Last time:

- application of CC: time/space tradeoffs for TMs → $D(EQ) = n+1$ $\quad \Omega(n)$
- randomized CC
- application of CC LBs to 1-tape TM LBs
- (surprising) power of randomness... ↳ $R_\varepsilon^{pub}(EQ) = O(\log \frac{1}{\varepsilon})$

Today:

- finish CC: $R_\varepsilon^{pub}(EQ) = O(\log \frac{1}{\varepsilon})$
- start unit on circuit complexity
  - circuit basics
  - non-explicit circuit LBs
  - start small-depth circuits

AB 6.5, AB 14.10

Questions?

A $\quad x \in \{0,1\}^n$ $\quad \stackrel{?}{=}$ $\quad y \in \{0,1\}^n$ B

$R_\varepsilon^{pub}(EQ) = O(\log \frac{1}{\varepsilon})$: use common rand. string $r_1 r_2 \ldots$ as follows:

Repeat following $\leq \log \frac{1}{\varepsilon}$ times:

- let r be next n bits of rand. string
- A computes $x \cdot r = x_1 r_1 + \ldots + x_n r_n \bmod 2$
- B " $y \cdot r = y_1 r_1 + \ldots + y_n r_n \bmod 2$

A sends 1 bit to B.

If the bit A sent is $\neq$ to $*$,

B says "NOT EQUAL" } 1 bit
Otherwise, B says "REPEAT"

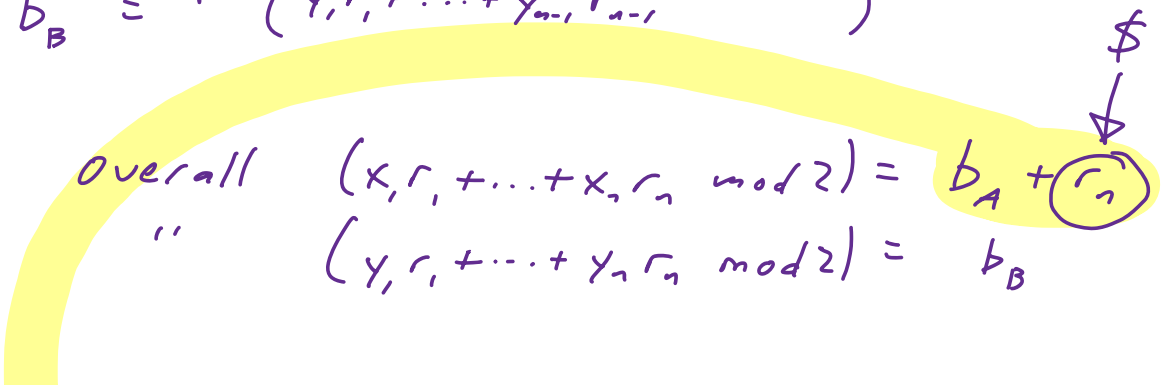
After $\log \frac{1}{\varepsilon}$ trials, they say "EQUAL".

- $2 \log \frac{1}{\varepsilon}$ bits of comm.
- If $x = y$, say EQUAL for sure.
- Correctness follows from

Claim: If $x \neq y$, (in a fixed round) $\Pr[\text{NOT EQUAL}] = \frac{1}{2}$.

Pf: Sps $x_n \neq y_n$. WLOG $x_n = 1$, $y_n = 0$.
For any outcome of

$$b_A = (x_1 r_1 + \dots + x_{n-1} r_{n-1} \bmod 2)$$
$$b_B = + (y_1 r_1 + \dots + y_{n-1} r_{n-1})$$



overall $(x_1 r_1 + \dots + x_n r_n \bmod 2) = b_A + r_n$
" $(y_1 r_1 + \dots + y_n r_n \bmod 2) = b_B$

fair coin toss;
= ly likely to be b_B or $\overline{b_B}$.

