PROOF COMPLEXITY AS A COMPUTATIONAL LENS

LECTURE 17

Continue to explore space complexity in resolution and polynomial calculus (by which we mean PCR, i.e., we have dual variables x & $\bar{x}$)

Focus on $\boxed{\text{CLAUSE SPACE}}$ in resolution and $\boxed{\text{MONOMIAL SPACE}}$ in PCR — space measures that count same objects as size measures

Let us compare and contrast what we know about these measures:

① Same (tight) space lower bounds for
- pigeonhole principle (PHP) formulas
- graph PHP formulas
- Tseitin formulas for expander graphs with two copies per edge
- random k-CNF formulas

[LAST TIME: Result by [Bonacina & Galesi '15]
Simplified exposition by [LMNV '26]

② Some space lower bounds for resolution remain open (but very believable) for PCR
- 3-CNF version of PHP
- functional PHP (3-CNF version or not doesn't matter [FLMNV '25])
- Tseitin for any expander
- ordering formulas
- pebbling formulas

And Bonacina-Galesi framework provably doesn't work!

Let F_n denote k-CNF formula over n variables for $k = O(1)$

So $S(F_n) = |F_n| = |Vars(F_n)| = \Theta(n)$

(3) $\boxed{Sp_R(F_n \vdash \bot) \geq W_R(F_n \vdash \bot) + O(1)}$ [AD'08]

(4) Clause space almost maximally separated from width & length/size: $\exists F_n$

$$Sp_R(F_n \vdash \bot) = \Omega(n/\log n)$$
$$W_R(F_n \vdash \bot) = O(1)$$
$$L_R(F_n \vdash \bot) = O(n)$$

[BN'08]

(5) Slightly stronger separation in polynomial calculus: $\exists F_n$

$$MSp_{PCR}(F_n \vdash \bot) = \Omega(n)$$
$$Deg_{PC}(F_n \vdash \bot) = O(1)$$
$$S_{PC}(F_n \vdash \bot) = O(n \log n)$$

but depends on field characteristic!

Shown for $GF(2)$ by [FLMNV'25]

(Seems generalizable to any finite characteristic.)

So clause space in resolution and monomial space in PCR seem very similar

And we have no separations between clause space and monomial space!

But many open problems for space in PCR

Today: Monomial space v.s. resolution width

Previously known:

$$\boxed{MSp(F[\oplus_2] \vdash \bot) = \Omega(W(F \vdash \bot))}$$

[FLMNV '25], from 2013

Right bound, but we want it without xorification

Galesi, Kołodziejczyk, Thapen [conference 2019, journal 2025]

THEOREM A

If F is a k-CNF formula such that $MSp_{PCR}(F \vdash \bot) = s$, then $W_R(F \vdash \bot) \leq s^2 - s + k$

As a by-product, we get a very clean proof of the following result by [Bonacina '16]

THEOREM B

If F is a k-CNF formula such that $W(F \vdash \bot) > w \geq k$, then $TotSp_R(F \vdash \bot) > w^2/8$.

Let us recall some formal definitions to make the meaning of these two theorems precise.

Let $\mathcal{P}$ be sequential, implicational proof system, i.e.,

(a) proofs are sequences of lines

(b) every line is a constraint in input $\left(\begin{array}{c}\text{today:}\\ \text{CNF formula}\end{array}\right)$ or is implied by previous lines

$\boxed{\text{CONFIGURATION-STYLE}}$ derivation (or CONFIGURATIONAL derivation)

$\pi = (\mathbb{M}_0, \mathbb{M}_1, \ldots, \mathbb{M}_\tau)$ where CONFIGURATIONS $\mathbb{M}_t$ are sets of constraints of syntactic type specified by $\mathcal{P}$

$\mathbb{M}_0 = \emptyset$

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

(i) AXIOM DOWNLOAD of input or proof system axiom $\quad \mathbb{M}_t = \mathbb{M}_{t-1} \cup \{A\}$

(ii) INFERENCE of new constraint by derivation rules applied to $\mathbb{M}_{t-1}$ $\quad \mathbb{M}_t = \mathbb{M}_{t-1} \cup \{C\}$

(iii) ERASURE $\mathbb{M}_t \subseteq \mathbb{M}_{t-1}$

REFUTATION if $\perp \in \mathbb{M}_\tau$

Let $\mathcal{M}$ be a space measure for configurations, e.g.:

