Lecture 3 March, 6, 9

Date / /

No. 3-1

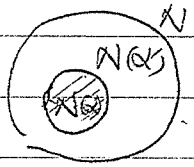
Principle of Inclusion and Exclusion (PIE, 容斥原理)

(Inside) (Outside)

1. One property: α, α': the property which is not α or $\alpha' = \sim\alpha$ (Negation of α)

Let N be set of all items we count.

$N(\alpha)$: the # of items in N with property α.

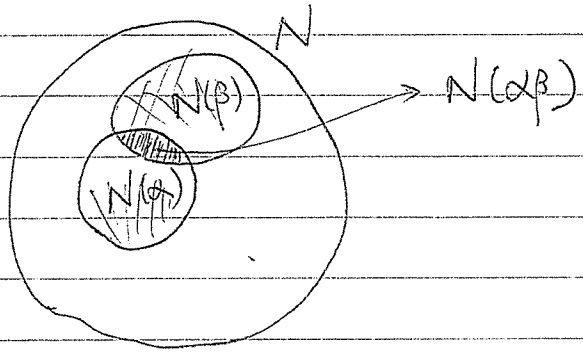


$N(\alpha')$: ——— without property α

(•) $N(\alpha') = N - N(\alpha)$.

2. Two properties α and β

We use $\alpha\beta$ to denote the property satisfying α and β.



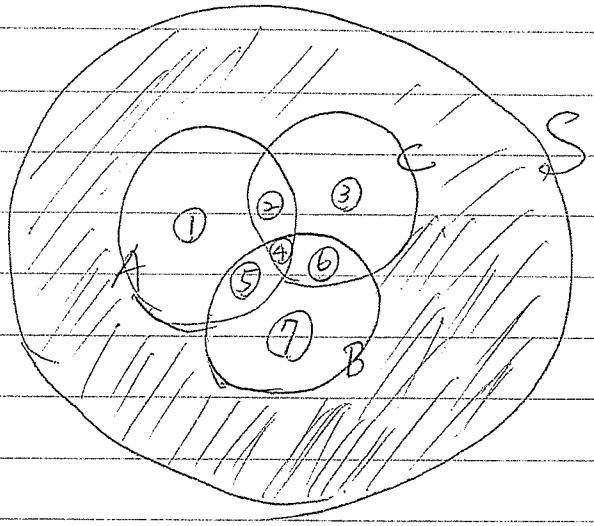
$\alpha'\beta' \approx (\sim\alpha)\cdot(\sim\beta)$

Read: not "α" and not "β".

(••) $N(\alpha'\beta') = N - N(\alpha) - N(\beta) + N(\alpha\beta)$.

(•••) $N(\alpha'\beta'\gamma') = N - (N(\alpha)+N(\beta)+N(\gamma)+(N(\alpha\beta)+N(\alpha\gamma)+N(\beta\gamma))$

$- N(\alpha\beta\gamma)$.



A : Items with property α $\quad |A| = N(\alpha)$

B : " β $\quad |B| = N(\beta)$

C : " γ $\quad |C| = N(\gamma)$

$N(\alpha)+N(\beta)+N(\gamma) = (①+②+④+⑤)+(②+③+④+⑥)+(④+⑤+⑥+⑦)$

$= \underline{①+②+③+④+⑤+⑥+⑦} + \underline{②+④+⑥+④}$ ——(1)

$+⑤$; $=$

$(②+④)+(④+⑥)+(④+⑤)-④$ ——(2)

$N(\alpha'\beta'\gamma') = |S \setminus (A \cup B \cup C)|$

$= N-(1)+(2) = (\cdots)$ (Last page)

r properties

Theorem (PIE) $N(\alpha_1'\alpha_2'\cdots\alpha_r') = N - \sum_{i=1}^{r} N(\alpha_i) + \sum_{1\le i\ne j\le r} N(\alpha_i\alpha_j)$

$- \sum_{i,j,k} N(\alpha_i\alpha_j\alpha_k) + \cdots + (-1)^r N(\alpha_1\alpha_2\cdots\alpha_r)$.

Proof. Consider an item @.

