Lecture 3: Elementary Counting

Product of Sets and The Multiplication Principle. For any set \( S \), we let \(|S|\) denote the cardinality or size of \( S \). When \( S \) is finite, \(|S|\) is the number of elements that are contained in \( S \), and we call \( S \) an \(|S|\)-element set or an \(|S|\)-set. If we know the sizes of two finite sets \( A \) and \( B \), then we can easily find the size of their Cartesian product

\[ A \times B := \{ (a, b) \mid a \in A \text{ and } b \in B \}. \]

Indeed, suppose that \( A \) is an \( m \)-set and \( B \) is an \( n \)-set for some \( m, n \in \mathbb{N}_0 \), and write

\[ A = \{ a_1, \ldots, a_m \} \text{ and } B = \{ b_1, \ldots, b_n \}. \]

After placing the elements of \( A \times B \) in an \( m \times n \) table letting \((a_i, b_j)\) be the pair occupying the \( i \)-th row and \( j \)-th column, we see that \(|A \times B| = m \times n = |A| \cdot |B|\). We can now use induction to argue that if \( A_1, \ldots, A_k \) are finite sets, then

\[ |A_1 \times \cdots \times A_k| = |A_1| \cdots |A_k|, \tag{0.1} \]

where \( A_1 \times \cdots \times A_k \) consists of all (ordered) \( k \)-tuples \((a_1, \ldots, a_k)\) with \( a_i \in A_i \) (for every \( i \in [k] \)). We call \( A_1 \times \cdots \times A_k \) the (Cartesian) product of the sets \( A_1, \ldots, A_k \).

We can rephrase the identity (0.1) in the following less formal way.

Multiplication Principle. In a given sequence of \( k \) activities, suppose we can do (independently) the first one in \( n_1 \) ways, the second one in \( n_2 \) ways, and so on. Then we can do the full sequence of activities in a total of \( n_1 \cdots n_k \) different ways.

Example 1. Suppose that we have an alphabet consisting of \( n \) symbols. For each \( k \in \mathbb{N}_0 \), how many \( k \)-characters passwords can we create over this alphabet? Well, for every \( i \in [k] \), we can think of choosing the \( i \)-th symbol as our \( i \)-th activity. Since there is a total of \( k \) activities, and we can do each of them in \( n \) different ways, it follows from the multiplication principle that we can form a total of \( n^k \) passwords over the given alphabet. Now we can add the restriction that passwords cannot contain repeated symbols. In this case, we can choose the first symbol in \( n \) different ways, the second one in \( n - 1 \) different ways, and so on. Therefore we can form \( n(n - 1) \cdots (n - k + 1) \) \( k \)-character passwords that do not repeat any symbol.

Notation: It is common to denote \( n(n - 1) \cdots (n - k + 1) \) by \((n)_k\).
Permutations and Bijections. A permutation of a finite number of objects is a specific sequential arrangement of such objects.

Example 2. Suppose that we want to organize the 35 students taking 18.211 in a line. This can be done as in the second part of Example 1. For every \(i \in [35]\), and starting from the first position, we can fill the \(i\)-th position with one of the \(35 - i + 1\) students who are not in line yet. Thus, we can organize all the students in a line in a total of \(35! = 1 \cdot 2 \cdot 3 \cdots 35\) different ways.

Following the method in the previous example, we see that given \(n\) objects (often labeled by \(1, 2, \ldots, n\)), there is a total of \(n!\) permutations of such objects. The notion of a permutation is crucial in combinatorics, and so we highlight the previous statement as a proposition.

Proposition 3. For any \(n \in \mathbb{N}\), the number of permutations of \(n\) given objects is \(n!\).

By convenience, we will always assume that \(0! = 1\). Each permutation of an \(n\)-set \(S\) can be interpreted as a bijective function \(\pi : [n] \to [n]\) as follows.

Example 4. Let \(S\) be a set consisting of \(n\) elements, namely, \(S = \{s_1, \ldots, s_n\}\). Let \(\pi\) be a permutation of the elements of \(S\), that is, a linear arrangement of them. Then we can think of \(\pi\) as a function \(\pi : [n] \to [n]\), where \(\pi(i)\) denotes the position of \(s_i\) in the given linear arrangement. As distinct elements in the arrangement occupy distinct positions, the function \(\pi\) is injective, and because every position is occupied by an element, \(\pi\) is surjective. Thus, \(\pi : [n] \to [n]\) is bijective. Conversely, any bijective function \(\pi : [n] \to [n]\) naturally determines a permutation of the elements of \(S\), where the element \(s_i\) occupies the position \(\pi(i)\) of the linear arrangement.

