

RANDOMIZED COMPLEXITY

TUESDAY NOVEMBER 22

MATRIX MULTIPLICATION

$L = \{ (M_1, M_2, N) \mid M_1, M_2 \text{ and } N \text{ are matrices and } M_1 M_2 = N \}$

If M_1 and M_2 are $n \times n$ matrices, multiplying them takes time at least $O(n^{2.37})$

$O(n^2)$ randomized algorithm:

If $M_1 M_2 \neq N$, then $\Pr [M_1 M_2 r = N r] \leq 1/2$

If we pick 300 random vectors and test them all, what is the probability failing?

TESTING POLYNOMIALS

Let p an n -variable polynomial over a finite field. How do we determine if p is always 0?

$$(2332x_1 + 4603x_2 - 3878x_3)(5566x_1 + 31x_4 - 171) \\ (677x_7 - 1)(x_5 + 7x_6 + 3x_2 + 1001x_1) = 0 \pmod{6709}$$

Theorem (Schwartz-Zippel): Let F be a finite field and let p be a nonzero polynomial on the variables x_1, x_2, \dots, x_m , where each variable has degree at most d .

If a_1, \dots, a_m are selected randomly in F , then:

$$\Pr [p(a_1, \dots, a_m) = 0] \leq md/|F|$$

Proof (by induction on m):

Base Case ($m = 1$):

$$\Pr [p(a_1) = 0] \leq d/|F|$$

A polynomial of degree d can have at most d roots

Inductive Step ($m > 1$):

Assume true for $m-1$ and prove true for m

Let x_1 be one of the variables

For each $i \leq d$ let p_i be the polynomial comprising the terms of p containing x_1^i , but where x_1^i has been factored out:

$$p = p_0 + x_1 p_1 + x_1^2 p_2 + \dots + x_1^d p_d$$

If $p(a_1, \dots, a_m) = 0$, one of two things can happen:

(1) All p_i evaluate to 0

(2) Some p_i doesn't evaluate to 0 and a_1 is a root of the single variable polynomial that results when evaluating p_0, \dots, p_m with a_2, \dots, a_m

$$p = p_0 + x_1 p_1 + x_1^2 p_2 + \dots + x_1^d p_d$$

If $p(a_1, \dots, a_m) = 0$, one of two things can happen:

(1) All p_i evaluate to 0

(2) Some p_i doesn't evaluate to 0 and a_1 is a root of the single variable polynomial that results when evaluating p_0, \dots, p_m with a_2, \dots, a_m

$$\Pr [(1)] \leq (m-1)d/|F|$$

$$\Pr [(2)] \leq d/|F|$$

$$\Pr [(1) \text{ or } (2)] \leq md/|F|$$

Theorem: Let F be a finite field and let p be a nonzero polynomial on the variables x_1, x_2, \dots, x_m , where each variable has degree at most d .

If a_1, \dots, a_m are selected randomly in F , then:

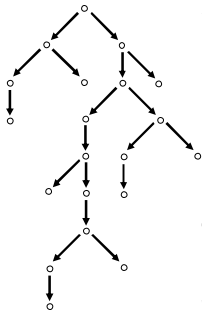
$$\Pr [p(a_1, \dots, a_m) = 0] \leq md/|F|$$

PROBABILISTIC ALGORITHMS

Why do we study probabilistic algorithms?

1. Can be simpler than deterministic
2. Can be more efficient than deterministic

PROBABILISTIC TMs



A probabilistic TM M is a non-deterministic TM where:

Each non-deterministic step is called a coin flip

Each non-deterministic step has only two legal next moves

The probability of branch b is:

$$\Pr [b] = 2^{-k}$$

Where k is the number of coin flips that occur on branch b

$$\Pr [M \text{ accepts } w] = \sum_{\substack{b \text{ is an accepting} \\ \text{branch}}} \Pr [b]$$

Definition: M recognizes language A with error probability ϵ if:

$w \in A$ implies that $\Pr [M \text{ accepts } w] \geq 1 - \epsilon$

$w \notin A$ implies that $\Pr [M \text{ doesn't accept } w] \geq 1 - \epsilon$

BPP = { $L \mid L$ is recognized by a probabilistic poly-time TM with error probability of $1/3$ }

Why $1/3$?

Theorem: Let ϵ be a constant strictly between 0 and 1/2 and $p(n)$ be a polynomial.

If M_1 has error probability ϵ then there exists an equivalent M_2 with error probability $2^{-p(n)}$

Proof Idea:

M_2 simply runs M_1 many times and takes the majority output

BPP = { L | L is recognized by a probabilistic poly-time TM with error probability of 1/3 }

Is BPP \subseteq NP?

Is NP \subseteq BPP?

Is BPP \subseteq PSPACE?

ZERO-POLY = { p | p is a polynomial over a finite field that is zero everywhere }

ZERO-POLY \in BPP

PRIMES = { p | p is a prime number }

PRIMES \in P

Definition: A language is in RP (randomized P) if there exists a nondeterministic polynomial time TM M such that:

If $x \notin A$ then no paths accept

If $x \in A$ then at least half of the paths accept

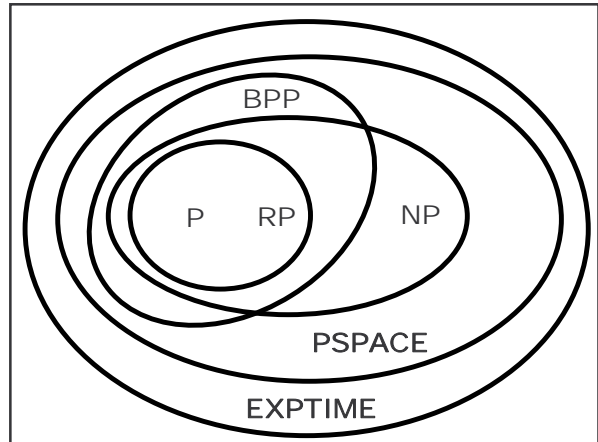
Theorem: Language A is in RP if and only if for all k there exists a probabilistic poly-time TM such that:

If $x \notin A$ then M(x) always rejects

If $x \in A$ then M(x) accepts with probability at least $1 - 2^{-|x|^k}$

Is $RP \subseteq NP$?

Is $RP \subseteq BPP$?



WWW.FLAC.WS

Read Chapter 10.2 of the book for next time