Proofs

1 What is a Proof?

A proof is a method of ascertaining truth. But what constitutes a proof differs among fields.

- *Legal* truth is ascertained by a jury based on allowable evidence presented at trial.
- *Authoritative* truth is ascertained by a trusted person or organization.
- *Scientific* truth is hypothesized, and the hypothesis is confirmed or refuted by experiments.
- *Probable* truth is obtained from statistical analysis of sample data. For example, public opinion is ascertained by polling a small random sample of people.
- *Philosophical* proof involves careful exposition and persuasion based on consistency and plausibility. The best example is "Cogito ergo sum," a Latin sentence that translates as "I think, therefore I am." It comes from the beginning of a 17th century essay by the Mathematician/Philospher, René Descartes, and it is one of the most famous quotes in the world: do a web search on the phrase and you will be flooded with hits.

  Deducing your existence from the fact that you're thinking about your existence is a pretty cool and persuasive-sounding first axiom. However, with just a few more lines of proof in this vein, Descartes goes on to conclude that there is an infinitely beneficent God. This ain't Math.

Mathematics also has a specific notion of "proof."

Definition. A *formal proof* of a *proposition* is a chain of *logical deductions* leading to the proposition from a base set of *axioms*.

The three key ideas in this definition are highlighted: proposition, logical deduction, and axiom. In the next sections, we'll discuss these three ideas along with some basic ways of organizing proofs.

2 Propositions

Definition. A *proposition* is a statement that is either true or false.

This definition sounds very general, but it does exclude sentences such as, "Wherefore art thou Romeo?" and "Give me an A!".

But not all propositions are mathematical. For example, "Albert's wife's name is 'Irene' " happens to be true, and could be proved with legal documents and testimony of their children, but it's not a mathematical statement.

Mathematically meaningful propositions must be about well-defined mathematical objects like numbers, sets, functions, relations, *etc.*, and they must be stated using mathematically meaningful terminology, like 'AND' and 'FORALL'. It's best to illustrate this with a few examples about numbers and planar maps that are all mathematically meaningful.

Proposition 2.1. *2 + 3 = 5.*

This proposition is true.

Proposition 2.2. *Let* $p(n) ::= n^2 + n + 41$.

$$\forall n \in \mathbb{N}.\ p(n) \text{ is a prime number}.$$

The symbol $\forall$ is read "for all". The symbol $\mathbb{N}$ stands for the set of *natural numbers*, which are 0, 1, 2, 3, ... (ask your TA for the complete list). The period after the $\mathbb{N}$ is just a separator between phrases.

A *prime* is a natural number greater than one that is not divisible by any other natural number other than 1 and itself, for example, 2, 3, 5, 7, 11, ...

Let's try some numerical experimentation to check this proposition: $p(0) = 41$ which is prime. $p(1) = 43$ which is prime. $p(2) = 47$ which is prime. $p(3) = 53$ which is prime. $\ldots p(20) = 461$ which is prime. Hmmm, starts to look like a plausible claim. In fact we can keep checking through $n = 39$ and confirm that $p(39) = 1601$ is prime.

But if $n = 40$, then $p(n) = 40^2 + 40 + 41 = 41 \cdot 41$, which is not prime. Since the expression is not prime *for all* n, the proposition is false! In fact, it's not hard to show that *no* nonconstant polynomial can map all natural numbers into prime numbers. The point is that in general you can't check a claim about an infinite set by checking a finite set of its elements, no matter how large the finite set. Here are two even more extreme examples:

Proposition 2.3. $a^4 + b^4 + c^4 = d^4$ *has no solution when* a, b, c, d *are positive integers. In logical notation, letting* $\mathbb{Z}^+$ *denote the positive integers, we have*

$$\forall a \in \mathbb{Z}^+ \forall b \in \mathbb{Z}^+ \forall c \in \mathbb{Z}^+ \forall d \in \mathbb{Z}^+.\ a^4 + b^4 + c^4 \neq d^4.$$

Strings of $\forall$'s like this are usually abbreviated for easier reading:

$$\forall a, b, c, d \in \mathbb{Z}^+.\ a^4 + b^4 + c^4 \neq d^4.$$

Euler (pronounced "oiler") conjectured this 1769. But the proposition was proven false 218 years later by Noam Elkies at a liberal arts school up Mass Ave. He found the solution $a = 95800, b = 217519, c = 414560, d = 422481$.

Proposition 2.4. $313(x^3 + y^3) = z^3$ *has no solution when* $x, y, z \in \mathbb{N}$.

