Chapter 7

Relations and Functions

7.1 Ordered pairs

The definition of a set explicitly disregards the order of the set elements, all that matters is who's in, not who's in first. However, sometimes the order is important. This leads to the notion of an *ordered pair* of two elements x and y, denoted (x, y). The crucial property is:

$$(x, y) = (u, v) \text{ if and only if } x = u \text{ and } y = v.$$

This notion can be extended naturally to define an *ordered n-tuple* as the ordered counterpart of a set with n elements.

Give two sets A and B, their *cartesian product* $A \times B$ is the set of all ordered pairs (x, y), such that $x \in A$ and $y \in B$:

$$A \times B = \{(x, y) : x \in A, y \in B\}.$$

Here is a useful special case:

$$A^2 = A \times A = \{(x, y) : x, y \in A\}.$$

And here is a general definition: $A^1 = A$, and for $n \geq 2$,

$$A^n = \big\{(x_1, x_2, \ldots, x_n) : x_1, x_2, \ldots, x_n \in A\big\}.$$

For example, $\mathbb{R}^2$ is the familiar cartesian plane, and $\mathbb{R}^n$ is often referred to as the n-dimensional Euclidean space. If we omit the parentheses and the commas, $\{a, b\}^4$ is comprised of child babble and a 70s pop band:

$$\{aaaa, baba, abab, baaa, baab, aaab, aaba, abaa, abba, bbaa, bbba, bbbb, aabb, abbb, babb, bbab\}.$$

Proposition 7.1.1. $(A \cup B) \times C = (A \times C) \cup (B \times C)$

Proof. Recall that for two sets X and Y, $X = Y$ if and only if $X \subseteq Y$ and $Y \subseteq X$.

Consider any element $(u, v) \in (A \cup B) \times C$. By definition, $u \in A \cup B$ and $v \in C$. Thus, $u \in A$ or $u \in B$. If $u \in A$ then $(u, v) \in A \times C$ and if $u \in B$ then $(u, v) \in B \times C$.

Thus (u, v) is in $A \times C$ or in $B \times C$, and $(u, v) \in (A \times C) \cup (B \times C)$. This proves that $(A \cup B) \times C \subseteq (A \times C) \cup (B \times C)$.

Now consider any element $(u, v) \in (A \times C) \cup (B \times C)$. This implies that $(u, v) \in A \times C$ or $(u, v) \in B \times C$. In the first case $u \in A$ and $v \in C$ and in the second case $u \in B$ and $v \in C$. Thus $u \in A \cup B$ and $v \in C$, which implies $(u, v) \in (A \cup B) \times C$. $\square$

7.2 Relations

Given a set A, a *relation on* A is some property that is either true or false for any ordered pair $(x, y) \in A^2$. For example, "greater than" is a relation on $\mathbb{Z}$, denoted by $>$. It is true for the pair $(3, 2)$, but false for the pairs $(2, 2)$ and $(2, 3)$. In more generality,

Definition 7.2.1. *Given sets A and B, a* relation between A and B *is a subset of $A \times B$.*

By this definition, a relation R is simply a specification of which pairs are related by R, that is, which pairs the relation R is true for. For the relation $>$ on the set $\{1, 2, 3\}$,

$$> = \{(2, 1), (3, 1), (3, 2)\}.$$

This notation might look weird because we do not often regard the symbol "$>$" as a meaningful entity in itself. It is, at least from the vantage point of the foundations of mathematics: This symbol is a particular relation.

The common usage of the symbol "$>$" (as in $3 > 2$) is an instance of a useful notational convention: For a relation R, $(a, b) \in R$ can also be specified as aRb. Thus, in the above example, $(2, 1) \in >$ can be written as $2 > 1$. How convenient!

Common mathematical relations that will concern us include $<$, $>$, $\leq$, $\geq$, $=$, $\neq$, $|$, $\equiv_n$, $\subset$, $\subseteq$, etc. For example, the relation $=$ on the set $\mathbb{Z}$ is precisely the set $\{(n, n) : n \in \mathbb{Z}\}$ and the relation $\leq$ on $\mathbb{R}$ is the set $\{(x, x + |y|) : x, y \in \mathbb{R}\}$.

The concept of a relation is as general as the concept of a set, and is not limited to strictly mathematical settings. For instance, we can define the relation *likes* between the set {Anna,Britney,Caitlyn} and the set {Austin,Brian,Carlos}, such that

likes = $\big\{$(Britney,Austin),(Caitlyn,Austin),(Britney, Carlos),(Anna,Austin),(Caitlyn,Brian)$\big\}$.

In this setting we can write *Britney likes Austin*.

