PROOF COMPLEXITY AS A COMPUTATIONAL LENS — SC I

LECTURE 15

Last lecture: size-space trade-offs in proof complexity from time-space trade-offs in pebbling

Roughly: If matching upper and lower bounds for black & black-white pebbling [or trade-offs for "not-too-white" black-white pebbling] then:
- size-space trade-offs with same parameters for resolution
- size-space trade-offs with log factor loss for polynomial calculus

EXAMPLE RESULTS

*) also need $g(n) = O(n^{1/3})$

THEOREM 1 [BN11] (using pebbling results in [Nordström '12])

Let $g(n) = \omega(1)$ be arbitrarily slowly growing function* and fix any $\varepsilon > 0$. Then $\exists$ explicitly constructible 6-CNF formulas $\{F_n\}_{n=1}^{\infty}$ of size $\Theta(n)$ such that

(a) F_n refutable in total space $O(g(n))$ in resolution and PC

(b) F_n refutable in simultaneous size $O(n)$ and total space $O\left(\left(n/(g(n))^2\right)^{1/3}\right)$ in resolution and PC

(c) Any resolution refutation ~~in clause space~~ PCR refutation in monomial space $O\left(\left(n/((g(n))^2/\log n)\right)^{1/3-\varepsilon}\right)$ must have super-polynomial size in resolution and PCR

THEOREM 2 [BN11] Using pebbling results in [Nordström '12]

There is a family of explicitly constructible 6-CNF formulas of size $\Theta(n)$ such that

(a) F_n refutable in total space $O(n^{1/11})$ in resolution and PC

(b) F_n refutable in simultaneous size $O(n)$ and total space $O(n^{3/11})$ in resolution and PC

(c) Any resolution refutation PCR refutation in clause space monomial space at most $n^{2/11}/(10 \log n)$ must have size at least $(n^{1/11})!$ in resolution and PCR

Technical core: Lift trade-offs between length and variable space to trade-offs between size and clause space for resolution

For polynomial calculus:

- Use that variable space is the same measure as for resolution
- Do substitution with XOR + random restriction argument

Pebbling formulas just happen to have such nice trade-offs

OPEN PROBLEM 1: For these other such formulas?

OPEN PROBLEM 2: Can we get tight results also for polynomial calculus?

Strength and weakness of results:

- Upper bounds for total space and syntactic proof systems
- Lower bounds for clause space / monomial space and SEMANTIC PROOF SYSTEMS?
  Anything implied can be derived in single step

But in this model all formulas are refutable in simultaneous linear size and linear space.

Traditionally, time-space trade-offs look something like

$$(\text{Space}) \cdot (\text{Time}) \geq n^2$$

or stronger

$$(\text{Space}) \cdot \log(\text{Time}) \geq n$$

These results say nothing about superlinear space

Recall question from last lecture:

> If F is refutable in length/size L, can F be refuted in length $\text{poly}(L)$ and linear clause/monomial space $O(S(F))$ simultaneously?

NO! For regular resolution and resolution [Beame, Beck, & Impagliazzo '12, '16]

Tight results for resolution + polynomial calculus

[Beck, Nordström, & Tang '13]

THEOREM 3 [BNT'13]
For $w = w(n)$ with $3 \le w(n) \le n^{1/4}$ there are explicitly constructible 3-CNF formulas $\{F_n\}_{n=1}^{\infty}$ of size $\Theta(n)$ such that

(a) F_n refutable in clause space $O(w \log n)$ and length $\exp(O(w \log n))$ in resolution

(b) F_n refutable in length $n^{O(1)} \exp(w)$ and clause space $\exp(w) + n^{O(1)}$ in resolution

(c) For any PCR refutation π_n over a field $\mathbb{F}$ s.t. $\mathrm{char}(\mathbb{F}) \neq 2$, the proof size is bounded by

$$S(\pi_n) = \left(\frac{\exp(\Omega(w))}{M_{\mathbb{F}}(\pi_n)} \right)^{\Omega\left(\frac{\log\log n}{\log\log\log n}\right)}$$

Fix $\boxed{w = K \log n}$ for suitably large constant K

Then resolution can refute formulas in

- length $\approx n^K$
- clause space $O(\log^2 n)$

But cause space, say, $n^{k/2}$ causes superpolynomial blow-up in proof size (Need to adjust constants for precise statement)

