

CS151 Complexity Theory

Lecture 8
April 22, 2021

Randomness

- 3 examples of the power of randomness
 - communication complexity
 - polynomial identity testing
 - complexity of finding unique solutions
- randomized complexity classes

April 22, 2021

CS151 Lecture 8

1. Communication complexity

two parties: Alice and Bob
function $f: \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}$
Alice holds $x \in \{0,1\}^n$; Bob holds $y \in \{0,1\}^n$

- **Goal:** compute $f(x, y)$ while communicating as few bits as possible between Alice and Bob
- count number of bits exchanged (computation free)
- at each step: one party sends bits that are a function of held input and received bits so far

April 22, 2021

CS151 Lecture 8

Communication complexity

- simple function (equality):
 $EQ(x, y) = 1$ iff $x = y$
- simple protocol:
 - Alice sends x to Bob (n bits)
 - Bob sends $EQ(x, y)$ to Alice (1 bit)
 - total: $n + 1$ bits
 - (works for any predicate f)

April 22, 2021

CS151 Lecture 8

Communication complexity

- Can we do better?
 - deterministic protocol?
 - **probabilistic protocol?**
 - at each step: one party sends bits that are a function of held input and received bits so far **and the result of some coin tosses**
 - required to output $f(x, y)$ **with high probability** over all coin tosses

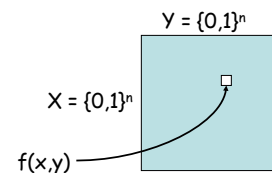
April 22, 2021

CS151 Lecture 8

Communication complexity

Theorem: no deterministic protocol can compute $EQ(x, y)$ while exchanging fewer than $n+1$ bits.

- Proof:
 - “input matrix”:

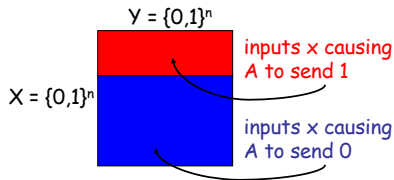


April 22, 2021

CS151 Lecture 8

Communication complexity

- assume 1 bit sent at a time, alternating (same proof works in general setting)
- A sends 1 bit depending only on x :

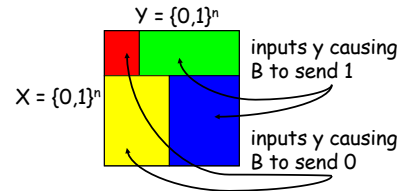


April 22, 2021

CS151 Lecture 8

Communication complexity

- B sends 1 bit depending only on y and received bit:



April 22, 2021

CS151 Lecture 8

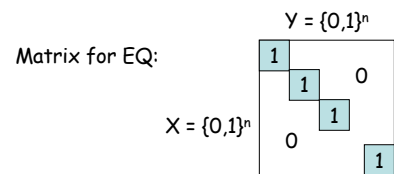
Communication complexity

- at end of protocol involving k bits of communication, matrix is partitioned into at most 2^k combinatorial rectangles
- bits sent in protocol are the same for every input (x, y) in given rectangle
- conclude: $f(x,y)$ must be constant on each rectangle

April 22, 2021

CS151 Lecture 8

Communication complexity



- any partition into combinatorial rectangles with constant $f(x,y)$ must have $2^n + 1$ rectangles
- protocol that exchanges $\leq n$ bits can only create 2^n rectangles, so must exchange at least $n+1$ bits.

April 22, 2021

CS151 Lecture 8

Communication complexity

- protocol for EQ employing randomness?
 - Alice picks random prime p in $\{1 \dots 4n^2\}$, sends:
 - p
 - $(x \bmod p)$
 - Bob sends:
 - $(y \bmod p)$
 - players output 1 if and only if:
 - $(x \bmod p) = (y \bmod p)$

April 22, 2021

CS151 Lecture 8

Communication complexity

- $O(\log n)$ bits exchanged
- if $x = y$, always correct
- if $x \neq y$, incorrect if and only if:
 - p divides $|x - y|$
- # primes in range is $\geq 2n$
- # primes dividing $|x - y|$ is $\leq n$
- probability incorrect $\leq 1/2$
- Randomness gives an exponential advantage!!