7.3 Kinds of relations

A relation R on a set A is called

- *reflexive* if for all $a \in A$, aRa.
- *symmetric* if for all $a, b \in A$, aRb implies bRa.
- *antisymmetric* if for all $a, b \in A$, aRb and bRa implies $a = b$.
- *transitive* if for all $a, b, c \in A$, aRb and bRc implies aRc.

Equivalence relations. A relation that is reflexive, symmetric, and transitive is called an *equivalence relation*. Clearly, the common relation $=$ on the set $\mathbb{R}$, say, is an equivalence relation. Also, we have seen earlier that the congruence relation $\equiv_n$ on the set $\mathbb{Z}$ is reflexive, symmetric, and transitive, thus it is also an equivalence relation. The similarity relation on the set of triangles in the plane is another example.

Equivalence relations are special in that they naturally partition the underlying set into *equivalence classes*. For example, the relation $\equiv_2$ partitions the integers into even and odd ones. These are, respectively, the integers that are related (by $\equiv_2$) to 0, and the ones related to 1. Let's formalize these concepts.

Definition 7.3.1. *A* partition *of a set A is a set $\mathcal{X} \subseteq 2^A \setminus \{\emptyset\}$, such that*

(a) Each $a \in A$ belongs to some $S \in \mathcal{X}$.

(b) If $S, T \in \mathcal{X}$, either $S = T$ or $S \cap T = \emptyset$.

Stated differently, this definition says that the set A is the union of the members of $\mathcal{X}$, and these members are disjoint. Now, given an equivalence relation R on A, the *equivalence class* of $a \in A$ is defined as

$$R[a] = \{b \in A : aRb\}.$$

Theorem 7.3.2. *Let R be an equivalence relation on a set A. Then $\{R[a] : a \in A\}$ is a partition of A.*

Proof. Consider an equivalence relation R on A. Due to reflexivity, every element $a \in A$ belongs to $R[a]$, which implies (a). Now, consider two equivalence classes $R[a]$ and $R[b]$. If aRb, then for any $c \in R[a]$, by transitivity and symmetry, bRc and $c \in R[b]$. This shows $R[a] \subseteq R[b]$. We can symmetrically argue that $R[b] \subseteq R[a]$, which together implies $R[a] = R[b]$.

Otherwise, if $a \not R b$ then consider some $c \in R[a]$. If $c \in R[b]$ then aRc and bRc, which imply, by transitivity and reflexivity, aRb, leading to a contradiction. Thus no element of $R[a]$ belongs to $R[b]$ and $R[a] \cap R[b] = \emptyset$. This shows (b) and concludes the theorem. □

Order relations. A relation that is reflexive, antisymmetric, and transitive is called a *partial order*. The relations $\leq$, $\geq$, and $|$ on the set $\mathbb{Z}$, as well as the relation $\subseteq$ on the powerset 2^A of any set A, are familiar partial orders. Note that a pair of elements can be *incomparable* with respect to a partial order. For example, $|$ is a partial order on $\mathbb{Z}$, but $2 \not| 3$ and $3 \not| 2$. A set A with a partial order on A is called a *partially ordered set*, or, more commonly, a *poset*.

A relation R on a set A is a *total order* if it is a partial order and satisfies the following additional condition:

- For all $a, b \in A$, either aRb or bRa (or both).

For example, the relations $\geq$ and $\leq$ are total orders on $\mathbb{R}$, but $|$ is not a total order on $\mathbb{Z}$. Finally, a *strict order* on A is a relation R that satisfies the following two conditions:

- For all $a, b, c \in A$, aRb and bRc implies aRc. (Transitivity.)

- Given $a, b \in A$, exactly one of the following holds (and not the other two): aRb, bRa, $a = b$.

The familiar $<$ and $>$ relations (on $\mathbb{R}$, say) are examples of strict orders.

7.4 Creating relations

There are a few ways to define new relations from existing ones, and we describe two important such ways below.

Restrictions of relations. Here is one notion that is sometimes useful: Given a relation R on a set A, and a subset $S \subseteq A$, we can use R to define a relation on S called the *restriction* of R to S. Denoted by $R|_S$, it is defined as

$$R|_S = \big\{(a, b) \in R : a, b \in S\big\}.$$

Compositions of relations. For three sets A, B, C, consider a relation R between A and B, and a relation S between B and C. The *composition of R and S* is a relation T between A and C, defined as follows: aTc if and only if there exists some $b \in B$, such that aRb and bSc. The composition of R and S is commonly denoted by $R \circ S$.

