Inclusion-Exclusion Principle
(Last change Nov 23 2015)

November 23, 2015

Example. A sporting event has a road cycling race and a mountain biking race. The US team has 10 road cyclists and 9 mountain bikers. This includes 3 team members who participate in both events. How many members are on the team?

We can express this in a set terminology, as follows. Let R and M denote the sets of road cyclists and mountain bikers. Thus we have $|R| = 10$, $|M| = 9$, and $|R \cap M| = 3$. We want to compute the cardinality of the union, $|R \cup M|$.

The idea is this: if we compute the sum $|R| + |M|$, then the members who ride both types of bikes would be counted twice in this sum. Thus we can get the correct count by subtracting the size of the intersection, which gives us the formula

$$|R \cup M| = |R| + |M| - |R \cap M|.$$

Plugging in the numbers, we obtain that the team has $|R \cup M| = 10 + 9 - 3 = 16$ members.

Example. Let us now try to extend this idea to three sets. Let's say we have finite sets R, M and B and that we know the cardinalities of the three sets and all intersections, that is the cardinalities of all sets R, M, B, $R \cap M$, $R \cap B$, $M \cap B$ and $R \cap M \cap B$. We want to compute the cardinality of their union, $R \cup M \cup B$.

As the first approximation, let's compute $|R| + |M| + |B|$. In this formula all elements that belong to only one set are counted just once, but we over-count elements that below to two or three sets. So we subtract the size of all intersections, giving us $|R| + |M| + |B| - |R \cap M| - |R \cap B| - |M \cap B|$. This will correct the count for elements that belong to exactly two sets. But those that belong to all three have their count equal to 0. We can then correct it again, by adding the intersection of all three sets, giving us the final formula:

$$|R \cup M \cup B| = |R| + |M| + |B| - |R \cap M| - |R \cap B| - |M \cap B| + |R \cap M \cap B|.$$

We can generalize it to an arbitrary number k of sets, by following the same idea: starting with the sum of the cardinalities of individual sets, subtracting the cardinalities of pairwise intersections, then adding the cardinalities of all triple intersections, and so on. This gives us the following theorem.

Theorem 1 (Inclusion-Exclusion) *For any finite sets $S_1, S_2, ..., S_k$, we have*

$$\Big|\bigcup_{i=1}^{k} S_i\Big| \quad = \quad \sum_{j=1}^{k} (-1)^{j+1} \sum_{l_1 < l_2 < ... < l_j} \big|S_{l_1} \cap S_{l_2} \cap ... \cap S_{l_j}\big|$$

Example. For four sets S_1, S_2, S_3, S_4, we get

$$\begin{aligned}|S_1 \cup S_2 \cup S_3 \cup S_4| \quad = \quad & |S_1| + |S_2| + |S_3| + |S_4| \\ & -|S_1 \cap S_2| - |S_1 \cap S_3| - |S_1 \cap S_4| - |S_2 \cap S_3| - |S_2 \cap S_4| - |S_3 \cap S_4| \\ & +|S_1 \cap S_2 \cap S_3| + |S_1 \cap S_2 \cap S_4| + |S_1 \cap S_3 \cap S_4| + |S_2 \cap S_3 \cap S_4| \\ & -|S_1 \cap S_2 \cap S_3 \cap S_4|.\end{aligned}$$

0.1 Application to Computing Euler's Totient Function

Define $\phi(n)$ to be the Euler's totient function, defined as the number of integers in $\{1, 2, ..., n\}$ that are relatively prime to n. We now want to derive a formula for $\phi(n)$.

Example. For $n = 9$ we get $\phi(9) = 6$, because among numbers $1, 2, 3, 4, 5, 6, 7, 8, 9$ there are 6 numbers that are relatively prime to 9: $1, 2, 4, 5, 7, 8$.

We start by looking at numbers with a few prime factors. If $n = p$ itself is prime, then all numbers $1, 2, ..., p - 1$ are relatively prime to p, so $\phi(p) = p - 1$. Note that we can write it as $\phi(p) = p(1 - 1/p)$. Why would we write it in this funny form? We'll see soon ...

More generally, suppose that n is a power of a prime, say $n = p^b$. Only the multiples of p are not relatively prime to n, namely the numbers $p, 2p, 3p, ..., (p^{b-1})p$, and there are p^{b-1} of them. So

$$\phi(n) = n - p^{b-1} = n(1 - 1/p).$$

This looks just like the formula we had for the case when n was a prime, no?