$\boxed{Sp(\mathbb{M})}$ = # clauses in $\mathbb{M}$

$\boxed{MSp(\mathbb{M})}$ = # monomials in $\mathbb{M}$

$\boxed{TotSp(\mathbb{M})}$ = total # literals in $\mathbb{M}$ counted with repetitions

Then $\mathcal{M}(\pi) = \max_{\mathbb{M}_t \in \pi} \{\mathcal{M}(\mathbb{M}_t)\}$

$$\mathcal{M}(F \vdash \perp) = \min_{\pi : F \vdash \perp} \{\mathcal{M}(\pi)\}$$

The PCR space lower bounds hold for a slightly stronger proof system, which we can call $\boxed{\text{FUNCTIONAL MONOMIAL CALCULUS}}$ (FMC)

(Avoiding notational decision whether 0/1 is true/false)

An FMC configuration of space s is a Boolean function $\mathbb{M} : \{0,1\}^s \to \{\top, \bot\}$ together with s monomials $m_1, \ldots, m_s$ over $\{x_i, \overline{x}_i \mid i \in [n]\}$

An $\boxed{\text{FMC refutation}}$ of F is a sequence of FMC configurations $\pi : (\mathbb{M}_0, \mathbb{M}_1, \ldots, \mathbb{M}_\tau)$ such that

- $\mathbb{M}_0$ is $\top$ (function of arity 0 evaluating to true)
- $\mathbb{M}_\tau$ is $\bot$ (— " — false)
- for all $t \in [\tau]$ $\mathbb{M}_t$ follows from $\mathbb{M}_{t-1}$ by

  AXIOM DOWNLOAD $\quad \mathbb{M}_t = \mathbb{M}_{t-1} \wedge A$ for some $A \in F$

  INFERENCE $\quad \mathbb{M}_{t-1} \vDash \mathbb{M}_t$

  (but note that the configurations can be over different sets of monomials)

Clearly, FMC space is a lower bound on PCR monomial space. In particular, FMC only counts distinct monomials

RESOLUTION TOTAL SPACE IS WIDTH SQUARED

Recall the Prosecutor - Defendant game that characterizes resolution

DEF Let F be a k-CNF formula. A $\boxed{\text{MEMORY-}w}$ $\boxed{\text{DEFENDANT STRATEGY}}$ for F is a non-empty family of partial truth value assignments $\mathcal{A}$ to $Vars(F)$ such that for each $\alpha \in \mathcal{A}$

(i) $|dom(\alpha)| \leq w$

(ii) If $\beta \subseteq \alpha$, then $\beta \in \mathcal{A}$

(iii) If $|dom(\alpha)| < w$ and $x \in Vars(F) \setminus dom(\alpha)$, then $\exists\, \beta \supseteq \alpha$ in $\mathcal{A}$ such that $x \in dom(\beta)$

(iv) α does not falsify any clause in F

To save typing in what follows, we will allow ourselves to write $|\alpha| = |dom(\alpha)|$.

LEMMA 1 [AD08]
Let F be a k-CNF formula and $w \geq k$. Then $W_R(F \vdash \bot) > w$ if and only if there exists a memory-$(w+1)$ Defendant strategy for F.

Recall that Atserias and Dalmau used this characterization to prove a lower bound on clause space in terms of width

THEOREM 2 [AD '08]
If F is an unsatisfiable k-CNF formula (not containing the empty clause), then

$$Sp_R(F \vdash \bot) - 3 \geq W_R(F \vdash \bot) - k.$$

Proof sketch Suppose $W_R(F \vdash \bot) = s+k-3$.
We want to prove that $Sp_R(F \vdash \bot) \geq s$. (Assume $s > 3$, otherwise we are already done.)
Let π be derivation in space $< s$,
$\pi = (\mathbb{C}_0, \mathbb{C}_1, \ldots, \mathbb{C}_\tau)$.

Fix memory-$(s+k-3)$ Defendant strategy $\mathcal{A}$ (which exists since $W_R(F \vdash \bot) > s+k-4 \geq k$.
Inductively find $\alpha_t \in \mathcal{A}$ satisfying $\mathbb{C}_t$ and $|\alpha_t| \leq |\mathbb{C}_t|$. The only interesting case is axiom download, in which case $|\mathbb{C}_t| \leq (s-1)-2$ since we need space for one download plus at least one inference (or else we could erase before downloading. Enlarge α_{t-1} by asking about all $\leq k$ variables in downloaded axiom. By property (iv), get satisfying assignment to at least one literal ℓ in C.
Set $\alpha_t = \alpha_{t-1} \cup \{\ell\}$ and erase other literals ☐

THEOREM 3 [GKT '25]
Let F be a k-CNF formula and let $r, s \in \mathbb{N}$ with $r \geq k$. Suppose that F has a configuration style resolution refutation in which each configuration contains at most s clauses of width $> r$. Then $\boxed{W_R(F \vdash \bot) \leq 2r+s}$

COROLLARY [Bonacina '16]: THEOREM B
If $W_R(F \vdash \bot) > w \geq k = W(F)$, then $TotSp_R(F \vdash \bot) > w^2/8$.

