Predicates & Sets

1 More Proof Techniques

1.1 Proof by Contradiction

In a ***proof by contradiction*** or ***indirect proof***, you show that if a proposition were false, then some logical contradiction or absurdity would follow. Thus, the proposition must be true. So proof by contradiction would be described by the inference rule

Rule.

$$\frac{\neg P \longrightarrow \mathbf{F}}{P}$$

Proof by contradiction is *always* a viable approach. However, as the name suggests, indirect proofs can be a little convoluted. So direct proofs are generally preferable as a matter of clarity.

1.2 Method

In order to prove a proposition P by contradiction:

1. Write, "We use proof by contradiction."
2. Write, "Suppose P is false."
3. Deduce a logical contradiction.
4. Write, "This is a contradiction. Therefore, P must be true."

Example

Remember that a number is *rational* if it is equal to a ratio of integers. For example, $3.5 = 7/2$ and $0.1111\ldots = 1/9$ are rational numbers. On the other hand, we'll prove by contradiction that $\sqrt{2}$ is irrational.

Theorem 1.1. *$\sqrt{2}$ is irrational.*

Proof. We use proof by contradiction. Suppose the claim is false; that is, $\sqrt{2}$ is rational. Then we can write $\sqrt{2}$ as a fraction a/b in *lowest terms*.

Squaring both sides gives $2 = a^2/b^2$ and so $2b^2 = a^2$. This implies that a is even; that is, a is a multiple of 2. Therefore, a^2 must be a multiple of 4. Because of the equality $2b^2 = a^2$, we know $2b^2$ must also be a multiple of 4. This implies that b^2 is even and so b must be even. But since a and b are both even, the fraction a/b is not in lowest terms.

This is a contradiction. Therefore, $\sqrt{2}$ must be irrational. □

1.3 Potential Pitfall

Often students use an indirect proof when a direct proof would be simpler. Such proofs aren't wrong; they just aren't excellent. Let's look at an example. A function f is *strictly increasing* if $f(x) > f(y)$ for all real x and y such that $x > y$.

Theorem 1.2. *If f and g are strictly increasing functions, then $f + g$ is a strictly increasing function.*

Let's first look at a simple, direct proof.

Proof. Let x and y be arbitrary real numbers such that $x > y$. Then:

$$\begin{aligned} f(x) > f(y) &\qquad \text{(since } f \text{ is strictly increasing)} \\ g(x) > g(y) &\qquad \text{(since } g \text{ is strictly increasing)} \end{aligned}$$

Adding these inequalities gives:

$$f(x) + g(x) > f(y) + g(y)$$

Thus, $f + g$ is strictly increasing as well. □

Now we *could* prove the same theorem by contradiction, but this makes the argument needlessly convoluted.

Proof. We use proof by contradiction. Suppose that $f+g$ is not strictly increasing. Then there must exist real numbers x and y such that $x > y$, but

$$f(x) + g(x) \leq f(y) + g(y)$$

This inequality can only hold if either $f(x) \leq f(y)$ or $g(x) \leq g(y)$. Either way, we have a contradiction because both f and g were defined to be strictly increasing. Therefore, $f + g$ must actually be strictly increasing. □

1.4 Proof by Cases

In Week1 Notes we verified by truth table that the two expressions $A \vee (\overline{A} \wedge B)$ and $A \vee B$ were equivalent. Another way to prove this would be to reason *by cases*:

A is **T**. Then $A \vee$ anything will have truth value **T**. Since both expressions are of this form, in this case, both have the same truth value, namely, **T**.

A is **F**. Then $A \vee P$ will have the same truth value as P for any proposition, P. So the second expression has the same truth value as B. Similarly, the first expression has the same truth value as $\overline{\mathbf{F}} \wedge B$ which also has the same value as B. So in this case, both expressions will have the same truth value, namely, the value of B.

Here's a slightly more interesting example. Let's agree that given any two people, either they have met or not. If every pair of people in a group has met, we'll call the group a ***club***. If every pair of people in a group has not met, we'll call it a group of ***strangers***.