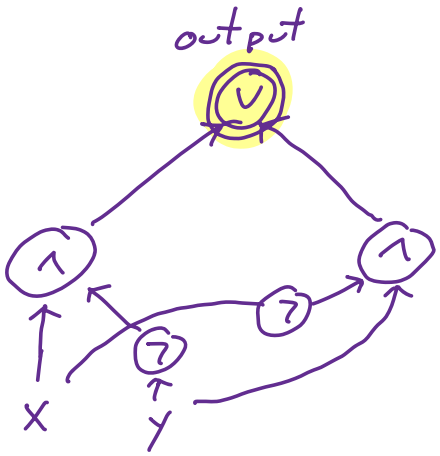
CIRCUIT COMPLEXITY

ckt cxity

- Natural way to compute $f: \{0,1\}^* \to \{0,1\}$.

- Unless we say otherwise, a ckt is composed of binary gates:

Ex: $PAR(x,y) = x+y \bmod 2$:

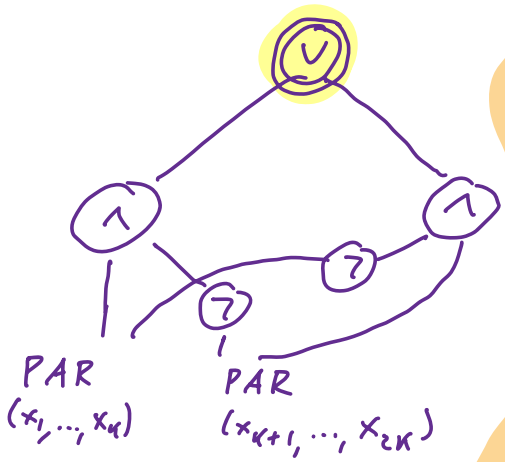


01 → "1"

10 → =1

o/w → 0

$PAR_{2k}(x_1, \ldots, x_{2k})$:



total # gates

This gives a ckt of size $O(n)$, depth $O(\log n)$ for PAR_n.

length of longest directed path.

Recall: a fn $f: \{0,1\}^* \to \{0,1\}$ has circuit cxity $s(n)$ if $\forall n$, f restricted to $\{0,1\}^n$ has an $s(n)$-size ckt.

Recall: $L \in P \Rightarrow L$ has poly(n)-size ckts.

Dream of ckt cxity: for a "natural" lang. L, show it doesn't have poly-size ckts.

We think CLIQUE, SAT

input: (G, k) i.e. an $\binom{n}{2} + \log n$ bit string

HAM PATH ←

⋮

don't have poly-size ckts.

Don't know how to prove these fns are hard.

But, easy to show most functions require huge ($\exp(n)$) size ckts!

"nonconstructive ckt lower bounds"

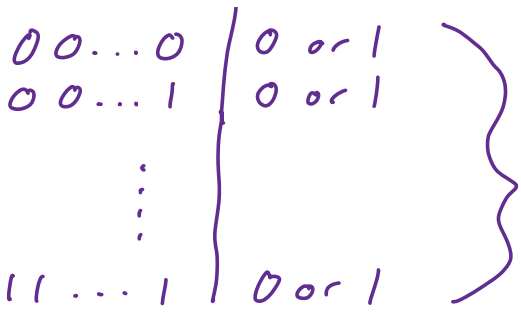
Thm: [Shannon] All but $\leq \frac{1}{2^n}$ fraction of fns $f: \{0,1\}^n \to \{0,1\}$ have ckt size $\geq \frac{2^n}{2 \cdot n}$. (bin fanin $\wedge, \vee, \neg$ ckts)

Idea: "only 1000 small ckts"

"1,000,000 Bool fns f"

$\Rightarrow$ 999,000 fns f don't have a small ckt.

Claim: There are 2^{2^n} many $f: \{0,1\}^n \to \{0,1\}$



Claim: There are $\leq ((n+5)m^2)^m$ distinct ckts of size m in our model over $x_1, \ldots, x_n$.

Pf: To specify an m-gate ckt, must specify, for each gate $1, \ldots, m$,

- gate's label: $x_1, \ldots, x_n, 1, 0, \neg, \vee, \wedge$: $\leq n+5$
- inputs to gate: at most m choices for each of at most 2 inputs: $\leq m^2$

So # ckts of size m is $\leq$

$$((n+5)\cdot m^2)^m.$$

Pf of thm: take $m = \frac{2^n}{2n}$. Get $((n+5)m^2)^m$ is

$$\leq \left(\frac{(n+5)\,2^{2n}}{4n^2} \right)^{\frac{2^n}{2 \cdot n}}$$

$$= \left(\frac{n+5}{4n^2} \right)^{\frac{2^n}{2 \cdot n}} \cdot \left(2^{2n} \right)^{\frac{2^n}{2 \cdot n}} = 2^{2^n}$$

$$= \left(\frac{n+5}{4n^2} \right)^{\frac{2^n}{2 \cdot n}} \cdot 2^{2^n}$$

$$< \left(\frac{1}{2} \right)^{\frac{2^n}{2 \cdot n}} \cdot 2^{2^n} << \frac{1}{2^n} \cdot 2^{2^n}.$$

So,
there aren't enough small ckts to go around.

