3
The Principle of Inclusion and Exclusion

Let A and B be two disjoint finite sets. The addition principle states that $|A \cup B| = |A| + |B|$. If $A \cap B \neq \emptyset$, then we have

$$|A \cup B| = |A| + |B| - |A \cap B| \ .$$

But what happens if there are more sets?

3.1 The principle and proofs

Theorem 3.1 (Principle of inclusion and exclusion). *For any collection of finite sets $A_1, A_2, \dots, A_n$, it holds that*

$$\begin{aligned}\left|\bigcup_{i=1}^{n} A_i\right| &= \sum_{i=1}^{n} |A_i| - \sum_{1 \le i < j \le n} |A_i \cap A_j| + \cdots - (-1)^n \left|\bigcap_{i=1}^{n} A_i\right| \\ &= \sum_{k=1}^{n} (-1)^{k-1} \sum_{S \subseteq [n], |S| = k} \left|\bigcap_{i \in S} A_i\right| \\ &= \sum_{\emptyset \neq S \subseteq [n]} (-1)^{|S|-1} \left|\bigcap_{i \in S} A_i\right| \ .\end{aligned}$$

Proof. We prove the principle by noticing that each element x contributes the same number to each side of the equation.

Fix x and let $I \subseteq [n]$ be the set of i for which $x \in A_i$. If $I = \emptyset$, clearly x contributes 0 to both sides. Otherwise, x contributes 1 to the left hand side and 1 to every $|\cap_{i \in S} A_i|$-term of the right hand side where $S \subseteq I$. Applying the equation

$$k - \binom{k}{2} + \binom{k}{3} - \cdots - (-1)^k \binom{k}{k} = \sum_{i=1}^{k} (-1)^{i-1} \binom{k}{i} = 1 \,,$$

we can complete the proof. $\square$

In combinatorics, we usually use the complement form, where $B_1, B_2, \ldots, B_n$ can be viewed as a family of "bad events" and we hope to count the number of "good" elements so that none of the bad events happens.

Corollary 3.2. *For any collection of subsets $B_1, B_2, \ldots, B_n$ of some finite universal set U, the number of elements of which lie in none of the subsets is*

$$\sum_{S \subseteq [n]} (-1)^{|S|} \left| \bigcap_{i \in S} B_i \right| ,$$

where we set $\cap_{i \in \emptyset} B_i = U$ conventionally.

3.2 *Surjections, derangements and permanents*

Now we consider problem of counting mappings under some special restrictions.

The first example is to count the number of *surjections*. Actually, the number of surjections $[n] \to [m]$ is counted in the Case 9 of the twelvefold way, which is $m! \left\{ {n \atop m} \right\}$. We now find its explicit formula by the inclusion and exclusion principle.

A mapping $f : [n] \to [m]$ is a *surjection* if for all $y \in [m]$, there exists $x \in [n]$ such that $f(x) = y$.

Let U be the set of all mappings from $[n]$ to $[m]$, and B_i be the set of all mappings where no element is mapped to i. Then we have $|U| = m^n$, and

$$\left| \bigcap_{i \in S} B_i \right| = (m - |S|)^n \quad \text{for all } S \subseteq [m] .$$

Applying Corollary 3.2, it follows that

$$\begin{aligned} m! \left\{ {n \atop m} \right\} &= \sum_{S \subseteq [n]} (-1)^{|S|} \left| \bigcap_{i \in S} B_i \right| \\ &= \sum_{k=0}^{m} \binom{m}{k} (-1)^k (m-k)^n \\ &= \sum_{k=0}^{m} (-1)^{m-k} \binom{m}{k} k^n , \end{aligned}$$

which is the same as the result in Section 2.3.

Another example is the number of bijections with no fixed points. Let $f : [n] \to [n]$ be a bijection (or permutation) on n. A fixed point of f is an element $x \in [n]$ such that $f(x) = x$. If f has no fixed point, it is known as a *derangement*. We would like to count the number D_n of derangements over $[n]$.