Theorem. *Every collection of 6 people includes a club of 3 people or a group of 3 strangers.*

Proof. The proof is by case analysis[1]. Let x denote one of the six people. There are two cases:

1. Among the remaining 5 people, at least 3 have met x.
2. Among the remaining 5 people, at least 3 have not met x.

We first argue that at least one of these two cases must hold.[2] We'll prove this by contradiction. Namely, suppose neither case holds. This means that at most 2 people in the group met x and at most 2 did not meet x. This leaves at least 1 of the remaining 5 people unaccounted for. That is, at least 1 of the people neither met x nor did not meet x, which contradicts our agreement that every pair has met or has not met. So at least one of these two cases must hold.

Case 1: Suppose that at least 3 people that did meet x.

This case splits into two subcases:

> **Case 1.1:** no pair among those people met each other. Then these people are a group of at least 3 strangers. So the Theorem holds in this subcase.
>
> **Case 1.2:** some pair among those people have met each other. Then that pair, together with x, form a club of 3 people. So the Theorem holds in this subcase.

This implies that the Theorem holds in Case 1.

Case 2: Suppose that there exist at least 3 people that did not meet x.

This case also splits into two subcases:

[1] Describing your approach at the outset helps orient the reader.

[2] Part of a case analysis argument is showing that you've covered all the cases. Often this is trivial, because the two cases are of the form "P" and "not P". However, the situation above is not so simple.

Case 2.1: every pair among those people met each other. Then these people are a club of at least 3 people. So the Theorem holds in this subcase.

Case 2.2: some pair among those people have not met each other. Then that pair, together with x, form a group of at least 3 strangers. So the Theorem holds in this subcase.

This implies that the Theorem also holds in Case 2, and therefore holds in all cases. □

2 Predicates

A ***predicate*** is a proposition whose truth depends on the value of one or more variables. For example,

$$\text{“}n \text{ is a perfect square”}$$

is a predicate whose truth depends on the value of n. The predicate is true for $n = 4$ since 4 is a prefect square, but false for $n = 5$ since 5 is not a perfect square.

Like other propositions, predicates are often named with a letter. Furthermore, a function-like notation is used to denote a predicate supplied with specific variable values. For example, we might name our earlier predicate P:

$$P(n) = \text{“}n \text{ is a perfect square”}$$

Now $P(4)$ is true, and $P(5)$ is false.

This notation for predicates is confusingly similar to ordinary function notation. If P is a predicate, then $P(n)$ is either *true* or *false*, depending on the value of n. On the other hand, if p is an ordinary function, like $n^2 + 1$, then $p(n)$ is a *numerical quantity*. Students frequently confuse these two.

2.1 Quantifying a Predicate

There are a couple kinds of assertion one commonly makes about a predicate: that it is *sometimes* true and that it is *always* true. For example, the predicate

$$\text{“}x^2 \geq 0\text{”}$$

is always true when x is a real number. On the other hand, the predicate

$$\text{“}5x^2 - 7 = 0\text{”}$$

is only sometimes true; specifically, when $x = \pm\sqrt{7/5}$.

There are several ways to express the notions of “always true” and “sometimes true” in English. The table below gives some general formats on the left and specific examples using those formats on the right. You can expect to see such phrases hundreds of times in mathematical writing!

Always True

For all n, $P(n)$ is true.	For all x, $x^2 \geq 0$.
$P(n)$ is true for every n.	$x^2 \geq 0$ for every x.

Sometimes True

There exists an n such that $P(n)$ is true.	There exists an x such that $5x^2 - 7 = 0$.
$P(n)$ is true for some n.	$5x^2 - 7 = 0$ for some x.
$P(n)$ is true for at least one n.	$5x^2 - 7 = 0$ for at least one x.

All these sentences quantify how often the predicate is true. Specifically, an assertion that a predicate is always true is called a ***universal*** quantification, and an assertion that a predicate is sometimes true is an ***existential*** quantification. Sometimes the English sentences are unclear with respect to quantification:

> "If you can solve any problem we come up with, then you get an A for the course."

The phrase "you can solve any problem we can come up with" could reasonably be interpreted as either a universal or existential quantification:

> "you can solve *every* problem we come up with"

or maybe

> "you can solve *at least one* problem we come up with"

In any case, notice that this quantified phrase appears inside a larger if-then statement. This is quite normal; quantified statements are themselves propositions and can be combined with and, or, implies, etc. just like any other proposition.

