \supseteq \beta'' \Vdash \neg \mathbb{M}_{t''}$, Lemma 11 implies that

$$\boxed{\alpha'' \Vdash \neg \mathbb{M}_{t''-1}}$$

Set $R' := t''-1$ and $\boxed{\alpha_{r+1} := \alpha''}$

Now set $\boxed{L_{r+1} := L'}$ $\boxed{R_{r+1} := R''}$

We claim that α_{r+1} and $\pi[L_{r+1}, R_{r+1}]$ satisfy the inductive hypothesis

Condition (iii) follows by inspection since

$$|\alpha_{r+1}| \leq |\alpha_r| + 4(s-r) \leq 4 \sum_{i=0}^{(r+1)-1} (s-i)$$

Condition (i) holds by construction since

$\alpha_{r+1} \supseteq \alpha' \Vdash \mathbb{M}_{L_{r+1}}$ and

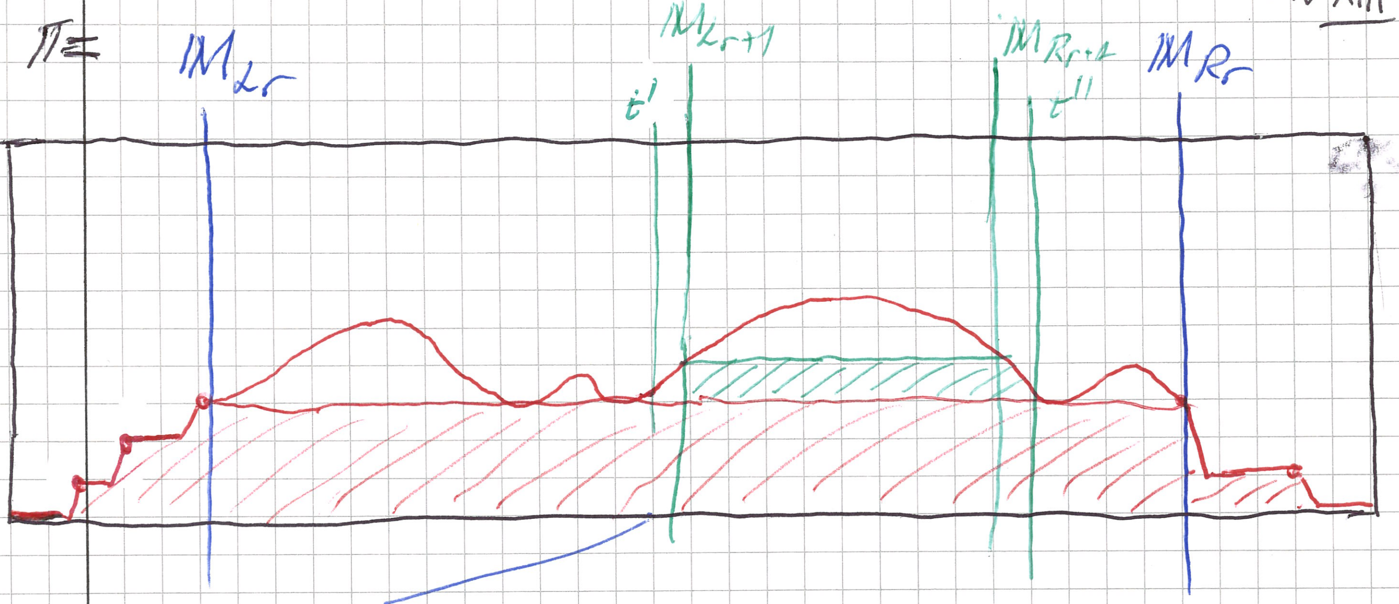
$\alpha_{r+1} \Vdash \neg \mathbb{M}_{R_{r+1}}$

For condition (ii) we know that α_r guarantees r non-zeros in $\pi[L_r, R_r]$. By the choice of L_{r+1} and R_{r+1} we know for $\gamma \in \mathcal{A}$, $\gamma \supseteq \alpha''$ and $t \in [L_{r+1}, R_{r+1}]$ that $|NZ(\mathbb{M}_t, \gamma)| \neq r$

Hence $\alpha'' = \alpha_{r+1}$ guarantees $> r$ non-zeros in $\pi[L_{r+1}, R_{r+1}]$

