Michael Forbes
miforbes@illinois.edu

2018-04-04.4 → 2018-04-04.1
2018-04-09.2 ←

cs579

cs579: Computational Complexity: Lecture 22

admin: ps 5 due
ps 6 : out

today: barrier results
relativization

barrier results

Q: is P vs NP possible hard to resolve?

proof vs truth

Thm: HALT = {<M,x> : M halts on x} is undecidable

Cor: in any "reasonable" proof system, some <M,x> - M does not halt on x - no proof that

Pf: suppose not

if M halts on x: can prove "M halts on x" by running M on x until halts

M does not halt: we assume proof exists that "M does not halt on x"

to decide HALT

on input <M,x>:

a) search for proofs that "M halts on x" ← one must exist
"M does not halt on x" ←

b) output answer from

Cor: any "reasonable" proof system is "incomplete"

Q: natural such statements? P vs NP?

true but unprovable statements
[how to think about this?]

3 5

P=NP any large enough oracle

Recall: Euclidean geometry:

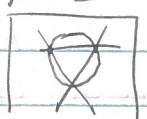
1
2
3
4
5. parallel postulate = ≤1 parallel line

Q: prove #5 from #1-4

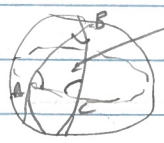
"less obvious" "obvious"

A (Bolyai, Gauss, Beltrami): no

Sketch: real world/model satisfies #1-4, #5



non standard model satisfies #1-4 not #5



Cor: parallel postulate is independent of #1-4

Q: is P vs NP independent? of "known" techniques?

barrier result: formalize "known" techniques
show ↳ cannot solve for given

Q:

Relativization:

michael farbey
mfarbey@illinois.edu
2018-04-09.2 ↔ 2018-04-09.1
2018-04-09.3
cs 579

$A \subseteq \{0,1\}^*$

def: an oracle TM

$y \leftarrow$ oracle tape contents
use '0', if $y \notin A$
1 if $\in$

$TIME^A(t) = \{ L = L(M^A),\ M^* \text{ } O(t(n)) \text{ time machine} \}$

$P^A = \bigcup_c TIME(n^c)^A$

$NTIME^A$ —

NP^A = —

relativization: show a result also holds in presence of any oracle A

i.e. $\mathcal{C} \subseteq \mathcal{D} \mapsto \mathcal{C}^A \subseteq \mathcal{D}^A$ any A

$\mathcal{C} \not\subseteq \mathcal{D} \mapsto \mathcal{C}^A \not\subseteq \mathcal{D}^A$ any A

Thm: any oracle A, $TIME^A(poly(t)) \not\subseteq TIME^A(t)$, time constructible function

pf: ‖ as before ‖ ← oracle TM, no A

D = "on input $\langle M^*, 1^k \rangle$

1) simulate M^A on $\langle M^*, 1^k \rangle$ for $t(|\langle M^*, 1^k \rangle|)$ steps of real time
2) accept $\langle M^*, 1^k \rangle$ iff ↗ rejects

Clm: $L(D) \in TIME^A(poly(t))$

pf: use universal simulation, time bound as before
if M^A uses oracle A, simulation does too

Clm: $L(D) \notin TIME^A(t)$

pf: as before.

Thm: any oracle A, $BPP^A \subseteq PH^A$ ‖ same proof ‖

Rmk: common relativizing techniques: diagonalizing over all TMs
simulating one TM by another
holds any oracle

can axiomatize ↑

good: show relativizing techniques cannot resolve P vs NP

standard model  $P = NP$

nonstandard model $P^A = NP^A$

nonstandard model $P^A \neq NP^A$

thm [Baker Gill Solovay]: exists oracle A s.t. $P^A = NP^A$

pf: idea: make A big enough so P, NP both time

A = TQBF

Clm: $P^A = PSPACE$

pf: ⊇: TQBF is PSPACE-complete
⊆: TQBF $\in$ PSPACE

Michael Forbes
MForbes@illinois.edu
2018-04-09.2 → 2018-04-09.3
2018-04-09.4 ← CS579

Savitch

Clm: $NP^A = NPSPACE = PSPACE$

Pf: $\supseteq$: $NP^A \supseteq P^A = PSPACE$

$\subseteq$: all oracle calls solvable in PSPACE + NP nondeterminism $\subseteq NPSPACE$

$\Rightarrow P^A = NP^A$.

Thm [BGS]: exists oracle B, $P^B \neq NP^B$

idea: create model by hand, put in NP easily, outside P by diagonalization

oracle $B|_{\{0,1\}^n}$ is "input" of size 2^n

each oracle call is query to input

use $P^{query} \neq NP^{query}$

Pf: define $OR^L = \{ 1^n : \text{exists } x \in \{0,1\}^n \ L(x) = 1 \}$.

Lem: $OR^L \in NP^L$ any L ← single query

Pf: guess x, check $L(x) = 1$

Prop: M° $t(n)$-time oracle machine

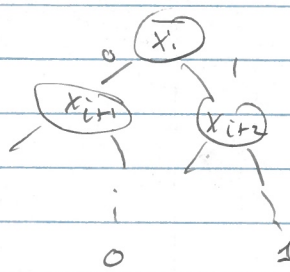
suppose $M^L = OR^L$ any L, only queries n-bit oracle questions on n-bit problem

$\Rightarrow$ $t(n)$-depth decision tree for 2^n-bit OR.

Pf: run M° for $t(n)$ steps

on each query $L(\bar{x}_i) = ?$ branch on both answers

on termination of branch output result



Lem: some B w/ $OR^B \notin P^B$

$\Rightarrow$ thm

Pf: let $M_1, M_2, \ldots$ be enumeration of oracle TM's

M_i runs in $\leq n^i + i$ steps

(it repeat TMs, this includes all P° machines)

define B in stages. initially all undecided.

in stage i: find n large enough so: $B|_{\{0,1\}^n}$ undefined

$n^i + i < 2^n$

run M_i° on $B|_{\{0,1\}^n}$ - on $B|_{\{0,1\}^{\leq n}}$ answer { consistently w/ the defined arbitrarily w/ undefined

- on $B|_{\{0,1\}^{=n}}$ query

$\rightarrow$ decision tree for OR_{2^n} of depth $n^i + i$

define $B|_{\{0,1\}^n}$ so yields wrong answer

possible as $n^i + i < 2^n$ decision tree complexity of OR

$\Rightarrow M_i^B(1^n) \neq OR^B(1^n)$

$\Rightarrow$ any i since n

$\Rightarrow$ $OR^B \notin P^B$

Richard Faber
rfaber@illinois.edu
2018-04-09.4 ⟷ 2018-04-11.1
CS 574

Rmk: $\mathcal{B}$ is computable
Any P vs NP proof must notice no oracle
most complexity results relativize
most open problems require non relativizing techniques
arithmetization is non-relativizing

exists A s.t. $coNP^A \not\subseteq \Sigma_P^A$

but $coNP \subseteq P^{\#SAT} \subseteq \Sigma_P$

used $f: \{0,1\}^n \to \{0,1\} \mapsto \hat{f}: \mathbb{F}^n \to \mathbb{F}$

↳ need to do this to oracle also

algebraization [Aaronson Wigderson]: ↳ still doesn't help for P vs NP

next time: natural proofs barrier