2.2 More Cryptic Notation

There are symbols to represent universal and existential quantification, just as there are symbols for "and" ($\wedge$), "implies" ($\longrightarrow$), and so forth. In particular, to say that a predicate $P(n)$ is true for all values of x in some set, D, one writes:

$$\forall x \in D.\ P(n)$$

The symbol $\forall$ is read "for all", so this whole expression is read "for all x in D, $P(x)$ is true". To say that a predicate $P(x)$ is true for at least one value of x in D, one writes:

$$\exists x \in D.\ P(x)$$

The backward-E is read "there exists". So this expression would be read, "There exists an x in D such that $P(x)$ is true. The symbols $\forall$ and $\exists$ are always followed by a variable and then a predicate, as in the two examples above.

As an example, let Probs be the set of problems we come up with, Solves(x) be the predicate "You can solve problem x", and A be the proposition, "You get an A for the course." Then the two different interpretations of

If you can solve any problem we come up with, then you get an A for the course.

can be written as follows:

$$(\forall x \in \text{Probs. Solves}(x)) \longrightarrow A,$$

or maybe

$$(\exists x \in \text{Probs. Solves}(x)) \longrightarrow A.$$

2.3 Mixing Quantifiers

Many mathematical statements involve several quantifiers. For example, Goldbach's Conjecture states:

"Every even integer greater than 2 is the sum of two primes."

Let's write this more verbosely to make the use of quantification clearer:

For every even integer n greater than 2, there exist primes p and q such that $n = p + q$.

Let Ev be the set of even integers greater than 2, and let Primes be the set of primes. Then we can write Goldbach's Conjecture in logic notation as follows:

$$\underbrace{\forall n \in \text{Ev}}_{\substack{\text{for every even} \\ \text{integer } n \geq 2}} \ \underbrace{\exists p \in \text{Primes}\ \exists q \in \text{Primes.}}_{\substack{\text{there exist primes} \\ p \text{ and } q \text{ such that}}} \ n = p + q.$$

2.4 Order of Quantifiers

Swapping the order of different kinds of quantifiers (existential or universal) changes the meaning of a proposition. For another example, let's return to one of our initial, confusing statements:

"Every American has a dream."

This sentence is ambiguous because the order of quantifiers is unclear. Let A be the set of Americans, let D be the set of dreams, and define the predicate $H(a, d)$ to be "American a has dream d.". Now the sentence could mean there is a single dream that every American shares:

$$\exists d \in D\ \forall a \in A.\ H(a, d)$$

Or it could mean that every American has their personal dream:

$$\forall a \in A\ \exists d \in D.\ H(a, d)$$

Swapping quantifiers in Goldbach's Conjecture creates a patently false statement that every even number ≥ 2 is the sum of *the same* two primes:

$$\underbrace{\exists p \in \text{Primes}\ \exists q \in \text{Primes}}_{\substack{\text{there exist primes} \\ p \text{ and } q \text{ such that}}} \ \underbrace{\forall n \in \text{Ev.}}_{\substack{\text{for every even} \\ \text{integer } n \geq 2}} \ n = p + q$$

2.4.1 Variables over One Domain

When all the variables in a formula are understood to take values from the same nonempty set, D, it's conventional to omit mention of D. For example, instead of $\forall x \in D\ \exists y \in D.\ Q(x, y)$ we'd write $\forall x \exists y.\ Q(x, y)$. The unnamed nonempty set that x and y range over is called the ***domain*** of the formula.

It's easy to arrange for all the variables to range over one domain. For example, Goldbach's Conjecture could be expressed with all variables ranging over the domain $\mathbb{N}$ as

$$\forall n.\ n \in \text{Ev} \longrightarrow (\exists p \exists q.\ p \in \text{Primes} \land q \in primes \land n = p + q).$$

2.5 Negating Quantifiers

There is a simple relationship between the two kinds of quantifiers. The following two sentences mean the same thing:

> It is not the case that everyone likes to snowboard. There exists someone who does not like to snowboard.

In terms of logic notation, this follows from a general property of predicate formulas:

$$\neg\forall x.\ P(x) \qquad \text{is equivalent to} \qquad \exists x.\ \neg P(x).$$

Similarly, these sentences mean the same thing:

> There does not exist anyone who likes skiing over magma. Everyone dislikes skiing over magma.

