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 (w/log 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)

$\text{pred}_G(v) = \{u \mid (u,v) \in E\}$ $\text{succ}_G(u) = \{v \mid (u,v) \in E\}$

Single SINK z with $\text{succ}_G(z) = \emptyset$

SOURCE vertices s have $\text{pred}_G(s) = \emptyset$

Bounded fan-in $|\text{pred}_G(v)| = O(1)$ $\forall v \in V$

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 $x_U = \prod_{v \in U} x_v$

PEBBLING CONTRADICTION Peb_G

Source axioms $pred_G(s) = \emptyset$: x_s , $1 - x_s$

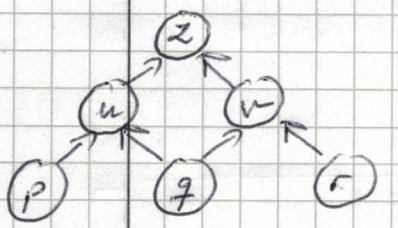
Pebbling axioms : $\bigvee_{u \in pred_G(v)} \overline{x}_u \vee x_v$, $x_{pred_G(v)} (1 - x_v)$

Sink axiom : $\overline{x}_z$, x_z

Example

$A_v \doteq x_{pred_G(v)} (1 - x_v)$

$A_{sink} \doteq x_z$



$$x_p \wedge x_q \wedge x_r \wedge (\overline{x}_p \vee \overline{x}_q \vee x_u) \wedge (\overline{x}_q \vee \overline{x}_r \vee x_v) \wedge (\overline{x}_u \vee \overline{x}_v \vee x_z) \wedge \overline{x}_z$$

$$1 - x_p \quad 1 - x_q \quad 1 - x_r \quad x_p x_q (1 - x_u) \quad x_q x_r (1 - x_v) \quad x_u x_v (1 - x_z) \quad x_z$$

Sometimes we simplify notation and identify v and x_v

We will need to study the **REVERSIBLE PEBBLE GAME** [Bennett '89]. Black pebble game where 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

$P_0 = P_{\tilde{\tau}} = \emptyset$

$z \in \bigcup_{t \in [\tilde{\tau}]} P_t$

For all $t \in [\tilde{\tau}]$ P_t follows from P_{t-1} by

(1) Pebble placement on v

$P_t = P_{t-1} \cup \{v\}$ $\quad v \notin P_{t-1}$, $pred_G(v) \subseteq P_{t-1}$

(2) Pebble removal from v

$P_t = P_{t-1} \setminus \{v\}$ $\quad v \in P_{t-1}$, $pred_G(v) \subseteq P_{t-1}$

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

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

Alternative, equivalent, definition

$\mathcal{P} = (P_0, \dots, P_{\tilde{\tau}})$

$P_0 = \emptyset$, $z \in P_{\tilde{\tau}}$, $time(\mathcal{P}) = 2\tilde{\tau}$

Because of reversibility, once we have $z \in P_{\tilde{\tau}}$ we can run pebbling in reverse

(Technically, these are all visiting pebblings — we could also define persistent pebblings with $P_{\tilde{\tau}} = \{z\}$, 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 $P = (P_0, \ldots, P_\tau)$ such that $P_0 = \emptyset$, $z \in P_\tau$ into a Nullstellensatz refutation

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

$$\boxed{x_{P_{t-1}} - x_{P_t}} \qquad (\dagger)$$

Telescope to get

$$\sum_{t \in [\tau]} x_{P_{t-1}} - x_{P_t} = 1 - x_{P_\tau}$$

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

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

$$P_{t-1} \cap P_t = (P_{t-1} \cup P_t) \setminus \{v\}$$

$$pred(v) \subseteq P_{t-1} \cap P_t$$

Set $\boxed{R_t = (P_{t-1} \cap P_t) \setminus pred(v)}$

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

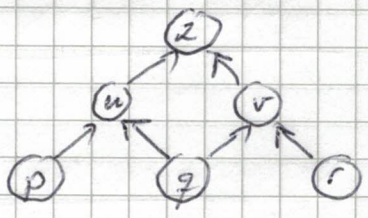
monomials = $2 \cdot \tau + 1$ = pebbling time + 1

Note:

- No Boolean axioms
- Multilinear NS refutation

Example

CANCELLATIONS



$$1 - p$$

$$+ \; p \cdot (1 - q)$$

$$+ \; pq \, (1 - u)$$

$$- \; qu \cdot (1 - p)$$

$$+ \; qu \cdot (1 - r)$$

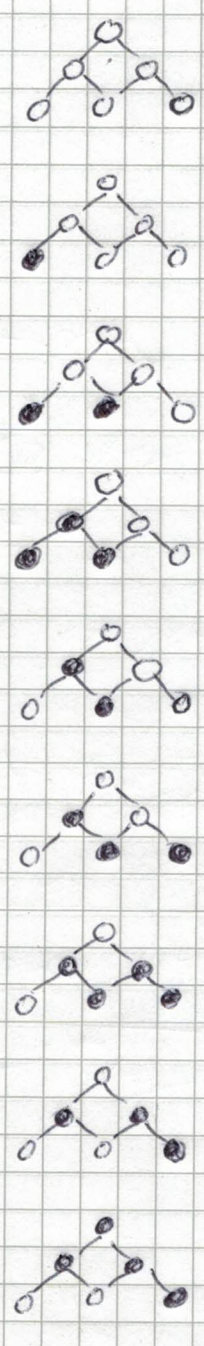
$$+ \; u \cdot qr \, (1 - v)$$

$$- \; ruv \cdot (1 - q)$$

$$+ \; r \cdot uv \, (1 - z)$$

$$+ \; ruv \cdot z$$

$$= \; 1$$



Now convert NS refutation to reversible pebbling

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

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

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

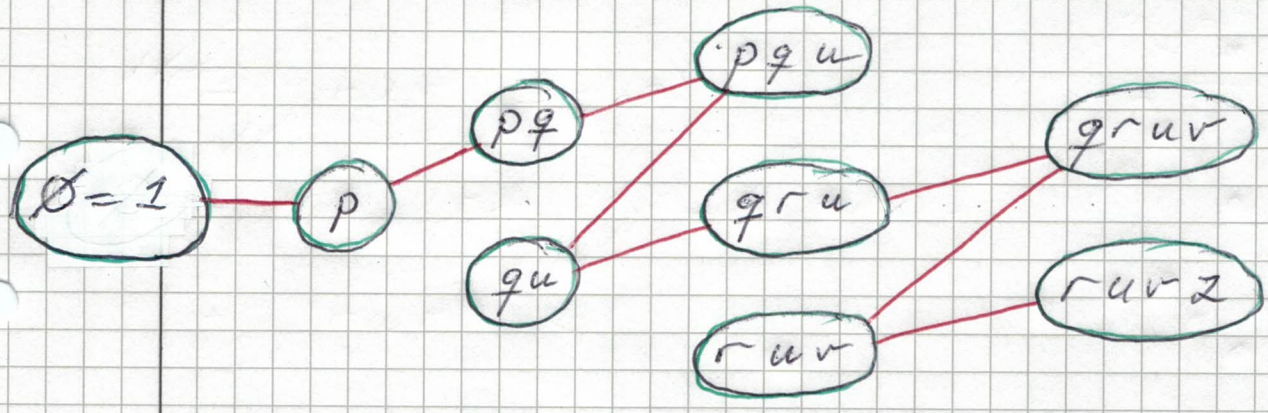
$$\sum_i = \sum_{v \in V} g_v \cdot A_v + \sum g_{sink} \cdot A_{sink} = 1$$

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

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

Note that g_{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 $H(\pi)$ from $\emptyset \equiv 1$ to some U s.t. $z \in U$
- This corresponds to (half of) a valid pebbling P
- $space(P) \leq Deg(\pi)$ by construction
- $time(P) \leq 2 \cdot |E(H(\pi))| \leq 2 \cdot \frac{S(\pi) - 1}{2}$

$$= S(\pi) - 1$$

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 improvements 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 [dRNNR '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) $\mathrm{Deg}_{NS}(F_n \vdash 1) \leq d_1 = O(\sqrt[6]{n} \log n)$.

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

(iii) For any NS refutation $\pi : F_n \vdash 1$ such that $\mathrm{Deg}(\pi) \leq K d_2 / \log n = O(\sqrt[3]{n})$ 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