If @ has property α_j, then @ is counted once in N and once in $\sum_{i=1}^{r} N(\alpha_i)$. Hence, contributes "0" to the right hand side. If @ has properties j and k, then @ is counted once in N, twice in $\sum_{i=1}^{r} N(\alpha_i)$ and once in $\sum_{i<j} N(\alpha_i \alpha_j)$. Hence, @ contributes "$1-2+1=0$" to the right hand side. So, assume that @ has properties $j_1, j_2, \cdots, j_s$ where $s \le r$. Then @ contributes $\underbrace{1-\binom{s}{1}+\binom{s}{2}+\cdots+(-1)^s\binom{s}{s}}_{\| \; (1+(-1))^s = 0}$ to the right hand side.

On the other hand, if @ contains no properties, then @ is counted once in N, but "0" in the other terms. Hence, @ contributes "1" to the right hand side, this concludes the proof. ∎

One most popular application : Derrangement

(Hatcheck problem or Baseball cap problem)

(◦)

1	2	⋯	n
a_1	a_2	⋯	a_n

$a_i \neq i \quad \forall\, i = 1, 2, \cdots, n$

Definition A derrangement of an n-set $A=\{1,2,\cdots,n\}$ is a permutation φ of A such that for each $i \in A$, $\varphi(i) \neq i$. The number of different derrangements of A is denoted by D_n.

(*) The problem asks for the probability "$D_n/n!$".

Solution for D_n

Let α_i be the property that $\varphi(i)=i$, $i \in A$.

Therefore D_n is the number of permutations satisfying $\alpha_1'\alpha_2'\cdots\alpha_n'$.

$$N(\alpha_1'\alpha_2'\cdots\alpha_n') = N - \sum_{i=1}^{n} N(\alpha_i) + \sum_{i\neq j}^{n} N(\alpha_i\alpha_j) + \cdots + (-1)^n N(\alpha_1\alpha_2\cdots\alpha_n)$$

(sometimes $N(0)$)

$$= n! - \binom{n}{1}(n-1)! + \binom{n}{2}\cdot(n-2)! + \cdots + \binom{n}{r}(n-r)! + \cdots + \binom{n}{n}\cdot 1$$

$$= n!\left(1 - \binom{n}{1}\frac{1}{n} + \binom{n}{2}\cdot\frac{1}{n\cdot(n-1)} + \cdots + (-1)^n/n!\right)$$

$$= n!\left(1 - 1 + \frac{1}{2!} - \frac{1}{3!} + \cdots + (-1)^n/n!\right)$$

$$\approx n!\cdot e^{-1} \quad (\text{As } n \to +\infty)$$

$$D_n/n! \approx \frac{1}{e}.$$

We may also consider special permutations.

Example 1 A permutation of $\{1,2,\cdots,n\}$ without two consecutive integers.

Sol. Let α_i be the property that $i\,i+1$ occurs in permutation, $i=1,2,\cdots,n-1$. Therefore, we have $n-1$ properties and the number of permutations without $\alpha_1, \alpha_2, \cdots, \alpha_{n-1}$ is

$$N(0) = N(\alpha_1'\alpha_2'\cdots\alpha_{n-1}')$$

$$= N - \sum_{i=1}^{n-1} N(\alpha_i) + \sum_{i\neq j} N(\alpha_i\alpha_j) + \cdots + (-1)^{n-1} N(\alpha_1\alpha_2\cdots\alpha_{n-1})$$

$$= n! - \binom{n-1}{1}\cdot(n-1)! + \binom{n-1}{2}\cdot(n-2)! - \cdots + (-1)^{n-1}\cdot\binom{n-1}{n-1}\cdot 1!$$

$$= \sum_{i=0}^{n-1} (-1)^i \binom{n-1}{i}(n-i)!$$

$$= 5 \text{ min. later} = \boxed{D_n + D_{n-1}}$$

3-5

Example 2. (problème des rencontres)

(The permutations with exactly r agreements $a_i = i$. $(a_1 a_2 \cdots a_n)$)

Let the number of such permutations be $D_n^{(r)}$.