We can express the equivalence in logic notation this way:

$$(\neg\exists x.\ Q(x)) \longleftrightarrow \forall x.\ \neg Q(x). \tag{1}$$

The general principle is that *moving a "not" across a quantifier changes the kind of quantifier.*

2.6 Validity

A propositional formula is called ***valid*** when it evaluates to **T**no matter what truth values are assigned to the individual propositional variables. For example, the propositional version of DeMorgan's is that $P \land (Q \lor R)$ is equivalent to $(P \land Q) \lor (P \land R)$. This is the same as saying that

$$[P \land (Q \lor R)] \longleftrightarrow [(P \land Q) \lor (P \land R)]$$

is valid.

The same idea extends to predicate formulas, but to be valid, a formula now must evaluate to true no matter values its variables may take over any unspecified domain, and no matter what interpretation a predicate variable may be given. For example, we already observed that the rule for negating a quantier is captured by the valid assertion (1).

Another useful example of a valid assertion is

$$\exists x \forall y.\ P(x, y) \longrightarrow \forall y \exists x.\ P(x, y).$$

We could prove this as follows:

Proof. Let D be the domain for the variables and P_0 be some binary predicate on D. We need to show that if $\exists x \forall y.\ P(x, y)$ holds under this interpretation, then so does $\forall y \exists x.\ P(x, y)$.

So suppose $\exists x \forall y.\ P(x, y)$. So some element $x_0 \in D$ has the property that $P_0(x_0, y)$ is true for all $y \in D$. So for every $y \in D$, there is some $x \in D$, namely x_0, such that $P_0(x, y)$ is true. That is, $\forall y \exists x.\ P(x, y)$ holds under this interpretation, as required. □

On the other hand,

$$\forall y \exists x.\ P(x, y) \longrightarrow \exists x \forall y.\ P(x, y).$$

is *not* valid. We can prove this simply by describing an interpretation where the hypothesis $\forall y \exists x.\ P(x, y)$ is true but the conclusion $\exists x \forall y.\ P(x, y)$ is not true. For example, let the domain be the integers and $P(x, y)$ mean $x > y$. Then the hypothesis would be true because, given the value of y we could choose x to be $y + 1$, for example. But under this interpretation the conclusion asserts that there is an integer that is bigger than all integers, which is certainly false. An interpetation like this which falsifies an assertion is called a *counter model* to the assertion.

3 Mathematical Data Types

We've been assuming that the concepts of sets, sequences and functions were already familiar ones, and we've mentioned them repeatedly. Now we'll do a quick review of the definitions.

Informally, a ***set*** is a bunch of objects, which are called the ***elements*** of the set. The elements of a set can be just about anything: numbers, points in space, or even other sets. The conventional way to write down a set is to list the elements inside curly-braces. For example, here are some sets:

$$\begin{array}{rcll} \mathbb{N} & = & \{0, 1, 2, 3, \ldots\} & \text{the natural numbers} \\ C & = & \{\text{red}, \text{blue}, \text{yellow}\} & \text{primary colors} \\ D & = & \{\text{Alex}, \text{Tippy}, \text{Shells}, \text{Shadow}\} & \text{dead pets} \\ P & = & \{\{a, b\}, \{a, c\}, \{b, c\}\} & \text{a set of sets} \end{array}$$

The order of elements is not significant, so $\{x, y\}$ and $\{y, x\}$ are the same set written two different ways. Also, any object is, or is not, an element of a given set. It doesn't make sense to think of an element appearing more than once in a set. So writing $\{x, x\}$ is just indicating the same thing twice, namely, that x is in the set. In particular, $\{x, x\} = \{x\}$.

The expression $e \in S$ asserts that e is an element of set S. For example, $7 \in \mathbb{N}$ and blue $\in C$, but Tailspin $\notin D$ yet.

Sets are simple, flexible, and everywhere. You'll find at least one set mentioned on almost every page in these notes.