∎

$\Pi =$



$\beta' \Vdash \mathbb{M}_{t'}$

$\beta' \leq \alpha' \Vdash \mathbb{M}_{t'+1}$

$\alpha' \leq \beta'' \Vdash \neg \mathbb{M}_{t''}$

$\beta'' \leq \alpha'' \Vdash \neg \mathbb{M}_{t''-1}$

$$
\begin{aligned}
|\alpha''| &\leq |\beta''| + (s-r) \\
&\leq |\alpha'| + 2(s-r) \\
&\leq |\beta'| + 3(s-r) \\
&\leq |\alpha| + 4(s-r)
\end{aligned}
$$

Nullstellensatz refutation of polynomials

$P = \{p_i \mid i \in [m]\}$ over $\{x_j \mid j \in [n]\}$

$$\sum_{i=1}^{m} q_i p_i + \sum_{j=1}^{n} r_j (x_j^2 - x_j) = 1$$

syntactic equality

for $q_i, r_j \in \mathbb{F}[x_1, \ldots, x_n]$

View as proof system for CNF formulas by translating clauses

$$C = \bigvee_{x \in P} x \vee \bigvee_{y \in N} \bar{y}$$

to polynomials

$$p_C = \prod_{x \in P} (1 - x) \prod_{y \in N} y$$

Today we think of $1 \equiv$ true, $0 \equiv$ false for variables

Focus on Nullstellensatz without dual variables

View polynomials p as linear combinations of monomials

$p = \sum_{i=1}^{s} a_i m_i \qquad a_i \in \mathbb{F}$

SIZE $S(p) = s$ = # monomials

DEGREE $Deg(p)$ = largest total degree of monomial in p (wlog multilinear)

Most focus on degree lower bounds

In contrast to resolution and polynomial calculus, large NS degree does not imply size lower bound

[Buresh-Oppenheim, Clegg, Impagliazzo, & Pitassi '02]

Degree lower bounds for

- pigeonhole principle [BCEIP '98]
- induction principle [BP '98]
- house-sitting principle [Buss '98, CEI '96]
- matching [BIKPRS '97]
- pebbling [BCIP '02]

Then research seems to have moved on to stronger algebraic proof systems like polynomial calculus

Renewed interest in Nullstellensatz in [RPRC '16, PR '17, PR '18, dRMNPRV '20] since NS lower bounds can be lifted to stronger computational models.

This research also led to strong size-degree trade-offs for Nullstellensatz by [de Rezende, Meir, Nordström & Robere '21] for PEBBLING CONTRADICTIONS — quick recap

$G = (V, E)$ directed acyclic graph (DAG)

$\boxed{pred_G(v)} = \{ u \mid (u,v) \in E \}$ $\boxed{succ_G(u)} = \{ v \mid (u,v) \in E \}$

Single SINK z with $succ_G(z) = \emptyset$

SOURCE vertices s have $pred_G(s) = \emptyset$

Bounded fan-in $|pred_G(v)| = O(1)$ $\forall v \in V$

Usually insist on fan-in 0 or 2 — not important

Can drop subscript G when clear from context (i.e., always)

Variable x_v for $v \in V$

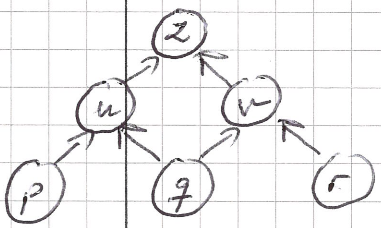
For $U \subseteq V$, use notation $\boxed{x_U = \prod_{v \in U} x_v}$

PEBBLING CONTRADICTION Peb_G

Source axioms $pred_G(s)=\emptyset$	x_s	$1-x_s$
Pebbling axioms	$\bigvee_{u \in pred_G(v)} \overline{x}_u \lor x_v$	$x_{pred_G(v)}(1-x_v)$
Sink axiom	$\overline{x}_z$	x_z

$$\boxed{\begin{aligned} A_v &\doteq x_{pred_G(v)}(1-x_v) \\ A_{sink} &\doteq x_z \end{aligned}}$$

Example



$$
\begin{array}{ll}
x_p & 1 - x_p \\
\land\ x_q & 1 - x_q \\
\land\ x_r & 1 - x_r \\
\land (\overline{x}_p \lor \overline{x}_q \lor x_u) & x_p x_q (1-x_u) \\
\land (\overline{x}_q \lor \overline{x}_r \lor x_v) & x_q x_r (1-x_v) \\
\land (\overline{x}_u \lor \overline{x}_v \lor x_z) & x_u x_v (1-x_z) \\
\land\ \overline{x}_z & x_z
\end{array}
$$

