Michael Forbes
miforbes@illinois.edu

2018-04-09.4 → 2018-04-11.1
2016-04-11.2 ← CS 579

CS 579:

Lecture 23: Computational Complexity

today: barrier results
natural proofs

admin: monday class cancelled

relativization: $\mathcal{C}$ vs $\mathcal{D}$ $\mapsto$ $\mathcal{C}^A$ vs $\mathcal{D}^A$ all A

Q: circuit complexity?

def: An oracle circuit is a circuit over $\{AND, OR, NOT, O\}$ (unbounded fan-in; O: fan-in 2, fan-in 1)
for oracle $A \subseteq \{0,1\}^*$, the ckt C^A computes in obvious way

Prop: any A, $P^A \subseteq SIZE^A(poly(n))$ [same proof, now via oracle gates]

Thm: PARITY $\notin AC^0$

Q: relativize ↑?

A: [oracle gates do not simplify under restrictions] ← proof seems to not relativize
↳ does not rule out the result relativizing

Q: barrier results for circuit complexity?
communication ?

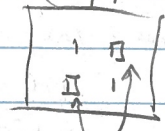
Q: how to formalize known techniques?

Communication complexity

$f(x,y)$ (= maximum)

Prop: $EQ(x,y)$ requires $\geq n$ bits of communication [as we saw]

pf: $S = \{(\{0,1\}^n)^2 : x \neq y\}$ a 1-fooling set for f
$\Rightarrow$ $f(x,y) = f(x',y') = 1$
$f(x',y), f(x,y')$ not both 1

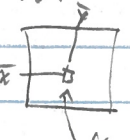


lem: $D^{cc}(f) \leq c \Rightarrow M_f \in \{0,1\}^{\{0,1\}^n \times \{0,1\}^n}$ is partitioned into 2^c monochromatic combinatorial rectangles [each leaf a rectangle]

lem: $D^{cc}(f) \geq \lg S$, S 1 fooling set for f [each leaf contains ≤ 1 element of S]
$S = \{(x,x)\}_{x \in \{0,1\}^n}$ is fool set for EQ

Prop: $f(x,y)$ w/ $D(f) \leq c \Rightarrow \operatorname{rank}_{\mathbb{F}} M_f \leq 2^c$

pf:

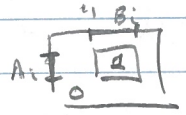


$\Rightarrow$

$\Rightarrow$ $A(x,y) = \sum_i \mathbb{1}[(x,y) \in R_i]$ (1-count rect)
$= \mathbb{1}[x \in A_i] \cdot \mathbb{1}[y \in B_i]$

Michael Forbes
MForbes@illinois.edu
2018-04-11.2 ← 2018-04-11.1 → 2018-04-11.3
CS574

$\Rightarrow$ $M_f = \sum_{i=1}^{2^c} \mathbb{1}[x \in A_i] \cdot \mathbb{1}[y \in B_i]$



← rank 1 matrix

$\Rightarrow$ rank $\le 2^c$

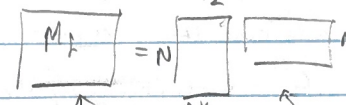
Prop: $D^{cc}(EQ) \ge n$

Pf: $M_{EQ} =$ 

← rank 2^n any $\mathbb{F}$

Rmk: rank method: - can compute $\operatorname{rank}_{\mathbb{F}}(M_f)$ in $\operatorname{poly}(N^2)$ ← constructive
↑ size of M_f largeness
- most f have $\operatorname{rank}_{(\mathbb{F})} \ge 2^n$

lem: $\Pr[f: \{0,1\}^n \to \{0,1\} \text{ has } \operatorname{rank}_{\mathbb{F}_2} M_f \le N/3] \le \frac{1}{2^{N^2/3}}$

Pf: rank $\le N/2$ if $M_f = N \cdot N$ 

$\le 2^{2 \cdot N \cdot N/3} = 2^{2/3 N^2}$
2^{N^2} total matrices

[] hence certifies most functions are hard

counting

failing test: - deciding if M_f has $\Omega(N)$-size testing set
↳ not obviously efficient in $\operatorname{poly}(N)$ time
- most f only have testing sets $\operatorname{poly}\log N$ size
↳ $\Rightarrow D(f) \ge \Omega(\log N)$

motivation:
largeness: most functions are hard, we want our lower bounds to help "understand" this [trivial]

constructivity: most "natural" math is also algorithmic, this is desirable

defn: $C \subseteq \{0,1\}^N$ a class of "simple" objects. A natural proof of a lower bound against C is a distinguisher $D: \{0,1\}^N \to \{0,1\}$ s.t.
- $D(x) = 0 \quad \forall x \in C$
- $\Pr[D(x) = 1] \ge \frac{1}{\operatorname{poly}(N)}$ largeness [[noticeable fraction of functions are hard]]
- size$(D) \le \operatorname{poly}(N)$ constructivity

ex: let $N = 2^n$ $C = \{f$ w/ size n^c ckts$\}$

non examples: - testing set method
- $D(x) = \mathbb{1}[x \notin C]$ - large - non constructive
- $D(f) = \mathbb{1}[f = SAT]$ - not large - constructive
assume NP $\not\subseteq$ P/poly