Note that by this definition, the composition of relations on the same set A is always well-defined. In particular, given a relation R on A we can recursively define $R^1 = R$ and $R^n = R^{n-1} \circ R$ for all $n \geq 2$. Now consider the infinite union

$$T = \bigcup_{i \in \mathbb{N}^+} R^i.$$

This relation T is called the *transitive closure* of R.

Proposition 7.4.1. *Important properties of transitive closure:*

(a) T is transitive.

(b) T is the smallest transitive relation that contains R. (That is, if U is a transitive relation on A and $R \subseteq U$, then $T \subseteq U$.)

(c) If $|A| = n$ then

$$T = \bigcup_{i=1}^{n} R^i.$$

7.5 Functions

The general concept of a function in mathematics is defined very similarly to relations. In fact, as far as the definitions go, functions *are* relations, of a special type:

Definition 7.5.1. *Given two sets A and B, a function $f : A \to B$ is a subset of $A \times B$ such that*

(a) If $x \in A$, there exists $y \in B$ such that $(x, y) \in f$.

(b) If $(x, y) \in f$ and $(x, z) \in f$ then $y = z$.

A function is sometimes called a *map* or *mapping*. The set A in the above definition is the *domain* and B is the *codomain* of f.

A function $f : A \to B$ is effectively a special kind of relation between A and B, which relates every $x \in A$ to *exactly one* element of B. That element is denoted by $f(x)$.

If the above definition is followed rigidly, particular functions should be defined by specifying all the pairs $(x, f(x))$. This is often cumbersome and unnecessary, and we will mostly continue describing a function from A to B as we did before: as a rule for picking an element $f(x) \in B$ for every element $x \in A$. As in, "Consider a function $f : \mathbb{R} \to \mathbb{R}$, where $f(x) = x^2$ for all $x \in \mathbb{R}$."

Kinds of Functions. For a function $f : A \to B$, the set $f(A) = \{f(x) : x \in A\}$ is called the *range* of f. The range is a subset of the codomain but may be different from it. If $f(A) = B$ then we say that f is *onto*. More precisely, a function $f : A \to B$ is a *surjection* (or *surjective*), or *onto* if each element of B is of the form $f(x)$ for at least one $x \in A$.

Today is the day of weird names, so: A function $f : A \to B$ is an *injection* (or *injective*), or *one-to-one* if for all $x, y \in A$, $f(x) = f(y)$ implies $x = y$. Put differently, $f : A \to B$ is one-to-one if each element of B is of the form $f(x)$ for at most one $x \in A$.

As if this wasn't enough: A function $f : A \to B$ is a *bijection* (or *bijective*), or a *one-to-one correspondence* if it is both one-to-one and onto. Alternatively, $f : A \to B$ is a bijection if each element of B is of the form $f(x)$ for exactly one $x \in A$.

Compositions and Inverse Functions. Given two functions $f : A \to B$ and $g : B \to C$ we can define a new function $g \circ f : A \to C$ by $(g \circ f)(x) = g(f(x))$ for all $x \in A$.

One useful function that can be defined for any set A is the *identity function* $i_A : A \to A$, defined by $i_A(x) = x$ for all $x \in A$. We can use identity functions to define *inverse functions*. Specifically, if $f : A \to B$ is a bijection, then its inverse $f^{-1} : B \to A$ is defined so that $f^{-1} \circ f = i_A$ and $f \circ f^{-1} = i_B$. Of course, we haven't shown that f^{-1} even exists or that it is unique, but these properties do hold, assuming that $f : A \to B$ is a bijection. (This assumption is necessary.)

Another result that is sometimes used is the following: If $f : A \to B$ and $g : B \to C$ are bijections then $g \circ f : A \to C$ is a bijection, and

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}.$$

We omit the proof.

Bijections and cardinality. Bijections allow us to rigorously define when two sets are of the same cardinality:

Definition 7.5.2. *Two sets A and B have the same number of elements if and only if there exists a bijection $f : A \to B$.*

Chapter 8

Mathematical Logic

Perhaps the most distinguishing characteristic of mathematics is its reliance on logic. Explicit training in mathematical logic is essential to a mature understanding of mathematics. Familiarity with the concepts of logic is also a prerequisite to studying a number of central areas of computer science, including databases, compilers, and complexity theory.

8.1 Propositions and predicates

A *proposition* is a statement that is either true or false. For example, "It will rain tomorrow" and "It will not rain tomorrow" are propositions, but "It will probably rain tomorrow" is not, pending a more precise definition of "probably".