Beame, Beck & Impagliazzo have much sharper results for regular resolution

OPEN PROBLEM 3: Improve the parameters in the trade-offs in Thm 3. Is it possible to extend the much stronger trade-off results for regular resolution also to general resolution? What about exponential trade-offs? *

*) Not for the formulas we talk about today

Trade-off formulas: TSEITIN CONTRADICTIONS

Graph $G = (V, E)$

Charge function $\chi : V \to \{0,1\}$ such that $\sum_{v \in V} \chi(v) \equiv 1 \pmod 2$

(ODD CHARGE)

$$\text{PARITY}_{V,\chi} = \text{“} \sum_{e \ni v} x_e \equiv \chi(v) \pmod 2 \text{”}$$

$$= \left\{ \bigvee_{e \ni v} x_e^{1-b_e} \;\middle|\; \sum_{e \ni v} b_e \not\equiv \chi(v) \pmod 2 \right\}$$

Recall $x^b = \begin{cases} x & \text{if } b = 1 \\ \bar{x} & \text{if } b = 0 \end{cases}$

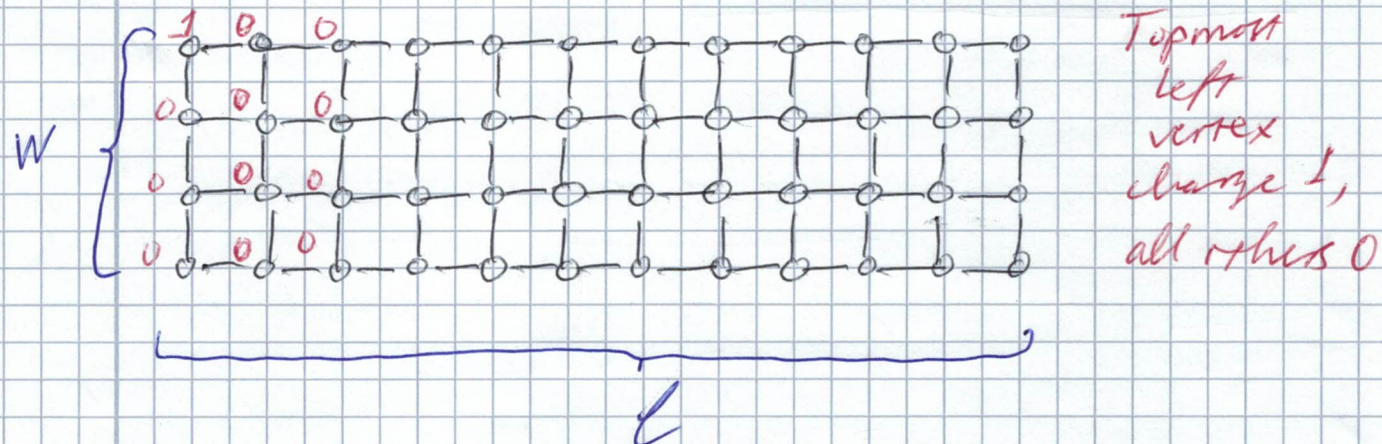
$$Ts(G,\chi) = \bigwedge_{v \in V} \text{PARITY}_{v,\chi}$$

Suppose G is connected.
Then $Ts(G,\chi)$ unsatisfiable
$\Leftrightarrow$
χ odd-charge function

Exact charge function does not matter – only whether charge is odd or even
Can use substitution to convert between different odd-charge functions

We know: G expander $\Rightarrow$ $Ts(G,\chi)$ exponentially hard

But we want only moderately hard formulas. Use rectangular grids with w rows and ℓ columns $(w \ll \ell)$



(We will need to tweak this a bit, but this is the idea

PROPOSITION 4

If F has resolution refutation in depth d, then tree-like resolution can refute F in simultaneous
- length $2^{d+1} - 1$
- clause space $d + 2$

Proof sketch
- Make resolution refutation tree-like — does not increase space
- # nodes in proof DAG $\leq 2^{d+1} - 1$
- Black-pebble proof DAG to get the stated bounds

□

PROPOSITION 5

Let G be $w \times l$ grid and let $\chi : V \to \{0,1\}$ be odd-charge function. Then $Ts(G, \chi)$ can be refuted in depth $O(w \log l)$