3.1 Some Popular Sets

Mathematicians have devised special symbols to represent some common sets.

symbol	**set**	**elements**
$\emptyset$	the empty set	none
$\mathbb{N}$	natural numbers	$\{0, 1, 2, 3, \ldots\}$
$\mathbb{Z}$	integers	$\{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$
$\mathbb{Q}$	rational numbers	$\frac{1}{2},\ -\frac{5}{3},\ 16,$ etc.
$\mathbb{R}$	real numbers	$\pi,\ e,\ -9,$ etc.
$\mathbb{C}$	complex numbers	$i,\ \frac{19}{2},\ \sqrt{2} - 2i,$ etc.

A superscript $+$ restricts a set to its positive elements; for example, $\mathbb{R}^+$ denotes the set of positive real numbers. Similarly, $\mathbb{R}^-$ denotes the set of negative reals.

3.2 Comparing and Combining Sets

The expression $S \subseteq T$ indicates that set S is a ***subset*** of set T, which means that every element of S is also an element of T. For example, $\mathbb{N} \subseteq \mathbb{Z}$ (every natural number is an integer) and $\mathbb{Q} \subseteq \mathbb{R}$ (every rational number is a real number), but $\mathbb{C} \not\subseteq \mathbb{Z}$ (not every complex number is an integer).

As a memory trick, notice that the $\subseteq$ points to the smaller set, just like a $\leq$ sign points to the smaller number. Actually, this connection goes a little further: there is a symbol $\subset$ analogous to $<$. Thus, $S \subset T$ means that S is a subset of T, but the two are not equal. So for every set A, $A \subseteq A$, but $A \not\subset A$.

There are several ways to combine sets. Let's define a couple for use in examples:

$$X = \{1, 2, 3\}$$
$$Y = \{2, 3, 4\}$$

- The **union** of sets X and Y (denoted $X \cup Y$) contains all elements appearing in X or Y or both. Thus, $X \cup Y = \{1, 2, 3, 4\}$.
- The **intersection** of X and Y (denoted $X \cap Y$) consists of all elements that appear in *both* X and Y. So $X \cap Y = \{2, 3\}$.
- The **difference** of X and Y (denoted $X - Y$) consists of all elements that are in X, but not in Y. Therefore, $X - Y = \{1\}$ and $Y - X = \{4\}$.

3.2.1 Complement of A Set

Sometimes we are focussed on a particular domain, D. Then for any subset, A, of D, we define $\overline{A}$ to be the set of all elements of D *not* in A. That is, $\overline{A} ::= D - A$. The set $\overline{A}$ is called the ***complement*** of A.

For example, when the domain we're working with is the real numbers, the complement of the positive real numbers is the set of negative real numbers together with zero. That is,

$$\overline{\mathbb{R}^+} = \mathbb{R}^- \cup \{0\}\,.$$

3.2.2 Power Set

The collection of all the subsets of a set, A, is called the ***powerset***, $\mathcal{P}(A)$, of A. So $B \in \mathcal{P}(A)$ iff $B \subseteq A$. For example, the elements of $\mathcal{P}(\{1,2\})$ are $\emptyset, \{1\}, \{2\}$ and $\{1,2\}$.

More generally, if A has n elements, then there are 2^n sets in $\mathcal{P}(A)$. For this reason, some authors use the notation 2^A instead of $\mathcal{P}(A)$.

3.3 Sequences

Sets provide one way to group a collection of objects. Another way is in a ***sequence***, which is a list of objects called ***terms*** or ***components***. Short sequences are commonly described by listing the elements between parentheses; for example, (a, b, c) is a sequence with three terms.

While both sets and sequences perform a gathering role, there are several differences.

- The elements of a set are required to be distinct, but terms in a sequence can be the same. Thus, (a, b, a) is a valid sequence, but $\{a, b, a\}$ is not a valid set.
- The terms in a sequence have a specified order, but the elements of a set do not. For example, (a, b, c) and (a, c, b) are different sequences, but $\{a, b, c\}$ and $\{a, c, b\}$ are the same set.
- The empty set is usually denoted $\emptyset$, and the empty sequence is typically λ.