We apply the complement form of the inclusion and exclusion principle. Let U be the set of all bijections / permutations, and B_i

be the set of bijections with $f(i) = i$. It is not difficult to find that $|U| = n!$ and

$$\left|\bigcap_{i\in S} B_i\right| = (n-|S|)!\,.$$

Thus, Corollary 3.2 yields that

$$D_n = \sum_{S\subseteq[n]} (-1)^{|S|} \left|\bigcap_{i\in S} B_i\right| = \sum_{k=0}^{n} \binom{n}{k} (-1)^k (n-k)! = \sum_{k=0}^{n} (-1)^k \frac{n!}{k!}\,.$$

The expression of D_n tells us that if we pick a bijection f over all possibilites uniformly at random, then as $n \to \infty$, the probability of f being a derangement is

$$\sum_{n=0}^{\infty} \frac{(-1)^n}{n!} = \frac{1}{e}\,.$$

In fact, we can also find the closed form of D_n by the exponential generating function. First, we give a recurrence relation of D_n. Suppose f is a derangement and $f(n) = k$ ($k \neq n$). Then there are two cases: $f(k) = n$ or $f(k) \neq n$. If $f(k) = n$ then f subject on $[n] \setminus \{k, n\}$ is also a derangement. So there are D_{n-2} such f's. If $f(k) \neq n$, then f subject on $[n-1]$ is a function satisfying $f(i) \in [n] \setminus \{k\}$ for all i, $f(j) \neq j$ for all $j \neq k$, and $f(k) \neq n$. It can be viewed as a derangement on domain $[n-1]$. Consequently, we obtain

$$D_n = (n-1)(D_{n-1} + D_{n-2})\,.$$

Note that the recurrence relation is equivalent to

$$D_n - nD_{n-1} = -(D_{n-1} - (n-1)D_{n-2})\,.$$

Hence, we also have another form of recurrence

$$D_n - nD_{n-1} = (-1)^n\,.$$

Similarly, we will have

$$D(x) - xD(x) = e^{-x}\,.$$

Thus, $D(x) = e^{-x}/(1-x)$.

Then we solve D_n by its exponential generating function. Let

$$D(x) = \sum_{n\geq 0} \frac{D_n}{n!} x^n\,.$$

Since $D_{n+1} = nD_n + nD_{n-1}$, we obtain that

$$\begin{aligned}
D'(x) &= \sum_{n\geq 0} \frac{nD_n}{n!} x^{n-1} = \sum_{n\geq 1} \frac{D_n}{(n-1)!} x^{n-1} = \sum_{n\geq 0} \frac{D_{n+1}}{n!} x^n\,,\\
xD'(x) &= \sum_{n\geq 1} \frac{D_n}{(n-1)!} x^n = \sum_{n\geq 1} \frac{nD_n}{n!} x^n\,,\\
xD(x) &= \sum_{n\geq 0} \frac{D_n}{n!} x^{n+1} = \sum_{n\geq 0} \frac{(n+1)D_n}{(n+1)!} x^{n+1} = \sum_{n\geq 1} \frac{nD_{n-1}}{n!} x^n\,,
\end{aligned}$$

which leads to

$$D'(x) = xD'(x) + xD(x)\,.$$

So

$$\frac{D'(x)}{D(x)} = \frac{x}{1-x} = -1 + \frac{1}{1-x}\,.$$

Note that the left hand side is $(\ln D(x))'$. Hence we conclude that

$$D(x) = \exp\left(\int -1 + \frac{1}{1-x}\,\mathrm{d}x\right) = \frac{e^{-x}}{1-x}\,.$$

