

CHAPTER 6: INCLUSION-EXCLUSION

WILLIAM T. TROTTER AND MITCHEL T. KELLER

ABSTRACT. In this chapter, we study a classic enumeration technique known as Inclusion-Exclusion. In many situations, we start with an exponentially large calculation and see that it reduces down to manageable size. We focus on three applications that every student of combinatorics should know: (1) counting surjections; (2) derangements; and (3) the Euler ϕ -function.

1. INTRODUCTION

We start this chapter with a very elementary example.

Example 1. Let X be the set of 63 students in this class. There are 47 computer science majors and 51 male students. Also, there are 45 male students majoring in computer science. Then the number of students who are female and not majoring in computer science is $63 - (47 + 59) + 45 = 2$.

More generally, we will consider a set X and a family $\mathcal{P} = \{P_1, P_2, \dots, P_m\}$ of *properties*. We intend that for every $x \in X$ and each $i = 1, 2, \dots, m$, either x satisfies P_i or it does not. There is no ambiguity. Ultimately, we are interested in determining the number of elements of X which satisfy *none* of the properties in \mathcal{P} .

Example 2. Let m and n be fixed positive integers and let $X = [n]$. Then for each $i = 1, 2, \dots, m$, and each $j \in X$, we say that j satisfies P_i if i is a divisor of j .

Example 3. Let m and n be fixed positive integers and let X consist of all functions from $[n]$ to $[m]$. Then for each $i = 1, 2, \dots, m$, and each function $f \in X$, we say that f satisfies P_i if i is in the range of f .

Example 4. Let m be a fixed positive integer and let X consist of all bijections from $[m]$ to $[m]$. Elements of X are called *permutations*. Then for each $i = 1, 2, \dots, m$, and each permutation $\sigma \in X$, we say that σ satisfies P_i if $\sigma(i) = i$.

Note that in this last example, we could have said that σ satisfies property P_i if $\sigma(i) \neq i$. But remembering that our goal is to count the number of elements satisfying none of the properties, we would then be counting the number of permutations satisfying $\sigma(i) = i$ for each $i = 1, 2, \dots, n$, and perhaps we don't need a lot of theory to accomplish this task—the number is one of course.

2. THE INCLUSION-EXCLUSION FORMULA

Let X be a set and let $\mathcal{P} = \{P_1, P_2, \dots, P_m\}$ be a family of properties. Then for each subset $S \subseteq \{1, 2, \dots, m\}$, let $N(S)$ denote the number of elements of X which satisfy property P_i whenever $i \in S$. Note that $N(\emptyset) = |X|$, as every element of X satisfies every property in S (which contains no actual properties).

Date: March 13, 2007.

Theorem 5. *The number of elements of X which satisfy none of the properties in \mathcal{P} is given by*

$$(1) \quad \sum_{S \subseteq \{1, 2, \dots, m\}} (-1)^{|S|} N(S).$$

Proof. We proceed by induction on m . If $m = 1$, then the formula reduces to $N(\emptyset) - N(\{1\})$. This is correct since it says just that the number of elements which do not satisfy property P_1 is the total number of elements minus the number which do satisfy property P_1 .

Now assume validity when $m \leq k$ for some $k \geq 1$ and consider the case where $m = k + 1$. Let $X' = \{x \in X : x \text{ satisfies } P_{k+1}\}$ and $X'' = X - X'$. Also, let $\mathcal{Q} = \{P_1, P_2, \dots, P_k\}$. Then for each subset $S \subseteq \{1, 2, \dots, k\}$, let $N'(S)$ count the number of elements of X' satisfying property P_i for each $i \in S$. Also, let $N''(S)$ count the number of elements of X'' satisfying property P_i for each $i \in S$. Let X'_0 denote the set of elements in X' which satisfy none of the properties in \mathcal{Q} , and let X''_0 denote the set of elements of X'' which satisfy none of the properties in \mathcal{Q} . Note that $N(S) = N'(S) + N''(S)$ for every $S \subseteq \{1, 2, \dots, k\}$.

