LECTURES 12 AND 13

~~OP I~~
12/13 : I

Talked in lec 4 (and 4½) about black-white pebble game

$\Rightarrow$ pebbling formulas

DAG G with constant fan-in (~~today~~ = 2) and unique sink z

- for each source vertex s, unit clause s
- for each non-source w with immediate predecessor u, v, clause $\overline{u} \vee \overline{v} \vee w$
- for sink, unit clause $\overline{z}$

Rough correspondence

- If there is a pebbling strategy for G in small time and space, then $\exists$ resolution refutation in short length and small total space
- If $\exists$ res ref in small length and small variable space, then $\exists$ pebbling in small time and space

Variable space

- ~~of~~ configuration $\mathbb{C}$ $VarSp(\mathbb{C}) = |Vars(\mathbb{C})|$
- of derivation $\pi = \{\mathbb{C}_0, \mathbb{C}_1, \ldots, \mathbb{C}_\tau\}$
  $VarSp(\pi) = \max_{\mathbb{C} \in \pi} \{VarSp(\mathbb{C})\}$
- of refuting F $VarSp(F \vdash \bot) = \min_{\pi : F \vdash \bot} \{VarSp(\pi)\}$

[12/13: I½

Questions about resolution left open after autumn term

Q1 If (k-CNF formula) F is easy wrt length, is it easy wrt clause space?

Q2 If F is refutable in length L and clause space s, can it be refuted in length O(L) and space O(s) simultaneously?

Q3 Since any formula F in size n is refutable in clause space O(n), is it true that a minimal-length refutation of F can be carried out in space O(n)

Answers [this and next lecture]

1. No, on the contrary maximally easy formulas wrt length can be maximally hard wrt space [BN08]

2. No, in worst case no meaningful simultaneous optimization of length and clause space possible [BN11]

3. No, even though linear clause space always possible, this can incur superpoly length blow-up [BBI11]

<u>Today</u>: start proving ① and ②

12/13: <u>II</u>

Interesting graphs yield promising formulas (all explicitly constructible)

<u>THM 1</u> $\exists$ 3-CNF formulas F_n of size $\Theta(n)$ s.t. $\mathcal{L}(F_n \vdash \bot) = O(n)$ but $VarSp(F_n \vdash \bot) = \Omega(n/\log n)$.

Follows from graphs analyzed in [PTC77, GT78]

<u>THM 2</u> Let $g(n)$, $\omega(1) = g(n) = O(n^{1/7})$ be any non-constant monotone function and fix any $\varepsilon > 0$. Then $\exists$ 3-CNFs F_n s.t.

- $TotSp(F_n \vdash \bot) = O(g(n))$
- $\exists\ \pi_n : F_n \vdash \bot$ s.t. $\mathcal{L}(\pi_n) = O(n)$ and $TotSp(\pi_n) = O\left((n/(g(n))^2)^{1/3}\right)$
- Any $\pi_n : F_n \vdash \bot$ ~~s.t.~~ $VarSp(\pi_n) = O\left((n/(g(n))^2)^{1/3 - \varepsilon}\right)$ has superpolynomial length $\mathcal{L}(\pi_n) = n^{\omega(1)}$

Follows from [CS80, CS82, Nor10].

<u>THM 3</u> Let K be sufficiently large constant. Then $\exists$ 3-CNFs F_n and a constant $K' \ll K$ s.t.

- $TotSp(F_n \vdash \bot) \leq K' \cdot n/\log n$
- $\exists\ \pi_n : F_n \vdash \bot$ s.t. $\mathcal{L}(\pi_n) = O(n)$ and $TotSp(\pi_n) = O(n)$
- Any $\pi_n : F_n \vdash \bot$ s.t. $VarSp(\pi_n) \leq K \cdot n/\log n$ has $\mathcal{L}(\pi_n) = \exp(n^{\Omega(1)})$.

Follows from [LT82]

Seems like promising formulas...
Only one problem.
All pebbling formulas refutable
in linear length and constant clause space
simultaneously $\Rightarrow$ No trade-offs!

