

SHORT NOTES ON BASIC MATH LANGUAGE

R. OBERLIN

1. MATHEMATICAL PROPOSITIONS

Roughly speaking, a *mathematical proposition* is a sentence or statement which is objectively either true or false. Henceforth we will suppress the word mathematical. Here are three examples:

- A) $1 + 1 = 2$
- B) $2 + 3 = 6$
- C) All odd numbers are divisible by 2

Of course *A* is true and *B* and *C* are false.

There is a basic way to form a new proposition from an old proposition, called *negation*. If *P* is a proposition then the negation of *P*, sometimes denoted $\sim P$, is the proposition which is true when *P* is false and which is false when *P* is true.

Given two propositions *P* and *Q*, there are several ways to form a new proposition, but two of these are perhaps the most natural. The proposition “*P* and *Q*”, denoted $P \wedge Q$, (called the *conjunction* of *P* and *Q*) is the proposition which is true when both *P* and *Q* are true and which is false otherwise. The proposition “*P* or *Q*”, denoted $P \vee Q$, (called the *disjunction* of *P* and *Q*) is the proposition which is true when at least one of *P* or *Q* is true, and false otherwise. We emphasize that $P \vee Q$ is true when $P \wedge Q$ is true, and so our version of “or” is not the “exclusive or”.

In addition to the conjunction and disjunction, there is the proposition “If *P* then *Q*”, sometimes said “*P* implies *Q*” and denoted $P \Rightarrow Q$, which is false when *P* is true and *Q* is false and which is true otherwise. We emphasize that $P \Rightarrow Q$ is true whenever *P* is false. Finally, we have “*P* if and only if *Q*” or “*P* is equivalent to *Q*”, denoted $P \Leftrightarrow Q$ which is true when $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$ is true and which is false otherwise.

To avoid the possible ambiguities and misinterpretations of language, the propositions above are best defined in terms of a truth table:

<i>P</i>	<i>Q</i>	$\sim P$	$P \wedge Q$	$P \vee Q$	$P \Rightarrow Q$	$P \Leftrightarrow Q$
T	T	F	T	T	T	T
T	F	F	F	T	F	F
F	T	T	F	T	T	F
F	F	T	F	F	T	T

Above, T stands for true and F stands for false.

A *propositional formula* is an expression involving finitely many logical connectives (such as $\sim, \wedge, \vee, \Rightarrow, \Leftrightarrow$) and unknown propositions (such as *P, Q, R*). For example, we have the propositional formula

$$\sim(P \wedge \sim Q) \Leftrightarrow (P \Rightarrow Q).$$

The formula above is said to be a *tautology* because it is true regardless of the truth values of the propositions P and Q (Exercise: check this example with a truth table.). If M and N are two propositional formulas and the propositional formula $M \Leftrightarrow N$ is a tautology, then the formulas M and N are said to be *equivalent*. Thus $\sim(P \wedge \sim Q)$ and $P \Rightarrow Q$ are equivalent.

2. METHODS OF PROOF

Often, theorems are propositions (or conjunctions of propositions) of the form $P \Rightarrow Q$ where P and Q are some specific propositions. For example

Theorem 2.1. *If m is an even integer then m^2 is divisible by 4.*

The theorem above is the proposition $P \Rightarrow Q$ with P being “ m is an even integer” and Q being “ m^2 is divisible by 4 (to be completely accurate, it is the conjunction of a collection of propositions, one for each m)”. The theorem may be proved as follows

Proof. Suppose m is an even integer. By definition of even there is an integer n such that $m = 2n$. Then $m^2 = (2n)^2 = 4n^2$. Since n^2 is an integer, we conclude that m^2 is divisible by 4. □

The proof above is a *direct proof* of $P \Rightarrow Q$, because it is of the form “1.) Assume that P is true, 2.) Make some indisputable argument from which we conclude that Q is true.” Sometimes a direct proof is inconvenient; below we present two alternatives.

A *proof by contrapositive* of the proposition $P \Rightarrow Q$ is a direct proof of the proposition $\sim Q \Rightarrow \sim P$. A proof by contrapositive is valid because $P \Rightarrow Q$ and $\sim Q \Rightarrow \sim P$ are equivalent propositional formulas (Exercise: check this with a truth table.), and so in particular $(\sim Q \Rightarrow \sim P) \Rightarrow (P \Rightarrow Q)$. On the other hand, since $(P \Rightarrow Q) \Rightarrow (\sim Q \Rightarrow \sim P)$ a proof by contrapositive is in essence not any harder than a direct proof.