Proof of Corollary

By contraposition. Suppose $\pi : F \vdash \bot$ has total space $\leq w^2/8$. Set $r = \lfloor w/4 \rfloor$ and $s = \lfloor w/2 \rfloor$. Clearly, no configuration in π can have more than s clauses of width $> r$.
Hence, by Thm 3 $W_R(F \vdash \bot) \leq 2r + s = w$. ▨

Proof of Thm 3

Let $\pi = (\mathbb{C}_0, \mathbb{C}_1, \ldots, \mathbb{C}_\tau)$ be a refutation as per the assumption in the theorem

Each $\mathbb{C}_t$ has some $\boxed{\text{narrow clauses}}$ $C_1, \ldots, C_q$, $W(C_i) \leq r$ and $\boxed{\text{wide clauses}}$ $D_1, \ldots, D_{s'}$ for $s' \leq s$, $W(D_j) > r$.

Suppose towards contradiction $W_R(F \vdash \bot) > 2r + s$

Fix $\boxed{\text{memory-}(2r+s+1)\text{-Defendant strategy } \mathcal{A}}$

Let $\boxed{R = \min \{ t \mid \exists \text{ narrow clause } C \in \mathbb{C}_t \text{ and } \alpha \in \mathcal{A} \text{ s.t. } \alpha(C) = \bot \}}$

Note that $R \leq \tau$, since $\bot \in \mathbb{C}_\tau$ is falsified by all $\alpha \in \mathcal{A}$. Fix such α and C

W.l.o.g $|\alpha| \leq W(C) \leq r$

C cannot be an axiom in F, so

$C = A \vee B$ for $A \vee x,\ B \vee \bar{x} \in \mathbb{C}_{R-1}$

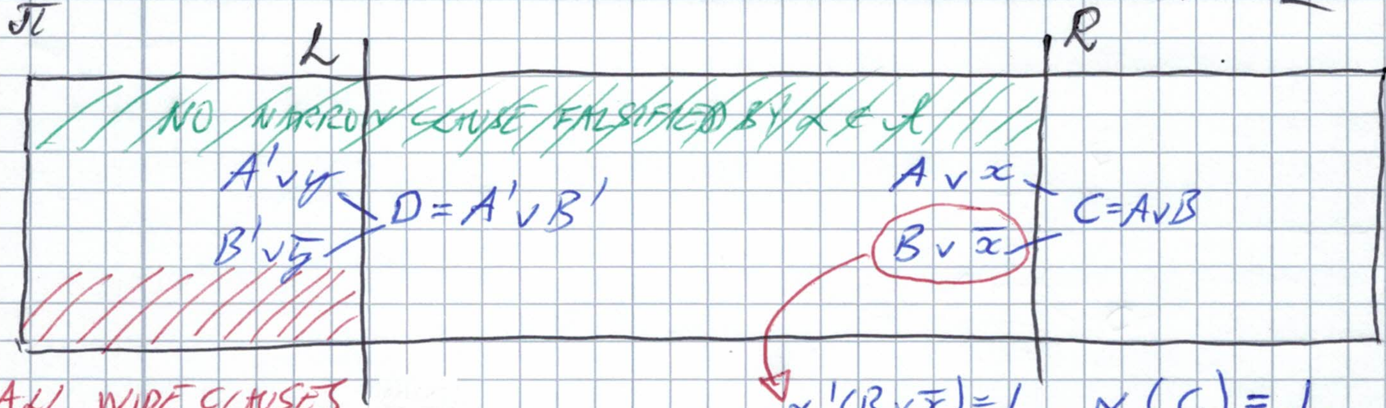
Extend α to $\alpha' \in \mathcal{A}$ s.t. $x \in \mathrm{dom}(\alpha')$