That's nice!

But... we want lb's against "structured" fns.
"explicit"

Decades of effort have yielded...

$5n - o(n)$ ckt size lb's against explicit fns.

Very hard to prove strong lb's for general circuits.

Main focus of ckt l.b. research: lb's against restricted classes of ckts. Here are two ↙ ↙:

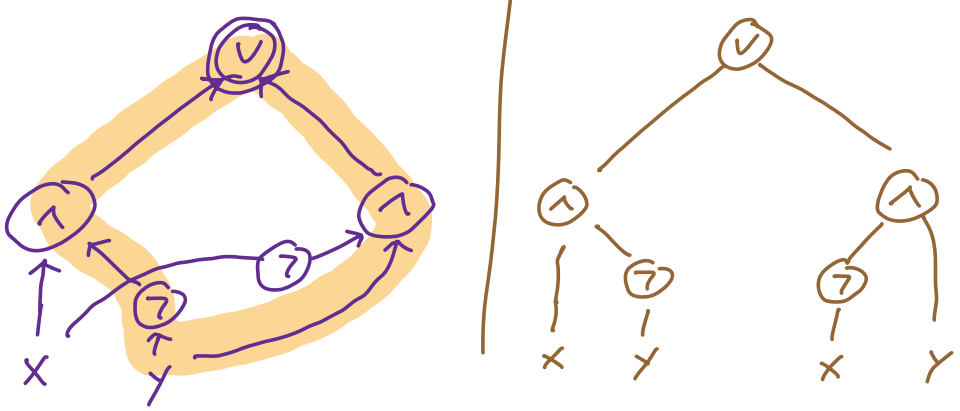
✳ ① small depth ckts;

---

② Boolean formulas (not circuits)

"tree circuit": no undirected cycles.

A formula for this:



a ckt, not a formula: has undir. cycle.

Small-depth circuits:

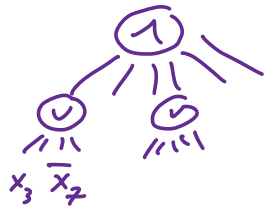
- AND / OR / NOT ckt model, but now consider "unbounded fanin" AND, OR gates:
  think of depth $O(1)$ (const), size very large...

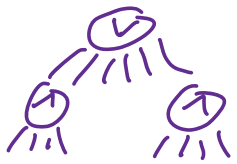
any # input wires is fine!

Why consider these?

1) CNF: depth-2 in this model

DNF: " " " " "





2) Highly // comput: depth d, size s $\Leftrightarrow$ // time d with s processors.

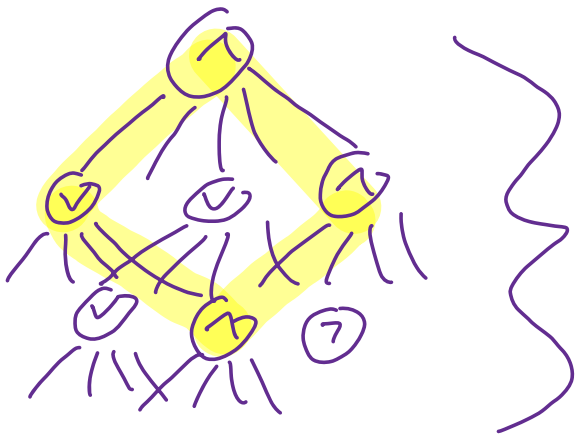
3) If can prove strong bounds on these, implies lbs for other models:

Valiant: if can show $2^{\frac{n}{\log\log n}}$ size lower bd for depth-3 ckts for

$f: \{0,1\}^n \to \{0,1\}$, implies there is no $O(n)$-size, $O(\log n)$-depth binary $\wedge, \vee, \neg$ ckt for f.