Finally, a *proof by contradiction* of $P \Rightarrow Q$ is a direct proof of the proposition

$$(P \wedge \sim Q) \Rightarrow (R \wedge \sim R)$$

where R is a proposition chosen depending on P and Q which allows the proof. As above, proof by contradiction is a valid and reasonable approach because for any proposition R , we have that $(P \wedge \sim Q) \Rightarrow (R \wedge \sim R)$ is equivalent to $P \Rightarrow Q$. (Exercise: check this; The main idea is that $\sim(R \wedge \sim R)$ is a tautology.)

The distinction between the methods of proof above is slightly artificial. Because of the equivalence of the relevant propositional formulas, you can rewrite (in a possibly ridiculous way) a proof using any one method above as a proof using any other method above. The idea is to choose the method in which the proof is the simplest. Often (especially with beginning students) the first proof conceived is a proof by contradiction, and after trimming away various irrelevant and unnecessary steps it becomes a direct proof or proof by contrapositive.

Another type of “proof by contradiction” (of which the version above is a special case) is to prove that a given proposition L is true by proving the equivalent proposition $(\sim L) \Rightarrow (R \wedge \sim R)$ for some proposition R .

3. QUANTIFIERS

As we saw in Section 1, the “and” and “or” operations produce a new proposition from two given propositions. By iteration, we can define similar operations which produce a proposition from any given finite number of propositions. For example $P_1 \wedge P_2 \wedge P_3$ can be defined $P_1 \wedge (P_2 \wedge P_3)$ (Exercise: check that permuted definitions such as $P_2 \wedge (P_3 \wedge P_1)$ yield the same proposition.). Quantifiers allow us to extend these operations to possibly infinite collections of propositions. Because it is impossible to write down an infinitely long truth table, we will have to define quantified propositions using the language of sets (see Section 4 for the relevant notation and definitions).

Let S be a set whose elements are propositions, and let S' be the set $\{P \in S : P \text{ is true}\}$. The proposition “for all $P \in S, P$ ”; denoted $\forall_{P \in S} P$ is the statement which is true when $S' = S$ and which is false otherwise. The symbol \forall is sometimes called the universal quantifier. When $S = \{P_1, \dots, P_n\}$ is a finite set, one can check that $\forall_{P \in S} P$ is equivalent to the proposition $P_1 \wedge P_2 \wedge \dots \wedge P_n$ alluded to above.

With S, S' as above, the proposition “there exists a $P \in S$ such that P ”; denoted $\exists_{P \in S} P$ is the statement which is false when $S' = \emptyset$ and which is true otherwise. The symbol \exists is sometimes called the existential quantifier. If $S = \{P_1, \dots, P_n\}$ is a finite set then $\exists_{P \in S} P$ is equivalent to the proposition $P_1 \vee P_2 \vee \dots \vee P_n$.

One can check that $\sim(P \wedge Q)$ is equivalent to $(\sim P) \vee (\sim Q)$ and that $\sim(P \vee Q)$ is equivalent to $(\sim P) \wedge (\sim Q)$. Analogous formulas give the negations of propositions formed from general existential and universal quantifiers. Indeed $\sim \forall_{P \in S} P$ is simply saying that $S \neq S'$. If we set $T = \{\sim P : P \in S\}$, then $S \neq S'$ is equivalent to $T' \neq \emptyset$ where $T' = \{Q \in T : Q \text{ is true}\}$. Thus $\sim \forall_{P \in S} P$ is equivalent to $\exists_{Q \in T} Q$. A clearer way to write the last proposition (so that we don't have to define T) is $\exists_{P \in S} \sim P$. Similarly, $\sim \exists_{P \in S} P$ is equivalent to $\forall_{P \in S} \sim P$.

