Applications of Inclusion-Exclusion

1. **Surjective maps**: Let us find the number of surjective maps
$$f : [m] \longrightarrow [n].$$
Let
$$X = \{ f \mid f \text{ is a map from } [m] \text{ to } [n] \}.$$
For $i = 1, \dots, n$, let
$$A_i = \{ f \in X \mid f(k) \neq i \text{ for any } k \in [m] \}.$$
Now $A_1 \cup \dots \cup A_n$ consists of maps f such that there is an $i \in \{1, \dots, n\}$ not in the image of f. In other words $A_1 \cup \dots \cup A_n$ is the set of maps that are not surjective, whence the set of surjective maps from $[m]$ to $[n]$ is
$$X \setminus (A_1 \cup \dots \cup A_n).$$
By the I-E formula
$$|X \setminus (A_1 \cup \dots \cup A_n)| = \sum_{S \subset [n]} (-1)^{|S|} \left| \bigcap_{i \in S} A_i \right| = \sum_{k=0}^{n} (-1)^k \sum_{\substack{S \subset [n] \\ |S| = k}} \left| \bigcap_{i \in S} A_i \right|$$
Now $f \in \bigcap_{i \in S} A_i$ if and only if $f(k) \notin S$ for any $k \in [m]$. This means $f \in \bigcap_{i \in S} A_i$ if and only if $f : [m] \longrightarrow [n] \setminus S$. This gives:
$$\left| \bigcap_{i \in S} A_i \right| = (n - |S|)^m.$$

Hence
$$|X \setminus (A_1 \cup \dots \cup A_n)| = \sum_{k=0}^{n} (-1)^k \sum_{\substack{|S| = k \\ S \subset [n]}} \left| \bigcap_{i \in S} A_i \right|$$
$$= \sum_{k=0}^{n} (-1)^k \sum_{\substack{|S| = k \\ S \subset [n]}} (n-k)^m.$$
$$= \sum_{k=0}^{n} (-1)^k (n-k)^m \sum_{|S| = k} 1$$
$$= \sum_{k=0}^{n} (-1)^k (n-k)^m \binom{n}{k}.$$
Thus the number of surjective maps from $[m]$ to $[n]$ is $\sum_{k=0}^{n} (-1)^k \binom{n}{k} (n-k)^m$. In particular this number is zero if $m < n$. (!!)

$$\boxed{\#\text{ of surjective maps from } [m] \text{ to } [n] = \sum_{k=0}^{n} (-1)^k \binom{n}{k} (n-k)^m.}$$

2. Derangements: A permutation of a set X is the set of bijective maps $f: X \longrightarrow X$. Suppose $|X| = n$. Then a permutation of X is what was called a permutation of length n. A derangement of X is a permutation $f: X \longrightarrow X$ such that $f(x) \neq x$ for any $x \in X$.

Let $X = [n]$. Let us calculate the number of derangements of X. To that end, let P be the set of permutations of X.

For $i = 1, \ldots, n$, set

$$A_i = \{ f \in P \mid f(x_i) = x_i \}.$$

It is clear that the set of derangements of X is $P \setminus (A_1 \cup \ldots \cup A_n)$.

Now for $S \subseteq [n]$, the set $\bigcap_{i \in S} A_i$ is essentially

the same as the set of bijective maps

$$[n] \setminus S \longrightarrow [n] \setminus S$$

i.e. the set of permutations on $[n] \setminus S$.

Thus $\left| \bigcap_{i \in S} A_i \right| = (n - |S|)!$

Now

$$|P \setminus (A_1 \cup \ldots \cup A_n)| = \sum_{S \subset [n]} (-1)^{|S|} \left| \bigcap_{i \in S} A_i \right|$$

$$= \sum_{k=0}^{n} (-1)^k \sum_{\substack{S \subset [n] \\ |S| = k}} \left| \bigcap_{i \in S} A_i \right|$$

$$= \sum_{k=0}^{n} (-1)^k \sum_{\substack{S \subset [n] \\ |S| = k}} (n-k)!$$

$$= \sum_{k=0}^{n} (-1)^k (n-k)! \sum_{\substack{S \subset [n] \\ |S|=k}} 1$$

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

Thus

$$\boxed{\text{The number of derangements of a set with } n \text{ elements} = n! \sum_{k=0}^{n} (-1)^k / k!}$$