Clearly, $D_n^{(r)} = \boxed{\binom{n}{r}\cdot D_{n-r}} = \frac{n!}{(n-r)!\,r!}\cdot(n-r)!\cdot\left(1-1+\frac{1}{2!}-\frac{1}{3!}+\cdots+(-1)^{n-r}/(n-r)!\right)$

$$= \frac{n!}{r!}\left(1-1+\frac{1}{2!}-\frac{1}{3!}+\cdots+(-1)^{n-r}/(n-r)!\right).$$

(*) Counting the number of "Special" permutations is the most important objects in "Enumerative Combinatorics".

Many applications can be derived from (or into) permutations.

Ref. Combinatorics of Genome Rearrangements

Generalized PIE (r properties in total)

(**) The number of objects with exactly m properties, e_m, is equal to

$$S_m - \binom{m+1}{1} S_{m+1} + \binom{m+2}{2} S_{m+2} - \binom{m+3}{3} S_{m+3} + \cdots + (-1)^k \binom{m+k}{k} S_{m+k} + \cdots + (-1)^{r-m} \binom{m+r-m}{r-m} S_r$$ where

$$S_t = \sum_{i_1 < i_2 < \cdots < i_t} N(\alpha_{i_1} \alpha_{i_2} \cdots \alpha_{i_t}).$$

The formula in (**) is known as the generalized PIE formula.

Proof: An object occurs with $r \geq$ ~~4~~ $\geq m$ properties is going to be counted 0 times (?).

↑

Please verify this yourself!

Example 3. Let $|A| = m$, $|B| = n$. Then the number of surjective functions from A onto B is equal to $\sum_{i=0}^{n} (-1)^i \binom{n}{i} (n-i)^m$.

Sol. (Proof)

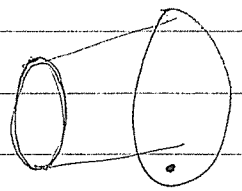
Case 1. $n \le m$, $B = \{b_1, b_2, \cdots, b_n\}$

Let α_i be the property that $b_i \in B$ is not in the image of a function from $f: A \to B$ (B^A). Then, the set of surjective functions from A onto B has cardinality

$$N(\alpha_1'\alpha_2' \cdots \alpha_n') = N - \sum_{i=1}^{n} N(\alpha_i) + \sum_{i \neq j}^{n} N(\alpha_i \alpha_j) - \sum_{i,j,k} N(\alpha_i \alpha_j \alpha_k) + \cdots + (-1)^n N(\alpha_1 \alpha_2 \cdots \alpha_n)$$

$$= n^m - \binom{n}{1}(n-1)^m + \binom{n}{2}(n-2)^m - \binom{n}{3}(n-3)^m + \cdots + (-1)^n \cdot 0$$

$$= \sum_{i=0}^{n} (-1)^i \binom{n}{i} (n-i)^m.$$



Case 2. $n > m$

[At least one element in B is not in the image for each function from A into B. No surjective functions can be found.] In fact,

$\sum_{i=0}^{n} (-1)^i \binom{n}{i} (n-i)^m = 0$ provided $n > m$. (?)

↑

Bonus problem

Definition (Euler's phi-function)

$$\varphi(n) = |\{ m \le n \mid \gcd(m,n) = 1 \}|.$$

↑ The number of positive integers m (not greater than n) which is relatively prime with n.

$\varphi(6) = 2$, $\varphi(7) = 6$.

Proposition Let $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$. Then

$$\varphi(n) = n - \sum_{i=1}^{k} \frac{n}{p_i} + \sum_{i \neq j} \frac{n}{p_i p_j} - \sum_{i,j,k} \frac{n}{p_i p_j p_k} + \cdots + (-1)^k \frac{n}{p_1 p_2 \cdots p_k}. \quad \langle 1 \rangle$$

Proof. Let α_i be the property that $p_i \mid n$. Then

$$\varphi(n) = N(0) = N(\alpha_1' \alpha_2' \cdots \alpha_k').$$ ∎

Proposition

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\cdot\left(1 - \frac{1}{p_2}\right)\cdot \cdots \cdot \left(1 - \frac{1}{p_k}\right) \quad \langle 2 \rangle$$

$$= n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right).$$

Proof. From $\langle 1 \rangle$

$$\varphi(n) = n \cdot \boxed{\left(1 - \sum_{i=1}^{k} \frac{1}{p_i} + \sum_{i \neq j} \frac{1}{p_i p_j} + \cdots + (-1)^k \frac{1}{p_1 p_2 \cdots p_k}\right)}$$

$$\| \quad \text{(By combinatorial arguments!)}$$

$$\prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)$$

Choose 1 or $\left(-\frac{1}{p_i}\right)$ from $\langle 2 \rangle$.