So let now $n = pq$, where p, q are different primes. The numbers that have a common factor with n are all multiples of p and all multiples of q. We have q multiples of p among $1, 2, ..., n$ and p multiples of p, with $n = pq$ counted in both sets. This gives us $p + q - 1$ numbers that are not relatively prime to n. Subtracting this from n, we get

$$\begin{aligned}\phi(n) &= n - (p + q - 1) \\ &= pq - p - q + 1 \\ &= (p - 1)(q - 1) \\ &= n(1 - 1/p)(1 - 1/q)\end{aligned}$$

where the last expression is obtained by factoring p out of $p - 1$ and q out of $q - 1$. Note that this is exactly the same function that we used in the RSA.

The formulas we obtained so far suggest that there may be a way to express $\phi(n)$ using prime factors of n, by multiplying n by all expressions $1 - 1/p$, where p is a prime factor of n. It turns out that this indeed works, as spelled out in the next theorem.

Theorem 2 *Let $p_1, p_2, ..., p_k$ be all different prime factors of n. Then*

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

Proof: (Sketch) The general strategy of the proof is to first compute how many numbers among $1, 2, ..., n$ are *not* relatively prime to n. Once we compute this number, we will subtract it from n, which will give us how many of these numbers *are* relatively prime to n. This is exactly the value $\phi(n)$ that we are seeking.

For each i, denote by S_i the set of numbers in this set that are multiples of p_i. Then $\bigcup_{i=1}^k S_i$ is exactly the set of numbers in $\{1, 2, ..., n\}$ that are not relatively prime to n. We can compute the cardinality of this union using Inclusion-Exclusion:

$$\Big|\bigcup_{i=1}^{k} S_i\Big| \quad = \quad \sum_{j=1}^{k} (-1)^{j+1} \sum_{l_1<l_2<...<l_j} \big|S_{l_1} \cap S_{l_2} \cap ... \cap S_{l_j}\big|$$

We now need to figure out how to compute the cardinalities of sets $S_{l_1} \cap S_{l_2} \cap ... \cap S_{l_j}$.

Let's start with a simple case: what is the cardinality of just one set, say S_a? Recall that this set has all multiples of p_a, namely the numbers p_a, $2p_a$, ..., $(n/p_a)p_a$, so there are n/p_a of them, that is $|S_a| = n/p_a$.

OK, that was easy. Now let's compute the cardinality of a pairwise intersection, say $S_a \cap S_b$. This set contains the numbers that are multiples of p_a and multiples of p_b. But a number z is a multiple of two different primes p_a, p_b if and only if z a multiple of their product $p_a p_b$. (This follows from the uniqueness of factorization.) So $S_a \cap S_b$ is exactly the set of $p_a p_b$ among the numbers $1, 2, ..., n$, and there are exactly $n/(p_a p_b)$ of them, that is $|S_a \cap S_b| = n/p_a p_b$.

Generalizing this, we conclude that the cardinality of $S_{l_1} \cap S_{l_2} \cap ... \cap S_{l_j}$ is $n/(p_{l_1} p_{l_2} ... p_{l_j})$, which, after plugging into formula (1) above and factoring out n, gives us

$$\Big|\bigcup_{i=1}^{k} S_i\Big| \quad = \quad n \cdot \sum_{j=1}^{k} (-1)^{j+1} \sum_{l_1<l_2<...<l_j} \frac{1}{p_{l_1} p_{l_2} ... p_{l_j}}. \qquad (1)$$

We actually want to compute how many numbers *are* relatively prime to n, that is the cardinality of the complement of $\bigcup_{i=1}^k S_i$, so after subtracting it from n and simplifying, will give

$$\phi(n) \quad = \quad n - \Big|\bigcup_{i=1}^{k} S_i\Big| = n \cdot \Big[1 - \sum_{j=1}^{k} (-1)^{j+1} \sum_{l_1<l_2<...<l_j} \frac{1}{p_{l_1} p_{l_2} ... p_{l_j}}\Big]. \qquad (2)$$

To finish off, we note that for any numbers $x_1, ..., x_k$, we have

$$(1 - x_1)(1 - x_2)...(1 - x_k) \quad = \quad 1 - \sum_{j=1}^{k} (-1)^{j+1} \sum_{l_1<l_2<...<l_j} x_{l_1} x_{l_2} ... x_{l_j}. \qquad (3)$$

The theorem follows by taking $x_a = 1/p_a$, for all $a = 1, 2, ..., k$, in the above identity, and plugging it into equation (2). □

0.2 Computing the Number of Integer Partitions

Integer partitions. We need to equip the US cycling team with 13 bicycles. All bicycles are identical, except possibly for color. Each bicycle can be painted in one of three colors: beige, scarlet and ultramarine. How may ways are there to do that?