3. Let $d_1, \ldots, d_m \in \mathbb{N}$. We will show, using I-E, that

$$(d_1 - 1)(d_2 - 1) \cdots (d_m - 1) = \sum_{S \subset [m]} (-1)^{|S|} \prod_{i \notin S} d_i$$

← note the $\notin$ sign

Let

$$X = \{ (x_1, \ldots, x_m) \mid x_i \in \mathbb{N},\ 1 \le x_i \le d_i,\ i = 1, \ldots, m \},$$

For $i = 1, \ldots, m$, set

$$A_i = \{ (x_1, \ldots, x_m) \in X \mid x_i = d_i \}.$$

For $S \subseteq [m]$, $\bigcap_{i \in S} A_i = \{ (x_1, \ldots, x_m) \in X \mid x_i = d_i,\ i \in S \}$

Clearly $\left| \bigcap_{i \in S} A_i \right| = \prod_{j \notin S} d_j$ (there are d_j choices for x_j if $j \notin S$, and only one choice for x_i, if $i \in S$)

Also $X \setminus (A_1 \cup \ldots \cup A_m) = \{ (x_1, \ldots, x_m) \in X \mid x_i \neq d_i \text{ for any } i \}$

Thus

$$|X \setminus (A_1 \cup \ldots \cup A_m)| = (d_1 - 1) \cdots (d_m - 1)$$

for, if $(x_1, \ldots, x_m) \in X \setminus (A_1 \cup \ldots \cup A_m)$ then the choices for x_1 are $\{1, 2, \ldots, d_1 - 1\}$, for x_2 are

$\{1,2,\dots,d_2-1\}$, ..., for x_m are $\{1,2,\dots,d_m-1\}$.

Apply the I-E formula, we get

$$|X \setminus (A_1 \cup \dots \cup A_m)| = \sum_{S \subset [m]} (-1)^{|S|} \left| \bigcap_{i \in S} A_i \right|$$

i.e.

$$(d_1-1)(d_2-1)\cdots(d_m-1) = \sum_{S \subset [m]} (-1)^{|S|} \prod_{j \notin S} d_j .$$

This was the original assertion.

Remark: The formula is true for $d_1,\dots,d_m \in \mathbb{R}$, (or for d_i in any commutative ring) not just for $d_1,\dots,d_m \in \mathbb{N}$. But in the latter case a combinatorial proof is possible.

4. The Euler ϕ-function:

Let $n \in \mathbb{N}$, with $n \geq 2$. Define

$$\phi(n) = \#\text{ of } x \in [n] \text{ s.t. } \gcd(x,n) = 1$$
$$= |\{x \in [n] \mid \gcd(x,n) = 1\}|$$

$\gcd(x,n) = 1$
$\iff$ x and n relatively prime.

$\phi : \{2,3,\dots\} \longrightarrow \mathbb{N}$ is called the Euler ϕ-function.

Some values of ϕ:

$\phi(2) = 1$ $\quad\quad \{1, \cancel{2}\}$

$\phi(4) = 2$ $\quad\quad \{1, \cancel{2}, 3, \cancel{4}\}$

$\phi(12) = 4$ $\quad\quad \{1, \cancel{2}, \cancel{3}, \cancel{4}, 5, \cancel{6}, 7, \cancel{8}, \cancel{9}, \cancel{10}, 11, \cancel{12}\}$

For $n \in \mathbb{N}$, $n \geq 2$, let

$$P(n) = \{p \in \mathbb{N} \mid p \text{ is prime and divides } n\}.$$

e.g.

$$P(12) = \{2,3\}, \quad P(126) = \{2,3,7\}.$$

Lemma: Let $n \geq 2$ be an integer, and $\{p_1,\dots,p_k\} \subset P(n)$, with the p_i, distinct. Then the number of elements of $[n]$ divisible by p_i for all i, is

$$\frac{n}{p_1 \cdots p_k} \in \mathbb{N}.$$

Proof:

Let $r = \dfrac{n}{p_1 \cdots p_k}$.

