DD2445 COMPLEXITY THEORY

LECTURE 11

LAST TIME

- Quick recap of NL = coNL proof
- Polynomial hierarchy
- PH doesn't have complete problems unless it collapses
- So inclusion PH ⊆ PSPACE probably strict
- Can also define PH in terms of
  - alternating Turing machines
  - oracle Turing machines
- Why care about the polynomial hierarchy?
  - Useful technical tool (e.g. time-space trade-offs for SAT)
  - Conditional complexity results ("Unless the polynomial hierarchy collapses <blah> holds.")
  - Classify problems seemingly harder than NP (e.g. is an NP-solution optimal)

TODAY

- Randomness as a computational resource
- Lots of deep & fascinating questions here — see Ch 8 in Arora-Barak
- We'll get straight to the point: study Turing machines that can flip fair random coins

DEF: PROBABILISTIC TURING MACHINE (PTM)

Turing machine with two transition functions δ_0, δ_1

In each step, apply

δ_0 with probability $1/2$

δ_1 with probability $1/2$

Output of M on x $M(x)$ now random variable

PTM runs in time $T(n)$ if $\forall x$ halts in $\leq T(|x|)$ steps regardless of random choices

What should it mean that such a machine decides a language?

Compare to nondeterminism

- NDTM accepts if $\exists$ one (out of exponentially many) accepting branch
- PTM: look at fraction of accepting branches

For language $L \subseteq \{0,1\}^*$ and $x \in \{0,1\}^*$, define

$$L(x) = \begin{cases} 1 & \text{if } x \in L \\ 0 & \text{if } x \notin L \end{cases}$$

Our (main) model for efficient probabilistic/randomized computation:

BPP bounded-error probabilistic polynomial time

DEF 2 A PTM M decides L in time $T(n)$ if $\forall x$ M halts in $T(|x|)$ steps and $\Pr[M(x) = L(x)] \geq 2/3$.

$BPTIME(T(n))$ = languages decided by PTMs in $O(T(n))$ time

$BPP = \bigcup_{c \in \mathbb{N}^+} BPTIME(n^c)$

Probability over random choices, not over input

Constant 2/3 arbitrary (will see later)

Don't need perfectly fair coins (but we'll ignore this)

PROB 3 $L \in BPP$ if exist poly-time (deterministic) TM M and polynomial p s.t. for every x

$$\Pr_{r \in_R \{0,1\}^{p(|x|)}}\left[M(x,r) = L(x) \right] \geq 2/3$$

Notational aside

Uniform sampling from $\{0,1\}^n$: $x \in_R \{0,1\}^n$

$x \sim \{0,1\}^n$

$x \sim U_n$

COR 4 $P \subseteq BPP \subseteq EXP$

Proof Can try all possible random strings in exponential time and compute success probability

Can't prove even $BPP \neq NEXP$

What about BPP vs P?

Fairly strong reasons to believe $P = BPP$!

[Discussed in Chs 19-20 in Arora-Barak — we won't have time to cover this.]

Example of the power of randomization

POLYNOMIAL IDENTITY TESTING

Given: polynomial (multivariate) with integer coeff. In implicit form

Decide: Is the polynomial identically zero?

Representation algebraic circuit

Like Boolean circuits, but gates are $+, -, \times$

Can also have constants $0, 1, \ldots$ if we wish

Inputs $x_1, \ldots, x_n$

Single output node (sink)

Not hard to see: computes some polynomial

$ZEROP = \{$ algebraic circuits corresponding to polynomials that are identically zero $\}$

Why identity testing?

Given C, C', construct $D = C - C'$ and check if $D \in ZEROP$.

Note compact representation

$\prod_{i=1}^{n} (1 + x_i)$ has 2^n terms

circuit of size $2n$

SCHWARTZ-ZIPPEL LEMMA

Let $p(x_1, x_2, \ldots, x_m)$ be non-zero poly of total degree $\leq d$. Let S finite set of integers. Then for $a_1, \ldots, a_m$ chosen from S uniformly randomly with replacements

$$Pr\left[p(a_1, \ldots, a_m) \neq 0 \right] \geq 1 - \frac{d}{|S|}$$

Proof Induction over ~~m~~.

Base case $m = 1$: Univariate polynomial Degree $\leq d$ $\Rightarrow$ at most d roots So p can evaluate to zero on at most d out of $|S|$ integers.