A *predicate* is a statement that contains a variable, such that for any specific value of the variable the statement is a proposition. Usually the allowed values for the variable will come from a specific set, sometimes called the *universe* of the variable, which will be either explicitly mentioned or clear from context. A simple example of a predicate is $x \geq 2$ for $x \in \mathbb{R}$. Clearly, for any real value of x, this statement is either true or false. We denote predicates in a similar way to functions, as in $P(x)$. In fact, the connection to functions runs deep: A predicate $P(x)$ can be considered a function, $P : \mathcal{U} \to \{0, 1\}$, where $\mathcal{U}$ is the universe of the variable x, 1 represents truth, and 0 represents falsehood.

A predicate may have more than one variable, in which case we speak of predicates in two variables, three variables, and so on, denoted as $Q(x, y)$, $S(x, y, z)$, etc.

8.2 Quantifiers

Given a predicate $P(x)$ that is defined for all elements in a set A, we can reason about whether $P(x)$ is true for all $x \in A$, or if it's at least true for some $x \in A$. We can state propositions to this effect using the *universal quantifier* $\forall$ and the *existential quantifier* $\exists$.

- $\forall x \in A : P(x)$ is true if and only if $P(x)$ is true for all $x \in A$. This proposition can be read "For all $x \in A$, $P(x)$."

- $\exists x \in A : P(x)$ is true if and only if $P(x)$ is true for at least one $x \in A$. This proposition can be read "There exists $x \in A$ such that $P(x)$."

Given a predicate in more than one variable we can quantify each (or some) of the variables. For example, the statement "For every real x and y, it holds that $x^2 - y^2 = (x - y)(x + y)$" can be formalized as

$$\forall x, y \in \mathbb{R} : x^2 - y^2 = (x - y)(x + y).$$

Somewhat more interestingly, the statement "There is no greatest integer" might be formulated as

$$\forall n \in \mathbb{Z}\ \exists m \in \mathbb{Z} : m > n.$$

It is crucial to remember that the meaning of a statement may change if the existential and universal quantifiers are exchanged. For example, $\exists m \in \mathbb{Z}\ \forall n \in \mathbb{Z} : m > n$ means "There is an integer strictly greater than all integers." This is not only contrary to the spirit of the original statement, but is patently wrong as it asserts in particular that there is an integer that is strictly greater than itself.

Exchanging the order of two quantifiers of the same type (either universal or existential) does not change the truth value of a statement. We do not prove this here.

8.3 Negations

Given a proposition P, the *negation* of P is the proposition "P is false". It is true if P is false, and false if P is true. The negation of P is denoted by $\neg P$, read as "not P." If we know the meaning of P, such as when P stands for "It will rain tomorrow," the proposition $\neg P$ can be stated more naturally than "not P," as in "It will not rain tomorrow." The truth-value of $\neg P$ can be represented by the following *truth table*:

P	$\neg P$
true	false
false	true

A truth table simply lists the truth values of particular statements in all possible cases. Something interesting can be observed in we consider the truth values of $\neg\neg Q$, which can be obtained by using the above table once with $P = Q$ and once with $P = \neg Q$:

Q	$\neg Q$	$\neg\neg Q$
true	false	true
false	true	false

We see that the statements Q and $\neg\neg Q$ have the same truth values. In this case we say that the two statements are *equivalent*, and write $Q \Leftrightarrow \neg\neg Q$. If $A \Leftrightarrow B$ we can freely use B in the place of A, or A instead of B in our logical derivations.

Negation gets really interesting when the negated proposition is quantified. Then we can assert that

$$\begin{aligned} \neg\forall x \in A : P(x) &\Leftrightarrow \exists x \in A : \neg P(x) \\ \neg\exists x \in A : P(x) &\Leftrightarrow \forall x \in A : \neg P(x) \end{aligned}$$

These can be interpreted as the claim that if $P(x)$ is not true for all $x \in A$ then it is false for some $x \in A$ and vice versa, and the claim that if $P(x)$ is not false for any $x \in A$ then it is true for all $x \in A$ and vice versa. What this means, in particular, is that if we want to disprove a statement that asserts something for all $x \in A$, it is sufficient to demonstrate *one* such x for which the statement does not hold. On the other hand, if we need to disprove a statement that asserts the existence of an $x \in A$ with a certain property, we actually need to show that for *all* such x this property does not hold.

Looked at another way, the above equivalences imply that if we negate a quantified statement, the negation can be "pushed" all the way inside, so that no negated quantifiers are left. Indeed, leaving any negated quantifiers is often considered a mark of poor style. Here is how how this elimination is done in a particular example:

$$\begin{aligned} \neg\forall n \in \mathbb{Z}\ \exists m \in \mathbb{Z} : m > n &\Leftrightarrow \\ \exists n \in \mathbb{Z}\ \neg\exists m \in \mathbb{Z} : m > n &\Leftrightarrow \\ \exists n \in \mathbb{Z}\ \forall m \in \mathbb{Z} : m \leq n & \end{aligned}$$

This can be read as "There exists an integer that is greater or equal to any other integer," which is the proper negation of the original statement.

