- +10 min
- take OR over 1-monochrom. rect
- draw natural proof diagram
- $B=\emptyset$ $(AC^0[2])^B \neq (AC^0)^B$

Michael Forbes
Miforbes@illinois.edu

2019-04-18.4 → 2019-04-23.1
2019-04-23.2 ←
CS579

CS579 Computational Complexity: Lecture 27

last week: circuit lower bounds
- random restrictions [I did switch in AC⁰]
- polynomial approximations

$\Rightarrow \oplus_n \notin AC^0$

today: "natural proofs" barrier

Q: can circuit complexity methods resolve P vs NP?
↑ requires nonrelativizing techniques

relativization: [proof of] $\mathcal{C}$ vs. $\mathcal{D}$ ⟼ $\mathcal{C}^A$ vs $\mathcal{D}^A$ all A [proof does more]

def: an oracle circuit is a circuit C over {AND, NOT, OR, ⊙} [how does this interact w/ circuits?]
(fan-in 2, 1, ↑ unbounded fan-in)

given oracle $A \subseteq \{0,1\}^*$, ckt C^A computes by treating "⊙" gates as queries to A, in addition to standard gates

prop: any A, $P^A \subseteq SIZE^A(poly(n))$ [same proof as before, now use oracle gates]

thm: $AC^0[2] \not\subseteq AC^0$ [mod 2]

Q: does ↑ relativize?

A: the proof doesn't – the oracle gates do not simplify under random restrictions [most A]
– " do not have low degree approximating polynomials

A: exist A, $AC^0[2]^A = (AC^0)^A$, eg A = parity

Q: barrier results for circuit complexity? [simpler setting for discussion]
" communication "

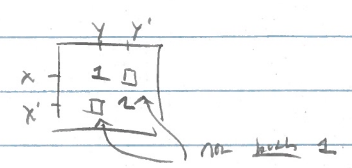
= question

Communication complexity: Alice $x \in \{0,1\}^n$ ——— Bob $y \in \{0,1\}^n$

$f(x,y)$

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

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



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

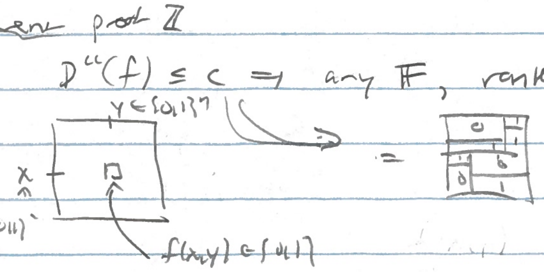
lem: $D^{cc}(f) \geq \lg|S|$, if S is 1-fooling set for f [each comb rect has ≤ 1 element of fooling set]

and $S = \{(x,x) : x \in \{0,1\}^n\}$ is 1 fooling set for EQ

[let's see a different proof]

Prop: $f(x,y)$ w/ $D^{cc}(f) \leq c \Rightarrow$ any $\mathbb{F}$, $\text{rank}_{\mathbb{F}} M_f \leq 2^c$ ($M_f \in \{0,1\}^{2^n \times 2^n}$)

Pf: M_f =



[what is rank of comb rect?]

Michael Forbes
miforbes@illinois.edu
2019-04-23.2 ⇐ 2019-04-23.1
2019-04-23.3
cs579

$f(x,y) = \bigvee_{i=1}^{2^c} [\![x \in A_i \wedge y \in B_i]\!]$ — $A_i \subseteq \{0,1\}^n$, $B_i \subseteq \{0,1\}^n$ [partition into f const rect] [indicator function]

unique OR; $[\![x \in A_i \wedge y \in B_i]\!] = [\![x \in A_i]\!] \cdot [\![y \in B_i]\!]$

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

$=$ (matrix with block of 1s on rows A_i, columns B_i) ← rank 1 matrix

$\Rightarrow \operatorname{rank} M_f \le 2^c$ ∎

Cor. $D^{cc}(EQ) \ge n$

Pf. $M_{EQ} = \begin{bmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{bmatrix}$ ← rank $= 2^n$ over any $\mathbb{F}$

$\Rightarrow D^{cc}(EQ) \ge \lg 2^n = n$ ∎

Rmk. rank method – constructive: can compute $\operatorname{rank}_{\mathbb{F}}(M_f)$ in poly(N^2) time [linear in size of M] [constructive]; $N = 2^n$, N^2 = size of M_f

– large: "most" f have $\operatorname{rank}_{\mathbb{F}_2}(M_f) \approx 2^n$ [largeness]

Prop. $\Pr_{f:(\{0,1\}^n)^2 \to \{0,1\}}[\operatorname{rank}_{\mathbb{F}_2} M_f \le N/3] \le \frac{1}{2^{N^2/3}}$ [tiny] [linear algebra] [most f can be efficiently proven to be hard] [most f are hard] [proof is doing many]

Pf. $\operatorname{rank}_{\mathbb{F}_2} M_f \le N/3$ iff $\underset{N \times N}{M_f} = \underset{N \times r}{A}\,\underset{r \times N}{B^T}$, $A, B \in \mathbb{F}_2^{N \times r}$, $r \le N/3$

