CHƯƠNG 2

BỔ SUNG KIẾN THỨC VỀ TOÁN

Tài liệu: Handbook of Applied Cryptography

Katz Jonathan, Menezes Alfred J, Van Oorschot Paul C, Vanstone Scott A

CRC Press

Nội dung

- Lý thuyết xác suất
- Lý thuyết thông tin
- Lý thuyết về số học

Xác suất

- $P[\text{sự } kiện\ A] = \frac{\#\ \text{sự } kiện \text{ sơ } cấp \text{ của } A}{\sum \text{sự } kiện \text{ sơ } cấp}$

Ví dụ 1:

- Tung xúc xắc 1 lần. Gọi A là số chấm xuất hiện. $\mathrm{P}[A = k] = {}^{1}/_{6}$
- Tung xúc xắc 2 lần độc lập. Gọi A là tổng số chấm. $\mathrm{P}[A = 3] = {}^{1}/_{18}$

Xác suất

- Ví dụ 2: Bài toán trùng ngày sinh nhật

Trong một phòng khách có n người. Hỏi khả năng xảy ra hai người có trùng ngày sinh là bao nhiêu?

- Bài toán tương tự:

Trong 1 bình chứa m quả bóng đánh số khác. Rút ngẫu nhiên lần lượt từng quả có hoàn lại. Tính xác suất sau n lần rút xuất hiện ít nhất hai quả giống nhau?

Xác suất

- Kết quả tổng quát:

$$P(m,n) = 1 - \frac{m(m-1)\dots(m-n+1)}{m^n}$$

$$\approx 1 - e^{-\frac{n^2}{2m}} \approx \frac{n^2}{2m} \; khi \; m \to \infty$$

- $P(m = 365, n = 23) \approx 1 - e^{-\frac{23^2}{2*365}} \approx 0.52$

- Trung bình số lần rút trước khi lặp lại quả đã rút là

$$\sqrt{\frac{\pi m}{2}}$$

Xác suất

- Ví dụ (về đung độ của hàm băm):

$$H(s) = \underbrace{11001 \ldots 10}_{n\ bit}, \qquad \forall\ x\hat{a}u\ s$$

  - Hỏi số trung bình thử các xâu đầu vào s là bao nhiêu để bắt gặp có 2 xâu cho cùng kết quả?
  - $\approx 2^{n/2}$

Entropy (Độ không chắc chắn)

- **Định nghĩa**: Giả sử X là một biến ngẫu nhiên nhận các giá trị $\{x_1, x_2, \dots, x_n\}$ và $P[X = x_i] = p_i$.

Entropy của X được xác định là:

$$H(X) = -\sum_{i=1}^{n} p_i log_2 p_i$$

$$với\ qui\ ước\ p_i = 0\ thì\ log_2 p_i = 0$$

Tính chất của Entropy

- $0 \leq H(X) \leq log_2 n$

  ($log_2 n$ phản ánh số đơn vị thông tin của n)

- $H(X) = 0 \Leftrightarrow p_i = 1$ với một số i và $p_i = 0$ với i còn lại,

  nghĩa là không có kết quả nào xuất hiện của X là không chắc chắn

- $H(X) = log_2 n \Leftrightarrow p_i = {}^1/_n \ \forall i$,

  nghĩa là tất cả các khả năng của X đều xảy ra như nhau

Hợp entropy của hai biến ngẫu nhiên

- $H(X,Y) = -\sum_{x,y} P(X=x, Y=y) log_2(P(X=x, Y=y)$

- $H(X,Y) \leq H(X) + H(Y)$

$$\text{Dấu} = \Leftrightarrow X, Y \text{độc } lập$$

Entropy điều kiện của hai biến ngẫu nhiên

- $H(X|Y = y)$

$$= -\sum_{x} P(X = x \mid Y = y) log_2(P(X = x \mid Y = y)$$

- $H(X|Y) = \sum_y P(Y = y)H(X \mid Y = y)$

Tính chất của entropy điều kiện

- $H(X|Y = y)$

$$= -\sum_{x} P(X = x \mid Y = y) log_2(P(X = x \mid Y = y)$$

- $H(X|Y) = \sum_y P(Y = y) H(X \mid Y = y)$

Lý thuyết số học

Định nghĩa:

Cho a, b là 2 số tự nhiên. Ta nói a chia hết b (hoặc a là ước của b; b chia hết cho a; a là nhân tử của b) nếu tồn tại số tự nhiên c sao cho $b = ac$

Khi a là ước số của b, ta ký hiệu $a \mid b$

Ví dụ:

- $5 \mid 15$
- $17 \mid 85$

Tính chất của phép chia:

- $a \mid a$
- Nếu $a \mid$ b và b $\mid c$ thì $a \mid c$
- Nếu $a \mid b$ và $a \mid$ c thì $a \mid (bx + cy)$, với $\forall\, x, y \in \mathbb{Z}$
- Nếu $a \mid$ b và b $\mid$ a thì $a = \pm b$

Định nghĩa: *(Phép chia hai số tự nhiên)*

Cho a, b là 2 số tự nhiên với $b \geq 1$, phép chia a cho b được thương là q và dư r sao cho:

$$a = qb + r, \text{ ở đó } 0 \leq r < b.$$

Cặp q, r là duy nhất. Ký hiệu phần thương và dư lần lượt là $a\ div\ b$, và $a\ mod\ b$.

Ví dụ:

- 15 mod 4 = 3, 15 div 4 = 3

Định nghĩa: *(ước số chung)*

- Số tự nhiên c gọi là ước chung của a và b nếu c|a và $c|b$.
- Một số không âm d gọi là ước chung lớn nhất của a và b, ký hiệu d = gcd(a, b), nếu thỏa mãn 2 điều kiện sau:
  - ✓ d là ước chung của a và b; và
  - ✓ ∀ c|a và c|b thì c|d

Ví dụ:

- gcd(15,10) = 5

Định nghĩa: *(bội số chung nhỏ nhất)*

Một số không âm d gọi là bội số chung nhỏ nhất của a và b, ký hiệu $d = \text{lcm}(a, b)$, nếu thỏa mãn 2 điều kiện sau:

- ✓ $a|d$, $b|d$
- ✓ $\forall$ $a|c$ và $b|c$ thì $d|c$

Chú ý: $ab = \text{lcm}(a, b).\gcd(a, b)$

Ví dụ:

- lcm(15,10) = 30

Định nghĩa: *(hai số nguyên tố cùng nhau)*

Hai số tự nhiên a, b gọi là nguyên tố cùng nhau nếu $\gcd(a, b) = 1$

Ví dụ:

- 21 và 17 là nguyên tố cùng nhau vì gcd(21,17) = 1

Định nghĩa: *(số nguyên tố)*

Số tự nhiên a gọi là số nguyên tố a chỉ có ước dương duy nhất là 1 và chính nó.
Nếu a không là số nguyên tố thì được gọi là hợp số.

Ví dụ:

- 17 là số nguyên tố
- 21 là hợp số

Tính chất của số nguyên tố:

- Nếu p là số nguyên tố và $p|ab$ thì $p|a$ hoặc $p|b$
- Tập các số nguyên tố là vô hạn
- $\lim_{x\to\infty} \frac{\pi(x)}{x/logx} = 1$, với $\pi(x)$ ký hiệu số các số nguyên tố $\leq x$.

Định lý: *(về phân tích ra thừa số nguyên tố)*

Mọi số tự nhiên n ≥ 2 đều được phân tích thành tích của lũy thừa các số nguyên tố:

$$n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k},$$

ở đó p_i là các số nguyên tố. Sự phân tích trên là duy nhất không kể thứ tự.

Ví dụ:

- $105 = 3.5.7$
- $196 = 2^2.7^2$

Tìm gcd và lcm của hai số:

Giả sử a = $p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$ và b = $p_1^{f_1} p_2^{f_2} \dots p_k^{f_k}$, khi đó:

- $\gcd(a, b) = p_1^{\min(e_1, f_1)} p_2^{\min(e_2, f_2)} \dots p_k^{\min(e_k, f_k)}$
- $\text{lcm}(a, b) = p_1^{\max(e_1, f_1)} p_2^{\max(e_2, f_2)} \dots p_k^{\max(e_k, f_k)}$

Định nghĩa: *(hàm Ơ le)*

Với số tự nhiên n ≥ 2, ký hiệu $\phi(n)$ là số các số tự nhiên trong khoảng $[1, n]$ mà nguyên tố cùng nhau với n.