Suppose w.l.o.g. $\boxed{\alpha'(x) = \top}$

Then $\boxed{\alpha'(B \vee \bar{x}) = \bot}$

By minimality of R we have

$\boxed{W(B \vee \bar{x}) > r}$ W.l.o.g $\boxed{|\alpha'| \leq r + 1}$



ALL WIDE CLAUSES IN $\mathbb{C}_t$ SATISFIABLE BY SOME ASSIGNMENT $\beta_t \supseteq \alpha'$, $\beta \in \mathcal{A}$

$\alpha'(B \vee \bar{x}) = \bot$ $\quad$ $\alpha(C) = \bot$

$W(B \vee \bar{x}) > r$ $\quad$ $\alpha' \supseteq \alpha$

$\alpha'(x) = T$

$\beta(D) \neq T$

$\beta' \supseteq \beta$

$\beta'(y) = T$

$\beta'(B' \vee \bar{y}) = ?!$

Now let

$$\boxed{\mathcal{L} = \max\left\{ t \;\middle|\; t < R,\ \exists\, \beta \supseteq \alpha',\ \beta \in \mathcal{A},\ \beta \text{ satisfies all wide clauses in } \mathbb{C}_t \right\}}$$

Note that $\mathcal{L} \geq 0$ since no wide clauses to satisfy in $\mathbb{C}_0 = \emptyset$

Fix $\beta \supseteq \alpha'$ satisfying all wide clauses in $\mathbb{C}_{\mathcal{L}}$. W.l.o.g.

$$\boxed{|\beta| \leq |\alpha'| + s \leq r + s + 1}$$

i.e., β can be extended in $\mathcal{A}$ to any additional subset of $\leq r$ variables

$B \vee \bar{x}$ wide clause
$B \vee \bar{x} \in \mathbb{C}_{R-1}$

Since for $\alpha \subseteq \beta$ $\quad \alpha(B \vee \bar{x}) = \bot$

$$\boxed{\mathcal{L} < R - 1}$$

By maximality of $\mathcal{L}$, $\boxed{\mathbb{C}_{\mathcal{L}+1} = \mathbb{C}_{\mathcal{L}} \cup \{D\}}$ for

$\boxed{\text{wide clause } D \text{ not satisfied by any } \gamma \supseteq \beta \supseteq \alpha,\ \gamma \in \mathcal{A}}$ (*)

$D \notin F$ since axiom clauses have width $\leq k \leq r$ and so are narrow

Hence $\boxed{D = A' \vee B'}$ for $A' \vee y,\ B' \vee \bar{y} \in \mathbb{C}_{\mathcal{L}}$

Extend β to $\beta' \supseteq \beta$, $\beta' \in \mathcal{A}$ s.t. $y \in dom(\beta')$

Suppose w.l.o.g.

$\boxed{\beta'(y) = T}$ $\boxed{|\beta'| \leq |\beta| + 1 \leq r + s + 2}$

$\boxed{\text{We claim } \beta'(B' \vee \bar{y}) = T}$

But if so $\beta'(B') = T$

and since $B' \subseteq D$ also

$\beta'(D) = T$

contradicting (*) that no $\gamma \supseteq \beta$, $\gamma \in \mathcal{A}$, can satisfy D ↯

Case analysis to establish claim:

<u>$B' \vee \bar{y}$ is wide</u>: Then β satisfies $B' \vee \bar{y}$ by $\boxed{\text{definition of } \mathcal{L}}$.

<u>$B' \vee \bar{y}$ is narrow</u>: Then $W(B') = W(B' \vee \bar{y}) - 1 \leq r - 1$

Extend β' in $\leq r - 1$ steps to $\gamma \supseteq \beta'$, $\gamma \in \mathcal{A}$, s.t. $Vars(B \vee \bar{y}) \subseteq dom(\gamma)$

$$|\gamma| \leq |\beta'| + r - 1 \leq 2r + s + 1$$

Since $Vars(B \vee \bar{y}) \subseteq dom(\gamma)$, γ gives a truth value to $B \vee \bar{y}$.

By $\boxed{\text{minimality of } R}$ $\gamma(B' \vee \bar{y}) = T$ ▨

QUESTIONS

(Q1) Proof of Thm 2 can be made "Defendant-oblivious". Can use small-space resolution refutation to construct Prosecutor strategy that works against any Defendant (and hence convert small-space refutation syntactically to small-width refutation as shown in [FLMNV 15])
For proof of Thm 3, we need to inspect (non-existing) Defendant strategy to derive contradiction. Can we get a more constructive version of Thm 3

(Q2) Is it possible to prove an analogous result for total space in PCR?

