Last time:
- more on PH ("collapse theorem")
- oracles & oracle THs (r-PH)
- nonuniform computation, P/poly

\[ \varepsilon^P = NP \]

\[ \text{P/poly etc.} \]

Papad. 4.3, 11.4; AB ch. 6; Ca: 4.1, 4.2

Today:
- more nonuniformity: Boolean circuits
- P/poly corrs. to poly-size clts
- Karp-Lipton theorem \( \implies \) AB 6.4, Ca: 4.2, P. 17.3

\[ \text{NP has poly-size clts } \implies \text{PH collapses} \]

- Baker-Gill-Solovay thm: \( \implies \) AB 3.4, Ca: 12.1

- \( \exists \) oracle A s.t. \( P^A = NP^A \)

- \( \exists \) oracle B s.t. \( P^B \neq NP^B \)

Questions?

We saw P/poly: advice.

Another nonuniform model: Boolean circuits

\[ \text{(Cai: p. 52; elsewhere)} \]

\[ n = 4 \]

\[ 4 \text{ vars } \{0,1\}^4 \rightarrow \{0,1\} \]

This is a circuit
Any given ckt has some fixed # inputs.

Diff cchts for diff values of $n$: non-uniform model.

Why consider non-uniform comput.?
- get to do massive precompute. for each input length. Does this help?
- Cchts closer to reality than TMs: hardware, chips, etc.
- Seems to open new attack approaches for exity.

Convention: our cchts unless otherwise specified, are cchts over $\lor$, $\land$, $\lnot$.

Note:

\[ \begin{array}{c}
\text{fixed set} \\
A \text{ finite of gates that you allow for your cchts: a basis.}
\end{array} \]

A basis is universal if cchts over this basis can compute any Bool \( f : \{0,1\}^n \rightarrow \{0,1\} \).

Ex: Any $\lor$ is comput. as a DNF:
$\begin{align*}
\begin{array}{c}
\text{x} \\
\hline
0 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 \\
0 & 1 & 0 & 0 \\
1 & 1 & 1 & 1
\end{array}
\end{align*}$

\begin{align*}
\text{hence} \\
\{ v, \land_2, \lor \} \text{ is} \\
a \text{ univ. basis}
\end{align*}

\begin{align*}
\begin{array}{c}
\text{Some other univ. bases:} \\
\mathbb{F}_2^n
\end{array}
\end{align*}

\begin{align*}
\cdot \{ v, \land \} \quad \text{also} \quad \{ v, \lor \}
\end{align*}

\begin{align*}
\cdot \text{ } \mathbb{B}_2^4 = \text{ all } 16 \text{ } 2 \text{ var. f's} \quad \{0,1\}^2 \to \{0,1\}
\end{align*}

\begin{align*}
\cdot \text{ } \{ \text{NAND} \} \quad x \text{ NAND } y = 1 \text{ (x } \land \text{ y).} \\
\cdot \text{ } \{ \land_2, \lor_2 \}
\end{align*}

\begin{align*}
\begin{array}{c|c|c|c|c}
\text{x} & \text{y} & \text{x} \lor \text{y} & \text{x} \land \text{y} \\
\hline
0 & 0 & 0 & 1 \\
0 & 1 & 1 & 0 \\
1 & 0 & 1 & 0 \\
1 & 1 & 0 & 1
\end{array}
\end{align*}

\begin{align*}
\text{Some bases that are not univ:} \\
\cdot \{ \lor_2 \} \quad \text{(can only compute } \sum \text{ x; mod 2 \text{ for } s \leq [n] )}
\end{align*}

\begin{align*}
\cdot \{ \land_2, v_2 \} \quad \text{no neg: imposs. to compute } \overline{x_i} \\
\quad \quad \text{(univ. basis for class of all monotone Bool fags)}
\end{align*}

\begin{align*}
\begin{array}{c}
\text{uni. basis for class of all monotone Bool fags}
\end{array}
\end{align*}
Def: Let \( f : \{0,1\}^n \rightarrow \{0,1\} \). The circuit complexity of \( f \) is the \# of gates in the smallest (fewest gate) chf for \( f \).

Note: changing basis only affects by an \( O(1) \) factor.

- We don't count the inputs \( x_1, \ldots, x_n \) towards \# gates. (only \( n \) anyway).

Def: A function \( f : \{0,1\}^n \rightarrow \{0,1\} \) has chf complexity \( s(n) \) if \( \forall \, n, \) for \( \{0,1\}^n \) is computed by an \( s(n) \)-size chf.

Model: \( \{ \text{chf family} \ C_1, C_2, \ldots, C_n, \ldots \} \)

Def: \( \text{Lang } L \leq \{0,1\}^* \) has \( s(n) \)-size chfs if

- \( \exists \) chf fam \( \{C_1, C_2, \ldots \} \) s.t.
  - \( |C_n| \leq s(n) \)
  - \( \forall \, x \in \{0,1\}^n, \ C_{1^{x_1}}(x) = 1 \iff x \in L \).