Ví dụ:

- $\phi(10) = 4$ vì trong khoảng từ 1,…,10 có 4 số nguyên tố cùng nhau với 10 là: 1, 3, 7, 9

Tính chất của hàm Ơ le:

- Nếu p là số nguyên tố thì $\phi(p) = p - 1$
- Hàm ϕ bảo toàn với phép nhân, tức là nếu

  $\gcd(m, n) = 1$ thì $\phi(m.n) = \phi(\mathrm{m}).\ \Phi(\mathrm{n}).$
- Nếu có phân tích thành nhân tử $\mathrm{n} = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$

  thì: $\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \ldots (1 - \frac{1}{p_k})$

Lý thuyết đồng dư

Định nghĩa:

Với 2 số tự nhiên a, b, khi đó a được gọi là đồng dư với b modulo n, ký hiệu $a \equiv b \pmod{n}$, nếu $n \mid (a - b)$. Số n gọi là modulo của đồng dư.

Ví dụ:

- $15 \equiv 3 \pmod{4}$ vì $4 \mid (15-3)$

Tính chất của đồng dư:

- $a \equiv b\ (mod\ n) \Leftrightarrow a, b$ có cùng số dư khi chia cho n.
- $a \equiv a\ (mod\ n)$
- $a \equiv b\ (mod\ n)\ \Rightarrow b \equiv a\ (mod\ n)$
- Nếu $a \equiv b\ (mod\ n), b \equiv c\ (mod\ n)\ \Rightarrow\ a \equiv c\ (mod\ n)$
- Nếu $a \equiv b\ (mod\ n), c \equiv d\ (mod\ n)$

$$\Rightarrow\ a + c \equiv b + d\ (mod\ n)$$

$$\Rightarrow\ ac \equiv bd\ (mod\ n)$$

Lý thuyết đồng dư

Định nghĩa: *(tập các lớp đồng dư)*

Tập các số tự nhiên modulo n, ký hiệu $\mathbb{Z}_n$, là tập các số tự nhiên gồm $\{0, 1, \dots, n-1\}$ (hay chính xác là lớp các số có cùng số dư). Ở đó các phép toán cộng ,trừ, nhân được thực hiện theo modulo n.

Ví dụ:

- Trong $\mathbb{Z}_{13}$ thì 6+7 =0, 7+9 = 3

Lý thuyết đồng dư

Định nghĩa: *(nghịch đảo modulo)*

Giả sử $a \in \mathbb{Z}_n$, ta gọi nghịch đảo modulo n của a (nếu có) là số x sao cho $ax \equiv 1 \ (mod\ n)$.

Trong trường hợp tồn tại x thì ta nói a khả nghịch và nghịch đảo của a ký hiệu là a^{-1}.

Phép chia a cho b theo modulo n là phép nhân a với nghịch đảo của b nếu tồn tại.

Ví dụ:

- Trong $\mathbb{Z}_9$ thì 5, 7 khả nghịch và $5^{-1} = 2, 7^{-1} = 4$
- Và trong $\mathbb{Z}_9$ thì 5:7 = 5.4 = 2

Kết quả chú ý:

- $a \in \mathbb{Z}_n, a$ khả nghịch $\Leftrightarrow \gcd(a, n) = 1$
- Hệ phương trình:

$$\begin{cases} x \equiv a_1 \ (mod\ n_1) \\ x \equiv a_2 \ (mod\ n_2) \\ \vdots \\ x \equiv a_k \ (mod\ n_k) \end{cases}$$

ở đó $\{n_i\}$ là nguyên tố cùng nhau từng đôi có nghiệm duy nhất $x \equiv \sum_{i=1}^{k} a_i N_i M_i \ (mod\ n), n = n_1 n_2 \dots n_k,$

