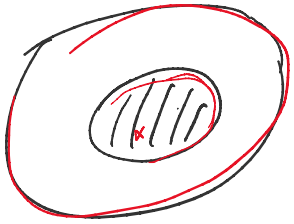

Pick a random $\underline{a}$

Miller-Rabin Rand. Alg'm

for $i = 1 \ldots t$ {
  pick $\underline{a} \in \{1, \ldots, N-1\}$ AT RANDOM
  if a is witness then return "composite"
}
return "prime"

polytime worst case

Analysis of Error Prob:

if N is prime, always correct

if N is composite,

$$\Pr(\text{error}) \le \frac{N/4}{N-1} \lesssim \frac{1}{4}$$

$\Rightarrow$ polytime Monte-Carlo alg'm
one-sided error

To lower err prob, repeat!

$$\Pr[\text{whole alg'm error}] = \Pr[\text{error in } \underline{\text{all}}\ t \text{ iterations}]$$

$$= \Pr\left(\bigcap_{i=1}^{t} \text{error in } i^{th} \text{ iterations}\right)$$

$$= \prod_{i=1}^{t} \Pr(\text{error in } i^{th} \text{ iter})$$

$$\le \prod_{i=1}^{t} \frac{1}{4}$$

$$= \frac{1}{4^t}$$

$\left(\Pr(\bigcap_i E_i) = \prod_i \Pr(E_i)\right.$ if E_i independent events$\left.\right)$

no bad input

Can error be completely removed?

Later: Adleman, Huang '87 Las Vegas polytime
Agrawal - Kayal - Saxena '02 det. polytime

Assumption: access to rand. number generator

rand-bit() $\to$ 0 or 1

rand(a, b) $\to$ a or a+1 or ... or b

assume unif. distributed
& independence ...

Quick Probability Review

events E, E', rand. var X, Y

$$\Pr(E \cup E') \le \Pr(E) + \Pr(E')$$ equal if disjoint

(called "union bd")

$$\Pr(E^c) = 1 - \Pr(E)$$

$$\Pr(E \cap E') = \Pr(E)\Pr(E')$$

$$\Pr\left(\bigcap_i E_i\right) = \prod_i \Pr(E_i)$$

if independent

$$\Pr(E \mid E') = \frac{\Pr(E \cap E')}{\Pr(E')}.$$

conditional prob.

$$E[X] = \sum_x x \cdot \Pr(X = x)$$ (integral if continuous)

$$E[X+Y] = E[X] + E[Y]$$

(linearity of expectation)

$$E[cX] = c\,E[X]$$

$$E[XY] = E[X]\,E[Y]$$

$$E\left[\prod X_i\right] = \prod E[X_i]$$

if independent

$$E(XY) = E(X)E(Y)$$

$$E\left(\prod_i X_i\right) = \prod_i E(X_i)$$

e.g. Markov's ineq: If $X \geq 0$ and $E(X) = \mu$,

$$\Pr[X \geq c\mu] \leq \frac{1}{c}.$$

(thus, Las Vegas converted to Monte Carlo w. worst-case runtime)

One-Line Pf:

$$\mu = E(X) \geq \sum_{x \geq c\mu} x \cdot \Pr(X = x) \geq \sum_{x \geq c\mu} c\mu \Pr(X = x)$$

$$= c\mu \Pr[X \geq c\mu]. \quad \square$$

e.g. Chebyshev's Ineq Let $\mu = E(X)$,

$$\sigma^2 = \mathrm{Var}(X) = E((X-\mu)^2)$$

$$(= E(X^2) - E(X)^2)$$

$$\Rightarrow \Pr(|X - \mu| \geq c\sigma) \leq \frac{1}{c^2}.$$

Pf: $\Pr((X-\mu)^2 \geq c^2\sigma^2)$ by Markov. $\square$

Randomized Complexity Classes

ZPP = all languages (i.e. decision problems) with Las Vegas alg'ms in expected polytime

"Zero-error Probabilistic Polytime"

RP = all languages L with one-sided Monte Carlo alg'ms A in worst-case polytime

... in worst-case poly...

s.t. $\forall$ input x,

$$\begin{cases} \text{if } x \in L \Rightarrow \Pr[\mathcal{A} \text{ outputs yes on } x] \geq \frac{1}{2} \\ \text{if } x \notin L \Rightarrow \Pr[\mathcal{A} \text{ outputs no on } x] = 1. \end{cases}$$

Rmk: $\frac{1}{2}$ can be changed to any const $\in (0,1)$ by repeating & taking OR of output (with t iterations, err prob $\leq \frac{1}{2^t}$).

(e.g. Miller-Rabin: COMPOSITE $\in$ RP)
Adleman-Huang: " $\in$ ZPP)
AKS: " $\in$ P)

Fact 1. $\underbrace{P \subseteq ZPP \subseteq RP}_{\text{(by Markov)}}$.

Fact 2. $RP \subseteq NP$.

Pf: certificate = seq of rand bits. $\square$

Fact 3. $ZPP = RP \cap co\text{-}RP$.

Pf: next time ...