Another idea is to consider the number of fixed points in all bijections / permutations. Clearly the number of bijections on $[n]$ with exactly k fixed points is $\binom{n}{k} D_{n-k}$. So we have

$$\sum_{k=0}^{n} \binom{n}{k} D_{n-k} = n!\,.$$

Comparing with the multiplication of exponential generating functions, we know that the EGF of $(1, 1, 2, 6, \dots, n!, \dots)$ is the product of the EGF of $(D_0, D_1, D_2, \dots, D_n, \dots)$ and the EGF of $(1, 1, 1, \dots, 1, \dots)$. That is

$$D(x) \cdot \left(\sum_{n \geq 0} \frac{1}{n!} x^n \right) = \sum_{n \geq 0} \frac{n!}{n!} x^n = \frac{1}{1-x},$$

which also implies that

$$D(x) = \frac{e^{-x}}{1-x}.$$

By the expression of $D(x)$, we obtain that

$$\begin{aligned} \frac{D_n}{n!} &= [x^n] D(x) = [x^n] \left(\sum_{n \geq 0} \frac{(-1)^n}{n!} x^n \cdot \sum_{n \geq 0} x^n \right) \\ &= \sum_{k=0}^{n} \frac{(-1)^k}{k!}. \end{aligned}$$

Finally, we consider a generalization of derangements: permutations with restricted positions. It is also known as the *permanent* of a 0-1 matrix, or the number of *perfect matchings* in a bipartite graph.

Definition 3.3 (Permanent). Given an $n \times n$ matrix $A = (a_{i,j})_{1 \leq i,j \leq n}$, the permanent of A is defined by

$$\operatorname{perm} A \triangleq \sum_{\sigma \in \mathcal{S}_n} \prod_{i=1}^{n} a_{i,\sigma(i)},$$

where $\mathcal{S}_n$ is the set of all permutations on $[n]$.

Clearly, if A is a 0-1 matrix, then $\operatorname{perm} A$ counts the number of permutations with restrictions $\sigma(i) \neq j$ for all $a_{i,j} = 0$. In particular,

$$D_n = \operatorname{perm} (\mathbf{1}_n - I_n),$$

where $\mathbf{1}_n$ is the all 1 matrix, and I_n is the identity matrix. If A is an adjacency matrix of a *balanced bipartite graph*, then $\operatorname{perm} A$ counts the number of perfect matchings.

A bipartite graph is *balanced* if its two parts have the same number of vertices.

Remark 3.4. The permanent can be viewed as the *unsigned* version of the determinant. However, while determinants is well-known to be calculated in polynomial time using Gaussian elimination, computing permanents, even for 0-1 matrix, is #P-complete.

Now we compute permanents by the inclusion and exclusion principle. Let U be the set $\mathcal{S}_n$, and B_i be the set of permutations that

$a_{i,\sigma(i)} = 0$. But how to compute the cardinality of the intersections of B_i's? Let

$$R = \{(i,j) \in [n] \times [n] \mid a_{i,j} = 0\}$$

be the set of coordinates of all 0 entries, and

$$r_k = \left| \left\{ T \in \binom{R}{k} \mid \forall (i_1, j_1), (i_2, j_2) \in T, i_1 \neq i_2 \wedge j_1 \neq j_2 \right\} \right|$$

be the number of size-k subsets of R such that no two elements share a common coordinate. A key observation is that

Why?

$$\sum_{|S|=k} \left| \bigcap_{i \in S} B_i \right| = r_k \cdot (n-k)!\,.$$

So by Corollary 3.2, we have

$$\operatorname{perm} A = \sum_{k=0}^{n} (-1)^k r_k (n-k)!\,.$$

However, this formula is correct but meaningless, because r_k is also difficult to count. Note that this problem actually has two kinds of restrictions: (1). σ is a permutation, and (2). $\sigma(i) \neq j$ for all $a_{i,j} = 0$. Above analysis applies Corollary 3.2 on the second kind of restrictions and defines bad events as violating $a_{i,\sigma(i)} = 1$. In fact, a more clever idea is to apply Corollary 3.2 on the first kind of restrictions.