Denoting by b, s and u the numbers of bicycles of each color, this gives us an equation

$$b + s + u = 13, \quad \text{where } \ 0 \le b, s, u \le 13.$$

So our goal is to compute the number of solutions (b, s, u) of this equation.

Each solution (b, s, u) of this equation is called a *partition* of 13. More precisely, it's sometimes called an ordered partition, since we treat here solutions that have the same numbers but in a different order as different. (In unordered partitions, for example, $(5,4,4)$ and $(4,5,4)$ would be considered the same partition, as it partitions 13 into two 4's and one 5.) But we will simply use the term "partition" here.

To compute the partitions of 13, we do the following trick: draw 13 points on a line. Add two more points, so that we have the total of 15. Then mark two points. Let b be the number of points before the first mark, s the number of points between the marks, and u the number of points after the second mark. Then $b+s+u=13$. Further, any solution of the system above can be obtained in this way. So there is a 1-1 correspondence between the solutions of the linear system above and the markings. Since we mark two points out of 15, the number of partitions of 13 is

$$S = \binom{15}{2} = 105.$$

We can generalize this idea to any number of variables:

Theorem 3 *The number of solutions of* $x_1 + x_2 + ... + x_k = m$*, where* $0 \le x_i \le m$ *for all* i*, is* $\binom{m+k-1}{k-1}$.

Partitions with lower bounds. We now consider our equation, but with an additional constraint that $b \ge 5$, that is

$$b+s+u = 13, \quad \text{where } 5 \le b \le 13 \text{ and } 0 \le s,u \le 13.$$

This is not hard to handle. The intuition is, b contributes 5 or more to both sides, so we can subtract 5 from both sides of the equation and obtain an equation without lower bounds. More precisely, we can write b as $b = b' + 5$, where $b' \ge 0$. Substituting, our equation reduces to

$$b' + s + u = 8, \quad \text{where}$$
$$0 \le b', s, u \le 8.$$

There is a 1-1 correspondence between the solutions of the two equations, by mapping b to b'. So the number of solutions is

$$S(b \ge 5) = \binom{10}{2} = 45.$$

We can in fact extend it to any number of lower bounds, getting the following theorem:

Theorem 4 *Let* $a_1, ..., a_n$ *be non-negative integers such that* $A = \sum_{i=1}^{k} a_i \le m$*. The number of solutions of* $x_1 + x_2 + ... + x_k = m$*, where* $a_i \le x_i \le m$ *for all* i*, is* $\binom{m-A+k-1}{k-1}$.

Or's of Lower Bounds. The next question we look at is this: How many solutions will the equation $b+s+u=13$ have if either $b \ge 5$ or $s \ge 6$ or $u \ge 7$? This can be represented as a sum of sets of solutions, so to compute the number, we can use the inclusion-exclusion principle:

$$\begin{aligned} S(b \ge 5 \vee s \ge 6 \vee u \ge 7) &= S(b \ge 5) + S(s \ge 6) + S(u \ge 7) \\ &\quad - S(b \ge 5 \wedge s \ge 6) - S(b \ge 5 \wedge u \ge 7) - S(s \ge 6 \wedge u \ge 7) \\ &\quad + S(b \ge 5 \wedge s \ge 6 \wedge u \ge 7) \\ &= \binom{10}{2} + \binom{9}{2} + \binom{8}{2} - \binom{4}{2} - \binom{3}{2} - \binom{2}{2} + 0 \\ &= 45 + 36 + 28 - 6 - 3 - 1 = 99. \end{aligned}$$

Partitions with upper bounds. Finally, let us compute the number of solutions of $b + s + u = 13$ for $0 \leq b \leq 4$, $0 \leq s \leq 5$ and $0 \leq u \leq 6$. Note that this set is exactly the complement of the set of solutions we just calculated, so we get

$$S(b \leq 4 \wedge s \leq 5 \wedge u \leq 6) \;=\; S - S(b \geq 5 \vee s \geq 6 \vee u \geq 7) \;=\; 105 - 99 \;=\; 6.$$

Just in case, let's verify. Enumerating all partitions of 13 that satisfy $0 \leq b \leq 4$, $0 \leq s \leq 5$ and $0 \leq u \leq 6$, we obtain the following partitions:

b	4	4	4	3	3	2
s	5	4	3	5	4	5
u	4	5	6	5	6	6

So we have indeed 6 partitions.

0.3 Other Examples

Example 1. Suppose we have three sets, X, Y, Z with the following properties:

$$\begin{aligned}
|X| = 128, |Y| &= 108, |Z| = 114 \\
|X \cap Y| &= |X \cap Y \cap Z| + 22 \\
|X \cap Z| &= |X \cap Y \cap Z| + 6 \\
|Y \cap Z| &= |X \cap Y \cap Z| + 2 \\
|X \cup Y \cup Z| &= 2|X \cap Y \cap Z|
\end{aligned}$$

Determine the number of elements in $X \cup Y \cup Z$.