8.4 Logical connectives

The symbol $\neg$ is an example of a *connective*. Other connectives combine two propositions (or predicates) into one. The most common are $\wedge$, $\vee$, $\oplus$, $\rightarrow$ and $\leftrightarrow$. $P \wedge Q$ is read as "P and Q"; $P \vee Q$ as "P or Q"; $P \oplus Q$ as "P xor Q"; $P \rightarrow Q$ as "P implies Q" or "if P then Q"; and $P \leftrightarrow Q$ as "P if and only if Q". The truth-value of these *compound propositions* (sometimes called *sentences*) depends on the truth values of P and Q (which are said to be the *terms* of these sentences), in a way that is made precise in the truth-table below.

We will not concern ourselves much with the $\oplus$ and $\leftrightarrow$ connectives, as they are encountered somewhat less frequently.

One interesting thing about the above table is that the proposition $P \rightarrow Q$ is false only when P is true and Q is false. This is what we would expect: If P is true but Q is false then, clearly, P does not imply Q. The important thing to remember is that if

P	Q	$P \wedge Q$	$P \vee Q$	$P \oplus Q$	$P \to Q$	$P \leftrightarrow Q$
T	T	T	T	F	T	T
T	F	F	T	T	F	F
F	T	F	T	T	T	F
F	F	F	F	F	T	T

P is false, then $P \to Q$ is true. One way this can be justified is by remembering that we expect a proposition to be either false or true. Now, $P \to Q$ being false says that P does not imply Q, which means precisely that P is true but Q is still false. In all other cases we expect $P \to Q$ to be true. (Did I succeed in turning something obvious into a confusing mess? Well, we all know what is paved with good intentions...)

Now, there is another statement involving P and Q that is false precisely when P is true and Q is false. It is, of course, $\neg P \vee Q$. As the following truth table demonstrates, the proposition $\neg P \vee Q$ is equivalent to $P \to Q$:

P	Q	$P \to Q$	$\neg P \vee Q$
T	T	T	T
T	F	F	F
F	T	T	T
F	F	T	T

This means something rather interesting: We can replace a proposition that involves implication by an equivalent one that instead has negation ($\neg$) and disjunction ($\vee$). Also, since $P \to Q$ is false only when P is true and Q is false, the proposition $\neg(P \to Q)$ is equivalent to $P \wedge \neg Q$:

$$\neg(P \to Q) \Leftrightarrow P \wedge \neg Q.$$

This means that in a negated implication, the negation can be "pushed inside", somewhat like with quantifiers. In fact, similar equivalences exist for other negated compound statements, as can be verified using truth tables (do it!):

$$\begin{aligned} \neg(P \vee Q) &\Leftrightarrow \neg P \wedge \neg Q \\ \neg(P \wedge Q) &\Leftrightarrow \neg P \vee \neg Q \end{aligned}$$

These are the famous *DeMorgan's laws*. What they mean is that we can eliminate negated compounds (sounds like a military operation, doesn't it?) just as we can eliminate negated quantifiers.

Here is another important logical equivalence: The implication $P \to Q$ is equivalent to the *contrapositive* implication $\neg Q \to \neg P$:

$$(P \to Q) \Leftrightarrow (\neg Q \to \neg P).$$

This is demonstrated by the following truth table:

P	Q	$P \to Q$	$\neg Q$	$\neg P$	$\neg Q \to \neg P$
T	T	T	F	F	T
T	F	F	T	F	F
F	T	T	F	T	T
F	F	T	T	T	T

Indeed, an implication of the form "If P then Q" is sometimes proved by assuming that Q does not hold and showing that under this assumption P does not hold. This is called a proof by contrapositive. (Despite the similarity, it is different from a proof by contradiction.)

8.5 Tautologies and logical inference

A sentence that is true regardless of the values of its terms is called a *tautology*, while a statement that is always false is a *contradiction*. Another terminology says that tautologies are *valid* statements and contradictions are *unsatisfiable* statements. All other statements are said to be *satisfiable*, meaning they can be either true or false.

Easy examples of a tautology and a contradiction are provided by $P \vee \neg P$ and $P \wedge \neg P$, as demonstrated by the following truth table:

P	$\neg P$	$P \vee \neg P$	$P \wedge \neg P$
T	F	T	F
F	T	T	F

Note that by our definition of logical equivalence, all tautologies are equivalent. It is sometimes useful to keep a "special" proposition $\mathcal{T}$ that is always true, and a proposition $\mathcal{F}$ that is always false. Thus any tautology is equivalent to $\mathcal{T}$ and any contradiction is equivalent to $\mathcal{F}$.

