Mathematics for Computer Scientists

Lecture notes for the module G51MCS

Venanzio Capretta
University of Nottingham
School of Computer Science

Chapter 5

Combinatorics

5.1 Quantifiers

When we want to say that each element of a set satisfies some property, we use phrases like *'for all ...'* or *'for every ...'*. Similarly, to say that at least one object satisfies the property, we use phrases like *'there exists ...'* or *'for some ...'*. That's what we have done so far. Now we want to use mathematical symbols to express the same statements. They will make the sentences more precise and it will be easier to do correct proofs. We call these new symbols *quantifiers*: they are operators that use a variable name to denote an arbitrary element of a set. Here are the two main quantifiers used in symbolic logic:

symbol	**name**	**meaning**
$\forall$	Universal quantifier	*for all* *for every* *for each*
$\exists$	Existential quantifier	*there is* *for some* *there exists*

Suppose S is a certain set and P is a property that elements of S may or may not satisfy. Then to express that all elements of S satisfy it, or that at least one element of S satisfies it, we would use the following two formulas, respectively:

$\forall x \in S.P(x)$ Every element of S satisfies P;
$\exists x \in S.P(x)$ There exists an element of S that satisfies P.

For example, to state the existence of quotient and remainder for natural numbers, we can express it in English:

> For every two natural numbers n and m such that $m > 0$, there are a quotient q and a remainder r such that $n = q \cdot m + r$ and $0 \leq r < m$.

Alternatively we can write the same statement more compactly in mathematical notation:

$$\forall n \in \mathbb{N}.\forall m \in \mathbb{N}.m > 0 \Rightarrow \exists q \in \mathbb{N}.\exists r \in \mathbb{N}.(n = q \cdot m + r) \wedge (0 \leq r < m).$$

Often, when the universal set has been specified in advance and there is no need to explicitly state what kind of objects the variables denote, we can omit the set over which we quantify. For example, if it is clear from the context that we are talking about natural numbers, we can simplify the previous proposition to:

$$\forall n.\forall m.m > 0 \Rightarrow \exists q.\exists r.(n = q \cdot m + r) \wedge (0 \leq r < m).$$

Another example of the use of the existential quantifier is the definition of the *less than or equal* relation on natural numbers. Remember that we defined $n \leq m$ to mean that $m = n + h$ for some natural number h. We can now formulate this definition as an equivalence expressed in purely symbolic language:

$$n \leq m \quad \Leftrightarrow \quad \exists h.n + h = m.$$

There are formal rules to use the quantifiers, of the same kind as those that we learnt for the connectives. However, they are not the topic of this course. So we leave them for more advanced courses and we continue to use our intuitive understanding to reason about the universal and existential quantifiers.

5.2 Finite sets

When talking about sets we intuitively defined their *cardinality* as the number of elements they contained. We can now give a precise definition, using the notion of bijection. This will help in reasoning rigorously about the size of collections. We choose, for every natural number n, a canonical set with n elements, which we indicate by $\mathbb{N}_n$ or $\mathbb{Z}_n$: it consists of the first n natural numbers.

$$\begin{aligned}\mathbb{Z}_n &= \{0, 1, 2, \cdots, n-1\} \\ &= \{i \in \mathbb{N} \mid i < n\}\end{aligned}$$

(Note: the number n itself doesn't belong to $\mathbb{Z}_n$).

The set $\mathbb{Z}_0$ has zero elements, so it is the empty set. Here are the first few of the canonical finite sets:

$$\begin{aligned}\mathbb{Z}_0 &= \{\} = \varnothing \\ \mathbb{Z}_1 &= \{0\} \\ \mathbb{Z}_2 &= \{0, 1\} \\ \mathbb{Z}_3 &= \{0, 1, 2\} \\ \mathbb{Z}_4 &= \{0, 1, 2, 3\}\end{aligned}$$

Now we can give a formal definition of finite cardinality: a set has cardinality n if it can be put in bijective correspondence with $\mathbb{Z}_n$.

Definition 11 *Let S be a set and n a natural number. We say that S has* cardinality n*, and we write $|S| = n$, if there is a bijection from S to $\mathbb{Z}_n$. In formulas:*

$$|S| = n \quad \Leftrightarrow \quad \exists f : S \to \mathbb{Z}_n . f \text{ is bijective.}$$

For example, in the previous lecture we proved that the set $\{\mathsf{apple}, \mathsf{banana}, \mathsf{cherry}, \mathsf{peach}\}$ has four elements by giving the following bijection:

$$\begin{aligned} &\mathsf{fn} : \{\mathsf{apple}, \mathsf{banana}, \mathsf{cherry}, \mathsf{peach}\} \to \mathbb{Z}_4 \\ &\quad \mathsf{fn}(\mathsf{apple}) = 2 \\ &\quad \mathsf{fn}(\mathsf{banana}) = 0 \\ &\quad \mathsf{fn}(\mathsf{cherry}) = 3 \\ &\quad \mathsf{fn}(\mathsf{peach}) = 1 \end{aligned}$$

The bijections from $\mathbb{Z}_n$ to itself are particularly interesting. They are called *permutations* and they have some elegant properties. For example, we can always find the inverse of a permutation by composing it with itself a number of times. Let's consider, for example, the following bijection on the set with six elements:

$$\begin{aligned} &f : \mathbb{Z}_6 \to \mathbb{Z}_6 \\ &\quad f(0) = 3 \\ &\quad f(1) = 5 \\ &\quad f(2) = 0 \\ &\quad f(3) = 2 \\ &\quad f(4) = 4 \\ &\quad f(5) = 1 \end{aligned}$$

Let's now compose it with itself a number of times and see what happens. We use the exponential notation f^m to indicate the composition of f with itself m times: $f^2 = f \circ f$, $f^3 = f \circ f \circ f = f \circ f^2$, $f^4 = f \circ f^3$ and so on. We also, for completeness, put $f^0 = \mathsf{id}$ and $f^1 = f$.

$f^2 : \mathbb{Z}_6 \to \mathbb{Z}_6$;	$f^3 : \mathbb{Z}_6 \to \mathbb{Z}_6$;	$f^4 : \mathbb{Z}_6 \to \mathbb{Z}_6$;	$f^5 : \mathbb{Z}_6 \to \mathbb{Z}_6$;	$f^6 : \mathbb{Z}_6 \to \mathbb{Z}_6$
$f^2(0) = 2$	$f^3(0) = 0$	$f^4(0) = 3$	$f^5(0) = 2$	$f^6(0) = 0$
$f^2(1) = 1$	$f^3(1) = 5$	$f^4(1) = 1$	$f^5(1) = 5$	$f^6(1) = 1$
$f^2(2) = 3$	$f^3(2) = 2$	$f^4(2) = 0$	$f^5(2) = 3$	$f^6(2) = 2$
$f^2(3) = 0$	$f^3(3) = 3$	$f^4(3) = 2$	$f^5(3) = 0$	$f^6(3) = 3$
$f^2(4) = 4$	$f^3(4) = 4$	$f^4(4) = 4$	$f^5(4) = 4$	$f^6(4) = 4$
$f^2(5) = 5$	$f^3(5) = 1$	$f^4(5) = 5$	$f^5(5) = 1$	$f^6(5) = 5.$

We found out that $f^6 = \mathsf{id}$. This tells us that f^5 is the inverse of f: $f^5 = f^{-1}$. This is not a coincidence: it is always possible to write the inverse of a bijection on a finite set as a composition with itself a certain number of times.

5.3 The pigeonhole principle

The pigeonhole principle: If a mailman has to deliver 21 letters to 20 pigeonholes, then there will be at least one pigeonhole with at least two letters.

The so-called *pigeonhole principle* is an apparently trivial fact, but it is very useful in proving theorems about finite sets. It holds more generally: if n letters must be delivered to m pigeonholes and $n > m$, then there will be at least one pigeonhole with at least two letters. In mathematical terms, we can see the delivery as a function from the set of letters to the set of pigeonholes. The fact that there must be at least one pigeonhole with at least two letters amounts to the function not being injective. We formulate the principle in the contrapositive way:

Theorem 12 (The Pigeonhole Principle) *Let $f : \mathbb{Z}_n \to \mathbb{Z}_m$; if f is injective, then $n \leq m$.*

The proof is by induction on n and is not completely trivial. We omit it here.

There are other equivalent formulations and important consequences. Two of the most useful ones are the following.

Theorem 13 *Let $f : \mathbb{Z}_n \to \mathbb{Z}_m$; if f is surjective, then $n \geq m$.*

Theorem 14 *Let $f : \mathbb{Z}_n \to \mathbb{Z}_n$; then*

$$f \text{ is injective} \quad \Leftrightarrow \quad f \text{ is surjective.}$$

We formulated the principle and its consequences on the canonical finite sets $\mathbb{Z}_n$, but it is of course valid for all finite sets. So if $f : X \to Y$ is an injective function and $|X| = n$, $|Y| = m$, then we can conclude by the pigeonhole principle that $n \leq m$.