This proposition is also false, but the smallest counterexample has more than 1000 digits!

Proposition 2.5. *Every map can be colored with 4 colors so that adjacent*[1] *regions have different colors.*

This proposition is true and is known as the "four-color theorem". However, there have been many incorrect proofs, including one that stood for 10 years in the late 19th century before the mistake was found. An extremely laborious proof was finally found in 1976 by mathematicians Appel and Haken who used a complex computer program to categorize the four-colorable maps; the program left a couple of thousand maps uncategorized, and these were checked by hand by Haken and his assistants—including his 15-year-old daughter. There was a lot of debate about whether this was a legitimate proof: the argument was too big to be checked without a computer, and no one could guarantee that the computer calculated correctly, nor did anyone have the energy to recheck the four-colorings of thousands of maps that was done by hand. Finally, about five years ago, a humanly intelligible proof of the four color theorem was found (see http://www.math.gatech.edu/ thomas/FC/fourcolor.html). [2]

Proposition 2.6 (Goldbach). *Every even integer greater than 2 is the sum of two primes.*

No one knows whether this proposition is true or false. This is the "Goldbach Conjecture," which dates back to 1742.

For a Computer Scientist, some of the most important questions are about program and system "correctness" – whether a program or system does what it's supposed to. Programs are notoriously buggy, and there's a growing community of researchers and practitioners trying to find ways to prove program correctness. These efforts have been successful enough in the case of CPU chips that they are now routinely used by leading chip manufacturers to prove chip correctness and avoid mistakes like the notorious Intel division bug in the 1990's.

Developing mathematical methods to verify programs and systems remains an active research area. We'll consider some of these methods later in the course.

3 The Axiomatic Method

The standard procedure for establishing truth in mathematics was invented by Euclid, a mathematician working in Alexadria, Egypt around 300 BC. His idea was to begin with five *assumptions* about geometry, which seemed undeniable based on direct experience. (For example, "There is a straight line segment between every pair of points.) Propositions like these that are simply accepted as true are called ***axioms***.

Starting from these axioms, Euclid established the truth of many additional propositions by providing "proofs". A ***proof*** is a sequence of logical deductions from axioms and previously-proved statements that concludes with the proposition in question. You probably wrote many proofs in high school geometry class, and you'll see a lot more in this course.

[1] Two regions are adjacent only when they share a boundary segment of positive length. They are not considered to be adjacent if their boundaries meet only at a few points.

[2] The story of the four-color proof is told in a well-reviewed recent popular (non-technical) book: "Four Colors Suffice. How the Map Problem was Solved." *Robin Wilson*. Princeton Univ. Press, 2003, 276pp. ISBN 0-691-11533-8.

There are several common terms for a proposition that has been proved. The different terms hint at the role of the proposition within a larger body of work.

- Important propositions are called ***theorems***.
- A ***lemma*** is a preliminary proposition useful for proving later propositions.
- A ***corollary*** is an afterthought, a proposition that follows in just a few logical steps from a theorem.

The definitions are not precise. In fact, sometimes a good lemma turns out to be far more important than the theorem it was originally used to prove.

Euclid's axiom-and-proof approach, now called the ***axiomatic method***, is the foundation for mathematics today. In fact, there are just a handful of axioms, called ZFC, which, together with a few logical deduction rules, appear to be sufficient to derive essentially all of mathematics.

3.1 Our Axioms

The ZFC axioms are important in studying and justifying the foundations of Mathematics. But for practical purposes, they are much too primitive— by one reckoning, proving that $2 + 2 = 4$ requires more than 20,000 steps! So instead of starting with ZFC, we're going to take a *huge* set of axioms as our foundation: we'll accept all familiar facts from high school math!

This will give us a quick launch, but you *will* find this imprecise specification of the axioms troubling at times. For example, in the midst of a proof, you may find yourself wondering, "Must I prove this little fact or can I take it as an axiom?" Feel free to ask for guidance, but really there is no absolute answer. Just be upfront about what you're assuming, and don't try to evade homework and exam problems by declaring everything an axiom!

3.2 Proofs in Practice

In principle, a proof can be *any* sequence of logical deductions from axioms and previously-proved statements that concludes with the proposition in question. This freedom in constructing a proof can seem overwhelming at first. How do you even *start* a proof?

Here's the good news: many proofs follow one of a handful of standard templates. Proofs all differ in the details, of course, but these templates at least provide you with an outline to fill in. We'll go through several of these standard patterns, pointing out the basic idea and common pitfalls and giving some examples. Many of these templates fit together; one may give you a top-level outline while others help you at the next level of detail. And we'll show you other, more sophisticated proof techniques later on.