Theorem $n = \sum_{d|n} \varphi(d)$.

Proof. Let $A(d)$ be the set of integers $k \in \{1,2,\cdots,n\} = S$ such that $\gcd(k,n) = d$. (For example, $n=12$, $A(3) = \{3,9\}$.) Clearly, if $d_1 \neq d_2$, then $A(d_1) \cap A(d_2) = \phi$. (Suppose not. Let $x \in A(d_1) \cap A(d_2)$. Then $\gcd(x,n) = d_1$ and $\gcd(x,n) = d_2$, $d_1 \neq d_2$, $\rightarrow\leftarrow$.) Since $A(d) \subseteq \{1,2,\cdots,n\}$ for each $d \in \{1,2,\cdots,n\}$, $S \subseteq \bigcup_{d|n} A(d) \subseteq S$, $\sum_{d|n} |A(d)| = n$. ($\forall\ x \in S$, $\gcd(x,n) | n$, $\Rightarrow x \in A(d)$ for some $d|n$.)

Now, consider $|A(d)|$. Since for each $x \in A(d)$, $\gcd(x,n) = d$ iff $\gcd(\frac{x}{d}, \frac{n}{d}) = 1$, $|A(d)| = \varphi(\frac{n}{d})$. By the fact that $\sum_{d|n} \varphi(\frac{n}{d}) = \sum_{d|n} \varphi(d)$, we conclude the proof. ▨

If you are familiar with the generators for subgroups in $\langle \mathbb{Z}_n, + \rangle$, then the proof follows by showing that if $\gcd(g,n) = d$, then $\langle g \rangle$ generates a subgroup of order $\frac{n}{d}$. Since each element of $\mathbb{Z}_n$ can generate a subgroup of order $\frac{n}{d}$ a divisor of n, the proof is concluded.

Möbius Function $\mu(n)$

Let $n = p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s}$.

$$\mu(n) = \begin{cases} 1, & \text{if } n=1; \\ 0, & \text{if } e_i > 1 \text{ for some } i \in \{1,2,\cdots,s\}; \text{ and} \\ (-1)^s, & \text{if } e_i = 1 \text{ for all } i \in \{1,2,\cdots,s\}. \end{cases}$$

Fact 1 Let $n^* = p_1 p_2 \cdots p_s$. Then, $\sum_{d|n} \mu(d) = \sum_{d|n^*} \mu(d)$.

Proof. $\sum_{d|n} \mu(d) = \sum_{d|n^*} \mu(d) + \sum_{\substack{d \nmid n^* \\ d|n}} \mu(d)$ $\longrightarrow e_i > 1$ in d

$= \sum_{d|n^*} \mu(d) + 0$ ∎

Fact 2 $\sum_{d|n^*} \mu(d) = 0$, $n^* = p_1 p_2 \cdots p_s$.

Proof. $\sum_{d|n^*} \mu(d) = 1 + \binom{s}{1}(-1) + \binom{s}{2}\cdot(-1)^2 + \cdots + \binom{s}{s}(-1)^s$

$= (1+(-1))^s = 0$

Theorem (Möbius inversion formula)

Let f and g be two functions such that for each $n \in \mathbb{N}$,

$f(n) = \sum_{d|n} g(d)$. Then, $g(n) = \sum_{d|n} f(\frac{n}{d})\mu(d)$.