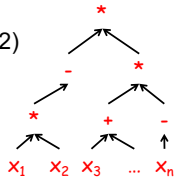
April 22, 2021

CS151 Lecture 8

2. Polynomial identity testing

- Given: polynomial $p(x_1, x_2, \dots, x_n)$ as arithmetic formula (fan-out 1):

- multiplication (fan-in 2)
- addition (fan-in 2)
- negation (fan-in 1)



April 22, 2021

CS151 Lecture 8

Polynomial identity testing

- Question: Is p **identically zero**?
 - i.e., is $p(\mathbf{x}) = 0$ for all $\mathbf{x} \in \mathbb{F}^n$
 - (assume $|\mathbb{F}|$ larger than degree...)
- “**polynomial identity testing**” because given two polynomials p, q , we can check the identity $p \equiv q$ by checking if $(p - q) \equiv 0$

April 22, 2021

CS151 Lecture 8

Polynomial identity testing

- try all $|\mathbb{F}|^n$ inputs?
 - may be exponentially many
- multiply out symbolically, check that all coefficients are zero?
 - may be exponentially many coefficients
- can randomness help?
 - i.e., flip coins, allow small probability of wrong answer

April 22, 2021

CS151 Lecture 8

Polynomial identity testing

Lemma (Schwartz-Zippel): Let

$$p(x_1, x_2, \dots, x_n)$$

be a **total degree d** polynomial over a field \mathbb{F} and let S be any subset of \mathbb{F} . Then if p is not identically 0,

$$\Pr_{r_1, r_2, \dots, r_n \in S} [p(r_1, r_2, \dots, r_n) = 0] \leq d/|S|.$$

April 22, 2021

CS151 Lecture 8

Polynomial identity testing

- Proof:
 - induction on number of variables n
 - base case: $n = 1$, p is univariate polynomial of degree at most d
 - at most d roots, so

$$\Pr [p(r_1) = 0] \leq d/|S|$$

April 22, 2021

CS151 Lecture 8

Polynomial identity testing

– write $p(x_1, x_2, \dots, x_n)$ as

$$p(x_1, x_2, \dots, x_n) = \sum_i (x_1)^i p_i(x_2, \dots, x_n)$$

– $k = \max. i$ for which $p_i(x_2, \dots, x_n)$ not id. zero

– by induction hypothesis:

$$\Pr [p_k(r_2, \dots, r_n) = 0] \leq (d-k)/|S|$$

– whenever $p_k(r_2, \dots, r_n) \neq 0$, $p(x_1, r_2, \dots, r_n)$ is a univariate polynomial of degree k

$$\Pr [p(r_1, r_2, \dots, r_n) = 0 \mid p_k(r_2, \dots, r_n) \neq 0] \leq k/|S|$$

April 22, 2021

CS151 Lecture 8

Polynomial identity testing

$$\Pr[p_k(r_2, \dots, r_n) = 0] \leq (d-k)/|S|$$

$$\Pr[p(r_1, r_2, \dots, r_n) = 0 \mid p_k(r_2, \dots, r_n) \neq 0] \leq k/|S|$$

– conclude:

$$\Pr[p(r_1, \dots, r_n) = 0] \leq (d-k)/|S| + k/|S| = d/|S|$$

– Note: can add these probabilities because

$$\Pr[E_1] = \Pr[E_1|E_2]\Pr[E_2] + \Pr[E_1|\neg E_2]\Pr[\neg E_2] \\ \leq \Pr[E_2] + \Pr[E_1|\neg E_2]$$

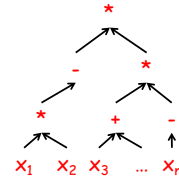
April 22, 2021

CS151 Lecture 8

Polynomial identity testing

- Given: polynomial $p(x_1, x_2, \dots, x_n)$

- Is p **identically zero**?



