What is computable w/ $O(n)$ size ckts?

- Addition of two n-bit #'s — OPEN: Mult??
- Error correcting codes (Spielman '95)

$\exists \varepsilon, \forall n$, matrix $E_n \in \mathbb{F}^{4n \times n}$

s.t. $\forall x \neq y \in \{0,1\}^n$,

$$H(E_n(x), E_n(y)) > \varepsilon \cdot n$$

- Universal hash fns.

Let $H_n \subseteq \{f : \{0,1\}^n \to \{0,1\}^m\}$

H_n is universal if $\forall x \neq y$, $\Pr_{h \in H_n}[h(x) = h(y)] = \frac{1}{2^m}$.

same prob. as if h were uniform random

Interesting when $|H_n|$ is small, like $n^{O(1)}$.

Thm [Ishai et al. '08]

$\exists \{H_n\}$ s.t. $\forall n$, H_n is universal and $\forall h \in H_n$, $C_{B_\Sigma}(h) \leq O(n)$.

Disproved a 20-year-old conjecture

Conj: (A. N. Kolmogorov) $\exists k$ $P \subset SIZE(O(n^k))$. (!)

Would imply $P \neq NP$: $P = NP \Rightarrow \Sigma_2 P = P$

$\Rightarrow P \not\subset SIZE(O(n^k)), \forall k \ldots$

Why?!

Hilbert's 13th Problem:

"Can all continuous fns on 3 vars be represented with a finite # of cont. fns on 2 vars?"

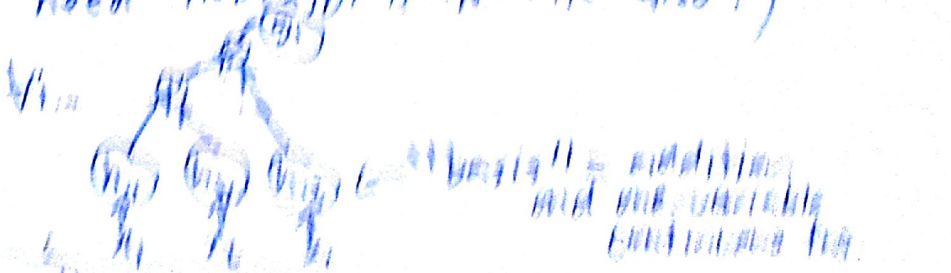
(At complexity in the continuous world...

YES!

Thm [Kol-Arnold '57] For all cont. $f: [0,1]^3 \to \mathbb{R}$,

$\exists g_i, h_{ij}$ s.t. $f(x_1, x_2, x_3) = \sum_{i=1}^{7} g_i \left(\sum_{j=1}^{3} h_{ij}(x_j) \right)$

(g_i, h_{ij}: one-var fns... need $ADD(x,y): \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ also!)



(Generalizing to all continuous $f: [0,1]^n \to \mathbb{R}$! by "[illegible]" [illegible]

Circuit Depth.

B_2 = basis, $f \in B_n$, $D(f)$ = min depth of a ckt computing f.
$C(f)$ = ckt compl of f.

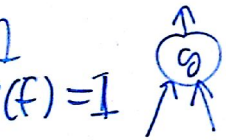
Prop: $D(f) \leq n + \log n$

Pf. Build an OR of ANDs (DNF) from the truth table of f:

Thm: $C(f) \leq 2^{D(f)} - 1$

Pf: Induction on $D(f)$. $\left(D(f) \geq \log_2 C(f)\right)$

$D(f) = 1$
$\Rightarrow C(f) = 1$ ✓

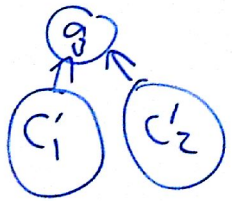


$D(f) = d > 1$.

C:

C_1, C_2 depth $d-1$.
IH $\Rightarrow \exists$ $2^{d-1} - 1$ ckts
C_1' & C_2' (formulas!)
$\equiv$ $\equiv$
C_1 C_2

$\Rightarrow$ C':



has size $2 \cdot (2^{d-1} - 1) + 1 = 2^d - 1$. □

When is $D(f) \leq O(\log C(f))$?