For any $x \in [r]$, let $f(x) = p_1 \cdots p_k x$.
Since $x \le r$, therefore
$$f(x) = p_1 \cdots p_k x \le p_1 \cdots p_k r = n.$$
Thus $f(x) \in [n]$, and moreover $f(x)$ is divisible by p_i for every $i = 1, \dots, k$.

Conversely if $y \in [n]$ is divisible by p_i $\forall i \in \{1, \dots, k\}$, then $x = \dfrac{y}{p_1 \cdots p_k} \in \mathbb{N}$ and $y = f(x)$.

Also, if $f(x) = f(y)$, then $p_1 \cdots p_k x = p_1 \cdots p_k y$, which means $x = y$. Thus f is one-to-one, and gives a bijective correspondence between $[r]$ and the set of elements in $[n]$ which are divisible of p_i for all $i \in \{1, \dots, k\}$. Since $|[r]| = r$, we are done. //

Theorem: Let $n \in \mathbb{N}$, $n \geq 2$ and $p_1, p_2, \dots, p_m$ be the distinct prime divisors of n. Then
$$\phi(n) = n \left(\frac{p_1 - 1}{p_1}\right)\left(\frac{p_2 - 1}{p_2}\right) \cdots \left(\frac{p_m - 1}{p_m}\right)$$
$$= n \prod_{i=1}^{m} \frac{p_i - 1}{p_i}.$$

Proof:

We have $\gcd(x, n) \neq 1$ if and only if $p_i \mid x$ for some i, and so
$$\phi(n) = \left| \{ x \in [n] \mid p_i \nmid x \text{ for all } i = 1, \dots, m \} \right|$$

Let $X = [n]$ and $A_i = \{ x \in [n] \mid p_i \mid x \}$, $i = 1, \dots, m$.
$$\phi(n) = \left| X \setminus (A_1 \cup \dots \cup A_m) \right|$$
$$= \sum_{S \subset [m]} (-1)^{|S|} \left| \bigcap_{i \in S} A_i \right| \qquad \text{(Inclusion-Exclusion)}$$

$$= \sum_{S \subset [m]} (-1)^{|S|} \frac{n}{\prod_{i \in S} p_i} \quad \text{(by Lemma)}$$

$$= \frac{n}{p_1 \cdots p_m} \sum_{S \subset [m]} (-1)^{|S|} \frac{p_1 \cdots p_m}{\prod_{i \in S} p_i}$$

$$= \frac{n}{p_1 \cdots p_m} \sum_{S \subset [m]} (-1)^{|S|} \prod_{i \notin S} p_i$$

From Example 3.

$$= \frac{n}{p_1 \cdots p_m} (p_1 - 1)(p_2 - 1) \cdots (p_m - 1)$$

$$= n \prod_{i=1}^{m} \frac{p_i - 1}{p_i}$$

as required.

Examples

1. The prime divisors of $12 = 2^2 \cdot 3$ are 2 and 3.

$$\phi(12) = 12 \frac{(2-1)(3-1)}{(2)(3)} = \frac{12(1)(2)}{6} = 4.$$ ← Same as earlier answer

2. Let us work out $\phi(450)$.

$$450 = 2 \times 3^2 \times 5^2$$

So the prime divisors of 450 are 2, 3 and 5.

$$\phi(450) = 450 \frac{(2-1)}{2} \frac{(3-1)}{3} \frac{(5-1)}{5} = 450 \left(\tfrac{1}{2}\right)\left(\tfrac{2}{3}\right)\left(\tfrac{4}{5}\right) = 120.$$

$$= 450 \left(\tfrac{1}{2}\right)\left(\tfrac{2}{3}\right)\left(\tfrac{4}{5}\right)$$

$$= 120$$

Note: In order to calculate $\phi(450)$ we did not have to check the 450 elements in $[450]$ and decide which were relatively prime to 450.

Chapter 8. Generating Functions

The **generating function** of a sequence

$$(a_0, a_1, a_2, \dots) = (a_n)_{n=0}^{\infty} \quad (= \{a_n : n \geq 0\})$$

is the power series

$$F(x) = \sum_{n=0}^{\infty} a_n x^n.$$

Note: The power series is not required to converge. It is a formal power series.