- Note: degree d is at most the size of input

April 22, 2021

CS151 Lecture 8

Polynomial identity testing

- randomized algorithm: field F , pick a subset $S \in F$ of size $2d$
 - pick r_1, r_2, \dots, r_n from S uniformly at random
 - if $p(r_1, r_2, \dots, r_n) = 0$, answer “yes”
 - if $p(r_1, r_2, \dots, r_n) \neq 0$, answer “no”
- if p identically zero, never wrong
- if not, Schwartz-Zippel ensures probability of error at most $\frac{1}{2}$

April 22, 2021

CS151 Lecture 8

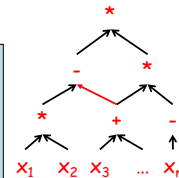
Polynomial identity testing

- Given: polynomial $p(x_1, x_2, \dots, x_n)$

- Is p **identically zero**?

What if polynomial is given as arithmetic **circuit**?

- max degree?
- does the same strategy work?



April 22, 2021

CS151 Lecture 8

3. Unique solutions

- a positive instance of SAT may have many satisfying assignments
- maybe the difficulty comes from not knowing which to “work on”
- if we knew # satisfying assignments was 1 or 0, could we zoom in on the 1 efficiently?

April 22, 2021

CS151 Lecture 8

Unique solutions

Question: given **polynomial-time algorithm** that works on SAT instances with **at most 1 satisfying assignment**, can we solve general SAT instances efficiently?

- Answer: yes
 - but (currently) only if “efficiently” allows randomness

April 22, 2021

CS151 Lecture 8

Unique solutions

Theorem (Valiant-Vazirani): there is a randomized poly-time procedure that given a 3-CNF formula

$$\varphi(x_1, x_2, \dots, x_n)$$

outputs a 3-CNF formula φ' such that

- if φ is not satisfiable then φ' is not satisfiable
- if φ is satisfiable then with probability at least $1/(8n)$ φ' has exactly one satisfying assignment

April 22, 2021

CS151 Lecture 8

Unique solutions

• Proof:

- given subset $S \subseteq \{1, 2, \dots, n\}$, there exists a 3-CNF formula θ_S on x_1, x_2, \dots, x_n and additional variables such that:
 - θ_S is satisfiable iff an even number of variables in $\{x_i\}_{i \in S}$ are true
 - for each such setting of the x_i variables, this satisfying assignment is unique
 - $|\theta_S| = O(n)$
 - not difficult; details omitted

April 22, 2021

CS151 Lecture 8

Unique solutions

- set $\varphi_0 = \varphi$
- for $i = 1, 2, \dots, n$
 - pick random subset S_i
 - set $\varphi_i = \varphi_{i-1} \wedge \theta_{S_i}$
- output random one of the φ_i

– $T =$ set of satisfying assignments for φ

– **Claim:** if $|T| > 0$, then

$$\Pr_{k \in \{0, 1, 2, \dots, n-1\}}[2^k \leq |T| \leq 2^{k+1}] \geq 1/n$$

April 22, 2021

CS151 Lecture 8

Unique solutions

Claim: if $2^k \leq |T| \leq 2^{k+1}$, then the probability φ_{k+2} has exactly one satisfying assignment is $\geq 1/8$

– fix $t, t' \in T$

S_i contains even # of positions i where $t_i \neq t'_i$

$t = 0101001010111$
 $t' = 1010111000101$

– $\Pr[t \text{ "agrees with" } t' \text{ on } S_i] = 1/2$

– $\Pr[t \text{ agrees with } t' \text{ on } S_1, S_2, \dots, S_{k+2}] = (1/2)^{k+2}$

April 22, 2021

CS151 Lecture 8

Unique solutions

- $\Pr[t \text{ agrees with some } t' \text{ on } S_1, \dots, S_{k+2}] \leq (|T|-1)(1/2)^{k+2} < 1/2$
- $\Pr[t \text{ satisfies } S_1, S_2, \dots, S_{k+2}] = (1/2)^{k+2}$
- $\Pr[t \text{ unique satisfying assignment of } \varphi_{k+2}] > (1/2)^{k+3}$

– sum over at least 2^k different $t \in T$ (disjoint events); claim follows.