$N_i = n/n_i\ , M_i = N_i^{-1}\ mod\ n_i\ .$

Nhóm $\mathbb{Z}_n^*$

Định nghĩa:

Ta gọi nhóm với phép nhân modulo n của $\mathbb{Z}_n$ là:

$$\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \mid gcd(a, n) = 1\}$$

Ví dụ:

- $\mathbb{Z}_8^* = \{1, 3, 5, 7\}$
- $\mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$
- $\mathbb{Z}_n^*$ có số phần tử bằng với số các số $\leq n$ và nguyên tố cùng nhau với n. Do đó số phần tử của $\mathbb{Z}_n^*$ là $\phi(n)$

Nhóm $\mathbb{Z}_n^*$

Định nghĩa: *(cấp của nhóm $\mathbb{Z}_n^*$)*

Ta gọi cấp của $\mathbb{Z}_n^*$ là số phần tử trong $\mathbb{Z}_n^*$ và ký hiệu là $|\mathbb{Z}_n^*|$.

Ta có $|\mathbb{Z}_n^*| = \phi(n)$

Ví dụ:

- $|\mathbb{Z}_{25}^*| = \phi(25) = 20$

Nhóm $\mathbb{Z}_n^*$

Kết quả chú ý:

- Nếu $a \in \mathbb{Z}_n^*$ thì $a^{\Phi(n)} \equiv 1(mod\ n)$
- Nếu p là số nguyên tố và $gcd(a, p) = 1$ thì

$$a^{p-1} \equiv 1(mod\ p)$$

- $\forall a \in \mathbb{Z}, a^p \equiv a(mod\ p)$

Nhóm $\mathbb{Z}_n^*$

Định nghĩa: *(cấp của phần tử trong $\mathbb{Z}_n^*$)*

Ta gọi cấp của $a \in \mathbb{Z}_n^*$, ký hiệu $\text{ord}(a)$, là số nguyên dương nhỏ nhất t sao cho $a^t \equiv 1 (mod\ n)$

Ví dụ: Trong $\mathbb{Z}_{21}^* = \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$
có $|\mathbb{Z}_{21}^*| = 12$

a	1	2	4	5	8	10	11	13	16	17	19	20
$\text{ord}(a)$	1	6	3	6	2	6	6	2	3	6	6	2

❖ Cấp của các phần tử đều là ước số của 12

Nhóm $\mathbb{Z}_n^*$

Định nghĩa: *(phần tử sinh của $\mathbb{Z}_n^*$)*

Giả sử $a \in \mathbb{Z}_n^*$, nếu $\text{ord}(a) = \phi(n)$ thì a được gọi là phần tử sinh của $\mathbb{Z}_n^*$.

Nếu $\mathbb{Z}_n^*$ có phần tử sinh thì ta nói $\mathbb{Z}_n^*$ là nhóm cyclic.

Ví dụ:

- $\mathbb{Z}_9^* = \{1, 2, 4, 5, 7, 8\}$, có 2 phần tử sinh là 2 và 5 nên là cyclic

a	1	2	4	5	7	8
$\text{ord}(a)$	1	6	3	6	3	2

- $\mathbb{Z}_{21}^*$ không có phần tử sinh nên không là nhóm cyclic

Phần tử sinh của $\mathbb{Z}_n^*$

Kết quả chú ý:

- $\mathbb{Z}_n^*$ có phần tử sinh $\Leftrightarrow n = 2, 4, p^k \; hoặc \; 2p^k$, với p là số nguyên tố lẻ
- Nếu a là phần tử sinh của $\mathbb{Z}_n^*$ thì

$$\mathbb{Z}_n^* = \{a^i \; mod \; n \; | 0 \leq i \leq \phi(n) - 1\}$$

- Nếu $a \in \mathbb{Z}_n^*$ là phần tử sinh thì $a^i \; mod \; n$ cũng là phần tử sinh của $\mathbb{Z}_n^*$. Do đó nếu $\mathbb{Z}_n^*$ là cyclic thì $\mathbb{Z}_n^*$ có $\phi(\phi(n))$ phần tử sinh

Thặng dư bậc hai modulo n

Định nghĩa:

Giả sử $a \in \mathbb{Z}_n^*$, a được gọi là thặng dư bậc hai hay số chính phương modulo n nếu tồn tại $x \in \mathbb{Z}_n^*$ sao cho $x^2 \equiv a \ (mod\ n)$.