↳ current best (size) l.b. for an explicit $f: \{0,1\}^n$ with depth-3 ckts:

$$2^{c\sqrt{n}} \qquad 1.6 < c < 2.$$



depth d ($\wedge$ / $\vee$)

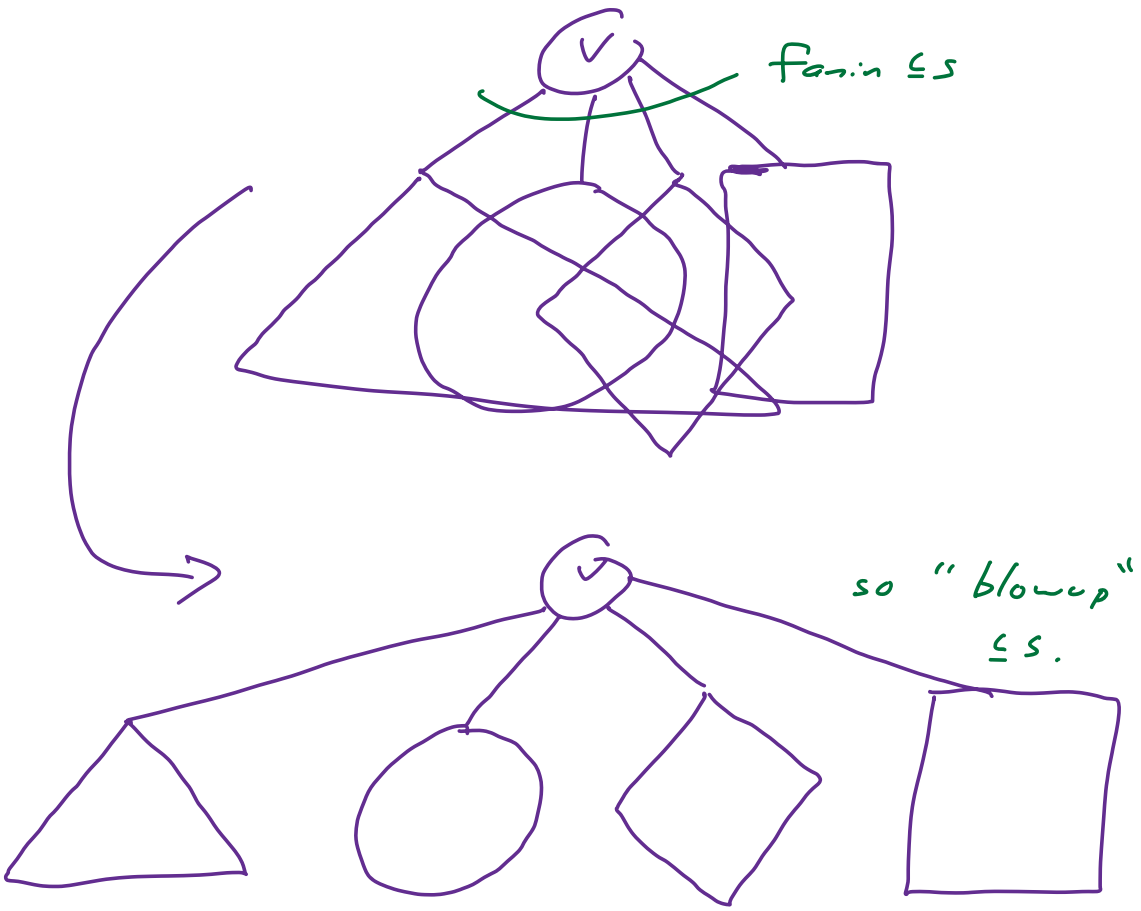
x_1 x_2 ....

Simplif. #1: Suff. to work with formulas:

Say C is an arbitrary size-s, depth-d ckt.

Then there is an equiv. size-(s^d), depth-d formula C' for C.

Pf: induc. on depth d: rewrite each subckt that's used multiple times:



factor of s for each layer of depth: s^d factor overall.

Enough to analyze depth-d formulas.

Next time:
- another simplif.
- depth-2 lower bd
- intuition for higher depth
- "switching lemma"
  - ↳ CDC lb's.