April 22, 2021

CS151 Lecture 8

Randomized complexity classes

- model: probabilistic Turing Machine
 - deterministic TM with additional read-only tape containing “coin flips”
- **BPP** (Bounded-error Probabilistic Poly-time)
 - $L \in \text{BPP}$ if there is a p.p.t. TM M :
 - $x \in L \Rightarrow \Pr_y[M(x,y) \text{ accepts}] \geq 2/3$
 - $x \notin L \Rightarrow \Pr_y[M(x,y) \text{ rejects}] \geq 2/3$
 - “p.p.t.” = probabilistic polynomial time

April 22, 2021

CS151 Lecture 8

Randomized complexity classes

- **RP** (Random Polynomial-time)
 - $L \in \text{RP}$ if there is a p.p.t. TM M :
 - $x \in L \Rightarrow \Pr_y[M(x,y) \text{ accepts}] \geq 1/2$
 - $x \notin L \Rightarrow \Pr_y[M(x,y) \text{ rejects}] = 1$
- **coRP** (complement of Random Polynomial-time)
 - $L \in \text{coRP}$ if there is a p.p.t. TM M :
 - $x \in L \Rightarrow \Pr_y[M(x,y) \text{ accepts}] = 1$
 - $x \notin L \Rightarrow \Pr_y[M(x,y) \text{ rejects}] \geq 1/2$

April 22, 2021

CS151 Lecture 8

Randomized complexity classes

One more important class:

- **ZPP** (Zero-error Probabilistic Poly-time)
 - $\text{ZPP} = \text{RP} \cap \text{coRP}$
 - $\Pr_y[M(x,y) \text{ outputs "fail"}] \leq 1/2$
 - otherwise outputs correct answer

April 22, 2021

CS151 Lecture 8

Randomized complexity classes

These classes may capture “efficiently computable” better than **P**.

- “1/2” in **ZPP**, **RP**, **coRP** definition unimportant
 - can replace by $1/\text{poly}(n)$
- “2/3” in **BPP** definition unimportant
 - can replace by $1/2 + 1/\text{poly}(n)$
- Why? **error reduction**
 - we will see simple error reduction by repetition
 - more sophisticated error reduction later

April 22, 2021

CS151 Lecture 8

Error reduction for RP

- given L and p.p.t. TM M :
 - $x \in L \Rightarrow \Pr_y[M(x,y) \text{ accepts}] \geq \epsilon$
 - $x \notin L \Rightarrow \Pr_y[M(x,y) \text{ rejects}] = 1$
- new p.p.t. TM M' :
 - simulate M k/ϵ times, each time with independent coin flips
 - accept if **any** simulation accepts
 - otherwise reject

April 22, 2021

CS151 Lecture 8

Error reduction

$$\begin{aligned} x \in L &\Rightarrow \Pr_y[M(x,y) \text{ accepts}] \geq \epsilon \\ x \notin L &\Rightarrow \Pr_y[M(x,y) \text{ rejects}] = 1 \end{aligned}$$

- if $x \in L$:
 - probability a given simulation “bad” $\leq (1 - \epsilon)$
 - probability all simulations “bad” $\leq (1 - \epsilon)^{(k/\epsilon)} \leq e^{-k}$
 - $\Pr_y[M'(x, y') \text{ accepts}] \geq 1 - e^{-k}$
- if $x \notin L$:
 - $\Pr_y[M'(x, y') \text{ rejects}] = 1$

April 22, 2021

CS151 Lecture 8

Error reduction for BPP

- given L , and p.p.t. TM M :
 - $x \in L \Rightarrow \Pr_y[M(x,y) \text{ accepts}] \geq 1/2 + \epsilon$
 - $x \notin L \Rightarrow \Pr_y[M(x,y) \text{ rejects}] \geq 1/2 - \epsilon$
- new p.p.t. TM M' :
 - simulate M k/ϵ^2 times, each time with independent coin flips
 - accept if **majority** of simulations accept
 - otherwise reject

