高级算法设计与分析-Lecture 1

2020年2月17日 12:38

Birthday Paradox

一年 N 天，k 人

$\Pr(\exists 2人同一天生日)$

$= 1 - \Pr(\nexists 2人同一天生日)$

$= 1 - (1-\frac{1}{N})(1-\frac{2}{N})\cdots(1-\frac{k-1}{N})$

$\geq 1 - e^{-\frac{1}{N}} \cdot e^{-\frac{2}{N}} \cdots e^{-\frac{k-1}{N}}$

$= 1 - e^{-\frac{k(k-1)}{2N}}$

$\sim 1 - e^{-1} \approx 63\%$

$k \sim \sqrt{2N+1}$

$x \in (0,1)$

$e^{-x} = 1 - x + \frac{x^2}{2!} - \frac{x^3}{3!} + \cdots$ （$\frac{x^2}{2!} - \frac{x^3}{3!} + \cdots > 0$，$x > 0$）

$e^{-x} > 1 - x$

$n^2 \to 2n^3 + n\log n$

$f, g : \mathbb{N} \to \mathbb{N}$.

$O(n^3) \cdot \Omega(n^3) = \Theta(n^3)$

$f(n) = O(g(n))$. $\exists C > 0$. $f(n) \leq C \cdot g(n)$.

$f(n) = \Omega(g(n))$ $\exists C > 0$. $f(n) \geq C \cdot g(n)$

$f(n) = O(g(n))$ & $f(n) = \Omega(g(n))$

$f(n) = \Theta(g(n))$

$k = \Theta(\sqrt{N})$

$\Pr(\exists 2人同一天生日) = constant$

生日攻击 (Hash函数)

SHA-256: $\{0,1\}^* \to \{0,1\}^{256}$

$x \neq y$. $H(x) = H(y)$

$\Pr(H(x) = 00\cdots0) = \frac{1}{2^{256}}$

$= \Pr(H(x) = 00\cdots01)$

$= \cdots$

$= \Pr(H(x) = 1\cdots11)$

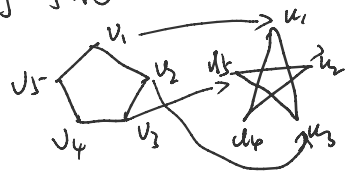
$N = 2^{256}$

$\sqrt{N} \sim 2^{128} \cdot C = m$

$x_1, x_2, \cdots, x_m$

$\exists H(x_i) = H(x_j)$ $\Pr(\cdots) \geq 0.9$

同构. (GI)



Alice如何向Bob证明 $G \cong H$？(Bob有计算能力有限)

同构. ✓

$u_1 \cdots u_n$ $v_1 \cdots v_n$

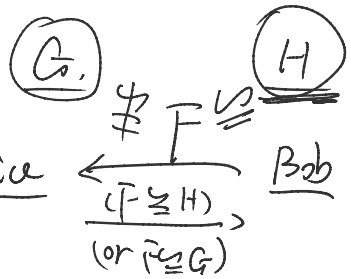
$f: u_1 \to v_2$

$u_2 \to v_1$

$\vdots$

$u_n \to v_{n-3}$

Alice $\xrightarrow{f}$ Bob



Bob 随机选取 G/H 之一. permute 所有顶点. 记所得的图为 F.

根据算法：repeat 10次... H…G HH…G

$F_1, F_2 \cdots F_{10}$

$\Pr(\text{Bob accepts } G \cong H \mid G \cong H) = (\frac{1}{2})^{10} = \frac{1}{1024}$.