Here is another tautology: $(P \wedge Q) \to P$:

P	Q	$P \wedge Q$	$(P \wedge Q) \to P$
T	T	T	T
T	F	F	T
F	T	F	T
F	F	F	T

The statement $(P \wedge Q) \to P$ is read "P and Q implies P". The fact that this is a tautology means that the implication is always true. Namely, if we know the truth of $P \wedge Q$, we can legitimately conclude the truth of P. In such cases the symbol $\Rightarrow$ is used, and we can write $(P \wedge Q) \Rightarrow P$. There is a crucial difference between $(P \wedge Q) \to P$ and $(P \wedge Q) \Rightarrow P$. The former is a single statement, while the latter indicates a relationship between two statements. Such a relationship is called an *inference rule*. A similar inference rule, $P \Rightarrow P \vee Q$ can be established analogously.

In general, any tautology of the form $A \rightarrow B$ can be used to "manufacture" the inference rule $A \Rightarrow B$ that says that if we know A we can conclude B. Similarly, a tautology of the form $A \leftrightarrow B$ can be converted into the equivalence $A \Leftrightarrow B$, which can be regarded as two inference rules, $A \Rightarrow B$ and $B \Rightarrow A$. A particularly important inference rule is called *modus ponens*, and says that if we know that P and $P \rightarrow Q$ are both true, we can conclude that Q is true. It follows from the tautology $(P \wedge (P \rightarrow Q)) \rightarrow Q$:

P	Q	$P \rightarrow Q$	$P \wedge (P \rightarrow Q)$	$(P \wedge (P \rightarrow Q)) \rightarrow Q$
T	T	T	T	T
T	F	F	F	T
F	T	T	F	T
F	F	T	F	T

We've already seen a number of inference rules above, like $(P \rightarrow Q) \Leftrightarrow (\neg Q \rightarrow \neg P)$, without calling them that. Here are three others, all corresponding to tautologies that you are invited to verify using truth tables:

$$\begin{aligned} (\neg P \rightarrow \mathcal{F}) &\Leftrightarrow P \\ (P \leftrightarrow Q) &\Leftrightarrow (P \rightarrow Q) \wedge (Q \rightarrow P) \\ (P \leftrightarrow Q) &\Leftrightarrow (P \rightarrow Q) \wedge (\neg P \rightarrow \neg Q) \end{aligned}$$

These three rules are of particular importance. The first formally establishes the validity of proofs by contradiction, and the second and third provide two means for proving "if and only if" statements. We've been using these all along, but now we know why they are justified.

Chapter 9

Counting

9.1 Fundamental principles

The subject of *enumerative combinatorics* is counting. Generally, there is some set A and we wish to calculate the size $|A|$ of A. Here are some sample problems:

- How many ways are there to seat n couples at a round table, such that each couple sits together?
- How many ways are there to express a positive integer n as a sum of positive integers?

There are a number of basic principles that we can use to solve such problems.

The sum principle: Consider n sets A_i, for $1 \leq i \leq n$, that are *pairwise disjoint*, namely $A_i \cap A_j = \emptyset$ for all $i \neq j$. Then

$$\left| \bigcup_{i=1}^{n} A_i \right| = \sum_{i=1}^{n} |A_i| .$$

For example, if there are n ways to pick an object from the first pile and m ways to pick on object from the second pile, there are $n+m$ ways to pick an object altogether.

The product principle: If we need to do n things one after the other, and there are c_1 ways to do the first, c_2 ways to do the second, and so on, the number of possible courses of action is $\prod_{i=1}^{n} c_i$. For example, the number of possible three-letter words in which a letter appears at most once that can be constructed using the English alphabet is $26 \cdot 25 \cdot 24$: There are 26 possibilities for the first letter, then 25 possibilities for the second, and finally 24 possibilities for the third.

The bijection principle: As we have seen, there exists a bijection from A to B if and only if the size of A equals the size of B. Thus, one way to count the number of elements in a set A is to show that there is a bijection from A to some other set B

and to count the number of elements in B. Often there is no need to explicitly specify the bijection and prove that it is such: At this point in the course, you can omit some low-level details from the written proofs in your homework solutions, *as long as you are certain that you could reproduce these details if asked to do so.* For example, you can simply state and use the observation that the number of ways to seat n people in a row is the same as the number of ways to order the integers $1, 2, \ldots, n$, which is the same as the number of n-element sequences that can be constructed from the integers $1, 2, \ldots, n$ (without repetition), which is the same as the number of bijections $f : A \to A$, for $A = \{1, 2, \ldots, n\}$. You should always make sure that you yourself fully understand why such equalities hold whenever you use them! Obviously, if you don't, you'll end up relying on equalities that are simply not true, which is not such a great idea. If in doubt, write down a complete proof to make sure your reasoning is correct.