What to do? Make formulas F a little bit harder
by substitution (Now 1 = TRUE again)

- Fix some Boolean function $f : \{0,1\}^d \to \{0,1\}$
  [eg $f(x_1, x_2) = x_1 \oplus x_2$ exclusive or]
  NOTATION $\boxed{\vec{x} = x_1, \ldots, x_d}$
- Replace every ~~variable~~ literal x with $f(x_1, \ldots, x_d)$
  and $\overline{x}$ with $\neg f(x_1, \ldots, x_d)$
- Expand out to new CNF formula
  $F[f]$

<u>Example</u> $C = \overline{x} \vee y \qquad f(x_1, x_2) = x_1 \oplus x_2$

$$\Downarrow$$

$$\neg(x_1 \oplus x_2) \vee (y_1 \oplus y_2)$$

$$\Downarrow$$

$$C[f] = \begin{array}{l} x_1 \vee \overline{x_2} \vee y_1 \vee y_2 \\ x_1 \vee \overline{x_2} \vee \overline{y_1} \vee \overline{y_2} \\ \overline{x_1} \vee x_2 \vee y_1 \vee y_2 \\ \overline{x_1} \vee x_2 \vee \overline{y_1} \vee \overline{y_2} \end{array}$$

If $W(F) = O(1)$ $F[f]$ at most constant factor size blow-up and also $W(F[f]) = O(1)$.

How refute $F[f]$?

One approach: mimic $\pi : F \vdash \bot$.

When π derives C, let π_f derive set of clauses $C[f]$

Obviously $L(\pi_f) \geq L(\pi)$

But also terrible space blow-up: $Sp(\pi_f) \geq VarSp(\pi)$

So surely we would want to do better...

But this is impossible! [BN 21]

<u>Idea of proof</u> (won't work, but good intuition)

Given resolution refutation π_f of $F[f]$, "extract" the refutation $\pi : F \vdash \bot$ that π_f is mimicking.

[Suppose again $f = \oplus$]

$F[\oplus]$ refutation blackboard	Shadow F refutation blackboard
If D_t implies e.g. $\neg(x_1 \oplus x_2) \vee (y_1 \oplus y_2) \ldots$	Write $\overline{x} \vee y$ on shadow blackboard. Do this for all ~~implications~~ such
In this way $\pi_f = \{D_0, D_1, \ldots, D_\tau\}$ gets translated ...	to resolution refutation $\pi = \{C_0, C_1, \ldots, C_\tau\}$ of F (w/ hope)
is upper bounded by $L(\pi_f)$	Length of $\underbrace{\pi \ldots}_{L(\pi)}$
is ~~lower bound~~ upper-bounded by $Sp(D_t)$	Variable space $VarSp(C_t)$ ...

If this worked, we would get trade-offs between length and clause space. This is a bit too optimistic, but we can do sth similar to get same results.

First need to show that $F[f]$ is not too hard

LEMMA 4

F unsat CNF $\quad f : \{0,1\}^d \to \{0,1\}$ Boolean func

If $\exists$ res ref $\pi : F \vdash \bot$ with

$$L(\pi) = L$$
$$TotSp(\pi) = s$$
$$W(\pi) = w$$

then $\exists$ res ref $\pi_f : F[f] \vdash \bot$ with

$$L(\pi_f) = L \cdot \exp(O(dw))$$
$$TotSp(\pi_f) = s \cdot \exp(O(dw))$$
$$W(\pi_f) = O(dw)$$

In particular, if $W(\pi) = O(1)$ then this is just a constant factor blow-up.

<u>Proof sketch</u>: Simulate π step-by-step

If π downloads axiom C, let π_f download all axioms in $C[f]$. (at most $\exp(O(d \cdot W(C)))$ clauses). If π resolves $C_1 \vee x$ and $C_2 \vee \bar{x}$ to derive $C_1 \vee C_2$, let π_f derive $(C_1 \vee C_2)[f]$ from $(C_1 \vee x)[f]$ and $(C_2 \vee \bar{x})[f]$.

When C is erased in π, erase $C[f]$ in π_f.

Details need to be checked, but this works.

We want to "project" any config $\mathbb{D}$ derived from $F[f]$ to $\mathbb{C}$ derived from F.