Proof of Thm 3 at a high level

Fix Defendant strategy $\mathcal{A}$

For $\alpha \in \mathcal{A}$ and derived clause C, say

- α satisfies C if $\alpha(C) = \top$
- α kind-of-falsifies C if $\forall \beta \supseteq \alpha$, $\beta \in \mathcal{A}$ $\beta(C) \neq \top$

Extend to configurations in obvious way

Given $\pi = (\mathbb{C}_0, \ldots, \mathbb{C}_\tau)$, show that

- It can never happen that α satisfies $\mathbb{C}_{t-1}$ and pseudo-falsifies $\mathbb{C}_t$ if π is small-space
- But since $\mathbb{C}_0 \equiv \top$ and $\mathbb{C}_\tau \equiv \bot$ if π refutation, can find such a transition ↯

Space lower bound follows

This is (according to [GKT'25]) a simple version of $\boxed{\text{FORCING}}$ as used in bounded arithmetic and other areas of logic

We will need to develop this notion to prove monomial space $\geq \sqrt{\text{resolution width}}$

In what follows, fix

- k-CNF formula F
- memory-w Defendant strategy $\mathcal{A}$ $\quad k, w \in \mathbb{N}^+$

Assignments α, β will always be in $\mathcal{A}$

m denotes monomial over $Lits(F)$ (i.e., variables + negated variables)

Assignments are to $Vars(F)$ and so respect meaning of negation

DEFINITION (FORCING OF MONOMIALS)

For $\alpha \in \mathcal{A}$ and m over $Lits(\mathbb{F})$.

(i) α FORCES $m = 0$ if α assigns some literal in m to 0

(ii) α FORCES $m = 1$ if no $\beta \supseteq \alpha$, $\beta \in \mathcal{A}$, assigns any literal in m to 0

For $b \in \{0,1\}$ we write $\boxed{\alpha \Vdash m = b}$ if α forces $m = b$ and say that α FORCES m

(In [GKT 19, GKT '25], α DECIDES or FIXES m if α forces $m = b$ for $b \in \{0,1\}$. We will just use the verb "force" regardless of whether value b is specified)

OBSERVATION 4 If for $\alpha \in \mathcal{A}$ $\alpha \Vdash m = b$, then for all $\beta \supseteq \alpha$, $\beta \in \mathcal{A}$, it holds that $\beta(m) \neq 1 - b$

$\beta \Vdash m = b$

That is, if α forces $m = b$, then no $\beta \supseteq \alpha$ can assign the opposite value $1 - b$ to m as long as $\beta \in \mathcal{A}$

DEFINITION (FORCING OF POLYNOMIALS AND CONFIGURATIONS)

For $\alpha \in \mathcal{A}$ and polynomial $p = \sum_i a_i m_i$, $a_i \in \mathbb{F}$

α $\boxed{\text{FORCES}}$ p if it forces all monomials in p

If so, α forces $p = c$, $\boxed{\alpha \Vdash p = c}$, if

$\forall i$ $\alpha \Vdash m_i = b_i$ for $b_i \in \{0,1\}$ such that $c = \sum a_i b_i$

α $\boxed{\text{FORCES}}$ p TO TRUE, denoted $\boxed{\alpha \Vdash p}$, if $\alpha \Vdash p = 0$

For a configuration $\mathbb{M} = \{p_1, \ldots, p_m\}$

α FORCES $\mathbb{M}$ TO TRUE, denoted $\alpha \Vdash \mathbb{M}$, if

$\alpha \Vdash p$ for all $p \in \mathbb{M}$

α $\boxed{\text{FORCES } p \text{ TO FALSE}}$, denoted $\boxed{\alpha \Vdash \neg p}$,
if $\alpha \Vdash p = c$ for $c \neq 0$

α FORCES $\mathbb{M}$ TO FALSE, denoted $\alpha \Vdash \neg \mathbb{M}$,
if α forces all $p \in \mathbb{M}$ and
$\exists\, p \in \mathbb{M}$ such that $\alpha \Vdash \neg p$

For a functional monomial calculus configuration
$\mathbb{M} : \{m_1, \ldots, m_s\} \rightarrow \{\top, \bot\}$, α FORCES $\mathbb{M}$ to
TRUE [or FALSE] if for all $i \in [s]$ $\alpha \Vdash m_i = b_i$
for $b_i \in \{0,1\}$ such that
$$\mathbb{M}(b_1, \ldots, b_s) = \top \;[\text{or } \mathbb{M}(b_1, \ldots, b_s) = \bot].$$

The forcing relation can behave in unintuitive ways.