Ngược lại thì a gọi là phi thặng dư bậc hai modulo n.

Ký hiệu tập các thặng dư, phi thặng dư bậc hai của $\mathbb{Z}_n^*$ là $Q_n, \bar{Q}_n$

Ví dụ:

- $\mathbb{Z}_9^* = \{1, 2, 4, 5, 7, 8\}$, có:

  $Q_9 = \{1, 4, 7\}$, $\bar{Q}_9 = \{2, 5, 8\}$

Căn bậc hai modulo n

Định nghĩa:

Giả sử $a \in Q_n$, nếu $x \in \mathbb{Z}_n^*$ thỏa mãn $x^2 \equiv a \ (mod\ n)$ thì x gọi là căn bậc hai của a modulo n.

Ví dụ:

- Trong $\mathbb{Z}_9^* = \{1, 2, 4, 5, 7, 8\}$ thì 2 và 7 là căn bậc hai của 4 modulo 9

Căn bậc hai modulo n

Kết quả chú ý:

- Nếu p là số nguyên tố lẻ và $p \in Q_n$ thì p có chính xác hai căn bậc hai
- $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$, ở đó p_i là các số nguyên tố lẻ đôi một khác nhau thì với mỗi $a \in Q_n$ sẽ có 2^k căn bậc hai của a

Ký hiệu Legendre

Định nghĩa:

Giả sử p là số nguyên tố lẻ, a là số tự nhiên. Ký hiệu Legendre $\left(\frac{a}{p}\right)$ xác định bởi:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 \ \ nếu\ p|a \\ 1 \ \ nếu\ a \in Q_p \\ -1\ nếu \ \ a \in \bar{Q}_p \end{cases}$$

Ví dụ:

- $\left(\frac{5}{9}\right) = -1, \qquad \left(\frac{4}{9}\right) = 1$

Ký hiệu Legendre

Kết quả chú ý: Nếu p và q là hai số nguyên tố lẻ khác nhau thì

- Định lý Euler: $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \ (mod\ p)$.

$$\text{Đặc biệt } \left(\frac{1}{p}\right) = 1, \left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$$

- $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$, nếu $a \in \mathbb{Z}_p^*$ thì $\left(\frac{a}{p}\right)^2 = 1$

- Nếu $a \equiv b \ (mod\ p)$ thì $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

- Luật tương hỗ: $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{(p-1)(q-1)/4}$

Ký hiệu Jacobi (mở rộng của Legendre)

Định nghĩa:

Giả sử $n \geq 3$ có phân tích ra thừa số nguyên tố $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$.

Khi đó ký hiệu Jacobi $\left(\frac{a}{n}\right)$ xác định bởi:

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{e_1} \left(\frac{a}{p_2}\right)^{e_2} \dots \left(\frac{a}{p_k}\right)^{e_k}$$

Ví dụ:

- $\left(\frac{5}{21}\right) = \left(\frac{5}{3}\right) * \left(\frac{5}{7}\right) = (-1) * (-1) = 1$

Ký hiệu Jacobi

Kết quả chú ý: m, n *lẻ và* ≥ 3

- $\left(\frac{a}{n}\right) \in \{0,1,-1\}, \left(\frac{a}{n}\right) = 0 \Leftrightarrow gcd(a,n) \neq 1.$
- $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$
- $\left(\frac{a}{nm}\right) = \left(\frac{a}{n}\right)\left(\frac{a}{m}\right)$
- Nếu $a \equiv b \ (mod\ n)$ thì $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$
- $\left(\frac{1}{n}\right) = 1, \left(\frac{-1}{n}\right) = (-1)^{(n-1)/2}, \left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8}$
- Luật tương hỗ:

$$\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right)(-1)^{(m-1)(n-1)/4}$$