Tiancheng Jiao
EECS 376
tcjiao

1- Probability

$Pr(A|B) = \frac{Pr(A \cap B)}{Pr(B)}$

Independent: $Pr(A \cap B) = Pr(A)Pr(B)$

Markov's Inequality: $Pr[X \geq a] \leq \frac{E[X]}{a}$ $(a > 0)$

or $Pr[X \geq a \cdot E[X]] \leq \frac{1}{a}$

即P中有比≥a的求和不能超过总数求和

次测试矩阵乘法 $AB = C$?, $Pr[ABr = Cr] \leq \frac{1}{2}$ $(r \in \{0,1\}^n)$ 若 $AB \neq C$)

方差 $Var[X_i] = E[X_i^2] - E[X_i]^2$

Chebyshev's inequality: $Pr[|X - E[X]| \geq a] \leq \frac{Var[X]}{a^2}$

$$Pr\left[\left|\frac{1}{n}X - E[X_i]\right| \geq \varepsilon\right] \leq \frac{Var(X_i)}{\varepsilon^2 n}$$

Chernoff-Hoeffding bounds:

$X_i \in [0,1]$, $Pr\left[\frac{1}{n} \leq E[X_i] - \varepsilon\right] \leq e^{-2\varepsilon^2 n}$ (lower tail bound)

$Pr\left[\frac{1}{n} \geq E[X_i] + \varepsilon\right] \leq e^{-2\varepsilon^2 n}$ (upper tail bound)

2- Cryptography Diffie-Hellman Protocol

large prime p, and its generator g

A random secret a, calculate g^a, give B

B random secret b, calculate g^b, give A

$g^{ab} = (g^a)^b = (g^b)^a$ is shared key

Fermat's Little Theorem

Any prime p, $0 < a < p$, $a^{p-1} \equiv 1 \pmod p$

Primality Test: random pick a $(1 < a < n)$, if $a^{n-1} \not\equiv 1 \pmod n$ return COMPOSITE else PRIME

Miller-Rabin Primality Test

Given (odd) n, write it as $n = 2^s d + 1$

Pick $a \in [2, p-1]$

If $a^{n-1} \equiv 1 \pmod n$ and $[(a^{2^r d} \equiv -1 \pmod n$ for some $0 \leq r < s)$ or $(a^d \equiv 1 \pmod n)]$,

return PRIME, else return COMPOSITE

Theorem: if n is prime, will return prime

if n is composite, Pr[returns composite] $\geq \frac{1}{2}$

Fermat's Little Theorem-Extended

$n=pq$ (p、q prime),

then $a^{1+k\phi(n)} \equiv a \pmod n$, ($\phi(n)=(p-1)(q-1)$)

$\phi(n)$ 为 Euler's Totient Function

RSA (extend Euclidean algorithm)

Generate $n=p\cdot q$, find $e\cdot d \equiv 1 \pmod{\phi(n)}$, make n、e public, p、q、d、$\phi(n)$ private

(n,e) is public key, d is private key, p、q可以不要

Encrypt: message m, calculate $c = m^e \pmod n$

Decrypt: $m' = c^d \pmod n = m^{de} \pmod n = m^{1+k\phi(n)} \pmod n \equiv m \pmod n$

Sign: message m, signature $s = m^d \pmod n$

Verify: check $s^e \equiv m \pmod n$

3、P vs NP

P = the set of all languages that can be decided by TM in polynomial time

NP: can verify in polynomial time, NP包含P

NP-hard: A language L is called NP-Hard if $L \in P$ implies that $NP = P$

SAT (satisfiability problem): 很多bool，通过and, or, not，找到为true的bool值

SAT是NP-hard

3-CNF: $(x \vee \neg y \vee z) \wedge (\neg x \vee z \vee w) \wedge \cdots$

clause: 一个组 $(x \vee \neg y \vee z)$，3-CNF是NP-Hard，也有3SAT

Language A is polynomial-time mapping reducible to language B, written $A \leq_p B$, if there is a poly-time computable mapping f such that:

$$x \in A \Leftrightarrow f(x) \in B$$

If $A \leq_p B$, then if $B \in P$ implies $A \in P$

for every $A \in NP$, $A \leq_p SAT$

怎样证明 NP-complete：先证明 $\in NP$，再用(或 $\leq_p$ 它)，证明 NP-Hard

在已知范围内，NP中既不是P又不是NP-Hard是不存在的，但理论上有可能

Search problem：不只是有或没有，要找到最优解
比如最大的 clique，最小的 vertex cover

考虑假设有 P-time decider，每次调用来判断/选择

α-approximation：α 是算法返回量/理论最优量
可以 >1，也可以 <1
比如 vertex cover >1
knapsack <1

incident：e is incident to v
adjacent

Independent set：其中k个 vertex，两两不 adjacent，即其中一个 edge 都没有