EXAMPLE 5 If $\alpha \in \mathcal{A}$, $|\alpha| = w$, and
$x \notin dom(\alpha)$, then $\alpha \Vdash x = 1$ and $\alpha \Vdash \bar{x} = 1$
(since there is no $\beta \supsetneq \alpha$, $\beta \in \mathcal{A}$)

But things are nicer when $\alpha \in \mathcal{A}$ is not too large.

OBSERVATION 6 If $\alpha \in \mathcal{A}$, $|\alpha| \leq w - k$, and
$C \in F$, then:
(i) There is $\beta \supseteq \alpha$, $\beta \in \mathcal{A}$, such that $\beta(C) = \top$
(ii) Hence, α does not force C to false

PTO for proof

EXAMPLE 7 Recall that a problematic scenario we
had for PCR space was when from $F = \bigwedge_{i=1}^{n} \bar{x}_i$
we could derive configuration $\mathbb{P} = \{1 - \prod_{i=1}^{n} x_i\}$
which could not be forced to true by small assignments
If $\mathcal{A}$ is memory-w strategy and $\alpha \in \mathcal{A}$, $|\alpha| \leq w$,
then $\alpha \Vdash 1 - \prod_{i=1}^{n} x_i$
This is so since no $\beta \supseteq \alpha$, $\beta \in \mathcal{A}$, sets $x_i = 0$
— this would violate an axiom clause

Proof of Obs 6: Since $|\alpha| \leq w-k$, can extend to $\beta \supseteq \alpha$, $\beta \in \mathcal{A}$, $Vars(C) \subseteq dom(\beta)$.
Since $\beta \in \mathcal{A}$ does not falsify $C \in F$, we have $\beta(C) = T$. ☒

OBSERVATION 8 Let $\alpha \in \mathcal{A}$ and let $\mathbb{M}$ be a PCR or FMC configuration. Then it cannot be that $\alpha \Vdash \mathbb{M}$ and $\alpha \Vdash \neg\mathbb{M}$ both hold.

Proof It can never be the case that $\alpha \Vdash m = 0$ and $\alpha \Vdash m = 1$ simultaneously, and so $\alpha \Vdash p$ and $\alpha \Vdash \neg p$ can never hold simultaneously for any polynomial and no Boolean function over monomials can be forced to more than one value. ☒

LEMMA 9 Let $\alpha \in \mathcal{A}$ and let $m_1, \ldots, m_s$ be monomials. Then $\exists \beta \in \mathcal{A}$, $\beta \supseteq \alpha$ such that β forces all m_i and $|\beta| \leq |\alpha| + s$

Proof By induction over #monomials s
Consider m_1. If $\exists \gamma \supseteq \alpha$, $\gamma \in \mathcal{A}$, setting literal ℓ in m_1 to 0, let $\beta := \alpha \cup \{\ell \to 0\}$. Since $\beta \subseteq \gamma$ it holds that $\beta \in \mathcal{A}$. If there is no such γ, $\beta = \alpha$ forces $m_1 = 1$. ☒

This means that if $\alpha \in \mathcal{A}$ is not too large and $\mathbb{M}$ does not have too large space, then $\exists \beta \supseteq \alpha$, $\beta \in \mathcal{A}$ forcing $\mathbb{M}$. And such forcing is consistent with some truth value assignment

LEMMA 10 Let $\alpha \in \mathcal{A}$, $|\alpha| < w$, and suppose $\alpha \Vdash m_i = b_i$ for $i \in [s]$. Then α can be extended to a total truth value assignment α^* such that $\alpha^*(m_i) = b_i$ for $i \in [s]$.

Proof Construct α^* by setting $\alpha^*(\ell)=1$ for all literals ℓ in monomials m_i such that $\alpha \Vdash m_i = 1$. Set all remaining variables arbitrarily.

Claim α^* is a truth value assignment. If not, $\exists x \in m_i$ and $\bar{x} \in m_j$ where $\alpha \Vdash m_i = m_j = 1$. But this is impossible — since $|\alpha| < w$, α can be extended to $\beta \supseteq \alpha$, $\beta \in \mathcal{A}$ such that $x \in dom(\beta)$, and β sets either m_i or m_j to 0. ◻

Now we are ready to prove that no $\alpha \in \mathcal{A}$ can force successive configurations to true and then false.