Hence we can think of permutations of \(n\) given objects as bijections on the set \([n]\), and we will do so often.

Theorem 5. \(^{1}\) If \(f : A \to B\) is a bijective function between finite sets, then \(|A| = |B|\).

Proof. Since \(f\) is injective, \(|A| = |f(A)| \leq |B|\). Now set \(n := |B|\), and then write \(B = \{b_1, \ldots, b_n\}\). Since \(f\) is surjective, for each \(i \in [n]\) we can choose \(a_i \in A\) with \(f(a_i) = b_i\). Therefore \(|A| \geq |\{a_1, \ldots, a_n\}| = |B|\). As \(|A| \leq |B|\) and \(|B| \leq |A|\), we conclude that \(|A| = |B|\). \(\square\)

For a set \(S\), the set \(2^S\) consisting of all subsets of \(S\) is called the power set of \(S\). As an application of Theorem 5, let us show that the size of \(2^S\) is \(2^{[S]}\) when \(S\) is finite.

Proposition 6. Let \(S\) be a finite set. Then \(|2^S| = 2^{[S]}|\).

\(^{1}\)This theorem does not require that the sets \(A\) and \(B\) are finite, but this will suffice for the moment.
Proof. Set \( n := |S| \). If \( n = 0 \), then the only subset of \( S \) is the empty set, and so \(|2^S| = 1 = 2^{|S|} \). Assume now that \( n \geq 1 \), and label the elements of \( S \) by \( 1, 2, \ldots, n \). Let \( B \) be the set consisting of all length-\( n \) binary strings (i.e., sequences of \( n \) elements whose terms are either 0’s or 1’s). For each \( X \) in \( 2^S \), let \( b(X) \) denote the length-\( n \) binary string having a 1 in the \( i \)-th position if and only if \( i \in X \). One can easily see that \( b: 2^S \to B \) is a bijection. On the other hand, it follows from the multiplication principle that \(|B| = 2^n \). Hence Theorem 5 allows us to conclude that \(|2^S| = |B| = 2^{|S|} \). \( \square \)

**Binomial Coefficients.** Now we are interested in counting the number of subsets of a fixed size of a given set. For a set \( S \) and \( k \in \mathbb{N}_0 \), we let \( \binom{n}{k} \) denote the set consisting of all the subsets \( X \) of \( S \) with \(|X| = k \). The number \( \binom{n}{k} := \left| \binom{n}{k} \right| \) plays a fundamental role in combinatorics and is called a **binomial coefficient**. Observe that when \( k \notin [0, n] \), the set \([n]\) does not have any \( k\)-subset and so \( \binom{n}{k} = 0 \).

**Proposition 7.** \( \binom{n}{k} = \frac{n!}{k!(n-k)!} \) for all \( n, k \in \mathbb{N}_0 \).

Proof. Let \( N(n, k) \) be the total number of ways to take \( k \) elements of the set \([n]\) and linearly order them. We can choose \( k \) elements of \([n]\) in \( \binom{n}{k} \) times, and we order the chosen elements in \( k! \) ways. Therefore \( N(n, k) = \binom{n}{k} k! \). On the other hand, we can choose the first element from \([n]\) in \( n \) different ways and make it the first element in our arrangement, then we can choose the second element of our arrangement in \( n-1 \) ways, and so on until we get to the \( k \)-th (and last) position of our arrangement, which can be chosen in \( n-k+1 \) different ways. So by the multiplication principle, we can create the desired arrangement in \( N(n, k) = n(n-1) \cdots (n-k+1) = \frac{n!}{(n-k)!} \) different ways. Hence \( \binom{n}{k} = \frac{N(n, k)}{k!} = \frac{n!}{k!(n-k)!} \). \( \square \)

The following proposition is often useful.