9.2 Basic counting problems

Choosing an ordered sequence of distinct objects with repetition. How many ways are there to pick an ordered sequence of k objects from a pool with n types of objects, when repetitions are allowed? (That is, we can pick an object of the same type more than once.) Well, by the product principle, there are n options for the first object, n options for the second, and so on. Overall we get n^k possible sequences. What follows is a somewhat more formal argument by induction. Observe that the number of sequences as above is the same as the number of functions from a set of k elements to a set of n elements. (Make sure you understand this.)

Theorem 9.2.1. *Given sets A and B, such that $|A| = k$ and $|B| = n$, the number of functions $f : A \to B$ is n^k.*

Proof. Induction on k. If $k = 0$ the set A has no elements and there is only one mapping from A to B, the empty mapping. (Recall that a function $f : A \to B$ is a subset of $A \times B$, and if $A = \emptyset$ then $A \times B = \emptyset$.) We suppose the claim holds for $|A| = m$ and treat the case $|A| = m + 1$. Consider some element $a \in A$. To specify a function $f : A \to B$ we can specify $f(a) \in B$ and a mapping $f' : A \setminus \{a\} \to B$. There are n possible values of $f(a) \in B$, and for each of these there are n^m mappings f' by the induction hypothesis. This results in n^{m+1} mappings f and completes the proof by induction. □

Choosing an ordered sequence of distinct objects *without* repetition. How many ways are there to pick an ordered sequence of k objects from a set of n objects when only one copy of each object is available, so there can be no repetitions? Again we can use the product principle. Observe that the first object in the sequence can be chosen from n distinct objects. Once the first one is picked, there are only $n - 1$ possibilities for the second object. After that there are $n - 2$ objects to choose from,

and so on. Overall we get that the desired quantity is

$$n(n-1)\cdots(n-k+1) = \prod_{i=0}^{k-1}(n-i).$$

This is called a *falling factorial* and denoted by $(n)_k$ or $n^{\underline{k}}$. We again provide a more formal proof by induction, observing that the number of ways to pick an ordered sequence of k objects from a collection of n distinct ones without replacement is equal to the number of *one-to-one* functions $f : A \to B$, where $|A| = k$ and $|B| = n$.

Theorem 9.2.2. *Given sets A and B, such that $|A| = k$ and $|B| = n$, the number of* one-to-one *functions $f : A \to B$ is $(n)_k$.*

Proof. Induction on k. When $|A| = 0$, there is one mapping f as described, the empty mapping, and $(n)_k$ is the empty product, equal to 1. Suppose the claim holds for $|A| = m$ and consider the case $|A| = m + 1$. Fix an element $a \in A$. To specify f we specify $f(a)$ and a mapping $f' : A \setminus \{a\} \to B$. There are n possible values for $f(a) \in B$. Consider a specific such value $f(a) = b$. Since f is one-to-one, no element of $A \setminus \{a\}$ can be mapped to b. Thus f' has to be a one-to-one-mapping from $A \setminus \{a\}$ to $B \setminus \{b\}$. By the induction hypothesis, the number of such mappings is $(n-1)_m$. The number of possible mappings f is thus $n \cdot (n-1)_m = (n)_{m+1}$. □

Permutations. How many ways are there to arrange n people in a row? How many ordered n-tuples are there of integers from the set $\{1, 2, \ldots, n\}$? Haw many distinct rearrangements are there of the integers $1, 2, \ldots, n$? How many bijections are there from the set $\{1, 2, \ldots, n\}$ to itself? The answer to these questions is the same, and follows from Theorem 9.2.2. A bijection from a set A to itself is called a *permutation* of A. The number of permutations of the set $\{1, 2, \ldots, n\}$ is precisely the number of one-to-one functions from this set to itself, and this number is $(n)_n = n \cdot (n-1) \cdots 2 \cdot 1$. This quantity is called "n factorial" and is denoted by $n!$. We can now observe that

$$(n)_k = \frac{n!}{(n-k)!}.$$

It is important to remember that $0! = 1$, since $0!$ is the empty product. Here is a list of values of $n!$ for $0 \leq n \leq 10$:

$$1, 1, 2, 6, 24, 120, 720, 5040, 40320, 362880, 3628800$$

Seating at a round table. We've arranged n people in a row, now it's time to sit them down. So how many ways are there to seat n people at a round table? Let's be precise about what we mean: Two seating arrangements are considered identical if every person has the same neighbor to her right. In other words, rotations around the table do not matter. Here is how this problem can be tackled: Fix one person a and sit her down anywhere. This now fixes $n - 1$ possible positions for the others: "first person to the right of a", "second person to the right of a", and so on until "$(n-1)$-st person to the right of a". The number of ways to arrange the others in these $n - 1$ positions is $(n-1)!$, which is also the answer to the original question.