Sometimes we simplify notation and identify v and x_v

We will need to study the REVERSIBLE PEBBLE GAME [Bennett '89]. Black pebble game when pebbling strategies run in reverse are also valid

Studied in the context of

- energy dissipation during computation
- quantum computing

Also in computational complexity theory

Pebble configuration $\mathbb{P}$ = subset of vertices $\mathbb{P} \subseteq V$

Reversible pebbling strategy

$\mathcal{P} = (\mathbb{P}_0, \mathbb{P}_1, \ldots, \mathbb{P}_\tau)$

sequence of configurations such that

$\mathbb{P}_0 = \mathbb{P}_\tau = \emptyset$

$z \in \bigcup_{t \in [\tau]} \mathbb{P}_t$

For all $t \in [\tau]$ $\mathbb{P}_t$ follows from $\mathbb{P}_{t-1}$ by

(1) Pebble placement on v

$\mathbb{P}_t = \mathbb{P}_{t-1} \cup \{v\}$ $\quad v \notin \mathbb{P}_{t-1}$, $pred_G(v) \subseteq \mathbb{P}_{t-1}$

(2) Pebble removal from v

$\mathbb{P}_t = \mathbb{P}_{t-1} \setminus \{v\}$ $\quad v \in \mathbb{P}_{t-1}$, $pred_G(v) \subseteq \mathbb{P}_{t-1}$

$time(\mathcal{P}) = \tau$

$space(\mathcal{P}) = max_{t \in [\tau]} \{ |\mathbb{P}_t| \}$

Alternative, equivalent, definition

$\mathcal{P} = (\mathbb{P}_0, \ldots, \mathbb{P}_\tau)$

$\mathbb{P}_0 = \emptyset$, $z \in \mathbb{P}_\tau$, $time(\mathcal{P}) = 2\tau$

Because of reversibility, once we have $z \in \mathbb{P}_\tau$ we can run pebbling in reverse

(Technically, these are all visiting pebblings — we could also define persistent pebblings with $\mathbb{P}_\tau = \{z\}$, which changes space by at most 1, as usual.)

THEOREM A [dRMNR '21]

Let G be single-sink DAG and let $\mathbb{F}$ be any field. Then there is a reversible pebbling strategy $\mathcal{P}$ for G in time at most $time(\mathcal{P}) \leq T$ and $space(\mathcal{P}) \leq S$ if and only if there is a Nullstellensatz refutation π over $\mathbb{F}$ of Peb_G such that $S(\pi) \leq T+1$ and $Deg(\pi) \leq S$

Let us first show how to convert a reversible pebbling $P = (\mathbb{P}_0, \ldots, \mathbb{P}_\tau)$ such that $\mathbb{P}_0 = \emptyset$, $z \in \mathbb{P}_\tau$ into a Nullstellensatz refutation

For each $t \in [\tau]$ derive

$$\boxed{x_{\mathbb{P}_{t-1}} - x_{\mathbb{P}_t}} \qquad (\dagger)$$

Telescope to get

$$\sum_{t \in [\tau]} x_{\mathbb{P}_{t-1}} - x_{\mathbb{P}_t} = 1 - x_{\mathbb{P}_\tau}$$

Since $z \in \mathbb{P}_t$ can derive $x_{\mathbb{P}_t}$ by multiplying A_{sink} and subtract

Suppose step t pebble placement on or removal from v. Note

$$\mathbb{P}_{t-1} \cap \mathbb{P}_t = (\mathbb{P}_{t-1} \cup \mathbb{P}_t) \setminus \{v\}$$
$$pred(v) \subseteq \mathbb{P}_{t-1} \cap \mathbb{P}_t$$

Set $\boxed{R_t = (\mathbb{P}_{t-1} \cap \mathbb{P}_t) \setminus pred(v)}$

For pebble placement, get $(\dagger)$ by

$$x_{R_t} \cdot A_v$$

For pebble removal

$$-x_{R_t} \cdot A_v$$

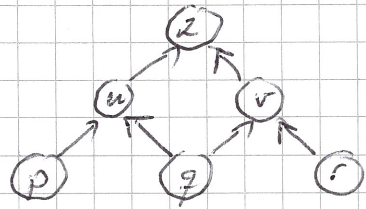
Clearly, degree = pebbling space

monomials = $2 \cdot \tau + 1$ = pebbling time + 1

Note:

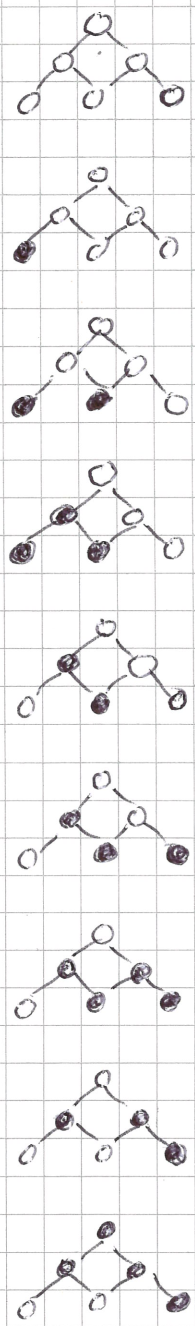
- No Boolean axioms
- Multilinear NS refutation

Example



CANCELLATIONS

$$
\begin{aligned}
& 1 - p \\
+ \; & p \cdot (1 - q) \\
+ \; & pq\,(1 - u) \\
- \; & qu \cdot (1 - p) \\
+ \; & qu \cdot (1 - r) \\
+ \; & u \cdot qr\,(1 - v) \\
- \; & ruv \cdot (1 - q) \\
+ \; & r \cdot uv\,(1 - z) \\
+ \; & ruv \cdot z \\
= \; & 1
\end{aligned}
$$



Now convert NS refutation to reversible pebbling

For simplicity, let us do this over $\mathbb{F}_2 = GF(2)$

$$\boxed{A_v \doteq x_{pred(v)}\,(1 + x_v)}$$

Also, consider multilinear setting without Boolean axioms $x_v^2 - x_v$ — only makes reduction stronger, since multilinearizing proof can only decrease proof size

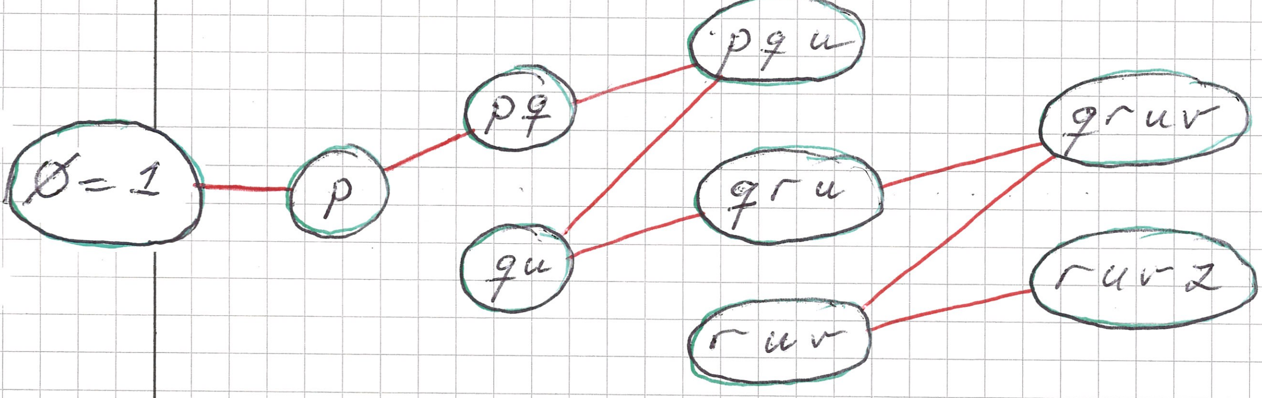
$$\boxed{\pi = \sum_{v \in V} q_v \cdot A_v + \sum q_{sink} \cdot A_{sink} = 1}$$

For every monomial x_U in refutation, add node U in graph $H(\pi)$

For every monomial x_W in every q_v, add edge $\boxed{(W \cup pred(v), W \cup pred(v) \cup \{v\})}$