Best known: Thm (Paterson & Valiant '77)

$$D(f) \leq O\left(C(f)/\log C(f)\right).$$

Given ckt of size s, $\exists$ depth $O(s/\log s)$ formula of size $2^{O(s/\log s)}$.

Analogies with Uniform Complexity

① ALG TIME $\approx$ CKT SIZE

"TIME : ALGS :: SIZE : CKTS"

→ TIME(t) $\subseteq$ SIZE($t^{O(1)}$)

→ Size s ckts sim. in $s^{O(1)}$ time:

CktEval $= \{(C, x) \mid$ ckt C on input x outputs $1\}$

Prop: CktEval $\in P$. (In fact, "P-complete")

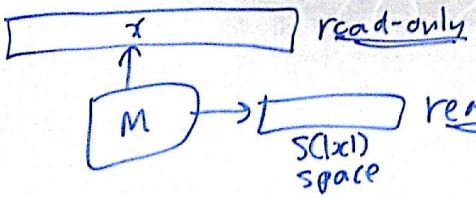
② ALG SPACE $\approx$ CKT DEPTH

(not perfect analogy...)

Let's briefly recall space complexity.

Space $s(n)$ machine M:

(note, TM model doesn't affect results... can use practically any other model)



Def. $L \subseteq \{0,1\}^*$ is in space $s(n)$ if

$\exists c, \exists$ TM M s.t. $\forall x$, $M(x)$ uses $\leq c \cdot s(|x|) + c$ cells on worktape.

$SPACE[s(n)] \triangleq \{L \mid L \text{ is in space } s(n)\}$.

Let $CircEvalD = \{(C,x,d) \mid C \text{ has depth } d \wedge (C,x) \in CircEval\}$

Thm [Borodin '77] $CircEvalD \in SPACE[d + \log n]$.

Recall $SP(s) \subseteq T(2^{O(s)})$ but $T(2^{O(s)}) \subseteq SP(s)$. (???)

Pf: Implement pf that $C(f) \leq 2^{p(f)}$

Eval (C,x,b) \\ return true iff $C(x)=b$

$O(\lg n)$ space ← Find output gate g of C.

g is an input → return true iff $g=b$.

$O(\lg n)$ space ← Let g_1, g_2 be inputs to g.

C_{g_i} := subcircuit of C with g_i = output. (contains all predecessors of g_i)

For all $(b_1,b_2) \in \{0,1\}^2$ s.t. $g(b_1,b_2) = b_1$

if Eval (C_{g_1},x,b_1) ∧ Eval (C_{g_2},x,b_2) then return true

End for

return false

push "(b_1,b_2)" on stack.

push "1" on a stack

then pop when call returns

push "2" on stack.

$O(1)$ bits per gate on longest path.

Cor. NC^1 CktEval $\in SPACE(\log n)$

$=$

$\{(C,x) \mid C \text{ has depth } 100 \cdot \log|x| \text{ & } C(x)=1\}$.

Opposite direction.

Thm [Ruzzo?] For $d(n) \geq \log n$,

$$SPACE(d) \subseteq SIZE\text{-}DEPTH(2^{O(d)}, d^2).$$

$=$ langs computable by ckt families of size $2^{O(d)}$ & depth $O(d^2)$.

Idea: Reduce $L \in SP(d)$ to iterative Boolean matrix mult then solve the matrix mult in low depth.

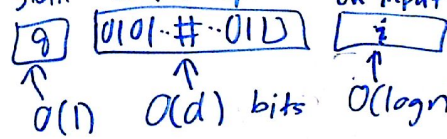
Need a few concepts...

For TM M w/ input x, cfg graph $G_{M,x}$ has:

nodes = cfgs: strings encoding positions of tape heads, machine state, work tape content.