Inductive step See Arora-Barak App A.6

TESTING IDEA

Circuit of size m $\Rightarrow$ $\leq m$ multiplications $\Rightarrow$ degree $\leq 2^m$

So pick $a_1, \ldots, a_m \in [1, 10 \cdot 2^m]$, evaluate circuit, and apply Schwartz-Zippel

If circuit C encodes zero poly $\Rightarrow$ result always 0 if non-zero poly $\Rightarrow$ 90% of non-zero output

Problem If degree $\approx 2^m$, then numbers grow as large as $(10 \cdot 2^m)^{2^m}$ $\Rightarrow$ exponentially many bits.

Hard to do in poly time...

Solution "fingerprinting" compute modulo $k \in [2^{2m}]$

Computing modulo k

After each operation, divide by k and take remainder

Suppose $y = C(a_1, \ldots, a_m)$

If $y = 0$, then $y = 0 \pmod k$

Claim 5

If $y \neq 0$, then randomly chosen $k \in [2^{2m}]$ will not divide y with prob $\geq \delta = \frac{1}{4m}$

Given this claim, run test $O(m)$ times and accept only if always get 0 output

$\Rightarrow$ arbitrarily high constant probability of success

Proof of Claim 5

Assume $y \neq 0$. $y \leq (10 \cdot 2^m)^{2^m}$

Let B = prime factors of y.

Sufficient to show that with prob $\geq \delta$ k is a prime not in B

y has at most $\log y \leq 5m\,2^m$ prime factors

By Prime Number Theorem (*) — constant is actually 1

$$\#\text{primes} \leq N \sim N / \ln N$$

$$\#\text{primes} \leq 2^{2m} \sim \frac{2^{2m}}{2m} > \frac{2^{2m}}{4m} \quad \text{for large enough } m$$

$$5m\,2^m = o\left(\frac{2^{2m}}{2m}\right) < \frac{2^{2m}}{8m} \quad \text{for large enough } m$$

$$\Pr[\,k \text{ prime not in } B\,] \geq \frac{2^{2m}/8m}{2^{2m}} = \frac{1}{8m}$$

*) See Thm A.23 in Arora-Barak for sufficient, simpler version

Many natural randomized algorithms have one-sided error

Might make mistake when $x \in L$ but never when $x \notin L$ or the other way round

(we just saw one such example)

DEF 6 $RTIME(T(n))$ contains every language L for which $\exists$ PTM M running in time $O(T(n))$ such that

$$x \in L \Rightarrow Pr[M(x) = 1] \geq 2/3$$
$$x \notin L \Rightarrow Pr[M(x) = 0] = 1$$

$$RP = \bigcup_{c \in \mathbb{N}^+} RTIME(n^c)$$

OBS 7 $RP \subseteq NP$

Pf Every accepting branch is a certificate.

Don't know if $BPP \subseteq NP$

RP: "Never false positives" (positive answers always right)

$coRP = \{L \mid \bar{L} \in RP\}$ "Never false negatives"

Given general PTM M, can define random variable

$T_{M,x}$ = running time of M on x.

Take expectation of this random variable

$$E[T_{M,x}] = \sum_{t=1}^{\infty} t \cdot Pr[T_{M,x} = t]$$

Say M has expected running time $T(n)$ if

$$\forall x \in \{0,1\}^* \quad E[T_{M,x}] \leq T(|x|)$$

DEF 8 $ZTIME(T(n))$ contains all languages L for which $\exists$ PTM M that runs in expected time $O(T(n))$ such that

$$Pr[\, M(x) = L(x) \mid M \text{ halts} \,] = 1$$

$$ZPP = \bigcup_{c \in \mathbb{N}^+} ZTIME(n^c)$$

"Zero-sided error"

ZPP zero-error probabilistic polynomial time

THM 9 $ZPP = RP \cap coRP$

Proof Exercise.

Also immediately clear from def

$$RP \subseteq BPP$$
$$coRP \subseteq BPP$$

ROBUSTNESS OF DEFINITIONS

(a) Error probability: constant 2/3 arbitrary
(b) Can use expected running time instead of worst case
(c) can use biased coins
(d) Can even use imperfect random sources ("weak random sources")

Will show (a) — see Sec 7.4 for the rest

LEMMA 10 For $c>0$ constant, let $BPP_{1/2+n^{-c}}$ denote class of languages L for which $\exists$ poly-time PTM M s.t. $\forall x \in \{0,1\}^*$

$$Pr[M(x)=L(x)] \geq \frac{1}{2} + |x|^{-c}$$

Then $BPP_{1/2+n^{-c}} = BPP$.

Need to show: can go from success prob $\frac{1}{2}+n^{-c}$ to $2/3$.