Let U be the set of all *mappings* $f : [n] \to [n]$ such that $f(i) \neq j$ if $a_{i,j} = 0$, and B_i be the set of all mappings in U such that $f^{-1}(i) = \emptyset$, namely, no element is mapped to i. Next, we calculate $|U|$ and $|\cap B_i|$. Note that for any $f \in U$, $f(1)$ has $\sum_{j=1}^{n} a_{1,j}$ choices, $f(2)$ has $\sum_{j=1}^{n} a_{2,j}$ choices, and so on. Thus,

$$|U| = \prod_{i=1}^{n} \left(\sum_{j=1}^{n} a_{i,j} \right).$$

Similarly, for any $S \subseteq [n]$, we have

$$\left| \bigcap_{k \in S} B_k \right| = \prod_{i=1}^{n} \left(\sum_{j \in [n] \setminus S} a_{i,j} \right).$$

Applying Corollary 3.2, Ryser proved the following theorem, which gives an algorithm to compute perm A in $O(2^n n)$ time instead of $O(n! \cdot n)$ time by definition.

This is the best known algorithm.

Theorem 3.5 (Ryser formula)**.**

$$\operatorname{perm} A = \sum_{S \subseteq [n]} (-1)^{|S|} \prod_{i=1}^{n} \left(\sum_{j \in [n] \setminus S} a_{i,j} \right).$$

3.3 *Number-theoretical Möbius inversion*

We now give some applications of the principle of inclusion and exclusion in number theory.

Definition 3.6 (Euler's totient function)**.** Given a positive integer n, the *Euler's totient function* $\varphi(n)$ is defined by the number of positive integers in $[n]$ that are relatively prime to n, i.e.,

$$\varphi(n) \triangleq \sum_{k=1}^{n} [\gcd(n,k) = 1]\,,$$

where $[p]$ is an indicator variable of proposition p, namely, $[p] = 1$ if p is true and $[p] = 0$ otherwise.

The totient function is a *multiplicative function*. If $\gcd(a,b) = 1$ then $\varphi(ab) = \varphi(a)\varphi(b)$. It is clear that $\varphi(p) = p - 1$ for any prime p, and $\varphi(p^r) = (p-1)p^{r-1}$ for any prime p and $r \geq 2$. Thus, it is easy to compute $\varphi(1), \ldots, \varphi(n)$ in $O(n)$ time by the *sieve method*.

Why $\varphi(n)$ is multiplicative? Because $n \mapsto (n \bmod a, n \bmod b)$ is a bijection from $[ab]$ to $[a] \times [b]$, and $\gcd(n, ab) = 1$ iff $\gcd(n \bmod a, a) = 1$ and $\gcd(n \bmod b, b) = 1$, provided that $\gcd(a,b) = 1$.

The following proposition is an important property of the totient function.

Proposition 3.7. *For any positive integer n, it holds that*

$$\sum_{d \mid n} \varphi(d) = n\,. \tag{3.1}$$

Proof. For each $k \in [n]$, consider $\gcd(n,k)$. If $\gcd(n,k) = d$ then we have $\gcd(n/d, k/d) = 1$. Thus,

$$\begin{aligned} n &= \sum_{d \mid n} \left|\{k \in [n] \mid \gcd(n,k) = d\}\right| \\ &= \sum_{d \mid n} \left|\{k \in [\tfrac{n}{d}] \mid \gcd(\tfrac{n}{d}, k) = 1\}\right| \\ &= \sum_{d \mid n} \varphi(\tfrac{n}{d}) = \sum_{d \mid n} \varphi(d)\,. \end{aligned}$$