The recipes below are very specific at times, telling you exactly which words to write down on your piece of paper. You're certainly free to say things your own way instead; we're just giving you something you *could* say so that you're never at a complete loss.

The ZFC Axioms

For the record, we list the axioms of Zermelo-Frankel Set Theory. Essentially all of mathematics can be derived from these axioms together with a few logical deduction rules.

Extensionality. Two sets are equal if they have the same members. In formal logical notation, this would be stated as:

$$(\forall z.\ (z \in x \longleftrightarrow z \in y)) \longrightarrow x = y.$$

Pairing. For any two sets x and y, there is a set, $\{x, y\}$, with x and y as its only elements.

Union. The union of a collection, z, of sets is also a set.

$$\exists u \forall x.\ (\exists y.\ x \in y \wedge y \in z) \longleftrightarrow x \in u.$$

Infinity. There is an infinite set; specifically, a nonempty set, x, such that for any set $y \in x$, the set $\{y\}$ is also a member of x

Subset. Given any set, x, and any proposition $P(y)$, there is a set containing precisely those elements $y \in x$ for which $P(y)$ holds.

Power Set. All the subsets of a set form another set.

Replacement. The image of a set under a function is a set.

Foundation. For every non-empty set, x, there is a set $y \in x$ such that x and y are disjoint. (In particular, this axiom prevents a set from being a member of itself.)

Choice. We can choose one element from each set in a collection of nonempty sets. More precisely, if f is a function on a set, and the result of applying f to any element in the set is always a nonempty set, then there is a "choice" function g such that $g(y) \in y$ for every y in the set.

We're *not* going to be working with the ZFC axioms in this course. We just thought you might like to see them.

4 Proving an Implication

An enormous number of mathematical claims have the form "If P, then Q" or, equivalently, "P implies Q". Here are some examples:

- (Quadratic Formula) If $ax^2 + bx + c = 0$ and $a \neq 0$, then $x = (-b \pm \sqrt{b^2 - 4ac})/2a$.
- (Goldbach's Conjecture) If n is an even integer greater than 2, then n is a sum of two primes.
- If $0 \leq x \leq 2$, then $-x^3 + 4x + 1 > 0$.

There are a couple standard methods for proving an implication.

4.1 Method #1

In order to prove that P implies Q:

1. Write, "Assume P."
2. Show that Q logically follows.

Example

Theorem 4.1. *If* $0 \leq x \leq 2$, *then* $-x^3 + 4x + 1 > 0$.

Before we write a proof of this theorem, we have to do some scratchwork to figure out why it is true.

The inequality certainly holds for $x = 0$; then the left side is equal to 1 and $1 > 0$. As x grows, the $4x$ term (which is positive) initially seems to have greater magnitude than $-x^3$ (which is negative). For example, when $x = 1$, we have $4x = 4$, but $-x^3 = -1$ only. In fact, it looks like $-x^3$ doesn't begin to dominate until $x > 2$. So it seems the $-x^3 + 4x$ part should be nonnegative for all x between 0 and 2, which would imply that $-x^3 + 4x + 1$ is positive.

So far, so good. But we still have to replace all those "seems like" phrases with solid, logical arguments. We can get a better handle on the critical $-x^3 + 4x$ part by factoring it, which is not too hard:

$$-x^3 + 4x^2 = x(2 - x)(2 + x)$$

Aha! For x between 0 and 2, all of the terms on the right side are nonnegative. And a product of nonnegative terms is also nonnegative. Let's organize this blizzard of observations into a clean proof.

Proof. Assume $0 \leq x \leq 2$. Then x, $2 - x$, and $2 + x$ are all nonnegative. Therefore, the product of these terms is also nonnegative. Adding 1 to this product gives a positive number, so:

$$x(2 - x)(2 + x) + 1 > 0$$

Multiplying out on the left side proves that

$$-x^3 + 4x + 1 > 0$$

as claimed. □

There are a couple points here that apply to all proofs:

- You'll often need to do some scratchwork while you're trying to figure out the logical steps of a proof. Your scratchwork can be as disorganized as you like— full of dead-ends, strange diagrams, obscene words, whatever. But keep your scratchwork separate from your final proof, which should be clear and concise.
- Proofs typically begin with the word "Proof" and end with some sort of doohickey like □ or "q.e.d". The only purpose for these conventions is to clarify where proofs begin and end.