In main tech lemma

LEMMA 11 Let $\mathcal{A}$ be a memory-w Defendant strategy for a k-CNF formula F for $w, k \in \mathbb{N}^+$, $k \geq 2$, and suppose $\alpha \in \mathcal{A}$ have size $|\alpha| \leq w-k$. Let $\mathbb{M}$ and $\mathbb{M}'$ be successive configurations in a PCR or FMC derivation from F. Then it cannot be the case that $\alpha \Vdash \mathbb{M}$ and $\alpha \Vdash \mathbb{M}'$.

Proof Either $\mathbb{M}' = \mathbb{M} \cup \{C\}$ for an axiom download of $C \in F$ or else $\mathbb{M} \vDash \mathbb{M}'$. Thus it is sufficient to prove the lemma when $\exists C \in F$ such that $\mathbb{M} \cup \{C\} \vDash \mathbb{M}'$. Suppose $\alpha \Vdash \mathbb{M}$ and $\alpha \Vdash \neg\mathbb{M}'$. Since $|\alpha| \leq w-k$, can extend to $\beta \supseteq \alpha$, $\beta \in \mathcal{A}$ such that $Vars(C) \subseteq dom(\beta)$ and $\beta(C) = T$ as in Observation 6. Choose α', $\alpha \subseteq \alpha' \subseteq \beta$ such that $\alpha'(C) = T$ and $|\alpha'| \leq |\alpha| + 1 < w$.

Let all monomials in $\mathbb{M}$ and $\mathbb{M}'$ be $m_1, \ldots, m_s$ and assume $\alpha \Vdash m_i = b_i$ for $i \in [s]$.

Note $\alpha' \Vdash m_i = b_i$ by Observation 4.

Hence $\alpha' \Vdash \mathcal{M} \wedge C$ and $\alpha' \Vdash \neg \mathcal{M}'$.

Use Lemma 10 to obtain $\alpha^* \supseteq \alpha$ such that

$\alpha^*(\mathcal{M} \wedge C) = \top$ and $\alpha^*(\mathcal{M}') = \bot$

But this contradicts $\mathcal{M} \wedge C \vDash \mathcal{M}'$ $\lightning$ $\square$

Proof idea 1 Given refutation $\pi = (\mathcal{M}_0, \ldots, \mathcal{M}_\tau)$

For any $\alpha \in \mathcal{A}$ $\alpha \Vdash \mathcal{M}_0 = \emptyset$ $\alpha \Vdash \neg \mathcal{M}_\tau = \{\bot\}$

Use Lemma 9 to find $\alpha_t \in \mathcal{A}$ forcing $\mathcal{M}_t$

Use Lemma 11 to argue $\alpha_t \Vdash \mathcal{M}_t$

Reach contradiction for α_τ and $\mathcal{M}_\tau = \{\bot\}$

Problem: α_t can grow by additive s at each step.

Missing: Locality lemma for erasures

But if for large $\alpha \in \mathcal{A}$ and high-degree m it holds that $\alpha \Vdash m = 1$, can we expect that this holds for small $\alpha' \subseteq \alpha$?

Proof idea 2 [GKT '25]

Make inductive proof scanning π from both ends

Grow $\alpha \in \mathcal{A}$ by size $\approx s$ only $\approx s$ times.

Possible if $W_R(F \vdash \bot) \gtrsim s^2$

We prove following theorem.

THEOREM A'

$MS_{Pcr}(F \vdash \bot) \leq s \Rightarrow W_R(F \vdash \bot) \leq 2s(s+1) + W(F)$

For functional monomial calculus, can improve this to $W_R(F \vdash \bot) \leq 2s^2 + W(F)$

For PCR, can get $W_R(F \vdash \bot) \leq s^2 - s + W(F)$

(Basically just more careful counting — we focus on main ideas)

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

$\pi = (\mathbb{M}_0, \ldots, \mathbb{M}_\tau)$ 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 $\alpha \in \mathcal{A}$

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

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

$\alpha \in \mathcal{A}$ GUARANTEES r 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

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 $MSp(\mathbb{M}) \leq s$ 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 $|\beta| \leq |\alpha| + s - r$.