Note that q_{sink} doesn't contribute edges

Example (cont.) $H(\pi)$



Observations

(a) $\deg_H(\emptyset)$ odd, since 1 doesn't cancel

(b) If $z \notin U \neq \emptyset$ then $\deg_H(U)$ is even since x_U cancels

(c) If $z \in U$, then $\deg_H(U)$ can be odd or even

(d) Every edge is a valid pebbling move between two configurations

Conclusions

- There is a path in $\mathcal{H}(\pi)$ from $\emptyset = 1$ to some $\mathcal{U}$ s.t. $z \in \mathcal{U}$
- this corresponds to (half of) a valid pebbling $\mathcal{P}$
- $space(\mathcal{P}) \leq Deg(\pi)$ by construction
- $time(\mathcal{P}) \leq 2 \cdot |E(\mathcal{H}(\pi))| \leq 2 \cdot \frac{S(\pi) - 1}{2}$
  $= S(\pi) - 1$

Analogous argument generalizes to arbitrary field $\mathbb{F}$ by defining weights of edges (in terms of coefficients $c \in \mathbb{F}$ in front of monomials) and doing more careful parity-like argument

So to get NS size-degree trade-offs just need time-space trade-offs for reversible pebbling

Not at all as well studied as for black and black-white pebbling! Probably significant room for improvement of pebbling results in [dRMNR '21]

But still can get several strong results, though not as tight as, e.g., trade-offs between length and clause space in resolution in [BN '11]

Example NS trade-off:

THEOREM 3 [dRMNR '21]
There exists constant $K > 0$ and family of explicitly constructible 3-CNF formulas $\{F_n\}_{n=1}^{\infty}$ of size $\Theta(n)$ such that for any $\varepsilon > 0$:

(i) $Deg_{NS}(F_n \vdash \bot) \leq d_1 = O(\sqrt[6]{n} \log n)$.

(ii) Exists NS refutation $\pi : F_n \vdash \bot$ such that
$S(\pi) = O(n^{1+\varepsilon})$
$Deg(\pi) = O(d_1 \cdot \sqrt[6]{n}) = O(\sqrt[3]{n} \log n)$.

(iii) For any NS refutation $\pi : F_n \vdash \bot$
such that $Deg(\pi) \leq K d_2 / \log n = O(\sqrt[3]{n})$
it holds that $S(\pi) \geq (\sqrt[6]{n})!$.

OPEN PROBLEMS

(P1) Stronger and tighter time-space trade-offs for reversible pebbling

(P2) In particular, would it be possible to get SHARP TRADE-OFFS where a small additive decrease in pebbling space = NS degree causes an exponential blow-up in pebbling time = NS size?

(P3) Can we get size-degree trade-offs for Nullstellensatz with dual variables?
In this setting the reduction from NS size to pebbling time breaks down

Summary of open problems

1. Is it possible in resolution to find k-CNF formulas F_n such that $Sp_R(F_n \vdash \bot) = \Omega(|F_n|)$ and $L_R(F_n \vdash \bot) = O(|F_n| \log |F_n|)$?

2. Can we find CNF formulas F_n such that $Sp_R(F_n \vdash \bot) = \omega(MSp_{PCR}(F_n \vdash \bot))$?

3. Can we separate monomial space for PCR over different fields ?

4. Can the bound for k-CNF formulas $MSp(F \vdash \bot) = \Omega\left(\sqrt{W(F \vdash \bot)}\right)$ be improved to $\Omega(W(F \vdash \bot))$?
Or is it tight for PCR ?
Or could it be tight for functional monomial calculus ?

5. If $\mathcal{P}$ is a set of polynomials of constant degree, is it true that $MSp(\mathcal{P} \vdash \bot) = \Omega\left((Deg(\mathcal{P} \vdash \bot))^{\delta}\right)$ for some $\delta > 0$?

6. Can we prove tight monomial space lower bounds for
   - FPHP and Onto-FPHP
   - Tseitin formulas
   - Ordering formulas (POP, LOP, DLO)
   - Pebbling formulas

Open
II

7 Can we find k-CNF formulas or polynomials P of constant degree such that

$$\mathrm{TotSp}_{\mathrm{PPCR}}(P \vdash \bot) = \Omega\left(|\mathrm{Vars}(P)|^2\right)$$

or is at least superlinear?

Such a lower bound is known for Complete Tree formulas CT_n, which consist of all width-n clauses over n variables, but CT_n has large, linear, width and exponential size [ABRW02]