Michael Forbes
mforbes@illinois.edu

2019-02-14.4 → 2019-02-19.1
← 2019-02-19.2
CS 579

Computational

CS 579 Complexity: Lecture 11 15

admin: out of town 02-21 → office hrs cancelled
→ Zander will lecture

last time: - time/space hierarchy
- $TIME(o(\frac{t}{\lg t})) \subsetneq TIME(t)$, for "reasonable" t
- $P \neq EXP$

today: - barrier results
- oracle reductions
- relativization barrier

barrier results [resolved P vs EXP, whereas is possible?]

Q: is P vs NP [possibly] ~~hard~~ possible [true in world] to resolve?
≤ proof vs truth [eg leprechauns]

thm: $HALT = \{\langle M, x\rangle : M \text{ halts on } x\}$ is undecidable [not solvable by TM]

Cor [~~Gödel's incompleteness thm~~]: in any "reasonable" [logical] proof system $\mathcal{L}$

exists some $\langle M, x\rangle$ - M does not halt on x
- no proof of $\langle\nearrow\rangle$ inside the proof system $\mathcal{L}$

Sketch. suppose not:

[if M halts on x: can prove $\langle M \text{ halts on } x\rangle$ in $\mathcal{L}$ by running M until it halts
M not halt on x: some proof in $\mathcal{L}$ that $\langle M \text{ does not halt on } x\rangle$]

→ to decide HALT: on input $\langle M, x\rangle$:

a) enumerate all proofs in $\mathcal{L}$ until find ($\langle M \text{ halts on } x\rangle$ / $\langle M \text{ does not halt on } x\rangle$)
b) accept / reject

[contradicts undecidability]

[one exists by above]

Cor [Gödel's [first] incompleteness thm]: any "reasonable" proof system is incomplete

↖ true but unprovable

Q: Is natural examples? P vs NP?

ex: Euclidean Geometry =
1. ——
2. ——
3. ——
4. ——
5. parallel postulate = given ——— line

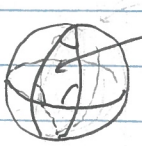
← = 1 parallel line

Q: prove #5 (less obvious) from #1-4 (obvious)

A (Bolyai, Gauss, Beltrami): no

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

non-standard world / model
#1-#4 satisfied



⇒ #5 fails

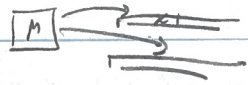
⇒ #5 cannot be proven from #1-#4, is independent

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

barrier result: - formalize "known" techniques
- show ↳ cannot resolve P vs NP

Michael Farber
mfarbes@illinois.edu
2019-02-19.2 ← 2019-02-19.1 → 2019-02-19.3
cs579

oracle reductions

def: $A \subseteq \Sigma^*$ an oracle TM M^A 

special q oracle $\in Q$

M^A computes as before
↳ if reach q oracle; y = oracle tape content (can ask any question)
$y \in A \Rightarrow$ oracle tape replaced w/ 1
$y \notin A \Rightarrow$ oracle tape replaced w/ 0

$TIME^A(t(n)) = \{ L = L(M^A) : M^A$ runs in $O(t(n))$ steps$\}$
$P^A = \bigcup_k TIME^A(n^k)$
also $NTIME^A$, NP^A
complexity class $P^{\mathcal{C}} = \bigcup_{L \in \mathcal{C}} P^L$
$NP^{\mathcal{C}} = \bigcup_{L \in \mathcal{C}} NP^L$

def: $A \leq_{p,oracle} B$ if $A \in P^B$

prop: - $A \leq_p B \Rightarrow A \leq_{p,oracle} B$ (converse is false, probably)
- $A \leq_{p,oracle} B$. $B \in P \Rightarrow A \in P$
$B \in NP \Rightarrow A \in P^{NP} \supseteq NP, \supseteq coNP$ (NP not closed under complement / not so useful here)
- $P^{NP} = P^{SAT}$ (complete sets)

Q: how does P^A compare w/ NP^A?

thm: any oracle A, $TIME^A(o(\frac{t}{\lg t})) \subsetneq TIME^A(t)$, time constructible t.
Pf (as before) ↳ is the theorem relativized?
D^A = "on input $\langle M^A \rangle 10^k$
1) simulate M^A on $\langle M^A \rangle 10^k$ for $\frac{t(n)}{\lg t(n)}$ steps
2) accept iff ↗ rejects (or no A)