$\forall x \in \{0,1\}^n$ ($\operatorname{poly}(N)$) $f(x) = SAT(x)$ (input) ($2^{O(n)} = \operatorname{poly}(N)$)

examples:

AC^0 lbs via restrictions:

$D(f)=0$ if some restriction ρ: $f|_\rho$ constant

$D(\text{physical } AC^0)=0$ ‖ what lb shows ‖ ρ leaves $n^{\Omega(1)}$ vars free

D is large ← exercise

D is constructive: $\leq 2^n$ possible restrictions $=\text{poly}(N)$

$f|_\rho$ computable in $\text{poly}(N)$ time

$AC^0[2]$ lbs: proof as given is not natural

but can find "relaxation" of proof that is natural

Q: how do we know if a result does not naturalize?

Thm [Razborov Rudich]: if strong crypto exists $\Rightarrow$ no natural proofs

def: a pseudorandom generator (PRG) is $G: \{0,1\}^n \to \{0,1\}^{\ell(n)}$ for $P/poly$ secure against $t(n)$-size ckts if $U_{\ell(n)} \simeq_{\frac{1}{t(n)}} G(U_n)$ (true randomness; error; pseudorandom; $\ell(n)$ computable in $\text{poly}(n)$ time)

‖ out $\Rightarrow$ PRG ‖

def: a pseudorandom function family (PRF) is $PRF: \{0,1\}^n \times \{0,1\}^m \to \{0,1\}$ computable in $\text{poly}(n,m)$ time

is $t(n)$-secure if for all $t(n)$-size ckts $D^{(\cdot)}(x)$

$$\left| \Pr_{k \in \{0,1\}^m}\left[D^{PRF(\cdot,k)}(1^n)=1\right] - \Pr_{f:\{0,1\}^n \to \{0,1\}}\left[D^{f}(1^n)=1\right] \right| \leq \frac{1}{t(n)}$$

‖ distribution indistinguishable from random ‖

Thm [Goldreich Goldwasser Micali]: $2^{n^{\Omega(1)}}$-secure PRG w $\ell(n)=2n$ $\Rightarrow$ $2^{m^{\Omega(1)}}$-secure PRF

(consistent w/ current crypto beliefs)

Thm [RR]: $\Rightarrow$ no natural proofs

Pf: Say $PRF: \{0,1\}^n \times \{0,1\}^m \to \{0,1\}$ ✓ $\text{poly}(n,m)$ size ckt $2^{m^{\Omega(1)}}$ secure

$D: \{0,1\}^{N=2^n} \to \{0,1\}$ size $\to \text{poly}(N)$ circuit w/ ‖ constructive ‖ ∫ large ‖

✓ $\Pr[D(f)=1] \geq \frac{1}{\text{poly}(N)}$

set m s.t. $2^{m^{\Omega(1)}} \geq$, i.e. $m = n^{\Theta(1)}$

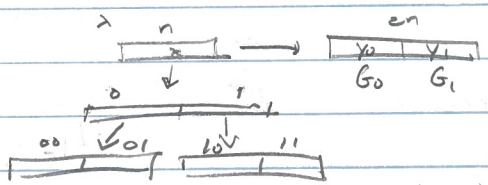
$\Rightarrow$ D cannot distinguish PRF from random

$$\Pr_k[D(PRF(\cdot,k))=1] \geq \underbrace{\Pr[D(f)=1]}_{\geq \frac{1}{\text{poly}(N)}} - \frac{1}{2^{m^{\Omega(1)}}} > 0 \quad \left(m = n^{\Theta(1)}\right)$$

$\Rightarrow \exists k \in \{0,1\}^n$ $D(\underbrace{PRF(\cdot,k)}_{\text{poly}(n,\text{poly}(m)) \text{ size}})=1$ $\Rightarrow$ [$P(P/poly) \neq 0$] not useful lb!

Michael Forbes
mforbes@illinois.edu
2018-04-11.4 ← 2018-04-11.3
→ 2018-04-16.1
CS579

Sketch of GGM =



$PRF(x_1 \cdots x_n, k) = G_{x_1}(\cdots G_{x_n}(k)\cdots)$

Rmk: conjectured PRFs "just beyond" AC^0 [Idea: ...]

Q: bypassing barrier?

relaxing largeness: use properties of SAT
- downward self-reducibility
- completeness ← used in $NEXP \not\subseteq AC^0[m]$

relaxing constructivity: diagonalization
???

admin: class cancelled on Monday