The product operation is one link between sets and sequences. A ***product*** of sets, $S_1 \times S_2 \times \cdots \times S_n$, is a new set consisting of all sequences where the first component is drawn from S_1, the second from S_2, and so forth. For example, $\mathbb{N} \times \{a, b\}$ is the set of all pairs whose first element is a natural number and whose second element is an a or a b:

$$\mathbb{N} \times \{a, b\} = \{(0, a), (0, b), (1, a), (1, b), (2, a), (2, b), \ldots\}$$

A product of n copies of a set S is denoted S^n. For example, $\{0, 1\}^3$ is the set of all 3-bit sequences:

$$\{0, 1\}^3 = \{(0, 0, 0), (0, 0, 1), (0, 1, 0), (0, 1, 1), (1, 0, 0), (1, 0, 1), (1, 1, 0), (1, 1, 1)\}$$

3.4 Set Builder Notation

One specialized, but important use of predicates is in ***set builder notation***. We'll often want to talk about sets that can not be described very well by listing the elements explicitly or by taking unions, intersections, etc. of easily-described sets. Set builder notation often comes to the rescue. The idea is to define a *set* using a *predicate*; in particular, the set consists of all values that make the predicate true. Here are some examples of set builder notation:

$$\begin{aligned} A &= \{n \in \mathbb{N} \mid n \text{ is a prime and } n = 4k + 1 \text{ for some integer } k\} \\ B &= \left\{x \in \mathbb{R} \mid x^3 - 3x + 1 > 0\right\} \\ C &= \left\{a + bi \in \mathbb{C} \mid a^2 + 2b^2 \leq 1\right\} \end{aligned}$$

The set A consists of all natural numbers n for which the predicate

$$\text{“}n \text{ is a prime and } n = 4k + 1 \text{ for some integer } k\text{”}$$

is true. Thus, the smallest elements of A are:

$$5, 13, 17, 29, 37, 41, 53, 57, 61, 73, \ldots$$

Trying to indicate the set A by listing these first few elements wouldn't work very well; even after ten terms, the pattern is not obvious! Similarly, the set B consists of all real numbers x for which the predicate

$$x^3 - 3x + 1 > 0$$

is true. In this case, an explicit description of the set B in terms of intervals would require solving a cubic equation. Finally, set C consists of all complex numbers $a + bi$ such that:

$$a^2 + 2b^2 \leq 1$$

This is an oval-shaped region around the origin in the complex plane.

3.5 Functions

A ***function*** assigns an element of one set, called the ***domain***, to elements of another set, called the ***codomain***. The notation

$$f : A \to B$$

indicates that f is a function with domain, A, and codomain, B. The familiar notation "$f(a) = b$" indicates that f assigns the element $b \in B$ to a. Here b would be called the *value* of f at *argument* a.

Functions are often defined by formulas as in:

$$f_1(x) ::= \frac{1}{x^2}$$

where x is a real-valued variable, or

$$f_2(y, z) ::= y\texttt{10}yz$$

where y and z range over binary strings, or

$$f_3(x, n) ::= \text{ the pair } (n, x)$$

where n ranges over the natural numbers.

Finite functions can be specified by a table that shows the value of the function at each element of the domain, as in the function $f_4(P, Q)$ where P and Q are propositional variables:

P	Q	$f_4(P,Q)$
T	**T**	**T**
T	**F**	**F**
F	**T**	**T**
F	**F**	**T**

Notice that f_4 could also have been described by a formula: $f_4(P, Q) = [P \longrightarrow Q]$.

A function might also be defined by a procedure for computing its value at any element of its domain, or by some other kind of specification. For example, define $f_5(y)$ to be the length of a left to right search of the bits in the binary string y until a `1` appears, so

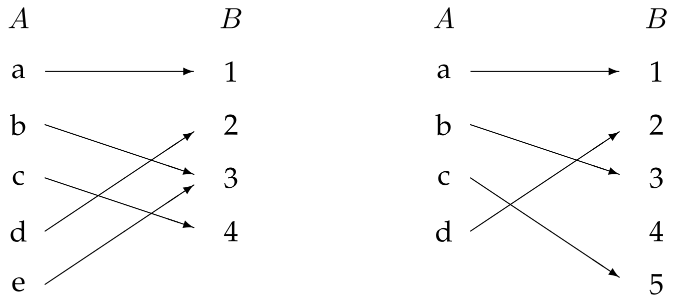
$$\begin{array}{rcl} f_5(0010) & = & 3, \\ f_5(100) & = & 1, \\ f_5(0000) & \text{is} & \text{undefined}. \end{array}$$

There are few properties of functions that will be useful when we take up the topic of counting because they imply certain relations between the sizes of domains and codomains. We say a function $f : A \to B$ is:

- ***total*** if every element of A is assigned to some element of B; otherwise, f is called a ***partial function***,
- ***surjective*** if every element of B is mapped to *at least once*,
- ***injective*** if every element of B is mapped to *at most once*, and
- ***bijective*** if f is total, surjective, and injective. In particular, each element of B is mapped to *exactly once*.