4. SET OPERATIONS

A *set* is a collection of mathematical objects, the objects in the set are called the *elements* of the set. We write $x \in S$ to denote “ x is an element of S .” If a set has only a (small) finite number of elements, it can be described by listing the elements within curly brackets, for example $\{1, 2, 3\}$ is the set whose elements are 1, 2, 3. Otherwise, one must describe the set as the “the set of objects which satisfy some list of properties” (There is actually a slight technical issue here, but it's not really something for a non-logician to worry about; inquiring minds should google Russell's paradox.). For example the even integers are “the set of integers which are divisible by two”, here the first property is “ x is an integer” and the second property is “ x is divisible by two”. Another way to write this is $\{x \in \mathbb{Z} : x \text{ is divisible by two}\}$; here the colon stands for “such that” and \mathbb{Z} stands for the set of integers.

Two sets are *equal* if they have the same elements, for example $\{3, 1, 1, 2, 5, 4\} = \{1, 2, 3, 4, 5\}$ since the elements in each set are 1, 2, 3, 4, 5. A set A is a *subset* of a set B , denoted $A \subset B$ (or $A \subseteq B$), if for all $x \in A$ we have $x \in B$ (in other words if “for all $P \in S, P$ ” is true, where $S = \{“x \in B” : x \in A\}$). The proposition $A = B$ is equivalent to $(A \subset B) \wedge (B \subset A)$; it is often convenient to take advantage of this when proving that two sets are equal, and split the task into the two easier tasks of proving that $A \subset B$ and $B \subset A$. One set of special importance is the set with no elements $\{\}$, called the *empty set* and denoted \emptyset .

The operations “and” and “or” have the following analogues for sets. If A, B are sets then we define the *intersection* of A and B , denoted $A \cap B$, to be $\{x : x \in A \text{ and } x \in B\}$. We define the *union* of A and B , denoted $A \cup B$, to be $\{x : x \in A \text{ or } x \in B\}$. If the intersection of two sets is the empty set, we say that they are *disjoint*.

The *complement* of B relative to A , denoted $A \setminus B$, is the set $\{x \in A : \sim(x \in B)\}$. The *Cartesian product* of A and B , denoted $A \times B$ is the set of all ordered pairs (a, b) such that $a \in A$ and $b \in B$ (here one can define an ordered pair (a, b) to be the set $\{\{a\}, \{a, b\}\}$; the main point is that $(a, b) = (c, d)$ if and only if $a = c$ and $b = d$). Ordered k -tuples for $k > 2$ can be defined recursively in terms of ordered pairs, for example you can set $(x, y, z) = (x, (y, z))$.

In analogy to the existential and universal quantifiers, we can take possibly infinite unions and intersections of sets. Let Ω be a collection of sets (i.e. a set whose elements are sets). We define the intersection over Ω , denoted $\bigcap_{A \in \Omega} A$, to be $\{x : \text{for all } A \in \Omega, x \in A\}$. The union over Ω , denoted $\bigcup_{A \in \Omega} A$, is $\{x : \text{there exists an } A \in \Omega \text{ such that } x \in A\}$.

5. BINARY RELATIONS

A binary relation R is an ordered triple (A, B, G) where A and B are any sets, and where G is a subset of $A \times B$. Then A is called the *domain* of R , B is called the *codomain* of R , and G is called the *graph* of R . We say that $x \in A$ is “ R -related” to $y \in B$ if $(x, y) \in G$.

5.1. Functions. A *function* f from A into B is a binary relation (A, B, G) which has the property that for every $x \in A$ there is one and only one $y \in B$ such that x is f -related to y ; this element y is denoted $f(x)$. Instead of saying “ f is a function from A into B ” one sometimes just writes $f : A \rightarrow B$.

A function f from A into B is said to be *injective* or “one-to-one” if for all $x_1, x_2 \in A$, the proposition $(f(x_1) = f(x_2)) \Rightarrow (x_1 = x_2)$ is true (note that this is sort of a backwards version of the condition in the definition of a function that each x is R -related to “at most one” y). The *range* of f is $\{y \in B : \text{there exists an } x \in A \text{ with } y = f(x)\}$ (a good abbreviated notation for this set is $\{f(x) : x \in A\}$). A function f is said to be *surjective* or “onto” if its range is equal to its codomain (note that this is sort of a backwards version of the condition that for each x there is at least one y is such that x is f -related to y). A function which is both injective and surjective is said to be *bijective* or a “one-to-one correspondence.”

