CSE 596 — Lecture Wed 11/14 — Fall 2018

To finish the PSPACE-completeness of TQBF, we initialize

$$\Phi_0(I,K) \equiv I = K \vee I \vdash_N K$$

as a qbf.

$I = \langle q, w, \vec{h} \rangle$

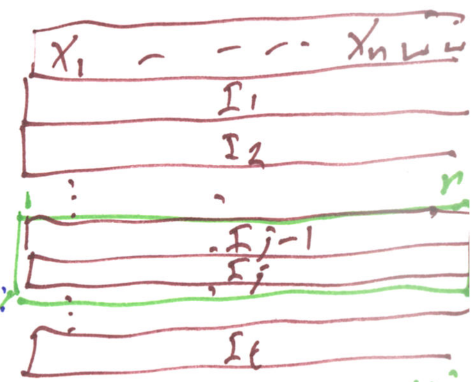
- q: state
- w: contents of $s(n)$ space not including the input x
- $\vec{h}$: head positions on k tapes.

$\therefore |I| = O(s(n)) \equiv_{def} r$. Hence we can represent I as an r-bit binary string using Boolean variables $x_1, \dots, x_r$. Say K uses $z_1 \dots z_r$.

$I = K$ then becomes $(x_1 = z_1) \wedge \cdots \wedge (x_r = z_r)$

$(x_1 = z_1) \equiv (x_1 \vee \bar{z}_1) \wedge (\bar{x}_1 \vee z_1)$

$I \vdash_N K$ uses two levels of the fmla from Cook-Levin:



Use that much

Need only $O(\log(r))$ space to keep track of what similar part you are outputting.

To output the final Φ_r, we just iterate the recursion:

$$\Phi_j = (\exists J)(\forall I', J')\left[\begin{matrix}(I' = I \wedge J' = J) \vee \\ (I' = J \wedge J' = K)\end{matrix}\right] \Rightarrow \Phi_{j-1}(I', J')$$

with (I, K) ... with

Allocates 3 new banks of vars

$I' = x'_1 \dots x'_r$

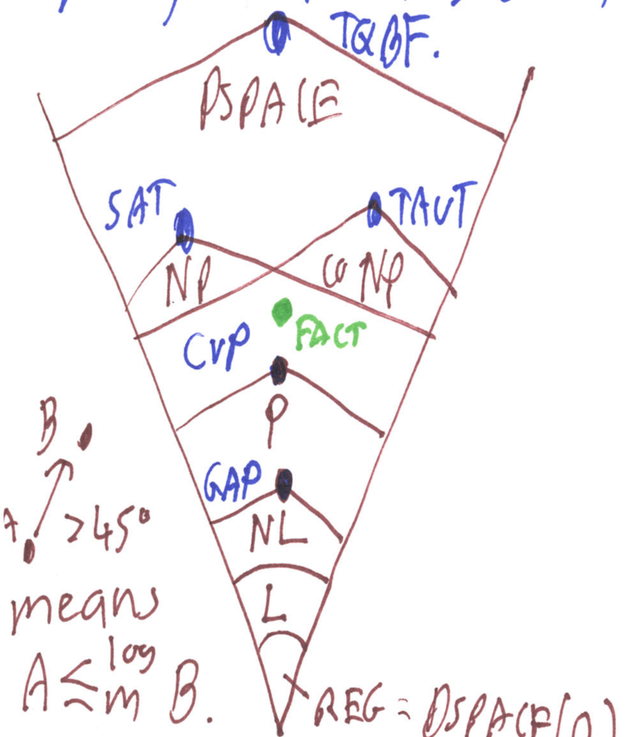
$J' = y'_1, \dots, y'_r$

$J = y_1, \dots, y_r$

At the very top level, allocate/fix $I^{(r)}$ as $I_0(x)$, $K^{(r)}$ as I_f.

Final qbf Φ_r has $O(r^2) = O(s(n)^2)$ size and is streamed computed in $O(\log s(n))$ space. When $s(n) = poly(n)$, this is a $\leq_m^{\log}$ reduction from ALL PSPACE to TQBF. ☒

Moreover, brute-force solving Φ_r decides A in $O(m^2) = O(s(n)^2)$ space, $\therefore$ NSPACE$[s(n)] \subseteq$ DSPACE$[s(n)^2]$ $\therefore$ Savitch's Theorem



means $A \le_m^{\log} B$.

Facts En-Route to the diagram:

- GAP is complete for NL under $\le_m^{\log}$. So NL = L $\iff$ GAP $\in$ L.

  GAP = $\{\langle G,s,t\rangle$: there is a path from s to t in the digraph $G\}$.

- The Circuit Value Problem CVP

  INST: A Boolean circuit C with n input gates and an $x \in \{0,1\}^n$.

  QUES: Is $C(x) = 1$?

  CVP is complete for P under $\le_m^{\log}$, so
  CVP $\in$ L $\iff$ P = L
  CVP $\in$ NL $\iff$ P = NL.

By Savitch, NL $\subseteq$ DSPACE$[(\log n)^2]$

which is not known to be within P because $2^{(\log n)^2}$ is > polynomial.

And PSPACE = NPSPACE.

Final Fact: NL = coNL, indeed for any $s(n)$ NSPACE$[s(n)]$ = co-NSPACE$[s(n)]$. Proof is Hard

FACTORING: As a function, if x is a number, $f(x)$ = its unique prime factorization. Can we do this in time $n^{O(1)}$ where $n = |x| = \Theta(\log_2 x)$?

As a language, FACT = $\{\langle x,w\rangle$: w is a prefix of the unique prime factorization of $x\}$

$\langle x,\varepsilon\rangle \in$ FACT. Is $\langle x,0\rangle \in$ FACT? $x = p_1^{a_1} \cdot p_2^{a_2} \cdots p_s^{a_s}$

Depends on binary code for <, ,, digits but $upf(x) = \langle p_1,a_1,p_2,a_2,\dots,p_s,a_s\rangle$ anyway, getting yes/no answer lets us build up the factorization bit-by-bit. Funny fact: $|upf(x)| = O(|x|)$!

FACT $\in$ NP $\cap$ coNP: whether w is right or wrong has the same witness of guessing $upf(x)$.