□

Now we calculate $\varphi(n)$ by the inclusion and exclusion principle. Suppose $n = p_1^{r_1} p_2^{r_2} \cdots p_m^{r_m}$ where p_i's are distinct prime numbers, and $r_i \geq 1$. Let $U = [n]$, and $B_i = \{k \in [n] \mid p_i \mid k\}$ be the set of all multiples of p_i in $[n]$. Then we known that $\varphi(n) = |U \setminus (B_1 \cup B_2 \cup \cdots \cup B_m)|$. Since $(\prod p_i) \mid n$, for any $S \subseteq [m]$, we have

$$\left|\bigcap_{i \in S} B_i\right| = \frac{n}{\prod_{i \in S} p_i}\,.$$

Applying Corollary 3.2, it follows that

$$\begin{aligned}\varphi(n) &= \sum_{S\subseteq[m]}(-1)^{|S|}\left|\bigcap_{i\in S}B_i\right| \\ &= \sum_{S\subseteq[m]}(-1)^{|S|}\frac{n}{\prod_{i\in S}p_i} \\ &= n\sum_{S\subseteq[m]}\prod_{i\in S}\frac{-1}{p_i} \\ &= n\prod_{i=1}^{m}\left(1-\frac{1}{p_i}\right).\end{aligned}$$

Let's observe the equation $\varphi(n) = \sum_{S\subseteq[m]}(-1)^{|S|}\frac{n}{\prod_{i\in S}p_i}$ again. Define the (number-theoretical) *Möbius function* by

$$\mu(n) \triangleq \begin{cases} 1 & n=1\,, \\ 0 & p^2 \mid n \text{ for some prime } p\,, \\ (-1)^k & n = p_1p_2\cdots p_k \text{ for distinct primes } p_1,\dots,p_k\,. \end{cases}$$

Then $\varphi(n)$ can be written as

$$\varphi(n) = \sum_{d\mid n}\mu(d)\cdot\frac{n}{d}\,. \tag{3.2}$$

If we use $*$ to denote the *convolution* for number-theoretical functions, namely,

$$(f*g)(n) = \sum_{d\mid n} f(d)\,g\left(\frac{n}{d}\right),$$

we can rewrite equations (3.1) and (3.2) as

$$\mathrm{id} = \varphi * \mathbf{1}\,, \quad \text{and} \quad \varphi = \mu * \mathrm{id}\,,$$

where $\mathrm{id}(n) = n$ is the identity function, and $\mathbf{1}(n) = 1$ is the all-1 function. This relation holds for general number-theoretical functions.

Theorem 3.8 (Möbius inversion formula)**.** *Let f, g be two number-theoretical functions. If*

$$f = g*\mathbf{1} = \sum_{d\mid n} g(d)\,,$$

then

$$g = f*\mu = \sum_{d\mid n} f(d)\,\mu\left(\frac{n}{d}\right) = \sum_{d\mid n}\mu(d)\,f\left(\frac{n}{d}\right).$$

Example 3.9. It is easy to see that $\mathbf{1}(n) = \sum_{d\mid n}[d=1]$. So we have $[n=1] = \mathbf{1}*\mu = \sum_{d\mid n}\mu(d)$. This can be verified by $\sum_{k=0}^{m}(-1)^k\binom{m}{k} = 0$ as long as $m \geq 1$.

Proof. We prove the inversion formula by PIE. Assign each number k a set $T_k = \{(k,1),(k,2),\ldots,(k,g(k))\}$. Now suppose $n = p_1^{r_1} p_2^{r_2} \cdots p_m^{r_m}$ where $p_1, p_2, \ldots, p_m$ are distinct primes. Let

$$U = \bigcup_{d|n} T_d = \{(d,j) \mid d \mid n, 1 \le j \le g(d)\},$$

and $B_i = \{(d,j) \in U \mid p_i^{r_i} \nmid d, 1 \le j \le g(d)\}$. We would like to count $g(n)$, the cardinality of set $\{(n,j) \mid 1 \le j \le g(n)\} = U \setminus (B_1 \cup B_2 \cup \cdots \cup B_m)$. Note that $|U| = \sum_{d|n} g(d) = f(n)$, and for any $S \subseteq [m]$,

$$\left|\bigcap_{i\in S} B_i\right| = \sum_{d \mid \frac{n}{\prod_{i\in S} p_i}} g(d) = f\left(\frac{n}{\prod_{i\in S} p_i}\right).$$