Choosing an *unordered* collection of distinct objects *without* repetition. How many ways are there to pick a *set* of k objects from a set of n objects? Since we are picking a set, we do not care about order, and there are no repetitions. Notice that every such set can be ordered in $k!$ ways. That is, each set corresponds to $k!$ distinct ordered k-tuples. Now, we know that the number of ordered k-tuples that can be picked from a collection of n distinct objects is $(n)_k$. Thus if we denote by X the number of sets of cardinality k that can be picked from a collection of n distinct objects, we get

$$\begin{aligned} X \cdot k! &= (n)_k \\ X &= \frac{(n)_k}{k!} \\ X &= \frac{n!}{k!(n-k)!}. \end{aligned}$$

This quantity X is denoted by $\binom{n}{k}$, read "n choose k". This is such an important quantity that we emphasize it again: The number of k-element subsets of an n-element set is $\binom{n}{k}$, defined as

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{\prod_{i=0}^{k-1}(n-i)}{k!}.$$

We can see that $\binom{n}{0} = \binom{n}{n} = 1$, and we define $\binom{n}{k} = 0$ when $k > n$ or $k < 0$.

The number of subsets. We have seen that the number of k-element subsets of an n-element set is $\binom{n}{k}$. How many subsets of an n-element set are there overall, of any size? Yes, it is time to prove the neat formula we've been using all along:

Theorem 9.2.3. *For a set A,*

$$\left|2^A\right| = 2^{|A|}.$$

Proof. By induction. When $|A| = 0$, $A = \emptyset$. Hence, A has only one subset (itself) and the formula holds since $2^0 = 1$. Assume the formula holds when $|A| = k$ and consider the case $|A| = k + 1$. Fix an element $a \in A$. A subset of A either contains a or not. The subsets of A that do not contain a are simply subsets of $A \setminus \{a\}$ and their number is 2^k by the induction hypothesis. On the other hand, each subset of A that does contain a is of the form $\{a\} \cup X$, for $X \subseteq A \setminus \{a\}$. Thus there is a bijective mapping between subsets of A that contain a and subsets of $A \setminus \{a\}$. The number of such subsets is again 2^k. Overall we get that the number of subsets of A is $2^k + 2^k = 2^{k+1}$, which completes the proof by induction. □

Here is another instructive way to prove Theorem 9.2.3: Consider the set of functions $f : A \to \{0, 1\}$. These functions assign a value of 0 or 1 to every element of A. In this way, such a function f uniquely specifies a subset of A. Namely, the elements x for which $f(x) = 1$ are the elements that belong to the subset of A specified by f. This defines a bijection between such functions f and subsets of A. By Theorem 9.2.1, the number of functions f from A to $\{0, 1\}$ is $2^{|A|}$, which proves Theorem 9.2.3.

We can use Theorem 9.2.3 to derive an interesting identity. We now know that the overall number of subsets of an n-element set is 2^n. Previously we have seen that the number of k-element subsets of an n-element set is $\binom{n}{k}$. By the sum principle, we get

$$\sum_{i=0}^{n} \binom{n}{i} = 2^n.$$

Choosing an *unordered* collection of distinct objects *with* repetition. How many ways are there to pick a collection of k objects from a pool with n types of objects, when repetitions are allowed? We can reason as follows: The number of ways to pick k objects from a pool with n types of objects is the same as the number of ways to put k balls into n bins. Imagine these bins aligned in a row. A "configuration" of k balls in n bins can be specified as a sequence of $n-1$ "|" symbols and k "*" symbols, as in

$$**||*|***|$$

This sequence encodes the configuration where $k = 6$ and $n = 5$, and there are two balls in bin number 1, one ball in bin number 3, and three balls in bin number 4. How many such configurations are there? A configuration is uniquely specified by the positions of the k "*" symbols. Thus specifying a configuration amounts to choosing which of the $n + k - 1$ symbols are going to be "*". This simply means we need to choose a k-element subset from a set of size $n + k - 1$. The number of ways to pick a collection of k objects from a pool of n types of objects with repetitions is thus

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