Intuition: if $\mathbb{D}$ implies $\neg f(\vec{x}) \vee f(\vec{y})$, then $\mathbb{D}$ should project $\overline{x} \vee y$.

Useful to not over-specify, but describe conditions that projection should satisfy and prove theorems for any projection that works, and for any proof system

Notation

$$x^1 = x \qquad x^0 = \overline{x}$$

Opposite of lec 9 & 11, but right notation for resolution

x^b is true iff $x = b$

$$f^1(\vec{x}) = f(\vec{x}) \qquad f^0(\vec{x}) = \neg f(\vec{x})$$

DEF 5 [PROJECTION]

$f : \{0,1\}^d \to \{0,1\}$ Boolean func

P sequential proof system

$\mathbb{D}$ Boolean functions over

$$Vars^d(V) = \{x_1, \ldots x_d \mid x \in V\}$$

of form specified by P

$\mathbb{C}$ disjunctive clauses over V

Then $proj_f : \mathbb{D} \to \mathbb{C}$ is an f-projection if it is ... (PTO)

$\mathbb{D} \models C[f]$

<u>Complete</u> If $\mathbb{D} \cancel{\models} \bigvee_{x^b \in C} f^b(\vec{x})$
then $C \supseteq C' \in proj_f(\mathbb{D})$

<u>Nontrivial</u> If $\mathbb{D} = \emptyset$ then $proj_f(\mathbb{D}) = \emptyset$

<u>Monotone</u> If $\mathbb{D}' \models \mathbb{D}$ and $C \in proj_f(\mathbb{D})$
then $C \supseteq C' \in proj_f(\mathbb{D}')$

<u>Incrementally sound</u>
Suppose A clause over V
$L_A \in A[f]$ as encoded by $\mathcal{P}$
If $C \in proj_f(\mathbb{D} \cup \{L_A\})$ it
holds $\forall a \in Lit(A) \setminus Lit(C)$ that
$\overline{a} \vee C \supseteq C_a \in proj_f(\mathbb{D})$.

Any projection will turn a $\mathcal{P}$-refutation
of $F[f]$ into a resolution refutation of F.

LEMMA 6
$\mathcal{P}$ seq proof syst, $f: \{0,1\}^d \to \{0,1\}$,
$proj_f$ f-projection. Then if $\pi_f = \{\mathbb{D}_0, \mathbb{D}_1, \ldots, \mathbb{D}_\tau\}$
is a $\mathcal{P}$ refutation of $F[f]$, it holds that
~~π~~ $\{proj_f(\mathbb{D}_0), proj_f(\mathbb{D}_1), \ldots, proj_f(\mathbb{D}_\tau)\}$
is the "backbone" of a resolution refutation
π of F in the sense that (PTO)

1. $\mathrm{proj}_f(\mathbb{D}_0) = \emptyset$
2. $\bot \in \mathrm{proj}_f(\mathbb{D}_\tau)$
3. All transitions $\mathrm{proj}_f(\mathbb{D}_{t-1}) \rightsquigarrow \mathrm{proj}_f(\mathbb{D}_t)$ can be carried out in resolution in such a way that $VarSp(\pi) = O(\max_{\mathbb{D} \in \pi_f}\{VarSp(\mathbb{D})\})$
4. $L(\pi)$ is upper-bounded by $L(\pi_f)$ in the (weak) sense that the only time π does a download of $C \in F$ is when π_f downloads some $L_C \in C[f]$ from $F[f]$.

This lemma works for any proof system P! But to be interesting also need to relate space measures in π_f and π.

DEF 7 [Space-faithful projection]

P seq proof syst with space measure $Sp_P(\cdot)$
$f: \{0,1\}^d \to \{0,1\}$ fixed Boolean function.
proj_f f-projection.
proj_f is <u>space-faithful of degree K</u> wrt P if $\exists$ poly Q of deg K s.t. always

$$Q(Sp_P(\mathbb{D})) \geq |Vars(\mathrm{proj}_f(\mathbb{D}))|$$

Linearly space-faithful $\Leftrightarrow$ $K = 1$
Exactly — " — $Q(n) = n$

Smaller $K \Rightarrow$ tighter reduction between P and resolution