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 $MSp(\mathbb{M}) \leq s$ 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 $|\beta| \leq |\alpha| + s - r$.
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 $m_1, \ldots, m_{s'}$, $s' \leq s$
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 $\gamma \supseteq \beta$, 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 M_t, $t \in [L, R]$
Using Lemma 11, it follows by induction over $t \in [L, R]$ that $\alpha_s \Vdash M_t$
But then $\alpha_s \Vdash M_R$ and $\alpha_s \Vdash \neg M_R$
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 $\alpha_0 = \emptyset$, $L_0 = 0$, $R_0 = \tau$. $\emptyset \Vdash M_0 \equiv \top$ and $\emptyset \Vdash \neg M_\tau$ for $M_\tau \equiv \bot$ 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 $|NZ(M_{t'}, \beta')| = r$ and $\beta' \Vdash M_{t'}$
(b) No such t' exists

In case (b), α_r must guarantee $\geq r+1$ non-zero
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

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

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

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

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

Since $|\alpha'| \leq w - k$, 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

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

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

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

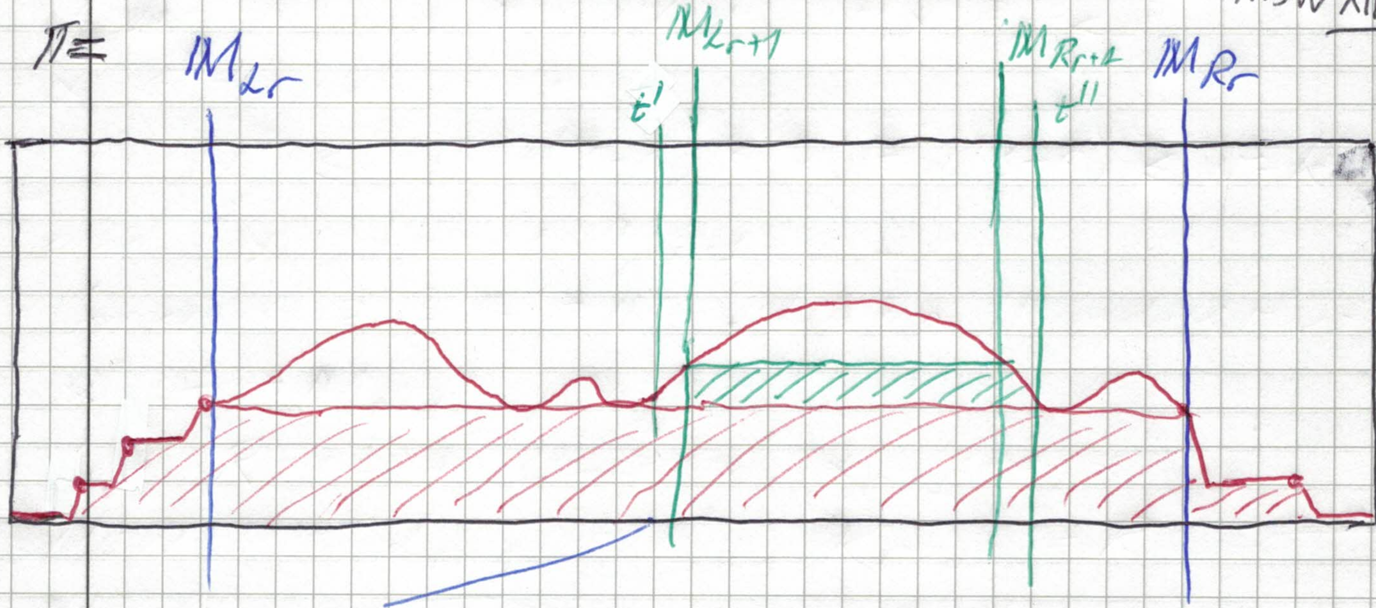
For condition (ii) we know that α_r guarantees r non-zeros in $\pi[L_r, R_r]$. By the choice of L_{r+1} and R_{r+1} we know for $\gamma \in \mathcal{A}$, $\gamma \supseteq \alpha''$ and $t \in [L_{r+1}, R_{r+1}]$ that

$|NZ(\mathbb{M}_{t}, \gamma)| \neq r$

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

$\blacksquare$

$\pi =$



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

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

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

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

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

Summary of open problems

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

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

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

4. Can the bound for k-CNF formulas
$$MSp(F \vdash \perp) = \Omega\left(\sqrt{W(F \vdash \perp)}\right)$$
be improved to $\Omega(W(F \vdash \perp))$?
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
$$MSp(\mathcal{P} \vdash \perp) = \Omega\left((Deg(\mathcal{P} \vdash \perp))^{\delta}\right)$$
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

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

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]