M_f: 2^{N^2} possibilities; A, B: $\le 2^{N \cdot r}$ many

$\Rightarrow \Pr[\;] \le \frac{(2^{N \cdot N/3})^2}{2^{N^2}} = \frac{2^{2N^2/3}}{2^{N^2}} = \frac{1}{2^{N^2/3}}$ ∎

Rmk. fooling set – deciding if M_f has $N^{\Omega(1)}$ size fooling set not obviously doable in poly(N) steps [not constructive]

– most f have fooling sets size $\le$ poly($\lg N$) [not large]

but: linear programming relaxation of fooling set method
– is constructive
– is large
can only yield $D^{cc}(f) \ge \Omega(\lg n)$

Motivation – largeness: most functions are hard [by counting], we want our lower bound method to "help understand" this

– constructivity: most "natural" mathematics [now formalize] is also algorithmic, so our lower bounds should also be

def. $\mathcal{C} \subseteq \{0,1\}^N$ is a class of "simple" objects. A *natural proof* of a lower bound against $\mathcal{C}$ is a distinguisher $D : \{0,1\}^N \to \{0,1\}$ s.t.

– useful: $D(x) = 0 \quad \forall x \in \mathcal{C}$ [useful]

– largeness: $\Pr_x[D(x) = 1] \ge 1/\text{poly}(N)$

– constructive: $\text{size}(D) \le \text{poly}(N)$

ex. $N = 2^n$, $\mathcal{C} = \{f \text{ w/ size } n^c \text{ ckts}\}$

$N = (2^n)^2$, $\mathcal{C} = \{f \text{ w/ } \operatorname{rank}_{\mathbb{F}_2} M_f \le 2^n/3\}$, $D = \{\text{checks rank}\}$

Michael Forbes
miforbes@illinois.edu

non examples: - fooling set method ← not large
- $D(f) = \mathbb{1}[f \notin SIZE(n^c)]$ - large - seems non constructive
- $D(f) = \mathbb{1}[f = SAT]$ - useful, if $NP \not\subseteq P/poly$ - constructive - not large

$\forall \varphi \in \{0,1\}^n\ f(\varphi) = SAT(\varphi)$ — poly(N), $2^{O(n)} \le poly(N)$

examples
- AC^0 lbs via random restrictions
  - $D(f) = 0$ if some restriction ρ st $f|_\rho$ constant leaving m vars free (parameter of proof)
  - $D(AC^0) = 0$
  - D is large ← exercise
  - D is constructive: - $\le 3^n$ restrictions $\rho : [n] \to \{0,1,*\}$ ($\le N^{\log_2 3} \le poly(N)$)
    - $f|_\rho$ computable in poly(N) steps

- $AC^0[2]$ lbs: proof as given not obviously natural
[so what?] but exists a "relaxation" which is natural

Thm [Razborov Rudich]: if strong cryptography exists ⇒ no natural proofs for [which we essentially use daily!] lower bounds against P/poly.
[ie existing methods cannot show $NP \not\subseteq P/poly$]

def: a pseudorandom generator (PRG) is $G : \{0,1\}^n \to \{0,1\}^{\ell(n)}$ (↑ stretch)
is secure against $t(n)$-size ckts, if $U_{\ell(n)} \approx_{1/t(n)} G(U_n)$
(true randomness, error, pseudorandomness)
[basic crypto object] [plausible] [scramble an egg]

def: a pseudorandom function family (PRF) is poly(n,m) computable
$PRF : \{0,1\}^n \times \{0,1\}^m \to \{0,1\}$ is $t(m)$ secure if for all
$t(m)$-size oracle circuits $D^\cdot$ [expands to lots of pseudorandomness!]

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

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

Thm [RR] ⇒ no natural proofs for P/poly

Pf: say $PRF : \{0,1\}^n \to \{0,1\}^m \to \{0,1\}$ w/ poly(n,m) size ckt and $2^{m^{\Omega(1)}}$ secure
$D : \{0,1\}^{N=2^n} \to \{0,1\}$ size poly(N) circuit ← constructive
w/ $\Pr_f [D(f) = 1] \ge \frac{1}{poly(N)}$ ← large
set m st $2^{m^{\Omega(1)}} \ge$, ie $m = n^{O(1)}$

Michael Forbes
miforbes@illinois.edu
2019-04-23.4 ⟵ 2019-04-23.1
⟶ 2019-04-25.1
CS579

$\Rightarrow$ D cannot distinguish PRF from random

$$\Pr_K[D(PRF(\cdot,K))=1] \geq \underbrace{\Pr_f[D(f)=1]}_{\geq \frac{1}{poly(N)}} - \frac{1}{2^{m^{\Omega(1)}}} > 0$$

$m = n^{O(1)}$

$\Rightarrow$ $\exists K \in \{0,1\}^*$ $D(\underbrace{PRF(\cdot,K)}_{poly(n,m) \leq poly(n) \text{ size ckt}})=1$ $\Rightarrow$ $D(P/poly) \neq 0$ ↑ not useful!

Remark: - exist plausible PRFs "just beyond" AC^0
↳ existing techniques cannot go much beyond AC^0 [Razborov-Rudich]
- $NEXP \not\subseteq AC^0[m]$, any $m = O(1)$ uses - non-relativizing technique
- non natural technique

next time: applications of circuit complexity