5.2. Equivalence relations. An *equivalence relation* R is a binary relation (A, A, G) which satisfies the following properties. First, every $x \in A$ is R -related to itself; this is called the *reflexive* property. Second, if x is R -related to y then y is R -related to x ; this is called the *symmetric property*. Finally, if x is R -related to y and y is R -related to z then x is R -related to z ; this is called the *transitive* property. For each $x \in A$ the *equivalence class* of x under R , sometimes denoted $[x]$ is the set $\{y \in A : x \text{ is } R\text{-related to } y\}$.

The equivalence classes have two important properties. First every $x \in A$ is in some equivalence class (namely $[x]$, this follows from the reflexive property). Second if $x, y \in A$ then either $[x] = [y]$ or $[x] \cap [y] = \emptyset$ (this follows from the symmetric and transitive properties). Conversely, one can check that any collection of pairwise disjoint sets whose union is A induces an equivalence relation on A .

One example of an equivalence relation is that which is used to define the rational numbers. Let $A = \{(p, q) \in \mathbb{Z} \times \mathbb{Z} : q \neq 0\}$ and $G = \{((p, q), (m, n)) \in A \times A : np = qm\}$. Then we write $\frac{p}{q}$ to denote the equivalence class of (p, q) under the relation (A, A, G) , and the set whose elements are these equivalence classes is the set of *rational numbers*, denoted \mathbb{Q} . One can then check that the addition and multiplication operations $\frac{p}{q} + \frac{m}{n} = \frac{np+qm}{qn}$ and $\frac{p}{q} \cdot \frac{m}{n} = \frac{pm}{qn}$ are “well-defined”, in other words if $\frac{p_1}{q_1} = \frac{p_2}{q_2}$ and $\frac{m_1}{n_1} = \frac{m_2}{n_2}$ then $\frac{n_1p_1+q_1m_1}{q_1n_1} = \frac{n_2p_2+q_2m_2}{q_2n_2}$, and similarly for multiplication.

Another example is given by *cardinality*. Two sets C and D are said to have the same cardinality if there exists a function $f : C \rightarrow D$ which is a bijection. If Ω is any set whose elements are sets, and we define $G = \{(C, D) \in \Omega \times \Omega : \text{there exists a bijection } f : C \rightarrow D\}$ then (Ω, Ω, G) is an equivalence relation (here one would like to take Ω to be the “set of all sets”, but there is a technical problem defining the “set of all sets”, again this is related to Russell’s paradox and to Cantor’s paradox which has to do with the fact in the next paragraph).

A set B is said to be *finite* if it has the same cardinality as $\{1, \dots, n\}$ for some $n \in \mathbb{N} = \{n \in \mathbb{Z} : n > 0\}$. If B is not finite then it is said to be *infinite*. An infinite set which does not have the same cardinality as \mathbb{N} is said to be *uncountable*, an infinite set which has the same cardinality as \mathbb{N} is said to be *countably infinite*. Finally, a set which is either finite or countably infinite is said to be *countable*.

If S is any set and \mathfrak{S} is the set whose elements are the subsets of S , then \mathfrak{S} does not have the same cardinality as S . Suppose for contradiction that $f : S \rightarrow \mathfrak{S}$ is a bijection, and consider $T = \{x \in S : x \notin f(x)\}$. Since f is surjective, there is an $x_0 \in S : f(x_0) = T$. Then by definition of T , if $x_0 \in T$ then $x_0 \notin T$ and if $x_0 \notin T$ then $x_0 \in T$, which is impossible. Note that what we actually use here is that f is surjective, this essentially means that \mathfrak{S} has “larger” cardinality than S .

5.3. Orders. A *partial order* \leq on a set A is a binary relation (A, A, G) which is reflexive, transitive, and *antisymmetric*. The first two properties were defined in the previous subsection, antisymmetric means that if x is \leq -related to y and y is \leq -related to x then $x = y$. We write $x \leq y$ to denote “ x is \leq -related to y ” and $x < y$ to denote $(x \leq y) \wedge (x \neq y)$. A *total order* on A is a partial order which has the additional property that for every $x, y \in A$ we have $x \leq y$ or $y \leq x$.

An example of a total order is the usual \leq on the integers, i.e. $(\mathbb{Z}, \mathbb{Z}, G)$ where $G = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} : x \leq y\}$. An example of a partial order is the subset relation \subset , i.e. if Ω is any set whose elements are sets then $(\Omega, \Omega, \{(C, D) \in \Omega \times \Omega : C \subset D\})$ is a partial order.