Applying Corollary 3.2, we obtain that

$$g(n) = f(n) - \sum_{S\subseteq[m]} (-1)^{|S|} f\left(\frac{n}{\prod_{i\in S} p_i}\right) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right). \qquad \square$$

An alternate proof is to see that the *associative law* holds for convolution. Thus,

$$f = g * \mathbf{1} \implies f * \mu = g * \mathbf{1} * \mu = g * [n=1] = g.$$

In particular, if we apply Theorem 3.8 on number-theoretical functions only defined on square-free numbers, we can deduce the following inversion formula for set functions.

Corollary 3.10. *Suppose that $f(S), g(S)$ are two functions defined on sets. If for any set S, we have*

$$f(S) = \sum_{T\subseteq S} g(T),$$

then it holds that

$$g(S) = \sum_{T\subseteq S} (-1)^{|S|-|T|} g(T).$$

We now introduce an application of Möbius inversion.

Question 3.11. How many monic irreducible polynomials of degree n over the field $\mathbb{F}_q$, where $q = p^t$ for some prime p and integer $t \ge 1$? A monic polynomial is a univariate polynomial whose coefficient of the highest order term is 1.

List all monic irreducible polynomials $f_1, f_2, \ldots, f_k, \ldots$. Let d_i be the degree of f_i, and let N_d be the occurrence of d, i.e., the number of m.i.p.'s of degree d. The key fact is that by the unique factorization of polynomials over $\mathbb{F}_q$, every monic polynomials can be expressed as

$$f(z) = f_1(z)^{r_1} f_2(z)^{r_2} \cdots f_k(z)^{r_k} \cdots ,$$

where $r_1, r_2, \ldots, r_k, \ldots \in \mathbb{N}$. Now we consider the OGF $F(x)$ of the numbers of monic polynomials. On the one hand, the number of monic polynomials of degree n over $\mathbb{F}_q$ is q^n. So $F(x) = \sum_{n\geq 0} q^n x^n$. On the other hand, by the factorization, we have

$$\begin{aligned} F(x) &= \left(1 + x^{d_1} + x^{2d_1} + \cdots\right)\left(1 + x^{d_2} + x^{2d_2} + \cdots\right)\left(1 + x^{d_3} + x^{2d_3} + \cdots\right) \cdots \\ &= \frac{1}{1 - x^{d_1}} \cdot \frac{1}{1 - x^{d_2}} \cdot \frac{1}{1 - x^{d_3}} \cdots \end{aligned}$$

Thus, it implies that

$$\frac{1}{1 - qx} = \sum_{n\geq 0} q^n x^n = \prod_{k=1}^{\infty} \frac{1}{1 - x^{d_k}} = \prod_{d=0}^{\infty} \Big(\frac{1}{1 - x^d}\Big)^{N_d} .$$

Taking logarithm to the both sides, it yields that

$$\sum_{n=1}^{\infty} \frac{q^n}{n} x^n = \sum_{d=0}^{\infty} N_d \sum_{k=1}^{\infty} \frac{1}{k} x^{dk} = \sum_{d=0}^{\infty} N_d \sum_{n=1}^{\infty} \frac{[d \mid n]}{n/d} x^n = \sum_{n=1}^{\infty} \sum_{d\mid n} \frac{dN_d}{n} x^n .$$

Comparing the coefficient of x^n term and then applying Möbius inversion, we obtain that

$$q^n = \sum_{d\mid n} dN_d ,$$

and thus

$$N_n = \frac{1}{n} \sum_{d\mid n} \mu(d)\, q^{n/d} .$$