Formal power series algebra:

Let $(a_n)_{n=0}^{\infty}$ and $(b_n)_{n=0}^{\infty}$ be sequences; $F(x) = \sum_{n=0}^{\infty} a_n x^n$ and $G(x) = \sum_{n=0}^{\infty} b_n x^n$. Then

(a) $\quad F(x) + G(x) = \sum_{n=0}^{\infty} (a_n + b_n) x^n$

(b) $\quad F(x) \cdot G(x) = \sum_{n=0}^{\infty} c_n x^n$

where $\quad c_n = \sum_{k=0}^{n} a_k b_{n-k}, \quad n = 0, 1, 2, \dots$

Note: If $F(x)$ and $G(x)$ are actual functions, (b) is a Proposition in Analysis/Calculus. Otherwise (b) is to be regarded as a definition.

Using (b) it is easy to see that

$$(1-x) \sum_{n=0}^{\infty} x^n = 1.$$

(Use $(a_n)_{n=0}^{\infty} = (1, -1, 0, \dots, 0)$ and $(b_n)_{n=0}^{\infty} = (1, 1, 1, \dots)$ and check that $c_0 = 1$, but $c_n = 0$ for $n > 0$, where $c_n = \sum_{k=0}^{n} a_k b_{n-k}$.)

In particular

$$\boxed{\sum_{n=0}^{\infty} x^n = \frac{1}{1-x}.}$$

Example: Let $(a_n)_{n=0}^{\infty}$ be the sequence $a_n = 1$, $\forall\, n \in \mathbb{N}_0$
$(a_n)_{n=0}^{\infty} = (1,1,1,\ldots)$. Its generating function is

$$F(x) = \sum_{n=0}^{\infty} x^n = \frac{1}{1-x}.$$

$F(x) = \sum_{n=0}^{\infty} x^n$ is called the infinite geometric series.

Example: The generating function of

$$(1,1,1,\ldots,1,0,0,\ldots) \quad \left.\begin{array}{l} a_i = 1 \text{ for } 0 \le i \le n \\ a_i = 0 \text{ for } i > n \end{array}\right\}$$

(0^{th} entry, n^{th} entry)

is

$$F(x) = 1 + x + x^2 + \ldots + x^n = \frac{1-x^{n+1}}{1-x}$$

The series $1 + x + x^2 + \ldots + x^n$ is called the finite geometric series.

Here are some useful calculations:
It is easy to see that

$$\frac{d^{k-1}}{dx^{k-1}}\left\{\frac{1}{1-x}\right\} = \frac{(k-1)!}{(1-x)^k}, \quad k \in \mathbb{N}$$

(with the understanding that the 0^{th} derivative of a function is the function itself).
Fix $k \in \mathbb{N}$. From the above formula we see that

$$\begin{aligned}
\frac{1}{(1-x)^k} &= \frac{1}{(k-1)!}\frac{d^{k-1}}{dx^{k-1}}\left\{\frac{1}{1-x}\right\} \\
&= \frac{1}{(k-1)!}\frac{d^{k-1}}{dx^{k-1}}\sum_{n=0}^{\infty} x^n \\
&= \frac{1}{(k-1)!}\sum_{n=0}^{\infty}\frac{d^{k-1}}{dx^{k-1}} x^n \quad \text{(formal differentiation)} \\
&= \frac{1}{(k-1)!}\sum_{n=k-1}^{\infty} n(n-1)\cdots(n-k+2)\,x^{n-k+1}
\end{aligned}$$

$$= \frac{1}{(k-1)!} \sum_{n=k-1}^{\infty} \frac{n!}{(n-k+1)!} x^{n-k+1}$$

$$= \sum_{n=k-1}^{\infty} \binom{n}{k-1} x^{n-k+1}$$

$$= \sum_{m=0}^{\infty} \binom{m+k-1}{k-1} x^{m} \qquad (\text{set } m=n-k+1)$$

Thus

$$\boxed{\frac{1}{(1-x)^k} = \sum_{n=0}^{\infty} \binom{n+k-1}{k-1} x^n}$$