5.4 Shaking hands

Let's try to solve the *hand-shaking* puzzle that we looked at on the first lecture:

> Mr and Mrs Smith invited four other couples to their house. At the party, some people shake hands with other guests, but not necessarily with everybody. Nobody shakes hands with their own spouse.
>
> At the end of the party, Mr Smith observes: *If you don't count me, there are no two people who shook hands the same number of times.*
>
> How many times did Mrs Smith shake hands?

There are 10 people at the party. Mr. Smith's observation tells us something about 9 of them (everybody except him). Let's assign conventional numbers to these 9 guests: we give number 0 to Mrs. Smith, numbers 1 and 2 to one couple, 3 and 4 to to the next, then 5 and 6 for the third couple, and finally 7 and 8 to the last couple. Now consider the function shakes that associates to every guest the number of people that she/he shook hands with. This number is at most 8 (since nobody shakes hands with themselves or their spouse). We then have:

$$\mathsf{shakes} : \mathbb{Z}_9 \to \mathbb{Z}_9$$

Mr. Smith's observation tells us that this function is injective. One of the consequences of the pigeonhole principle, Theorem 14, lets us conclude that it must also be surjective. So it is a bijection, because it is both injective and surjective. In particular, there must be one person that shook hands 0 times and another that shook hands 8 times.

Notice that it is impossible that Mrs. Smith shook hands 8 times. If she did, she should have shaken hands with all the guests except her husband. But then there would be no one who shook hands 0 times.

So it must be somebody else who shook hands 8 times. Let's say that it was person 1 (since we didn't make any distinction among the guests, apart from Mrs. Smith, it doesn't matter who we choose here). Then person 1 must have shaken hands with everybody except his/her spouse. So the only person who might have shaken hands 0 times is person 1's spouse, since everybody else shook hands with person 1. In conclusion it is person 2 who shook hands 0 times.

Now there also must be two people who shook hands 1 time and 7 times, respectively. Reasoning as above, we can conclude that it is impossible that Mrs. Smith shook hands 7 times (it would make it impossible for anybody to have shaken hands exactly 1 time). So it must be somebody else: let's say it was person 3. Then it is sure that it was person 3's spouse who shook hands 1 time (everybody else shook hands at least twice).

We can continue in the same line: the persons who shook hands 2 and 6 times must form a couple, those who shook hands 3 and 5 times must form another couple.

By exclusion we have to conclude that Mrs. Smith shook hands exactly 4 times.

Did you notice that this line of reasoning resembles induction? We repeated the same logical steps several times with a decreasing number: first for 8, then for 7, then for 6 and so on.

In fact, it is possible to generalise this puzzle and give the solution inductively. Suppose that the Smiths invited n couples to the party, where n can be any natural numbers. If Mr. Smith observes that everybody except him shook hands a different number of times, then Mrs. Smith must have shaken hands exactly n times. You can prove this by induction on n using a slight variation of the proof that we used for four couples.

5.5 Counting Functions and Subsets

How many different functions are there from $\mathbb{Z}_n$ to $\mathbb{Z}_m$? How would you go about counting them?

Let's see: think about what information you need to determine one function, then count all the possible different ways of choosing that information. A function $f : \mathbb{Z}_n \to \mathbb{Z}_m$ is picked by assigning values to every element of $\mathbb{Z}_n$; for every element we have m possible choices for its value; we have n elements to

which we assign values. So we need to multiply the number of possible choices for each element: m^n is the number of all possible functions.

Now let's restrict our attention to functions from $\mathbb{Z}_n$ to itself. We already know that there are n^n such functions. But how many of them are permutations? (Remember that, by the pigeonhole principle, talking about bijections is the same as talking about injections.) Proceeding as before, we just have to multiply all the possible choices for each element. We have n choices for the first element; but only $n-1$ choices for the second element, because we cannot choose the same value as for the first; then we have $n-2$ choices for the third element (we cannot choose the values of the first two; and so on. In conclusion: the number of all possible permutations is $n \cdot (n-1) \cdot (n-2) \cdots 1 = n!$.