The names "surjective" and "injective" are hopelessly unmemorable and nondescriptive. Some authors use the term ***onto*** for surjective and *one-to-one* for injective, which are shorter but arguably no more memorable.

We can explain all these properties in terms of a diagram where all the elements of the domain, A, appear in one column (a very long one if A is infinite) and all the elements of the codomain, B, appear in another column, and we draw an arrow from a point a in the first column to a point b in the second column when $f(a) = b$. For example, here are diagrams for two functions:



Here is what the definitions say about such pictures:

- "f is a function" means that every point in the domain column, A, has at *most one arrow out of it*. (If more than one arrow came out of any point in the first column, then f would be a *relation*, but not a function. We'll take up the topic of relations in a couple of weeks.)

- "f is total" means that *every* point if the A column has *at least one arrow out of it*, which really means it has *exactly one arrow out of it* since f is a function.
- "f is surjective" means that *every* point in the codomain column, B, has *at least one arrow into it*.
- "f is injective" means that every point in the codomain column, B, has *at most one arrow into it*.
- "f is bijective" means that *every* point in the A column has exactly one arrow out of it, and *every* point in the B column has exactly one arrow into it.

So in the diagrams above, the function on the left is total and surjective (every element in the A column has an arrow out, and every element in the B column has at least one arrow in), but not injective (element 3 has two arrows going into it). The function on the right is total and injective (every element in the A column has an arrow out, and every element in the B column has at most one arrow in), but not surjective (element 4 has no arrow going into it).

Everything about a function is captured by three sets: it domain, its codomain, and the set

$$\{(a, b) \mid f(a) = b\}$$

which is called the *graph* of f. Notice that the graph of f simply describes where the arrows go in a diagram for f.

The graph of f does not determine by itself whether f is total or surjective; we also need to know what the domain is to determine if f is total, and we need to know the codomain to tell if it's surjective. For example, a function defined by the formula $f(x) ::= 1/x^2$, is total if its domain is $\mathbb{R}^+$ but partial if its domain is some set of real numbers including 0. It is bijective if its domain and codomain are both $\mathbb{R}^+$, but neither injective nor surjective if its domain and codomain are both $\mathbb{R}$.

Surjections and injections imply certain size relationships between domains and codomains. If A is a finite set, we let $|A|$ be its size, that is, the number of element in A.

Lemma (Mapping Rule).

- *If $f : A \rightarrow B$ is surjective, then $|A| \geq |B|$.*
- *If $f : A \rightarrow B$ is total and injective, then $|A| \leq |B|$.*
- *If $f : A \rightarrow B$ is bijective, then $|A| = |B|$.*

It's often useful to find the set of values a function takes when applied to the elements in *a set* of arguments. So if $f : A \rightarrow B$, and $A' \subseteq A$, we define

$$\hat{f}(A') ::= \left\{b \in B \mid f(a') = b \text{ for some } a' \in A'\right\}.$$

For example, if we let $[r, s]$ denote the interval from r to s on the real line, then $\hat{f}_1([1, 2]) = [1/4, 1]$.

For another example, let's take the "search for a `1`" function, f_5. If we let X be the set of binary words which start with an even number of `0`'s followed by a `1`, then $\hat{f}_5(X)$ would be the even natural numbers.

Applying $\hat{f}$ to a set, A', of arguments is referred to as "applying f pointwise to A'." The distinction between f and $\hat{f}$ is kind of picky, and it's common practice to omit the hat on $\hat{f}$ and just write f. We'll do this too, since it's usually easy to figure out whether f is being applied to a single argument or pointwise to a set of them. But technically, f and $\hat{f}$ are quite different functions: for example, the domain of $\hat{f}$ is not A, but the set of subsets of A, that is, $\mathcal{P}(A)$, and the codomain of $\hat{f}$ is $\mathcal{P}(B)$.