**Proposition 8.** \( \binom{n}{k} = \binom{n}{n-k} \) for all \( n, k \in \mathbb{N}_0 \).

Proof. Define \( f: \binom{n}{n-k} \to \binom{n}{k} \) by letting \( f(S) \) be the complement of \( S \) in \([n]\), that is, \( f(S) = [n] \setminus S \). As \( f \) is clearly a bijection, the equality \( \binom{n}{k} = \binom{n}{n-k} \) must hold. \( \square \)

**Multisets.** In this last section we discuss the notion of a multiset, which is, roughly speaking, a set with repetitions allowed. More formally, for a set \( S \), a **multiset** on \( S \) is a pair \((S, f)\), where \( f: S \to \mathbb{N}_0 \). The number \( f(s) \), called the **multiplicity** of \( s \), specifies how many times \( s \) is repeated in the given multiset. When \( S \) is finite, the **cardinality** or **size** of \((S, f)\) is defined to be \( k := \sum_{s \in S} f(s) \) and, in this case, \((S, f)\) is said to be a **k-multiset** on \( S \). If \( S = \{ s_1, \ldots, s_n \} \), we often write \( \{ s_1^{f(s_1)}, \ldots, s_n^{f(s_n)} \} \) instead of \((S, f)\). For instance, \( \{1, 2, 2, 4, 4, 4\} = \{1, 2^2, 3^0, 4^2\} \) is a 5-multiset on the set \([4]\). We let \( \binom{n}{k} \) denote the set of all \( k \)-multisets on \( S \), and we let \( \binom{[n]}{k} \) denote the size of \( \binom{n}{k} \).
Theorem 9. \( \binom{n}{k} = \binom{n+k-1}{k} \) for all \( n, k \in \mathbb{N}_0 \).

Proof. For a k-multiset \( A = \{a_1, \ldots, a_k\} \) on \([n]\), where we assume that \( a_1 \leq \cdots \leq a_k \), set \( f(A) = \{a_1, a_2 + 1, \ldots, a_k + k - 1\} \). and note that \( f(A) \) is a k-subset of \([n+k-1]\). So we can define \( f: \left( \binom{n}{k} \right) \to \left( \binom{n+k-1}{k} \right) \) by the assignment \( f(A) \mapsto f(A) \). It is clear that the function \( f \) is injective. On the other hand, for a subset \( B := \{b_1, \ldots, b_k\} \) of \([n+k-1]\) with \( b_1 < \cdots < b_k \), we see that \( f(A) = B \), where \( A \) is the k-multiset \( \{b_1, b_2 - 1, \ldots, b_k - k + 1\} \) on \([n]\). Thus, \( f \) is also surjective and so a bijection. Hence \( \binom{n}{k} = |\left( \binom{n}{k} \right)| = |\left( \binom{n+k-1}{k} \right)| = \binom{n+k-1}{k} \). \( \square \)

Example 10. Suppose we want to place \( k \) identical balls into \( n \) different (distinguishable) boxes. After labeling the boxes by \( b_1, b_2, \ldots, b_n \), each placement can be identified with a k-multiset on \([n]\) as follows: the number of balls in box \( b_i \) specify the multiplicity of \( i \) in the k-multiset. By Theorem 9, the total number of configurations is \( \binom{n}{k} \).

Example 11. How many solutions has the equation \( x_1 + \cdots + x_{18} = 211 \) in \( \mathbb{N}_{18} \)? Well, observe that each solution \((s_1, \ldots, s_{18})\) can be identified with a 211-multiset \( M \) on \([18]\); the coordinate \( s_i \) specifies the multiplicity of \( i \) in \( M \). Hence it follows from Theorem 9 that the number of solutions of the given equation is \( \binom{228}{17} \).

Practice Exercises

Exercise 1. For a function \( f: A \to B \), prove the following statements.

1. If there is a function \( g: B \to A \) with \( f \circ g = g \circ f \), then \( f \) (and so \( g \)) is a bijection, in which case \( g \) is called the inverse of \( f \).
2. If \( |A| = |B| \), then \( f \) is injective if and only if \( f \) is surjective, in which case, it is a bijection.

Exercise 2. How many 9-tuples in \( \mathbb{N}^9 \) satisfy the inequality \( x_1 + \cdots + x_9 < 30 \)?

Exercise 3. [1, Exercise 3.7] How many five-digit positive integers contain the digit 9 and are divisible by 3?

References