Proof sketch

Use that tree-like resolution ⇕ decision tree

Do binary search

Query middle column

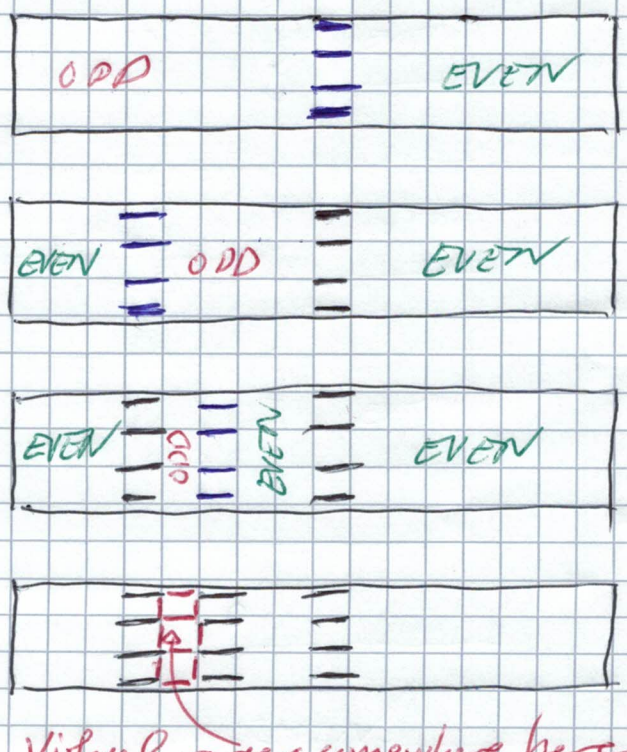
- disconnects graph

Recurse on odd-charge component

$O(\log l)$ recursive steps

w queries per step

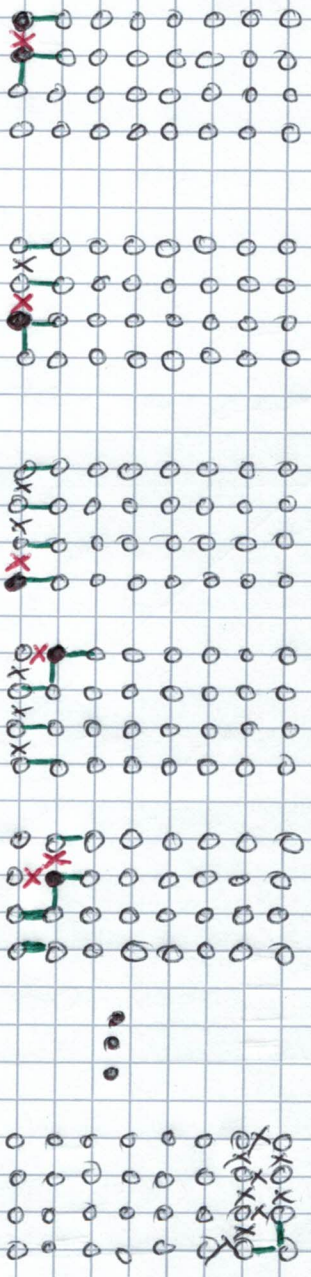
□



PROPOSITION 6

Let G $w \times l$ grid and χ odd-charge
Then $Ts(G, \chi)$ can be refuted in simultaneous length $l w 2^{O(w)}$ and clause space $2^{O(w)}$.

Proof Order edges from right to left and from top to bottom in each column
Resolve all clauses containing top left vertical edge
Keep resolvent in memory
Down load all axioms for third vertex in first column



FACT Resolving over all variables in fixed order yields resolution refutation
DAVIS-PUTNAM RESOLUTION
or VARIABLE ELIMINATION
Prove, e.g., by induction over # variables
In this case: Invariant is that sum of charges of cut edges is odd

Space $\leq w+1$ edges = variables $\Rightarrow \leq 2^{w+1}$ clauses

Length wl vertices $\times$ $2^{O(w)}$ steps per vertex ☐

w - parameter is tree-width of graph
This is special case of more general result.

How to prove trade-off?

HIGH-LEVEL IDEA

1. Formalize notion of PROGRESS of proof
2. Divide proof into large number of equal-sized EPOCHS
3. Prove the following claims:
   (a) If epochs are small, then no single epoch makes very much progress
   (b) If space is small, then not much progress can be carried over from one epoch to the next
   (c) To refute formula, proof needs to make substantial progress summed over all epochs
4. Hence, a proof that is too short and uses too little space cannot refute the formula