By the inductive hypothesis, we know

$$|X'_0| = \sum_{S \subseteq \{1, 2, \dots, k\}} (-1)^{|S|} N'(S)$$

and

$$|X''_0| = \sum_{S \subseteq \{1, 2, \dots, k\}} (-1)^{|S|} N''(S).$$

It follows that

$$\begin{aligned} |X''_0| &= \sum_{S \subseteq \{1, 2, \dots, k\}} (-1)^{|S|} N''(S) \\ &= \sum_{S \subseteq \{1, 2, \dots, k\}} (-1)^{|S|} (N(S) - N'(S)) \\ &= \sum_{S \subseteq \{1, 2, \dots, k\}} (-1)^{|S|} N(S) + \sum_{S \subseteq \{1, 2, \dots, k\}} (-1)^{|S|+1} N(S \cup \{m+1\}) \\ &= \sum_{S \subseteq \{1, 2, \dots, k+1\}} (-1)^{|S|} N(S). \end{aligned}$$

□

3. ENUMERATING SURJECTIONS

For positive integers n and m , let $S(n, m)$ denote the number of surjections from $\{1, 2, \dots, n\}$ to $\{1, 2, \dots, m\}$. Note that $S(n, m) = 0$ when $n < m$. In this section, we apply the Inclusion-Exclusion formula to determine a formula for $S(n, m)$. We start by setting X to be the set of all functions from $\{1, 2, \dots, n\}$ to $\{1, 2, \dots, m\}$. Then for each $f \in X$ and each $i = 1, 2, \dots, m$, we say that f satisfies property P_i if i is not in the range of f .

Lemma 6. *For each subset $S \subseteq \{1, 2, \dots, m\}$, $N(S)$ depends only on $|S|$. In fact, if $|S| = k$, then*

$$N(S) = (m - k)^n.$$

Proof. Let $|S| = k$. Then a function f satisfying property P_i for each $i \in S$ is a string of length n from an alphabet consisting of $m - k$ letters. This shows that $N(S) = (m - k)^n$. \square

Now the following result follows immediately, as there are $C(m, k)$ k -element subsets of $[m]$.

Theorem 7. *The number $S(n, m)$ of surjections from $\{1, 2, \dots, n\}$ to $\{1, 2, \dots, m\}$ is given by:*

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

For example,

$$\begin{aligned} S(5, 3) &= \binom{3}{0} (3 - 0)^5 - \binom{3}{1} (2^5) + \binom{3}{2} (1^5) - \binom{3}{3} (0^5) \\ &= 243 - 96 + 3 - 0 \\ &= 150 \end{aligned}$$

4. DERANGEMENTS

Fix a positive integer n and let X denote the set of all permutations on $\{1, 2, \dots, n\}$. A permutation $\sigma \in X$ is called a *derangement* if $\sigma(i) \neq i$ for all $i = 1, 2, \dots, n$. For example, the first permutation given below is a derangement, while the second is not.

$$\begin{array}{c|cccc} i & 1 & 2 & 3 & 4 \\ \hline \sigma(i) & 2 & 4 & 1 & 3 \end{array} \qquad \begin{array}{c|cccc} i & 1 & 2 & 3 & 4 \\ \hline \sigma(i) & 2 & 4 & 3 & 1 \end{array}$$

Lemma 8. *For each subset $S \subseteq \{1, 2, \dots, m\}$, $N(S)$ depends only on $|S|$. In fact, if $|S| = k$, then*

$$N(S) = (n - k)!$$

Proof. For each $i \in S$, the value $\sigma(i) = i$ is fixed. The other values of σ are a permutation among the remaining $n - k$ positions. \square

As before, the principal result of this section follows immediately.

Theorem 9. *For each positive integer n , the number d_n of derangements satisfies*

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

For example,

$$\begin{aligned} d_5 &= \binom{5}{0} 5! - \binom{5}{1} 4! + \binom{5}{2} 3! - \binom{5}{3} 2! + \binom{5}{4} 1! - \binom{5}{5} 0! \\ &= 120 - 120 + 60 - 20 + 5 - 1 \\ &= 44. \end{aligned}$$

The next result investigates the fraction of permutations that are derangements.

Theorem 10. For a positive integer n , let d_n denote the number of derangements of $\{1, 2, \dots, n\}$. Then

$$\lim_{n \rightarrow \infty} \frac{d_n}{n!} = \frac{1}{e}.$$

Proof. It is easy to see that

$$\begin{aligned} \frac{d_n}{n!} &= \frac{\sum_{k=0}^n (-1)^k \binom{n}{k} (n-k)!}{n!} \\ &= \sum_{k=0}^n (-1)^k \frac{n!}{k!(n-k)!} \frac{(n-k)!}{n!} \\ &= \sum_{k=0}^n (-1)^k \frac{1}{k!}. \end{aligned}$$

Recall from Calculus that the Taylor series expansion of e^x is given by

$$e^x = \sum_{k=0}^{\infty} \frac{x^k}{k!}$$

The result then follows by substituting $x = -1$. \square

It has been traditional to cast the preceding result as a story, called the Hat Check problem. The story belongs to the period of time when men wore top hats. For a fancy ball, 100 men check their top hats with the Hat Check person before entering the ballroom floor. Later in the evening, the mischeivous hat check person decides to return hats at random. Then the probability that all 100 men receive a hat different from their own is very close to $1/e$.

5. THE EULER ϕ FUNCTION

In this section, we produce an important example where the value of $N(S)$ *does* depend on $|S|$. Nevertheless, we are able to make a reduction to obtain a useful end result.

For a positive integer $n \geq 2$, let

$$\phi(n) = |\{m \in \mathbb{N} : 1 \leq m \leq n, \gcd(m, n) = 1\}|.$$

For example, $\phi(12) = 4$ since the only numbers from $\{1, 2, \dots, 12\}$ that are relatively prime to 12 are 1, 5, 7 and 11. As a second example, $\phi(9) = 6$ since 1, 2, 4, 5, 7 and 8 are relatively prime to 9. On the other hand, $\phi(p) = p - 1$ when p is a prime. Suppose you were asked to compute $\phi(321974)$. How would you proceed?

Early in the course, we studied a recursive procedure for determining the greatest common divisor of two integers, and we wrote a code for accomplishing this task. Let's assume that we have a function declared as follows:

```
int gcd(int m, int n);
```

that returns the greatest common divisor of m and n .

Then we can calculate $\phi(n)$ with this code snippet:

```

answer = 1;
for (m = 2; m < n; m++) {
    if (gcd(m,n) == 1) {
        answer++;
    }
}
return(answer);

```

I wrote a program called `phi.c` using the code snippet above and it answered almost immediately that $\phi(321974) = 147744$.

On the other hand, in just under two minutes my program reported that

$$\phi(319572943) = 319524480.$$

So how could we find

$$\phi(1369122257328767073)?$$

Clearly, the program is useless to tackle this beast! But fortunately, Inclusion-Exclusion comes to the rescue.

Theorem 11. *Let $n \geq 2$ be a positive integer and suppose that n has m distinct prime factors: p_1, p_2, \dots, p_m . Then*

$$(2) \quad \phi(n) = n \prod_{i=1}^m \frac{p_i - 1}{p_i}.$$

Proof. We present the argument when $m = 3$. The full result is an easy extension.

Our argument requires the following elementary proposition whose proof we leave as an exercise.

Proposition 12. *Let $n, k \geq 2$, and let p_1, p_2, \dots, p_k be distinct primes each of which divide n evenly (without remainder). Then the number of integers from $\{1, 2, \dots, n\}$ which are divisible by each of these k primes is*

$$\frac{n}{p_1 p_2 \cdots p_k}.$$

Then Inclusion-Exclusion yields:

$$\begin{aligned}
 \phi(n) &= n - \left(\frac{n}{p_1} + \frac{n}{p_2} + \frac{n}{p_3} \right) + \left(\frac{n}{p_1 p_2} + \frac{n}{p_1 p_3} + \frac{n}{p_2 p_3} \right) - \frac{n}{p_1 p_2 p_3} \\
 &= n \frac{p_1 p_2 p_3 - (p_2 p_3 + p_1 p_3 + p_1 p_2) + (p_3 + p_2 + p_1) - 1}{p_1 p_2 p_3} \\
 &= n \frac{p_1 - 1}{p_1} \frac{p_2 - 1}{p_2} \frac{p_3 - 1}{p_3}. \quad \square
 \end{aligned}$$

Example 13. Maple reports that

$$1369122257328767073 = (3)^3(11)(19)^4(31)^2(6067)^2$$

is the factorization of 1369122257328767073 into primes. It follows that

$$\phi(1369122257328767073) = 1369122257328767073 \frac{2}{3} \frac{10}{11} \frac{18}{19} \frac{30}{31} \frac{6066}{6067}.$$

Thus Maple quickly reports that

$$\phi(1369122257328767073) = 760615484618973600.$$

Example 14. The Professor decides to give Alice and Bob the same challenge, namely to find $\phi(n)$ when

$$\begin{aligned} n = & 31484972786199768889479107860964368171543984609017931 \\ & 390019221598516685310407085397223293249028133592 \\ & 4101693211209710523. \end{aligned}$$

However the Professor also tells Alice that $n = p_1 p_2$ is the product of two large primes where

$$p_1 = 470287785858076441566723507866751092927015824834881906763507$$

and

$$p_2 = 669483106578092405936560831017556154622901950048903016651289.$$

Is this information of any special value to Alice? Does it really make her job any easier than Bob's?

SCHOOL OF MATHEMATICS, GEORGIA INSTITUTE OF TECHNOLOGY, ATLANTA, GEORGIA 30332,
U.S.A.

E-mail address: `trotter@math.gatech.edu`

SCHOOL OF MATHEMATICS, GEORGIA INSTITUTE OF TECHNOLOGY, ATLANTA, GEORGIA 30332,
U.S.A.

E-mail address: `keller@math.gatech.edu`