Generalising a bit: how many injective functions are there from $\mathbb{Z}_n$ to $\mathbb{Z}_m$ (assuming that $n \leq m$, otherwise there are no injections at all)? Reasoning as above we conclude that the number of injection is

$$m \cdot (m-1) \cdots (m-n+1) = \frac{m!}{(m-n)!}.$$

Now let's count the subsets of a finite set that have a fixed cardinality. We already know that the number of all subsets of $\mathbb{Z}_n$ is 2^n.

Now we want to count the subsets of $\mathbb{Z}_n$ that contain a fixed number of elements. For example, how many subsets of $\mathbb{Z}_n$ have exactly two elements? How many have cardinality exactly 3? And so on. We have a special notation for this number:

$$\binom{n}{k} : \text{number of subsets of } \mathbb{Z}_n \text{ of cardinality } k.$$

Read this as *"n choose k."* These numbers are usually called *binomial coefficients.*

Let's start with an example. How many subsets with two elements does $\mathbb{Z}_3$ have? Let's proceed as before: we multiply all the possible choices for the first element with all the possible choices for the second element. We have 3 choices for the first and 2 for the second, so we get $3 \cdot 2 = 6$; but this is not yet the correct result. In fact, let's write down all the possible choices:

$$\begin{array}{lll} \{0,1\} & \{1,0\} & \{2,0\} \\ \{0,2\} & \{1,2\} & \{2,1\} \end{array}$$

Notice that, for example, $\{0,1\}$ is the same set as $\{1,0\}$, because sets are determined by what elements they contain, not by the order in which they are listed. Since every subset is repeated twice, their number is actually 3, not 6:

$$\binom{3}{2} = 3.$$

So, in general, the number of subsets of $\mathbb{Z}_n$ is obtained thus: we have n choices for the first element, $n-1$ choices for the second, but we get every pair

twice, so we have to divide by two.

$$\binom{n}{2} = \frac{n \cdot (n-1)}{2}$$

Let's now consider how many subsets with three elements $\mathbb{Z}_n$ has. Of course we have n choices for the first element, $n-1$ for the second, and $n-2$ for the third. But how many times do we get the same elements in different order? For example, if we are counting the subsets of cardinality three in $\mathbb{Z}_5$, how many times do we get $\{0,1,2\}$? Let's write them down:

$$\begin{array}{lll} \{0,1,2\} & \{0,2,1\} & \{1,0,2\} \\ \{1,2,0\} & \{2,0,1\} & \{2,1,0\} \end{array}$$

There are six different ways to get the same set. So we can conclude that:

$$\binom{n}{3} = \frac{n \cdot (n-1) \cdot (n-2)}{6}.$$

In general, if we want to count the number of subsets of $\mathbb{Z}_n$ with cardinality k we will count them like this: we have n choices for the first element, $n-1$ for the second, $n-2$ for the third, and so on until $n-k+1$ choices for the kth element. We multiply all these choices, but then we have to divide by all the different ways to obtain the same k elements in a different order; this is just the total number of permutations of k elements, that we already know to be $k!$. In conclusion:

$$\binom{n}{k} = \frac{n \cdot (n-1) \cdots (n-k+1)}{k!} = \frac{n!}{(n-k)! \cdot k!}.$$

5.6 Pascal's Triangle

An alternative way of determining the value of binomial coefficients uses a recursive definition.

Theorem 15 *Let n and k be two natural numbers, with $n > 0$ ad $0 < k < n$. Then*

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

Proof. We can prove the statement in two different ways. The first uses the definition of the binomial coefficients as the number of subsets of cardinality k of a set of cardinality n. The second uses the formula that gives the result of the binomial coefficient using the factorial. Let's look at both proofs, since they show two different ways of reasoning.

Proof 1. We have defined the binomial coefficient $\binom{n}{k}$ as the number of of subsets of $\mathbb{Z}_n$ with cardinality k. We can divide all those subsets in two groups: those that don't contain the element $n-1$ and those that do.

The subsets of the first group don't contain $n-1$, so they are actually subsets of $\mathbb{Z}_{n-1}$. Since each of them contains k elements, their total number is $\binom{n-1}{k}$.

The subsets of the second group will contain the element $n-1$ plus other $k-1$ elements. In other words, they are obtained by taking a subset of $\mathbb{Z}_{n-1}$ with $k-1$ elements and putting $n-1$ in it. The total number of different ways of doing this is equal to the number of subsets of $\mathbb{Z}_{n-1}$ with $k-1$ elements: $\binom{n-1}{k-1}$.