April 22, 2021

CS151 Lecture 8

Error reduction for BPP

- X_i random variable indicating "correct" outcome in i -th simulation (out of $m = k/\epsilon^2$)
 - $\Pr[X_i = 1] \geq \frac{1}{2} + \epsilon$
 - $\Pr[X_i = 0] \leq \frac{1}{2} - \epsilon$
- $E[X_i] \geq \frac{1}{2} + \epsilon$
- $X = \sum_i X_i$
- $\mu = E[X] \geq (\frac{1}{2} + \epsilon)m$

- Chernoff: $\Pr[X \leq m/2] \leq 2^{-\Omega(\epsilon^2 \mu)}$

April 22, 2021

CS151 Lecture 8

Error reduction for BPP

$x \in L \Rightarrow \Pr_y[M(x,y) \text{ accepts}] \geq \frac{1}{2} + \epsilon$
 $x \notin L \Rightarrow \Pr_y[M(x,y) \text{ rejects}] \geq \frac{1}{2} + \epsilon$

- if $x \in L$

$\Pr_y[M'(x, y') \text{ accepts}] \geq 1 - (\frac{1}{2})^{\Omega(k)}$

- if $x \notin L$

$\Pr_y[M'(x, y') \text{ rejects}] \geq 1 - (\frac{1}{2})^{\Omega(k)}$

April 22, 2021

CS151 Lecture 8

Randomized complexity classes

- We have shown:
 - polynomial identity testing is in **coRP**
 - a poly-time algorithm for detecting unique solutions to SAT implies
 $NP = RP$

April 22, 2021

CS151 Lecture 8

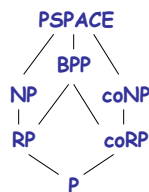
Relationship to other classes

- ZPP, RP, coRP, BPP, contain **P**
 - they can simply ignore the tape with coin flips
- all are in **PSPACE**
 - can exhaustively try all strings y
 - count accepts/rejects; compute probability
- **RP \subseteq NP** (and **coRP \subseteq coNP**)
 - multitude of accepting computations
 - **NP** requires only one

April 22, 2021

CS151 Lecture 8

Relationship to other classes



April 22, 2021

CS151 Lecture 8

BPP

- How powerful is **BPP**?
- We have seen an example of a problem in **BPP** that we only know how to solve in **EXP**.

Is randomness a **panacea** for intractability?

April 22, 2021

CS151 Lecture 8

BPP

- It is not known if **BPP = EXP** (or even **NEXP!**)
 - but there are strong hints that it does not
- Is there a deterministic simulation of **BPP** that does better than brute-force search?
 - yes, if allow non-uniformity

Theorem (Adleman): **BPP \subseteq P/poly**

April 22, 2021

CS151 Lecture 8

BPP and Boolean circuits

- Proof:
 - language $L \in \mathbf{BPP}$
 - error reduction gives TM M such that
 - if $x \in L$ of length n
 $\Pr_y[M(x, y) \text{ accepts}] \geq 1 - (1/2)^{n^2}$
 - if $x \notin L$ of length n
 $\Pr_y[M(x, y) \text{ rejects}] \geq 1 - (1/2)^{n^2}$

April 22, 2021

CS151 Lecture 8

BPP and Boolean circuits

- say “ y is bad for x ” if $M(x, y)$ gives incorrect answer
- for fixed x : $\Pr_y[y \text{ is bad for } x] \leq (1/2)^{n^2}$
- $\Pr_y[y \text{ is bad for some } x] \leq 2^n (1/2)^{n^2} < 1$
- Conclude: there exists some y on which $M(x, y)$ is **always correct**
- build circuit for M , hardwire this y

April 22, 2021

CS151 Lecture 8

BPP and Boolean circuits

- Does **BPP = EXP** ?
- Adleman’s Theorem shows:
BPP = EXP implies EXP \subseteq P/poly

If you believe that **randomness** is **all-powerful**, you must also believe that **non-uniformity** gives an **exponential advantage**.

April 22, 2021

CS151 Lecture 8

BPP

- Next:
further explore the relationship between
randomness
and
nonuniformity
- Main tool: **pseudo-random generators**

April 22, 2021

CS151 Lecture 8