Proof. $\sum_{d|n} f(\frac{n}{d})\mu(d) = \sum_{d|n} f(d)\mu(\frac{n}{d})$

$= \sum_{d|n}\left[\mu(\frac{n}{d}) \cdot \sum_{d'|d} g(d')\right] \overset{?}{=} \sum_{d'|n}\left[g(d') \sum_{m|\frac{n}{d'}} \mu(m)\right] = \begin{cases} g(n), & d'=n \\ +0, & d' \neq n. \end{cases}$ ∎

d: $15 \mid 105$ $\quad (d'=5)$ $\quad m \mid 21$

$$\sum_{d|n} f\left(\frac{n}{d}\right)\mu(d)$$

$$= \sum_{d|n} f(d)\,\mu\left(\frac{n}{d}\right)$$

$$= \sum_{d|n}\left(\sum_{d'|d} g(d')\right)\cdot\mu\left(\frac{n}{d}\right)$$

(?)

$$= \sum_{d'|n}\left[g(d')\cdot\sum_{m|\frac{n}{d'}}\mu(m)\right] \equiv \begin{cases} g(n), & d'=n \\ 0, & d'\neq n \end{cases}$$

$$= g(n)$$

For example $n=12$.

$$\sum_{d|12} f\left(\frac{12}{d}\right)\mu(d)$$

$$= \sum_{d|12} f(d)\,\mu\left(\frac{12}{d}\right)$$

$$= \sum_{d|12}\left[\left(\sum_{d'|d} g(d')\right)\cdot\mu\left(\frac{12}{d}\right)\right]$$

$$= \left[\sum_{d'|1} g(d')\right]\mu(12) + \left[\sum_{d'|2} g(d')\right]\cdot\mu(6) + \left[\sum_{d'|3} g(d')\right]\cdot\mu(4) + \left[\sum_{d'|4} g(d')\right]\cdot\mu(3) + \left[\sum_{d'|6} g(d')\right]\mu(2) + \left[\sum_{d'|12} g(d')\right]\cdot\mu(1)$$

$d = 1, 2, 3, 4, 6, 12$

$d_1' = 1, 2, 3, 4, 6, 12$.

$$+ g(1)\cdot\left(\sum_{m\mid 12}\mu(m)\right)$$

$$+ g(2)\cdot\left(\sum_{m\mid 6}\mu(m)\right)$$

$$+ g(3)\cdot\left(\sum_{m\mid 4}\mu(m)\right)$$

$$+ g(4)\cdot\left(\sum_{m\mid 3}\mu(m)\right)$$

$$+ g(6)\cdot\left(\sum_{m\mid 2}\mu(m)\right)$$

$$+ g(12)\cdot\left(\sum_{m\mid 1}\mu(m)\right) = g(n), \quad n=12$$

$= 0$

Theorem $\varphi(n) = \sum_{d|n} \mu(d) \cdot \frac{n}{d}$. (Take $f(n) = n$, $g(n) = \varphi(n)$.)

Proof. Since $n = \sum_{d|n} \varphi(d)$, $\varphi(n) = \sum_{d|n} \mu(d) f(\frac{n}{d})$

$$= \sum_{d|n} \mu(d) \cdot \frac{n}{d}.$$

$$\varphi(35) = \sum_{d|35} \mu(d) \frac{n}{d} = 35\mu(1) + \mu(5) \cdot 7 + \mu(7) \cdot 5 + \mu(35) \cdot 1$$

$$= 35 - 7 - 5 + 1 = 24$$

$35 = 5 \cdot 7$, $\varphi(35) = (5-1) \cdot (7-1) = 24$.

(*) $\forall\ n > 2$, $\varphi(n)$ is even. $\left(n = p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n}\right)$

$p_1 \le p_2 \le \cdots < p_n$

Sol. $\varphi(n) = n \cdot \prod_{i=1}^{n} (1 - \frac{1}{p_i})$

$$= p_1^{e_1 - 1} p_2^{e_2 - 1} \cdots p_n^{e_n - 1} (p_1 - 1)(p_2 - 1) \cdots (p_n - 1).$$

$n \ge 3$; $e_1 \ge 2$ and $p_1 = 2$, then $\varphi(n)$ is even.

$e_1 = 1$, p_i is odd for some i, $(p_i - 1)$ is even.

$\Rightarrow \varphi(n)$ is even.