4.2 Method #2 - Prove the Contrapositive

An implication ("P implies Q") is logically equivalent to its *contrapositive* "not Q implies not P"; proving one is as good as proving the other. And often proving the contrapositive is easier than proving the original statement. If so, then you can proceed as follows:

1. Write, "We prove the contrapositive:" and then state the contrapositive.
2. Proceed as in Method #1.

Example

Theorem 4.2. *If r is irrational, then $\sqrt{r}$ is also irrational.*

Recall that rational numbers are equal to a ratio of integers and irrational numbers are not. So we must show that if r is *not* a ratio of integers, then $\sqrt{r}$ is also *not* a ratio of integers. That's pretty convoluted! We can eliminate both "not"'s and make the proof straightforward by considering the contrapositive instead.

Proof. We prove the contrapositive: if $\sqrt{r}$ is rational, then r is rational.
Assume that $\sqrt{r}$ is rational. Then there exists integers a and b such that:

$$\sqrt{r} = \frac{a}{b}$$

Squaring both sides gives:

$$r = \frac{a^2}{b^2}$$

Since a^2 and b^2 are integers, r is also rational. □

5 Proving an "If and Only If"

Many mathematical theorems assert that two statements are logically equivalent; that is, one holds if and only if the other does. Here are some examples:

- An integer is a multiple of 3 if and only if the sum of its digits is a multiple of 3.
- Two triangles have the same side lengths if and only if all angles are the same.
- A positive integer $p \geq 2$ is prime if and only if $1 + (p-1) \cdot (p-2) \cdots 3 \cdot 2 \cdot 1$ is a multiple of p.

5.1 Method #1: Prove Each Statement Implies the Other

The statement "P if and only if Q" is equivalent to the two statements "P implies Q" and "Q implies P". So you can prove an "if and only if" by proving *two* implications:

1. Write, "We prove P implies Q and vice-versa."
2. Write, "First, we show P implies Q." Do this by one of the methods in Section 4.
3. Write, "Now, we show Q implies P." Again, do this by one of the methods in Section 4.

Example

Two sets are defined to be equal if they contain the same elements; that is, $X = Y$ means $z \in X$ if and only if $z \in Y$. (This is actually the first of the ZFC axioms.) So set equality theorems can be stated and proved as "if and only if" theorems.

Theorem 5.1 (DeMorgan's Law for Sets). *Let A, B, and C be sets. Then:*

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

Proof. We show $z \in A \cap (B \cup C)$ implies $z \in (A \cap B) \cup (A \cap C)$ and vice-versa.

First, we show $z \in A \cap (B \cup C)$ implies $z \in (A \cap B) \cup (A \cap C)$. Assume $z \in A \cap (B \cup C)$. Then z is in A and z is also in B or C. Thus, z is in either $A \cap B$ or $A \cap C$, which implies $z \in (A \cap B) \cup (A \cap C)$.

Now, we show $z \in (A \cap B) \cup (A \cap C)$ implies $z \in A \cap (B \cup C)$. Assume $z \in (A \cap B) \cup (A \cap C)$. Then z is in both A and B or else z is in both A and C. Thus, z is in A and z is also in B or C. This implies $z \in A \cap (B \cup C)$. □

5.2 Method #2: Construct a Chain of Iffs

In order to prove that P is true if and only if Q is true:

1. Write, "We construct a chain of if-and-only-if implications."
2. Prove P is equivalent to a second statement which is equivalent to a third staement and so forth until you reach Q.

This method is generally more difficult than the first, but the result can be a short, elegant proof.

Example

The *standard deviation* of a sequence of values $x_1, x_2, \ldots, x_n$ is defined to be:

$$\sqrt{(x_1 - \mu)^2 + (x_1 - \mu)^2 + \ldots + (x_n - \mu)^2}$$

where μ is the average of the values:

$$\mu = \frac{x_1 + x_2 + \ldots + x_n}{n}$$

Theorem 5.2. *The standard deviation of a sequence of values $x_1, \ldots, x_n$ is zero if and only if all the values are equal to the mean.*

For example, the standard deviation of test scores is zero if and only if everyone scored exactly the class average.

Proof. We construct a chain of "if and only if" implications. The standard deviation of $x_1, \ldots, x_n$ is zero if and only if:

$$\sqrt{(x_1 - \mu)^2 + (x_1 - \mu)^2 + \ldots + (x_n - \mu)^2} = 0$$

where μ is the average of $x_1, \ldots, x_n$. This equation holds if and only if

$$(x_1 - \mu)^2 + (x_1 - \mu)^2 + \ldots + (x_n - \mu)^2 = 0$$

since zero is the only number whose square root is zero. Every term in this equation is nonnegative, so this equation holds if and only every term is actually 0. But this is true if and only if every value x_i is equal to the mean μ. □

Problem 1. Reformulate the proof DeMorgan's Law for Sets as a chain of if-and-only-if implications.