Show sth stronger: can go to $1-2^{-n^d}$ exponentially small failure prob.

THM 11 (ERROR REDUCTION FOR BPP)

Suppose $\exists$ poly-time PTM M for L s.t.

$$\forall x \quad Pr[M(x)=L(x)] \geq 1/2 + |x|^{-c}.$$

Then $\forall d>0$ $\exists$ poly-time PTM M' s.t.

$$\forall x \quad Pr[M(x)=L(x)] \geq 1 - 2^{-|x|^d}$$

Proof

M' runs M for $k = 8|x|^{2c+d}$ times, collects answers, and takes majority vote.

How confident can we be that this is correct?

Use material from App A.2.1 & A.2.4

Let $X_i = \begin{cases} 1 & \text{if } i\text{th run of } M \text{ gets } x \text{ right} \\ 0 & \text{otherwise} \end{cases}$

$Pr[X_i = 1] = p$ for $p \geq \frac{1}{2} + |x|^{-c}$ [suppose $p = 1/2 + |x|^{-c}$ for simplicity]

$$E\left[\sum_{i=1}^{k} X_i\right] = kp = \underbrace{\frac{8|x|^{2c+d}}{2}}_{\text{half}} + \underbrace{8|x|^{c+d}}_{\text{margin}}$$

"If you repeat independent trials sufficiently many times, you will get very close to expected value with very high probability"

LEMMA 12 (CHERNOFF BOUND) — deviation from expected value

$$\Pr\left[\left|\sum_{i=1}^{k} x_i - pk\right| > \delta pk\right] < \exp\left(-\frac{\delta^2}{4} pk\right)$$

Plug in $p = \frac{1}{2} + |x|^{-c}$

$$\delta = |x|^{-c}/2$$

We will be correct unless $\sum_{i=1}^{k} x_i < pk - \delta pk$.
That probability is bounded by

$$\exp\left(-\frac{1}{4|x|^{2c}} \cdot \frac{8|x|^{2c+d}}{2}\right) = \exp\left(-|x|^d\right) < 2^{-|x|^d}$$ [12]

Relationship between BPP and other classes?

THM 12 $BPP \subseteq P/poly$

THM 13 $BPP \subseteq \Sigma_2^P \cap \Pi_2^P$ $(\subseteq PH)$

Both proofs use error reduction in Thm 12 plus some other ideas.

Proof of Thm 13 is extremely neat...
But will have to skip it due to time constraints.

Try to sketch proof of Thm 12

Proof of Thm 12

If $L \in BPP$, then by Thm 11 (and Prop 3)
$\exists$ PTM M that on input size n

- uses m random bits
- gets answer right except with prob $2^{-(n+1)}$

Let r be the random bits

Say r bad for x if $M(x,r) \neq L(x)$

For every x, M succeeds with prob $\geq 1 - 2^{-(n+1)}$

$\Rightarrow$ out of 2^m random strings, $\leq 2^m / 2^{n+1}$ bad for x.

$$\left| \{ r \mid r \text{ bad for some } x \} \right| \leq \sum_{x \in \{0,1\}^n} \left| \{ r \mid r \text{ bad for this } x \} \right|$$

$$\leq \frac{1}{2} 2^n \cdot \frac{2^m}{2^{n+1}} = 2^m / 2$$

But this means that there is at least one random string $r^* \in \{0,1\}^m$ (in fact, at least half) that are good for all $x \in \{0,1\}^n$

Run M with this r^* as advice!

Checking Thm 11 again, r^* will have poly size.

What about complete problems for BPP?

Typical complete problems

∃ TM of correct type running with resource bound such-and-such

"Correct type": DTM – easy to check
NDTM – easy to check
} syntactic

BPP-style: accept x with prob ≥ 2/3
or prob ≤ 1/3
but not in between

Undecidable to check

Hierarchy theorems?

Fail for similar reasons.

A final useful notion: Randomized reductions

DEF 14 Language B reduces to language C under randomized reductions, denoted $B \leq_r C$, if ∃ PTM M s.t.

$$\forall x \in \{0,1\}^* \quad Pr\left[C(M(x)) = B(x) \right] \geq 2/3$$

Not transitive

But if $C \in BPP$ and $B \leq_r C$ then $B \in BPP$

Could have defined NP in terms of randomized reductions instead (if BPP better formalization of "efficient computation")

$$NP = \{ L \mid L \leq_p 3\text{-SAT} \}$$

DEF 15

$$BP \cdot NP = \{ L \mid L \leq_r 3\text{-SAT} \}$$