Cryptography: Birthday Paradox

Yiheng Lin, Zhihao Jiang

1

1

Theorem 1.1. Let $S = \{1, 2, \cdots, N\}$. For n times, uniformly randomly draw one element from set S. Let x_t be the element we draw at time t. Then $\forall p > 0$, there exists a constant C_1 such that when $n \geq C_1\sqrt{N}$, we have

$$Pr[\exists 1 \leq i, j \leq n, i \neq j \text{ such that } x_i = x_j] > p$$

.

Proof. Let X denote the event that $\exists i, j \leq t, i \neq j$ such that $x_i = x_j$, then we have

$$\begin{aligned} Pr[\bar{X}] &= \frac{N(N-1)\cdots(N-n+1)}{N^n} \\ &= \prod_{i=1}^{n-1}(1 - \frac{i}{N}) \\ &\leq \prod_{i=1}^{n-1} exp(-\frac{i}{N}) \\ &= exp(-\frac{n(n-1)}{2N}) \end{aligned} \tag{1}$$

Let $C_1 = \sqrt{-2ln(1-p)} + 1$. Then when $n \geq C_1\sqrt{N}$, we have

$$n(n-1) > (1 + \sqrt{-2ln(1-p) \cdot N})(\sqrt{-2ln(1-p) \cdot N}) > 2ln(2) \cdot N \tag{2}$$

Which is equivalent to $-\frac{n(n-1)}{2N} < ln(1-p)$. Thus use (1) we have

$$Pr[\bar{X}] \leq exp(-\frac{n(n-1)}{2N}) < 1 - p$$

So we have

$$Pr[X] > p$$

□

2

Lemma 1.1. For positive integer $n < N$, we have

$$\sum_{i=1}^{n-1} ln(1 - \frac{i}{N}) > -\frac{n^2}{N}$$

Proof. Notice that $\forall x \in [1-\frac{i+1}{N}, 1-\frac{i}{N}]$ $(0 \le i \le n)$, we have $ln(x) < ln(1-\frac{i}{N})$. Thus

$$\frac{1}{N} ln(1-\frac{i}{N}) \ge \int_{1-\frac{i+1}{N}}^{1-\frac{i}{N}} ln(x)dx$$

Thus we have

$$\begin{aligned}\frac{1}{N}\sum_{i=1}^{n-1} ln(1-\frac{i}{N}) &\ge \int_{1-\frac{n}{N}}^{1} ln(x)dx \\ &= (xln(x)-x)|_{1-\frac{n}{N}}^{1} \\ &= -\frac{n}{N} - (1-\frac{n}{N})ln(1-\frac{n}{N}) \\ &> -\frac{n}{N} - (1-\frac{n}{N})(-\frac{n}{N}) \\ &= -\frac{n^2}{N^2}\end{aligned} \tag{3}$$

Thus

$$\sum_{i=1}^{n-1} ln(1-\frac{i}{N}) > -\frac{n^2}{N}$$

□

Theorem 1.2. Let $S = \{1, 2, \cdots, N\}$. For n times, uniformly randomly draw one element from set S. Let x_t be the element we draw at time t. Then $\forall p > 0$, there exists a constant C_2 such that when $n \le C_2\sqrt{N}$, we have

$$Pr[\exists 1 \le i, j \le n, i \ne j \text{ such that } x_i = x_j] < p$$

.

Proof. Let X denote the event that $\exists i, j \le t, i \ne j$ such that $x_i = x_j$.

Use Lemma 1.1, we have

$$\begin{aligned}Pr[\bar{X}] &= \frac{N(N-1)\cdots(N-n+1)}{N^n} \\ &= \prod_{i=1}^{n-1}(1-\frac{i}{N}) \\ &= exp(\sum_{i=1}^{n-1} ln(1-\frac{i}{N})) \\ &> exp(-\frac{n^2}{N})\end{aligned} \tag{4}$$

Let $C_2 = \sqrt{-ln(1-p)}$. Then when $n \le C_2\sqrt{N}$, we have

$$exp(-\frac{n^2}{N}) \ge 1-p$$

So $Pr[\bar{X}] > 1-p$, thus

$$Pr[X] < p$$

□

Acknowledgement: