Basic counting techniques

Periklis A. Papakonstantinou

Rutgers Business School

LECTURE NOTES IN Elementary counting methods

Periklis A. Papakonstantinou
MSIS, Rutgers Business School

Lecture 2

Elementary counting

We will survey elementary counting techniques. No previous background is assumed. This document is very non-dense and can be safely skipped if there is basic knowledge in combinatorics.

2.1 Basic counting principles

One way to formally introduce counting principles is through countable sets, the cardinality of these sets, operations among sets, and mappings between these sets. A more advanced treatment would have used "generative functions and formal power series" – we will not do this here (neither it is generally necessary).

Counting involves quantitative reasoning where intuition is the main component. A proof is often times implicit.

There are two basic intuitive principles: (i) *principle of sum* & (ii) *principle of product*.

(i) If there are m ways to perform a task and n ways to perform an *unrelated task*, then there are in total $m + n$ ways to perform the *combined task*.

(ii) If there are m ways to perform a task and n ways to perform a second task, then there are $m \times n$ ways for the combined task that performs *first* one and *second* the other task.

Formally speaking, the principle of sum corresponds to the size of the set $C = A \cup B$, i.e. $|A \cup B|$, of two disjoint sets $|A| = m$, $|B| = n$; whereas the principle of product is just the size of the set $C = A \times B$, i.e. $|A \times B|$, where A, B are not necessarily disjoint.

Before going further think of examples to which each principle applies.

Example 1 (Number of arrangements). *We have* 10 distinct *slots, e.g. say that they are numbered. We also have* 10 distinct *balls. To count the different arrangements of these balls into the slots we fix an order of the slots. In the first slot we can put one of the* 10 *balls. In the second slot we can put one out of the (remaining)* 9 *balls. . . . Continuing in the same way we see that in the last slot we only have one choice. In total, we can arrange the balls in* $10 \cdot 9 \cdot \ldots \cdot 2 \cdot 1 = 3628800$ *different ways.*

What if we could not distinguish among slots? That is, suppose that the balls are distinct say they are numbered as $1, 2, \ldots, 10$, but the slots are indistinguishable. In this case the arrangement $\langle 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 \rangle$ would be exactly the same as the arrangement $\langle 2, 3, 1, 4, 5, 6, 7, 8, 9, 10 \rangle$. In fact, every arrangement is indistinguishable from every other. Therefore, there is only 1 way to arrange the 10 balls in 10 indistinguishable slots. We would also have had only one way to arrange them if the balls were indistinguishable but the slots were distinct; and same thing if both were indistinguishable.

The question of whether the slots and the balls are distinct is specified in the description of the problem.

What if instead of balls and slots we had the following? How many 10-digit decimal numbers (we allow the numbers to start with a zero) exist, when we restrict the numbers to have each digit different from the rest? It should be clear that we can *model* our counting problem in an equivalent way as the balls-to-slots problem. In an

integer the position where each digit appears is clearly distinct and every digit is distinct from every other.

These two simple problems give rise to a general trick applied in counting arguments.

Say that A and B are two sets. A function f is a mapping from A onto B, $f : A \rightarrow B$; that is, for every $x \in A$ there exists one $f(x) \in B$. If there do *not* exist two distinct $x_1, x_2 \in A$ (i.e. $x_1 \neq x_2$) such that $f(x_1) = f(x_2)$ then the function is called $1 - 1$ (or injective). If for every element $y \in B$ there exists an $x \in A$, such that $f(x) = y$ then the function is called *onto* (or surjective). A function f that it is both $1 - 1$ and onto is called $1 - 1$ *correspondence* (or bijective). $1 - 1$ *correspondences* play a crucial role in counting arguments. Consider two finite sets A and B. Say that there exists an $f : A \rightarrow B$ which is an $1 - 1$ *correspondence*. Then $|A| = |B|$. In other words:

> Suppose that we know how to count the elements of a set A. Say that $n = |A|$. If we manage to show that there exists an $1 - 1$ *correspondence* f between A and B, then at the same time we have counted the elements of B, $|B| = n$.

In particular, the set A is the set containing as its elements arrangements of 10 distinct balls to 10 distinct slots. You can realize such an element as a sequence; example: $\langle 2, 3, 1, 4, 5, 7, 6, 8, 9, 10 \rangle$. The set B consists of 10-digit (with distinct digits) numbers. Therefore, an $1 - 1$ correspondence can be the one that for example maps $\langle 2, 3, 1, 4, 5, 7, 6, 8, 9, 10 \rangle$ to the number 2314576890. It is easy to show that under this mapping: (i) there are no two arrangements (of balls-to-slots) that are mapped to the same number and (ii) for every 10-digit number there exists one arrangement (of balls-to-slots) that corresponds to it. Therefore, if we have already counted the number of balls-to-slots arrangements and having established the $1 - 1$ correspondence, we also know the number of 10-digit numbers.

The technique is much stronger than its trivial application here. See Section 2.4 for more examples.

Definition 2. *Let $n \in \mathbb{Z}^{\geq 0}$. If $n \geq 1$, define $n! = n \cdot (n-1) \cdot \ldots \cdot 2 \cdot 1$. Define $0! = 1$.*

Arrangements of objects

We denote by $A(n)$ the number of arrangements of n distinct objects (into n distinct positions). Then, it should be clear that $A(n) = n \cdot (n-1) \cdot \ldots \cdot 2 \cdot 1 = n!$. Now, consider the two problems we have just looked. For both of these problems it is clear that there exists an $1-1$ correspondence between them and the set of all arrangements of 10 distinct objects (whose cardinality is $A(10)$).

As our last remark, consider again the problem of determining the number of 10-digit integers where each digit is distinct. We solve a different problem by not allowing integers to start with 0. How many integers exist under this modification? The answer is $A(10) - A(9) = 10! - 9! = (10-1)9! = 9 \cdot 9!$. Why?

Apply the principle of sum.

integers starting with zero + # integers not starting with zero
= # integers

therefore,

integers not starting with zero
= # integers - # integers starting with zero

Alternatively, we could have argued as follows: for the most significant digit we have 9 available choices (excluding 0). Then, for the second most significant digit we have 9 choices (we exclude the one we used for the first - but now we can use zero). For the third most significant digit we have 8 choices, etc. Therefore we have $9 \cdot 9 \cdot 8 \cdot 7 \cdot \ldots \cdot 2 \cdot 1 = 9 \cdot 9!$.

What is the difference between the above two different (valid) arguments for the same enumeration problem? In the first argument we use the fact that we already know how to count arrangements of objects, but since the problem is not a mere arrangement problem we have to exclude some cases (which again we count using $A(n)$). In the second argument we start from scratch.

2.2 Permutations and Combinations without repetition

Permutations

Let $n, k \in \mathbb{Z}^{\geq 0}$, $n \geq k$. We denote by $P(n,k)$ the different ways into which we can arrange k objects by choosing from a set of n objects (without reusing objects). Fix an order on k positions. For the first position we have n choices, for the second we have $n - 1 \ldots$ for the last we have $(n - k + 1)$. Therefore, $P(n,k) = n \cdot (n - 1) \cdot \ldots \cdot (n - k + 1) = \frac{n!}{(n-k)!}$.

Combinations

Basics

Let us solve a similar problem, where the order of objects does not count. That is, given a set of n distinct objects we want to count how many different subsets of k objects we can construct. We denote by $C(n,k)$ or $\binom{n}{k}$ the possible distinct combinations of k objects chosen from a set of n (distinct) objects. Using the principle of product we have:

$$C(n,k) \cdot (\text{\# arrangements of } k \text{ objects}) = P(n,k)$$

That is, the number of permutations $P(n,k)$ equals to the number of ways of first choosing sets of k objects (without caring about their order-arrangement) and then arranging (i.e. introducing ordering) the objects of each set in all possible ways.

Therefore, $C(n,k) \equiv \binom{n}{k} = \frac{P(n,k)}{A(k)} = \frac{n}{k!(n-k)!}$.

One immediate property of combinations $\binom{n}{k}$ (read as "n choose k") is that $\binom{n}{k} = \binom{n}{n-k}$.

Binomial Coefficients

One application of combinations is to determine coefficients of the polynomial $(s + t)^n$ (actually, the reason for initially introducing combinations was these coefficients). Binomial Coefficients are the constants of the terms of the polynomial $(s + t)^n$ (this is a polynomial on two variables s and t).

We first consider a simpler problem. Consider the polynomial $(1 + x)^n$ say over the field of reals. Just for fun, let us expand $(1 + x)^n$ for some small values of n. For $n = 2$ we have:

$$(1 + x)^2 = (1 + x)(1 + x) = 1 + x + x + x^2 = 1 + 2x + x^2$$

and for $n = 3$:

$$(1 + x)^3 = (1 + x)(1 + x)^2 = (1 + x)(1 + x + x + x^2)$$
$$= 1 + x + x + x^2 + x + x^2 + x^2 + x^3 = 1 + 3x + 3x^2 + x^3$$

In general we have $(1 + x)^n = c_0 + c_1 x + c_2 x^2 + \ldots + c_n x^n$ and we wish to determine the values of the constants $c_0, c_1, c_2, \ldots, c_n$. One (non-trivial) thing we could try is to guess the value of c_i and then prove it by induction. We will follow an alternative, combinatorial argument. We observe that in $(1 + x)^k$ the term x^k appears only once. Give a distinct name to each term $(1 + x)$ of the product $\underbrace{(1 + x)_1 (1 + x)_2 \ldots (1 + x)_n}_{(1+x) \; n \text{ times}}$. We observe that by the distributivity of multiplication if we write $(1 + x)^n = (1 + x)^{n-k}(1 + x)^k$ and we fix what we mean by $(1 + x)^{n-k}$ and by $(1 + x)^k$, there will be only one

x^k due to the fixed $(1 + x)^k$. This fixed x^k will eventually appear into the expansion if we successively apply the distributive law. So the problem in determining c_k reduces in counting how many different x^k we can have as a result of the expansion of $(1 + x)^n$. That is, in how many different ways we can write $(1 + x)^k$. We have considered each parenthesis $(1 + x)$ of the product $(1 + x)^n$ as distinct. Therefore, we have $\binom{n}{k}$ ways of choosing sets of different parenthesis $(1 + x)^k$.

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

Substituting $x = \frac{s}{t}$ we get the following:

$$(s + t)^n = \sum_{k=0}^{n} \binom{n}{k} s^k t^{n-k}$$

Properties of Binomial Coefficients

Here are some basic properties of the binomial coefficients:

1. $\binom{n}{r} = \binom{n}{n-r}$

2. $\binom{n}{r} = \binom{n-1}{r} + \binom{n-1}{r-1}$

3. $\binom{n}{r} = \frac{n}{r} \binom{n-1}{r-1}$

4. $\sum_{k=0}^{n} \binom{r+k}{k} = \binom{r+n+1}{n}$

5. $\binom{n}{m} \binom{m}{r} = \binom{n}{r} \binom{n-r}{m-r}$

6. $\sum_{k=0}^{n} \binom{r}{k} \binom{s}{n-k} = \binom{r+s}{n}$

Property 2 yields a representation called *Pascal's triangle*. Consider an arrangement of binomial coefficients on a triangle. On one vertex put $\binom{0}{0}$. Then consider $\binom{1}{0}$ and $\binom{1}{1}$ and put them below $\binom{0}{0}$ and align them to the left and to the right of $\binom{0}{0}$. In the same fashion consider

$\binom{2}{0}$, $\binom{2}{1}$ and $\binom{2}{2}$ and align them on the third row. In this way we get the Pascal's triangle, part of which is depicted below.

$$\binom{0}{0}$$
$$\binom{1}{0} \qquad \binom{1}{1}$$
$$\binom{2}{0} \qquad \binom{2}{1} \qquad \binom{2}{2}$$
$$\binom{3}{0} \qquad \binom{3}{1} \qquad \binom{3}{2} \qquad \binom{3}{3}$$

By property 2 a binomial coefficient is the sum of the two binomial coefficients in the triangle that are just above and just to the left and to the right.

Apart from a proof based on algebraic manipulations the above properties (1-6) can be shown using *combinatorial arguments* (as almost every argument presented in this document). For example, consider property 3. Algebraically the proof is trivial: $\frac{n}{r}\binom{n-1}{r-1} = \frac{n(n-1)!}{r(r-1)!(n-r)!} = \binom{n}{r}$. Here is a combinatorial proof: In order to choose r objects from n, it suffices to choose 1 and then choose $r - 1$ among (the remaining) $n - 1$. For the choice of the first object we have n choices and for the remaining we have $\binom{n-1}{r-1}$. Therefore, in total we have $n\binom{n-1}{r-1}$. But in this way we distinguish between the first chosen object and the rest (i.e. this way an order is imposed). Hence, $n\binom{n-1}{r-1} = \binom{n}{r}r$. That is, $n\binom{n-1}{r-1}$ equals to the number of ways of choosing (without an order) r objects from n and then choosing one of these r objects as the "special" object. Hence, $\frac{n}{r}\binom{n-1}{r-1} = \binom{n}{r}$.

Exercise 3. *Give a combinatorial proof for property 5.*

An application of the (Binomial) coefficients of the polynomial $(s + t)^n$

Say that a and b are constants. We wish to show that $(x + a)^b = \Theta(x^b)$. We have determined that $(x + a)^b = \sum_{k=0}^{b} \binom{b}{k}x^k a^{b-k}$. Since a and b are constants, for every k the factor $\binom{b}{k}a^{b-k}$ is also a constant. Therefore, $(x + a)^b = \Theta(x^b)$. (if you were asked to show that $(x +$

$a)^b = \Theta(x^b)$, as part of one of your assignments or tests you should have given the full proof).

2.3 Arrangements of objects containing indistinguishable objects

Consider n objects and say that there are r groups each containing identical (indistinguishable) objects. Say that the i-th group consists of q_i identical elements. Say that the number of distinct arrangements of the n objects are N. We apply the following combinatorial trick. Since we know how to count arrangements of distinct objects we will use this fact: For the moment modify the elements (for example, by adding a distinct subscript) within each group so as to make them distinct. Note that N (still)counts the objects as they initially are (i.e. with groups of indistinguishable objects). Arrange the objects of the first group. Then, arrange the objects of the second group etc. Therefore, we have $N q_1! q_2! \ldots q_r! = n!$. That is, the number of arrangements of object consisting of r groups of identical objects is

$$\frac{n!}{q_1! q_2! \ldots q_r!}$$

For the special case where there are only two groups having q_1 and q_2 identical elements (i.e. $n = q_1 + q_2$), the number of different arrangements is:

$$\frac{n!}{q_1! q_2!} = \frac{n!}{q_1!(n - q_1)!} = \binom{n}{q_1} = \binom{n}{q_2}$$

2.4 Permutations and Combinations with repetitions

Permutations with repetitions

Suppose that we have n distinct objects but unlike the previous cases, now we allow (infinitely many) repetitions of each object. We have n objects and we count the number of different ways we can arrange k

of them when repetition is allowed. Fix an order on k slots. For the first slot we have n choices. For the second we also have n choices (since we allow repetition of objects) etc. Therefore, there are n^k different permutations with repetitions.

Application of permutations with repetitions

Given n distinct objects we wish to count all different subsets (including the empty one) we can construct out of these n objects. That is, we want to determine the value of $\sum_{k=0}^{n} \binom{n}{k}$. One easy way to do so is to associate (i.e. establish a $1-1$ correspondence) between n-digit binary numbers (we allow the binary numbers to start with zero) and subsets of objects. Fix an ordering on the n objects. An object can either be included in a subset or not. For an arbitrary subset, we associate with every chosen object an 1 and with every non-chosen object a 0. For example, consider the 3 objects $\{a, b, c\}$. Fix an ordering, say $\langle a, b, c \rangle$. Then, the binary number 011 corresponds to the subset $\{b, c\}$. Note that for every object there is a unique binary number that corresponds to it. And, for every subset there exists a binary number which corresponds to it. That is, the mapping is an $1-1$ correspondence. Now, in order to determine $\sum_{k=0}^{n} \binom{n}{k}$ it suffices to determine the number of distinct n-digit binary numbers. This is just the number of permutations with repetition of two digits (0 and 1) into n positions. That is,

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n$$

Combinations with repetitions

Counting the number of combinations (i.e. the order does not count) with repetition is more trickier. In order to count the different subsets of size (cardinality) k from a set of n objects when repetition is allowed, this calls for the counting trick where we establish an $1-1$

correspondence between a set of things we know how to count and the target set of things we want to count. We give some hints for the general proof through an illustrative example.

Suppose that we have 4 objects say a, b, c, d and we want to count how many combinations with repetition we have resulting sets of 5 objects. Since we allow repetition we formally talk about multisets of 5 objects. A *multiset* is a set where an element appears together with its multiplicity (or equivalently may appear more than once). One possible choice is the multiset $\{a, b, b, c, d\}$ and another is $\{a, b, a, d, c\}$. In order to establish the "1-1" correspondence we introduce some ordering into the problem. Note that the way in which we will introduce this ordering does not hurt generality (i.e. the "un-ordered nature" of the multiset). Fix an ordering on the five objects, say $a \succ b \succ c \succ d \succ e$. We list the resulting multisets according to this order. For example:

$$
\begin{array}{|c|}
\hline
\{a, b, b, c, d\} \\
\{a, a, b, c, d\} \\
\{a, a, a, d, d\} \\
\{b, b, b, b, b\} \\
\{a, a, a, a, a\} \\
\vdots \\
\hline
\end{array}
$$

Our goal is to establish an $1 - 1$ correspondence with a set that we know how to count. We use $4 - 1 = 3$ vertical bars to somehow designate the begin and the end of each group of identical objects. For example, $a|bb|c|d$. The first vertical bar corresponds to objects a that are on the left of this bar. Between the first and the second vertical bar we have objects b. Between the second and the third vertical bar are objects c. And to the right of the third vertical bar we have objects d. Note that the introduced semantics for the vertical bars allows us to use only one symbol to denote objects. That is, if

we write $x|xx|x|x$ this uniquely corresponds to $\{a, b, b, c, d\}$. Hence, we have:

$\{a, b, b, c, d\}$	$x\|xx\|x\|x$
$\{a, a, b, c, d\}$	$xx\|x\|x\|x$
$\{a, a, a, d, d\}$	$xxx\|\|\|xx$
$\{b, b, b, b, b\}$	$\|xxxxx\|\|$
$\{a, a, a, a, a\}$	$xxxxx\|\|\|$
$\vdots$	$\vdots$

It is also easy to show that every arrangement of 5 x's and 3 vertical bars corresponds to a multiset. Therefore, we have established an $1 - 1$ correspondence from the multisets we want to count to the arrangements of $5 + (4 - 1) = 8$ objects, where we have one group of 5 identical objects and one group of $4 - 1 = 3$ identical objects. As we have already seen the number of these different arrangements is $\frac{8!}{5!3!}$.

It is a good exercise to attempt to count the above number of combinations with repetitions starting from basic principles (i.e. the principles of sum and product). The tempted reader will shortly realize that one could easily get into trouble.

It is worth stressing out that: (i) we may wish to establish a $1 - 1$ correspondence between the elements of the set we want to count (here an element is a multiset of size 4) and the elements of a set we know how to count (here an element is a sequence of 5 x's and 3 vertical bars) and (ii) the elements of the set we already know how to count might have quite different structure than the elements of the set we want to count. In the above example, a multiset does not have an order, where the sequences (arrangements) do; the multiset consisted of 5 elements where the arrangement of 8; the multiset consists of 4 different elements where the arrangement of 2.

Now, it is not hard to give a general proof of the following fact: The number of combinations where we choose with repetition k objects from n distinct objects is

$$\binom{n+k-1}{k}$$

Exercise 4. *Show that the number of combinations where we choose with repetition k objects from n distinct objects is $\binom{n+k-1}{k}$.*

Applications of combinations with repetition

Example 5. *We want to count the number of calls to* DO-SOMETHING *(line 7).*

NOTHING-SPECIAL$[n]$

```
1   for i ← 1 to n
2       do
3           for j ← 1 to i
4               do
5                   for k ← 1 to j
6                       do
7                           DO-SOMETHING[i,j,k]
```

It seems cumbersome to work from basic principles. We observe that if we try to count ordered permutations corresponding to (i,j,k) we would have run into the same troubles as if we were working from basic principles. The reason is that $(5,3,2)$ is valid, where $(5,10,2)$ is not (j can never get a higher value than i). Therefore, working in this way it seems that we have to exclude cases with "complex" interactions. It appears that a different "explicitly unordered" approach yields a straightforward answer. If we consider (multi)sets of three elements instead of permutations and we agree on the convention that the largest element corresponds to i, the second largest to j and the smallest to k then we have resolved the problem. Since i,j,k

may take the same value then we are talking about combinations with repetitions. Note that counting all the three element multisets which are subsets of $\{1, 2, \ldots, n\}$ we have every possible assignment of values for i, j and k. Therefore, the number of calls to DO-SOMETHING *is* $\binom{n+3-1}{3} = \binom{n+2}{3}$.

Example 6. *The following problem is from a well-studied type of problems known as* balls-to-bins. *Consider n distinct bins and r indistinguishable balls. What is the number of different placements of balls into bins? Note that a bin might be empty. We realize the problem as assigning* **bins to balls**. *We assign the bins as follows: (i) choose r bins, (ii) every bin can be chosen more than once and (iii) the order does not count since the balls are indistinguishable. Therefore, the number of placements is $\binom{n+r-1}{r}$.*

Before reading further convince yourself about the validity of (i), (ii), and especially for (iii).

Example 7. *Suppose that we want to count the number of non-negative integer solutions to the following equation:*

$$x_1 + x_2 + \ldots + x_n = r, \ n, r \in \mathbb{Z}^{\geq 0}$$

This problem is equivalent to the previous one, since we may consider the balls to correspond to 1s and the bins to x_i's. Therefore, the number of integer solutions is $\binom{n+r-1}{r}$.

Up to now it should be clear that the following are equivalent.

- The combinations with repetitions of r objects from n objects.

- The number of placements of r indistinguishable balls into n distinct bins.

- The number of non-negative integer solutions of $x_1 + x_2 + \ldots + x_n = r, \ n, r \in \mathbb{Z}^{\geq 0}$

2.5   Balls to bins

It is true that many counting problems can be modeled as a balls-to-bins problem. Here is a table giving the number of ways for placing balls into bins for some basic balls-to-bins problems.

Balls-to-Bins Problem	# of placements when we allow empty bins
n distinct bins r distinct balls	n^r
n distinct bins r distinct balls it also counts the order in which we place balls into bins	$\frac{(n+r-1)!}{(n-1)!}$
n distinct bins r indistinguishable balls	$\binom{n+r-1}{r}$

Exercise 8. *It is a good exercise to prove (using combinatorial arguments) each of the above.*

2.6 Principle of Inclusion-Exclusion

The principle

Often in counting problems we want to count the total number of *distinct* elements of two or more sets of objects. Say that we have two finite sets A and B. We want to count the number of elements that are in the union of the two sets. Straightforwardly this equals to

$$|A \cup B| = |A| + |B| - |A \cap B| \tag{2.1}$$

(that is the total number of distinct elements of A and B equals to the sum of their cardinalities minus the number of their common elements - i.e. the cardinality of their intersection.)

Remark 9. *One may wonder why is it simpler to compute the number of elements in $A \cup B$ by the above formula. Of course this is not always the case. But, in some cases we can* model *some counting problems such that we know (or we know how to compute) $|A|$, $|B|$ and we also do know (or we know how to compute) how to count their common elements. As a rule of thumb consider the sets A and B to correspond to the "bad cases" for a counting problem. Talking a bit abstractly consider the following example: Say that we have a set S and we have two ("bad") properties on the elements of S. Our goal is to count the number of elements of S that do* not *satisfy any of the two ("bad") properties. Suppose that we are given $|S| = n$ and the two properties such that P_1 elements of S satisfy the first and P_2 satisfy the second and that P elements of S satisfy both. Then, the number of elements that does not satisfy any of the two properties is $n - (P_1 + P_2 - P)$.*

What if we have more than two sets. This case gives rise to more

complicated interactions. For example

$$|A \cup B \cup C| = |(A \cup B) \cup C| = |A \cup B| + |C| - |(A \cup B) \cap C|$$

<div align="center">(it is easy to verify that ∩ is distributive for ∪ and vice-versa)</div>

$$
\begin{aligned}
&= |A \cup B| + |C| - |(A \cap C) \cup (A \cap B)| \\
&= |A| + |B| + |A \cap B| + |C| - |(A \cap C) \cup (A \cap B)| \\
&= |A| + |B| + |A \cap B| \\
&\quad + |C| - \big(|(A \cap C)| + |(A \cap B)| - |(A \cap C) \cap (A \cap B)|\big) \\
&= |A| + |B| + |C| + |A \cap B| \\
&\quad - |(A \cap C)| - |(A \cap B)| + |(A \cap B \cap C)|
\end{aligned}
$$

We derived the above result by repeatedly applying equation 2.1. Therefore, for n sets $A_1, A_2, \ldots, A_n$ it is easy to show by induction that:

$$
\left| \bigcup_{i=1}^{n} A_i \right| = \sum_{i=1}^{n} |A_i| - \sum_{1 \le i_1 < i_2 \le n} |A_{i_1} \cap A_{i_2}| + \sum_{1 \le i_1 < i_2 < i_3 \le n} |A_{i_1} \cap A_{i_2} \cap A_{i_3}|
$$
$$
- \ldots + (-1)^n \left| \bigcap_{i=1}^{n} A_i \right|
$$

You should try to give a combinatorial proof for the above.

Up to now we were discussing problems where we wanted to count in the exact sense. It is quite often the case that an upper or lower bound would be sufficient for a specific problem. It is also the case that for most problems it is hard to compute the number of elements in the intersections of sets. For example, say that after modeling our counting problem we have 4 sets A_1, A_2, A_3, A_4. Perhaps due to the nature of the problem it may be the case that it is easy to compute the cardinality of the intersection of any two sets ($|A_i \cap A_j|$, $i \neq j$); but on the other hand it gets quite non-trivial to compute the intersection of three or four sets.

A place where the following inequalities might appear helpful is:
(i) an upper or lower bound is sufficient and (ii) we may wish to
increase *m* up to the point we achieve the desired accuracy.

It is easy to show by induction that the following inequalities,
known as Boole-Bonferroni inequalities, hold.

For *m* ≤ *n odd*:

$$\left| \bigcup_{i=1}^{n} A_i \right| \le \sum_{i=1}^{n} |A_i| - \sum_{1 \le i_1 < i_2 \le n} |A_{i_1} \cap A_{i_2}|$$

$$+ \sum_{1 \le i_1 < i_2 < i_3 \le n} |A_{i_1} \cap A_{i_2} \cap A_{i_3}| - \ldots - \sum_{1 \le i_1 < \ldots < i_m \le n} \left| \bigcap_{k=1}^{m} A_{i_k} \right|$$

For *m* ≤ *n even*:

$$\left| \bigcup_{i=1}^{n} A_i \right| \ge \sum_{i=1}^{n} |A_i| - \sum_{1 \le i_1 < i_2 \le n} |A_{i_1} \cap A_{i_2}|$$

$$+ \sum_{1 \le i_1 < i_2 < i_3 \le n} |A_{i_1} \cap A_{i_2} \cap A_{i_3}| - \ldots + \sum_{1 \le i_1 < \ldots < i_m \le n} \left| \bigcap_{k=1}^{m} A_{i_k} \right|$$

Applications of the Principle of Inclusion-Exclusion

Yet another balls-to-bins problem

We wish to count the number of placements of 5 distinct balls to 4
distinct bins with the constraint that no bin is empty. Here is how
we apply the inclusion-exclusion principle. We already know that
there are n^r ways (Section 2.5) to place *r* balls into *n* bins, when we
allow empty bins. We wish to exclude the number of placements
which have (at least one) empty bin. Consider the set *A* of all place-
ments where empty bins are allowed. Choose your favorite way of
encoding a placement i.e. the elements of *A* [1]. Say that $\bar{A}_i$ is the set

---

[1]Perhaps you want to represent each placement as a set $\{(ball_i, bin_j) | \text{place ball } i \text{ into bin } j\}$. That is, the set *A* has as its
elements sets of the previous form, that correspond to placements of the *r* balls into *n* bins.

containing all the placements where *the i-th bin is empty.* Therefore, we want to count $|A| - |\bar{A}_1 \cup \bar{A}_2 \cup \bar{A}_3 \cup \bar{A}_4|$.

Remark 10. *To approach this problem from scratch (basic principles) we have to deal with the complex correlation between cases. That is, consider the case where the first bin is empty and the others not; and the case where the last two bins are empty and the first not; and so on. In general, you carefully consider all these complex interactions that arise in this counting problem. The Inclusion-Exclusion principle is nothing more than a systematic way of revealing all these interactions. The set $(\bar{A}_1 \cup \bar{A}_2 \cup \bar{A}_3 \cup \bar{A}_4)$ is nothing else but the set containing all placements where at least one of these bins is empty. Recall that the union $\cup$ between sets is defined as a logical OR of containing an element either from one or from the other set. Note that this OR is exactly what we want. Pay attention to the fact that a placement which is an element in $\bar{A}_1$ might as well be an element in $\bar{A}_2$.*

$$|\bar{A}_1 \cup \bar{A}_2 \cup \bar{A}_3 \cup \bar{A}_4| = \big(|\bar{A}_1| + |\bar{A}_2| + |\bar{A}_3| + |\bar{A}_4|\big) -$$
$$\big(|\bar{A}_1 \cap \bar{A}_2| + |\bar{A}_1 \cap \bar{A}_3| + |\bar{A}_1 \cap \bar{A}_4| + |\bar{A}_2 \cap \bar{A}_3| + |\bar{A}_2 \cap \bar{A}_4| + |\bar{A}_3 \cap \bar{A}_4|\big) +$$
$$\big(|\bar{A}_1 \cap \bar{A}_2 \cap \bar{A}_3| + |\bar{A}_1 \cap \bar{A}_2 \cap \bar{A}_4| + |\bar{A}_2 \cap \bar{A}_3 \cap \bar{A}_4| + |\bar{A}_1 \cap \bar{A}_3 \cap \bar{A}_4|\big) +$$
$$\big(|\bar{A}_1 \cap \bar{A}_2 \cap \bar{A}_3 \cap \bar{A}_4|\big)$$

How many placements exist such that the first bin is empty? These are just the number of placements of the 5 balls into the remaining 3 bins; i.e. $|\bar{A}_1| = 3^5$. Similarly, $|\bar{A}_i| = 3^5$, $1 \le i \le 4$. How many placements exist such that both the first and the second bin is empty? These are just the number of placements of the 5 balls into the remaining 2 bins. Therefore, $|\bar{A}_1 \cap \bar{A}_2| = 2^5$. Obviously, $|\bar{A}_i \cap \bar{A}_j| = 2^5$ for every $1 \le i < j \le 4$. Similarly, we have that $|\bar{A}_i \cap \bar{A}_j \cap \bar{A}_k| = 1^5$, for every $1 \le i < j < k \le 4$. Also $|\bar{A}_1 \cap \bar{A}_2 \cap \bar{A}_3 \cap \bar{A}_4| = 0$ (since the 5 balls must be placed somewhere).

Here is an observation regarding the *equation* in the Inclusion-Exclusion principle. How many terms $|\bar{A}_i|$ exist? There are $\binom{4}{1} = 4$. How many terms $|\bar{A}_i \cap \bar{A}_j|$ (where $i \neq j$) exist? There are exactly $\binom{4}{2} = 6$. How many terms $|\bar{A}_i \cap \bar{A}_j \cap \bar{A}_k|$? There are $\binom{4}{3} = 4$. And there is $\binom{4}{4} = 1$ term $|\bar{A}_1 \cap \bar{A}_2 \cap \bar{A}_3 \cap \bar{A}_4|$.

Therefore, $|\bar{A}_1 \cup \bar{A}_2 \cup \bar{A}_3 \cup \bar{A}_4| = \binom{4}{1}3^5 - \binom{4}{2}2^5 + \binom{4}{3}1^5 - \binom{4}{4}0 = 780$. Hence, the number of placements we were asked to compute is

$$|A| - |\bar{A}_1 \cup \bar{A}_2 \cup \bar{A}_3 \cup \bar{A}_4| = 4^5 - 780 = 240$$

Exercise 11. *Generalize the above result when the number of balls is r and the number of bins n.*

Exercise 12. *Suppose that we have 20 bins and 30 balls. Instead of counting the exact number of placements (with the constraint that each bin contains at least one ball) compute an upper and lower bound, using Boole-Bonferroni inequalities. Compute these bounds with two different accuracies. The lower bound for 2 and 4 terms and the upper bound for 1 and 3 terms.*

Exercise 13. *Count the number of arrangements of the digits $0, 1, \ldots, 9$ exist, under the constraint that the first digit is greater than 1 and the last digit is less than 8?*

Euler's ϕ function

We are going to determine a formula for a function known as *Euler's ϕ function*. This function plays an important role in many places – if you took a course in Algorithms you should have seen it in the analysis of the Miller-Rabin primality testing algorithm. First we need some definitions.

Definition 14.

- *Let $p, n \in \mathbb{Z}$, $p \neq 0$. We say that p divides n, $p|n$, or that p is a divisor of n iff there exists a natural number $k \neq 0$ such that $n = kp$.*

- *We say that $p \in \mathbb{Z}$, $p > 1$ is a* prime *number if its only divisors are 1 and p. Else, p is* composite.

- *Let a, b be two integers not both zero. We denote by $gcd(a, b)$ the greatest integer among the common divisors of a and b.*

- *We say that two integers a and b are relatively prime (or coprime) iff their greatest common divisor is the unit, $gcd(a, b) = 1$.*

The fundamental theorem of number theory is the *Unique Factorization* into powers of primes.

Theorem 15 (Unique Factorization). *A composite number $n \in \mathbb{Z}^+$ can be* uniquely *written as a product of powers of prime numbers $p_1, p_2 \ldots, p_i$, $n = p_1^{e_1} p_2^{e_2} \ldots p_i^{e_i}$, where $e_i \in \mathbb{Z}^+$.*

Definition 16. *For a given positive integer n, the Euler's ϕ function denotes the number of positive integers $m < n$ such that n and m are relatively prime.*

For example, $\phi(3) = 2$, $\phi(6) = 2$ and $\phi(7) = 7 - 1 = 6$. Clearly, when p is prime we have $\phi(p) = p - 1$. Our goal is to show for $n \in \mathbb{Z}^+$:

$$\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

where the product runs over all prime divisors of n.

As in the previous balls-to-bins example, we want to determine the "bad cases". Why? We want to express $\phi(n)$ in terms of prime divisors of n. It seems quite intuitive that the "bad cases" are the ones in which (i) we have this correlation and (ii) more importantly we do know how to compute the number of elements in each "bad case".

By the *Unique Factorization* theorem let $n = p_1^{e_1} p_2^{e_2} \ldots p_i^{e_i}$. It is clear that if $m < n$ is *not* relatively prime to n then there exist not all zero $e_1', e_2' \ldots e_i'$ where $0 \le e_k' \le e_k$, $k = 1, \ldots, i$ such that $m = p_1^{e_1'} p_2^{e_2'} \ldots p_i^{e_i'}$.

Say that $\bar{A}_l$ is the set of all integers a which are less than or equal to n such that $p_l | a$. Therefore, the set $\bigcup_{l=1}^{i} \bar{A}_l$ contains all integers that are less than or equal to n and they are not relatively prime to n. If $A = \{1, 2, \ldots, n\}$, then we have that $\phi(n) = |A| - |\bigcup_{l=1}^{i} \bar{A}_l| = n - |\bigcup_{l=1}^{i} \bar{A}_l|$. Thus, the problem reduces to the computation of $|\bigcup_{l=1}^{i} \bar{A}_l|$.

By the definition of $\bar{A}_k$, we have that $|\bar{A}_k| = \frac{n}{p_k}$. For the same reason $|\bar{A}_k \cap \bar{A}_j| = \frac{n}{p_k p_j}$, for every $1 \le k < j \le n$. Similarly, $|\bar{A}_{k_1} \cap \bar{A}_{k_1} \cap \ldots \cap \bar{A}_{k_v}| = \frac{n}{p_{k_1} p_{k_2} \cdots p_{k_v}}$, for every $1 \le k_1 < k_2 < \ldots < k_v \le n$. In the inclusion-exclusion formula we have i terms $|\bar{A}_k|$, $\binom{i}{2}$ terms $|\bar{A}_k \cap \bar{A}_j|$, ..., 1 term $|\bar{A}_1 \cap \bar{A}_1 \cap \ldots \cap \bar{A}_i|$. Now it is rather easy to show (by induction on i) that if we factorize $n - \left(\sum_{k=1}^{i} |\bar{A}_k| - \sum_{1 \le k_1 < k_2 \le i} |\bar{A}_{k_1} \cap \bar{A}_{k_2}| + \sum_{1 \le k_1 < k_2 < k_3 \le i} |\bar{A}_{k_1} \cap \bar{A}_{k_2} \cap \bar{A}_{k_3}| - \ldots + (-1)^i |\bigcap_{k=1}^{i} \bar{A}_k| \right)$ we get $n \prod_{i=1}^{i} \left(1 - \frac{1}{p_i}\right)$.

Therefore, $\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$.

Exercise 17. *How many are the positive divisors of* 2100?