"\( L \) has poly-size chfs": \( L \) has \( s(n) \)-size chfs for some poly \( s(n) \).

Ex: \( L = \{ x \in \{0,1\}^* : x \) has odd \# Is \}. PARITY (PAR)
Over $\mathbb{Z}_2$, $f_n$ is $\left( \sum_{i=1}^{n} x_i \right) \mod 2$.

\[ \equiv \text{PAR}_n \]

This $L \in P_{\text{poly}}$ has poly-size $\text{cks}$ of size $O(n)$.

Q: What languages have poly-size $\text{cks}$?

Thm: $L \in \text{P/poly}$ iff $L$ has poly-size $\text{cks}$.

(Poly-size $\text{cks} \equiv$ poly-time TMs with advice.)

PF: • Polytime TM w/ advice can sim. poly-size $\text{cks}$:

Have the advice string $\alpha_n$, encode $C_n$ $\alpha_n$;

the TM evaluates $C_n$ on $x$ ($|x| = n$).

• Poly size $\text{cks}$ can sim. polytime TMs w/ advice:

$(M; x_1, x_2, \ldots, x_n \ldots) \quad \forall n:$

There's a poly $(n)$ size $\text{ckt}$ which simulates
exec. of $M$ on $x$ with advice $\alpha_n$, outputs 1 iff
$M$ accepts $(x, \alpha_n)$. (circuitry)
Like Cook-Levin p.f. "unroll" comput. in space \(1x/n\).

Given \(M, x, 1x1\), we can write down a poly(n) x poly(n) square array where cell \((i,j) \leftrightarrow \text{tape location} j\) at time step \(i\).

\[\text{TM tape loc. of head state.}\]

\([x_1 \ x_2 \ x_3 \ldots]\]

\[\text{time } i\]

\[\text{poly(n)}\]

\[\text{poly(n)}\]

\(O(1)\) gates can capture state of \(M\) at time \(i\), whether or not tape head is at loc. \(j\), what's in tape cell \(j\).

\(i = 1\) : det. by \(x, x_1 x_1\).

\(i > 1\) : cell \((i, j)\) det. by cells \((i-1, j-1)\), \((i-1, j)\), \((i-1, j+1)\).

\(\text{polyn. size.}\)

\(\text{Special case:}\)

\(\text{Cor: } L \in P \Rightarrow L\ has\ p\text{-size ciks.}\)

\(\text{So... one way to attack } P \neq NP\ is to try to show that } (\text{say})\ \text{CLIQUE does not have } \text{polyn. size ciks.}\)
"circuit complexity"  
Feels like a plausible combinatorial angle to pursue...

Some big successes:

- **monotone**
  - CLIQUE has cKts over \{v, \bar{v}\}
  - But it's known that CLIQUE does not have poly(n)-size cKts over \{v, \bar{v}\}.

Karp-Lipton Thm  

How does P/poly relate to NP, PSPACE, etc?

"Feels like" P/poly "not that far from P"

But [P/poly \not\subset] NP \not\subset EXP

Even P/1 \not\subset DECIDABLE

\( \Rightarrow \) 1-bit \(\nu_n\): tells you whether (undecidable) the \(n\)th bitstring is / isn't in HALT.

Is NP \subseteq P/poly? We don't know, but prob. not... here's why
Karp-Lipton Thm:

If $\text{NP} \subseteq \text{P/poly}$ then $\text{PH} = \Sigma_2^P$.

If SAT has poly size cnfs then $\text{PH} = \Sigma_2^P$.

Recall: EO2 + Collapse Thm says:

If $\Pi_2^P \subseteq \Sigma_2^P$ then $\text{PH} = \Sigma_2^P$.

So fix $L \in \Pi_2^P$; plan is to use $\text{D}^L$ to show $L \in \Sigma_2^P$.

$x \in L \iff \forall y \exists z \left[ D(x, y, z) = 1 \right]$

Let's define

$L' = \{ (x, y) : \exists z \left[ D(x, y, z) = 1 \right] \}$

$L' \in \text{NP}$. So $L' \leq_p \text{SAT}$.

So given $(x, y)$, there's an eff. det. mapping $(x, y) \mapsto \emptyset_{x, y}$ s.t.

$\exists z \left[ D(x, y, z) = 1 \right] \iff \emptyset_{x, y} \in \text{SAT}$.

So $x \in L \iff \forall y \left[ \emptyset_{x, y} \in \text{SAT} \right]$.

Next time: finish pf, + Baker-Gill-Solovay

* start unit #3: relations between resources, hierarchy theorems.