Claim: $L(D^A) \in TIME^A(t)$
Pf: use simulation, if M^A calls A, D^A does too
Claim: $L(D^A) \notin TIME^A(o(\frac{t}{\lg t}))$
Pf: as before (diagonal proof)

def: a complexity result $\begin{cases} \mathcal{C} \subseteq \mathcal{D} \\ \mathcal{C} \not\subseteq \mathcal{D} \end{cases}$ relativizes if it holds for any oracle A $\begin{cases} \mathcal{C}^A \subseteq \mathcal{D}^A \\ \mathcal{C}^A \not\subseteq \mathcal{D}^A \end{cases}$
↳ eg: simulation techniques

goal: show that P vs NP requires non-relativizing techniques

Standard model: $P \supseteq NP$ 

non-standard models: - $P^A = NP^A$ 
- $P^B \neq NP^B$ 

Michael Forbes
miforbes@illinois.edu

2019-02-19.2 → 2019-02-19.3
2019-02-21.4 ← CS 579

thm [Baker Gill Solovay 1975]: exists oracle A where $P^A = NP^A$
B $P^B \neq NP^B$

Pf: A: idea: make P/A "so big" that P vs NP is easy
TQBF

Clm: P^A = PSPACE
Pf: ⊇: TQBF is PSPACE-complete
⊆: all oracle queries are ∈ poly(n) long TQBF queries,
∈ PSPACE.

Clm: NP^A = NPSPACE = PSPACE
Pf: ⊇: $NP^A \supseteq P^A \supseteq$ PSPACE
⊆: nondeterminism ∈ NPSPACE
⇒ $P^A = NP^A$

B: idea: create "world" from scratch, by diagonalization
define $OR^L = \{1^n : \exists x \in \{0,1\}^n \; x \in L\}$
Clm: $OR^L \in NP^L$ all L
Pf: guess x, check $x \in L$
Clm: exists B, $OR^B \notin P^B$ [want to show can't put ∈ P^B]
Pf: $M_1, M_2, \ldots M_i, \ldots$ all TM oracle [M_i may never halt]
$M_{i,j}$:= run M_i for $n^i + j$ steps
⇒ $L \in P^B$ iff $L = L(M_{i,j}^B)$ some i,j
idea: define B in stages, stage (i,j) shows $OR^B \neq L(M_{i,j}^B)$
stage 0: all strings x are undecided wrt B
stage i,j: a) pick n large enough s.t.
- $2^n > n^i + j$ [exp vs poly]
- all of $\{0,1\}^n$ is undecided wrt B
↳ each stage decides finite # strings
b) run $M_{i,j}^B$ on 1^n until it halts ← $n^i + j$ steps
↳ asks "$y \in B$?": $y \in B$ decided: answer "yes" [might ask 101 always]
∉ → "no"
undecided: → "no"
c) all $y \in \{0,1\}^n$ - undecided [not queried] [chose n large]
- decided $y \notin B$
$2^n > n^i + j$ ⇒ some $y \in \{0,1\}^n$ undecided [$M_{i,j}^B$ hasn't read this, use as leverage]

Michael Forbes
mforbes@illinois.edu
2019-02-19.4 ← 2019-02-19.3
→ 2019-02-21.1

CS 579

if M_i^B accepted: decide all $y \in \{0,1\}^n$ undecided $\rightsquigarrow y \notin B$
$\Rightarrow$ all $y \in \{0,1\}^n$ have $y \notin B$
$\Rightarrow OR^B(1^n) = 0$ but $M_i^B(1^n) = 1$
$\Rightarrow OR^B \neq L(M_i^B)$

If M_i^B rejected: $y_0 \in \{0,1\}^n$ undecided
decide $y_0 \in B \Rightarrow OR^B(1^n) = 1$ but $M_i^B(1^n) = 0$
$\Rightarrow OR^B \neq L(M_i^B)$

If only decided finitely many strings!

$\Rightarrow$ all i: $L(M_i^B) \neq OR^B$
$\rightsquigarrow OR^B \notin P^B$

Rmk: - B is computable if in exptime
- any resolution to P vs NP "must" notice lack of oracle
- Most known results relativize
- most open problems require non-relativizing techniques
- we'll see some ↪ still not enough for P vs NP

next time: Barrier on circuits