To solve this problem, we apply the inclusion-exclusion principle, which implies that

$$|X \cup Y \cup Z| = |X| + |Y| + |Z| - |X \cap Y| - |X \cap Z| - |Y \cap Z| + |X \cap Y \cap Z|.$$

Let $|X \cap Y \cap Z| = x$. So we have $|X \cap Y| = x + 22$, $|X \cap Z| = x + 6$, $|Y \cap Z| = x + 2$, and $|X \cup Y \cup Z| = 2 \cdot x$. Plugging these into the above equation, we get

$$2 \cdot x = 128 + 108 + 114 - (x + 22) - (x + 6) - (x + 2) + x.$$

The solution is $x = 80$. Thus $|A \cup B \cup C| = 2 \cdot x = 160$.

Example 2. Little Red Riding Hood is assembling a fruit basket for her sick grandmother. The basket will contain 26 fruit, including apples, bananas, mangos and strawberries (and no other fruit). The basket must contain

- at least 6 apples,
- at least 4 bananas,
- at least 5 mangos, and
- at least 3 and not more than 5 strawberries.

Determine the number of ways to assemble the fruit basked.

The number we seek is the number of integer solutions of

$$\begin{aligned} a+b+m+s &= 26 \\ 6 &\le a \\ 4 &\le b \\ 5 &\le m \\ 3 &\le s \le 5 \end{aligned}$$

After substitutions, this simplifies to computing the number of non-negative integer solutions of

$$\begin{aligned} a+b+m+s &= 8 \\ s &\le 2 \end{aligned}$$

Let S be the number of all solutions, $S(s \le 2)$ the number of solutions with $s \le 2$ and $S(s \ge 3)$ the number of solutions with $s \ge 3$. We now calculate $S(s \le 2)$ as follows

$$S(s \le 2) = S - S(s \ge 3) = \binom{8+3}{3} - \binom{8-3+3}{3} = 165 - 56 = 109.$$

Example 3. Determine the number of permutations of $0, 1, ..., 9$ that do not contain any of the following consecutive sequences of digits: 012, 2345, 89. For example, permutation 5123976048 satisfies this condition, but permutation 5123897604 does not, because it contains 89.

It will help to introduce some notation. For a sequence α, let P_α be the number of permutations that contain α. Similarly, for two sequences α, β, let $P_{\alpha,\beta}$ be the number of permutations that contain both α and β. Analogously we define $P_{\alpha,\beta,\gamma}$, etc.

Before we attack our problem, let's try to figure out how to compute P_{012}. A naïve way to approach this would be this: in any permutation of $0, 1, ..., 9$, the sequence 012 can appear in 8 locations, and the remaining digits can be permuted in 7! ways. This gives us that $P_{012} = 8 \cdot 7! = 8!$.

But there is a more elegant way to compute P_{012}: Since 012 need to appear consecutively, we can think of this sequence as one block $\boxed{012}$. Then P_{012} is the number of permutations of 8 objects, including seven digits $3, 4, ..., 9$ and our block $\boxed{012}$, so we get $P_{012} = 8!$.

We can apply the same trick to compute $P_{012,2345}$ or $P_{012,89}$. A permutation contains both 012 and 2345 if and only if it contains one sequence 012345 (because 012 and 2345 overlap on digit 2). To compute the number of such permutations, we note that this is equivalent to permuting 5 objects, so $P_{012,2345} = 5!$. For $P_{012,89}$, we have two blocks $\boxed{012}$ and $\boxed{89}$, plus 5 remaining digits, so $P_{012,89} = 7!$. Etc, etc.

Okay, now let's get back to our original question. Instead of computing the number of permutations without any sequence 012, 2345, 89, we will compute the cardinality of the complement of this set, namely those that *contain at least one* of these sequences. Let P be this quantity. We can express P as the cardinality of a union of sets, so applying the principle of inclusion-exclusion, the number of such sequences is

$$\begin{aligned} P &= P_{012} + P_{2345} + P_{89} - P_{012,2345} - P_{012,89} - P_{2345,89} + P_{012,2345,89} \\ &= 8! + 7! + 9! - 5! - 7! - 6! + 4! \\ &= 8! + 9! - 5! - 6! + 4! \end{aligned}$$

Then the number of permutations that *do not* contain any of 012, 2345, 89, is the number of all permutations minus P, that is

$$10! - P = 10! - 8! - 9! + 5! + 6! - 4! = 3226416.$$

And that's the final answer.