Adding together the number of elements of the two groups, we get the formula in the theorem.

Proof 2. Let's use the formula for the binomial coefficients in terms of the factorial functions. After a few arithmetical transformations we get what we want:

$$\begin{aligned}
\binom{n}{k} &= \frac{n!}{(n-k)!\cdot k!} && \text{formula for binomial coefficients} \\
&= \frac{n\cdot(n-1)!}{(n-k)!\cdot k!} && \text{definition of factorial} \\
&= \frac{(n-k+k)\cdot(n-1)!}{(n-k)!\cdot k!} = \frac{(n-k)\cdot(n-1)!}{(n-k)!\cdot k!} + \frac{k\cdot(n-1)!}{(n-k)!\cdot k!} && \text{arithmetic} \\
&= \frac{(n-1)!}{(n-k-1)!\cdot k!} + \frac{(n-1)!}{(n-k)!\cdot(k-1)!} && \text{definition of factorial} \\
&= \frac{(n-1)!}{(n-1-k)!\cdot k!} + \frac{(n-1)!}{(n-1-(k-1))!\cdot(k-1)!} && \text{arithmetic} \\
&= \binom{n-1}{k} + \binom{n-1}{k-1} && \text{formula for binomial coefficients.}
\end{aligned}$$

□

We can use this theorem to give a recursive way to compute the binomial coefficients. We know that there is only one subset of $\mathbb{Z}_n$ with 0 elements, the empty subset. We also know that there is only one subset with n elements, the whole of $\mathbb{Z}_n$. Using these two pieces of knowledge as the base cases we have, for every $n > 0$:

$$\begin{aligned}
\binom{n}{0} &= 1 \\
\binom{n}{n} &= 1 \\
\binom{n}{k} &= \binom{n-1}{k} + \binom{n-1}{k-1} \qquad \text{if } 0 < k < n.
\end{aligned}$$

You can see that at every recursive step we decrease the size of the top number by one. So eventually the recursion must stop and give a result. Notice that this recursion is a bit different from other recursive functions that we studied. There is no explicit case for $n = 0$: in fact the only possible binomial coefficient

with top number 0 is $\binom{0}{0}$, it has value 1 by either of the two base cases. We always reach one of the two base cases, usually with n different from zero.

Let's now arrange the binomial coefficients in lines. In every line we fix the value of n and write down the results of the binomial coefficients for the n possible values of k. So the first line will have just $\binom{0}{0} = 1$. The second line will have $\binom{1}{0} = 1$ and $\binom{1}{1} = 1$. The third line will have $\binom{2}{0} = 1$, $\binom{2}{1} = 2$ and $\binom{2}{2} = 1$. And so on. We get a table of all values, called *Pascal's triangle:*

$$
\begin{array}{ccccccccc}
 & & & & 1 & & & & \\
 & & & 1 & & 1 & & & \\
 & & 1 & & 2 & & 1 & & \\
 & 1 & & 3 & & 3 & & 1 & \\
1 & & 4 & & 6 & & 4 & & 1 \\
 & \cdots & & & & & & &
\end{array}
$$

The two sides of the triangle always contain the number 1; those are the base cases of the recursion. The other values are obtained by adding the numbers that are directly above them, slightly to the left and right; that's what the recursion step says.

5.7 Powers of a Binomial

Do you want to know why these numbers are called *binomial coefficients*?

In mathematics, a *binomial* is any expression which is the sum of two different terms, for example $x+y$. Let's compute the powers of this binomial: $(x+y)^0 = 1$, $(x+y)^1 = x+y$, $(x+y)^2 = x^2+2xy+y^2$, $(x+y)^3 = x^3+3x^2y+3xy^2+y^3$ and so on. Now look at the coefficients of every term in these powers. For example, in the formula for $(x+y)^3$ the term x^3 has coefficient 1, the term x^2y has coefficient 3, the term xy^2 has coefficient 3 and the term y^3 has coefficient 1. Those are exactly the values of $\binom{3}{0}$, $\binom{3}{1}$, $\binom{3}{2}$ and $\binom{3}{3}$. This is true in general.

Theorem 16 *For every natural number n we have that:*

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} \cdot x^{n-k} \cdot y^k.$$

We are not giving the proof of this fact. If you want to work it out for yourself, I'll give you a hint: do induction on n and use the recursive computation of binomial coefficients and the properties of summations.