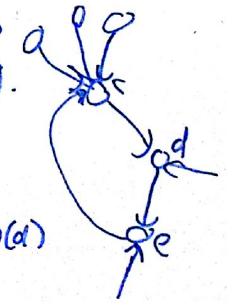
$\downarrow$

$2^{O(d)}$ nodes



$\longrightarrow O(d + \log n)$ bits.

directed edges $= \{(c,d) \mid$ running $M(x)$ from c reaches d in 1 step $\}$.



[could also add self-loops (c,c) "TM runs forever doing nothing" after acc/rej]

Let $A_{M,x}$ = adj matrix of $G_{M,x}$. $A_{M,x} \in \{0,1\}^{2^{O(d)} \times 2^{O(d)}}$.

Def BMM of $n \times n$ A & B:

$$(A * B)(i,j) = \bigvee_k (A(i,k) \wedge B(k,j))$$

$$A^2 = (A * A), \quad A^k = A * A^{k-1}$$

Claim: Let s = start node of $G_{M,x}$ (start cfg)

$M(x)$ acc. in $\leq t$ steps $\iff$ $\left(\bigvee_{\text{"accept nodes" } a} (A_{M,x})^t (s,a) \right) = 1.$

simulate this w/ $t = 2^{O(d)}$ in $2^{O(d)}$ size and $O(d^2)$ depth

Pf. $M(x)$ acc in $\leq t$ steps

$\iff \exists$ cfgs $s, c_1, \ldots, c_{t-1}, a$ (a "accept node")

$(s,c_1), (c_1,c_2), \ldots, (c_{t-1}, a)$ edges in $G_{M,x}$

$$\iff \bigvee_{s, c_1, \ldots, a \text{ acc node}} \left(A_{M,x}(s,c_1) \wedge \cdots \wedge A_{M,x}(c_{t-1}, a) \right) = 1$$

$$\iff \bigvee_a (A_{M,x})^t [s,a] = 1 \quad \square$$

Claim: $\forall$ TM M, $\exists$ $2^{O(d)}$-size $O(d)$-depth ckt C

s.t. $C(x,c,c') = A_{M,x}[c,c']$

Pf: Given cfgs c and c', can check that $c \vdash_{M,x} c'$ in $\text{poly}(|c|,|c'|)$ size and $O(\lg |c| \cdot |c'|)$ depth.

($2^{O(d)}$ bits; each bit of c' depends on $O(1)$ bits of c...)

Claim: $A, B \in \{0,1\}^{n \times n}$,

Can comp. $(A \times B)$ in $O(n^3)$ size & $O(\log n)$ depth.

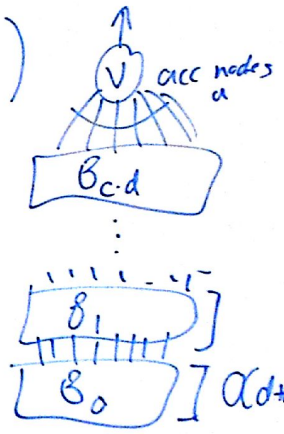
Pf: Each output bit is an OR of n ANDs of 2 inputs. □

Final ckt will iteratively square $A_{m,x}$:

$B_0 := A_{m,x}$

For $i = 1, \ldots, c \cdot d$, $B_i := (B_{i-1} * B_{i-1})$

Output $\left(\bigvee_{\substack{\text{acc} \\ \text{nodes} \\ a}} B_{cd}[s,a] \right)$



$\Rightarrow O((d + \log n) \cdot d)$ depth,

$O(n^3 \cdot cd)$ size. □

Cor. $NSPACE[d] \subset SIZE\text{-}DEPTH[2^{O(d)}, d^2]$.

Cfg graphs are same... except nodes have outdeg ≥ 1..

$NC^2 \triangleq \bigcup_{k \geq 1} SIZE\text{-}DEPTH[n^k, \log^2 n]$

Cor. $NLOGSPACE \subset NC^2$. (Improve to NC^1?? Open!)

($L \subseteq NC^1$?? Open!)