The set of values that arise from applying f to all possible arguments is called the *range* of f. That is

$$\text{range}\,(f) ::= f(\text{domain}\,(f)).$$

Some authors refer to the codomain as the range of a function, but the distinction between the two is important. The range and codomain of f are the same only when f is surjective.

4 Does All This Really Work?

So this is where mainstream mathematics stands today: there is a handful of axioms from which everything else in mathematics can be logically derived. This sounds like a rosy situation, but there are several dark clouds, suggesting that the essence of truth in mathematics is not completely resolved.

- The ZFC axioms weren't etched in stone by God. Instead, they were mostly made up by some guy named Zermelo. Probably some days he forgot his house keys.

- No one knows whether the ZFC axioms are logically consistent; there is some possibility that one person might prove a proposition P and another might prove the proposition $\neg P$. Then Math would be broken. This sounds like a crazy situation, but it has happened before. At the beginning of the 20th century, the logician Gotlob Frege made an initial attempt to axiomatize set theory using a few very plausible axioms. Several mathematicians— most famously Bertrand Russell[3]— discovered that Frege's axioms actually *were* self-contradictory!

- While the ZFC axioms largely generate the mathematics everyone wants— where $3 + 3 = 6$ and other basic facts are true— they also imply some disturbing conclusions. For example, the Banach-Tarski Theorem says that a ball can be divided into six pieces and then the pieces can be rearranged to give *two* balls, each the same size as the original!

- In the 1930's, Gödel proved that, assuming the ZFC axioms *are* consistent, then they are not *complete*: that is, there exist propositions that are true, but do not logically follow from the axioms. As a matter of fact, the proposition that ZFC is consistent (which is not too hard to express as a formula about sets) is an example of a true proposition that cannot be proved.

  There seems to be no way out of this disturbing situation; simply adding more axioms does not eliminate the problem.

These problems will not trouble us in 6.042, but they are interesting to think about!

[3] Bertrand Russell was a Mathematician/Logician at Oxford University at the turn of the Twentieth Century.
He reported that when he felt too old to do Mathematics, he began to study and write about Philosophy, and when he was no longer smart enough to do Philosophy, he began writing about Politics. He was jailed as a conscientious objector during World War I. He won two Nobel Prizes— one Literature Prize and one Peace Prize.

Russell's Paradox

Reasoning naively about sets quickly leads to the following contradiction— known as Russell's Paradox:

> Let S be a variable ranging over all sets, and define
>
> $$W ::= \{S \mid S \notin S\}.$$
>
> So by definition,
>
> $$S \in W \text{ iff } S \notin S,$$
>
> for every set S. In particular, we can let S be W, and obtain the contradictory result that
>
> $$W \in W \text{ iff } W \notin W.$$

This paradox revealed a fatal flaw in Frege's initial effort to axiomatize set theory. This was an astonishing blow to efforts to provide an axiomatic foundation for Mathematics.

But a way out was clear at the time: *we cannot assume that W is a set*. So the step in the proof where we let S be W is invalid, because S ranges over sets, and W is not a set.

But denying that W is a set means we must reject the axiom that every mathematically well-defined collection of elements is actually a set.

The problem faced by Logicians was how to axiomatize rules determining which well-defined collections are sets. Russell and his colleague Whitehead immediately went to work on this problem and spent a dozen years developing a huge new axiom system in an even huger monograph called *Principia Mathematica*.

The modern ZFC axioms for set theory are much simpler than the Russell/Whitehead system and are close to Frege's original axioms. They specify that sets must be built up from "simpler" sets in certain standard ways. In particular, no set is ever a member of itself. So the modern resolution of Russell's paradox goes as follows: since $S \notin S$ for all sets S, it follows that W, defined above, contains every set. So W can't be a set or it would be a member of itself.

These issues rarely come up in mainstream Mathematics. And they don't come up at all in Computer Science, where the focus is generally on "countable," and often just finite, sets. In practice, only Logicians and Set Theorists have to worry about collections that are too big to be sets.