6 How to Write *Good* Proofs

The *purpose* of a proof is to provide the reader with definitive evidence of an assertion's truth. To serve this purpose effectively, more is required of a proof than just logical correctness: a good proof must also be clear. These goals are usually complimentary; a well-written proof is more likely to be a correct proof, since mistakes are harder to hide.

In practice, the notion of proof is a moving target. Proofs in a professional research journal are generally unintelligible to all but a few experts who know all the lemmas and theorems assumed, often without explicit mention, in the proof. And proofs in the first weeks of a beginning course like 6.042 would be regarded as tediously long-winded by a professional mathematician. In fact, what we accept as a good proof later in the term will be different from what we consider good proofs in the first couple of weeks of 6.042. But even so, we can offer some general tips on writing good proofs:

State your game plan. A good proof begins by explaining the general line of reasoning, e.g. "We use case analysis" or "We argue by contradiction". This creates a rough mental picture into which the reader can fit the subsequent details.

Keep a linear flow. We sometimes see proofs that are like mathematical mosaics, with juicy tidbits of reasoning sprinkled across the page. This is not good. The steps of your argument should follow one another in a sequential order.

A proof is an essay, not a calculation. Many students initially write proofs the way they compute integrals. The result is a long sequence of expressions without explantion. This is bad. A good proof usually looks like an essay with some equations thrown in. Use complete sentences.

Avoid excessive symbolism. Your reader is probably good at understanding words, but much less skilled at reading arcane mathematical symbols. So use words where you reasonably can.

Simplify. Long, complicated proofs take the reader more time and effort to understand and can more easily conceal errors. So a proof with fewer logical steps is a better proof.

Introduce notation thoughtfully. Sometimes an argument can be greatly simplified by introducing a variable, devising a special notation, or defining a new term. But do this sparingly since you're requiring the reader to remember all that new stuff. And remember to actually *define* the meanings of new variables, terms, or notations; don't just start using them!

Structure long proofs. Long programs are usually broken into a heirarchy of smaller procedures. Long proofs are much the same. Facts needed in your proof that are easily stated, but not readily proved are best pulled out and proved in preliminary lemmas. Also, if you are repeating essentially the same argument over and over, try to capture that argument in a general lemma, which you can cite repeatedly instead.

Don't bully. Don't use phrases like "clearly" or "obviously" in an attempt to bully the reader into accepting something which you're having trouble proving. Also, go on the alert whenever you see one of these phrases is someone else's proof.

Finish. At some point in a proof, you'll have established all the essential facts you need. Resist the temptation to quit and leave the reader to draw the "obvious" conclusion. What is obvious to you as the author is not likely to be obvious to the reader. Instead, tie everything together yourself and explain why the original claim follows.

The analogy between good proofs and good programs extends beyond structure. The same rigorous thinking needed for proofs is essential in the design of critical computer system. When algorithms and protocols only "mostly work" due to reliance on hand-waving arguments, the results can range from problematic to catastrophic. An early example was the Therac 25, a machine that provided radiation therapy to cancer victims, but occasionally killed them with massive overdoses due to a software race condition. More recently, in August 2004, a single faulty command to a computer system used by United and American Airlines grounded the entire fleet of both companies— and all their passengers!

It is a certainty that we'll all one day be at the mercy of critical computer systems designed by you and your classmates. So we really hope that you'll develop the ability to formulate rock-solid logical arguments that a system actually does what you think it does!

7 Propositional Formulas

It's really sort of amazing that people manage to communicate in the English language. Here are some typical sentences:

1. "You may have cake or you may have ice cream."
2. "If pigs can fly, then you can understand the Chernoff bound."

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

4. "Every American has a dream."

What *precisely* do these sentences mean? Can you have both cake and ice cream or must you choose just one desert? If the second sentence is true, then is the Chernoff bound incomprehensible? If you can solve some problems we come up with but not all, then do you get an A for the course? And can you still get an A even if you can't solve any of the problems? Does the last sentence imply that all Americans have the same dream or might they each have a different dream?

Some uncertainty is tolerable in normal conversation. But when we need to formulate ideas precisely— as in mathematics— the ambiguities inherent in everyday language become a real problem. We can't hope to make an exact argument if we're not sure exactly what the individual words mean. (And, not to alarm you, but it is *possible* that we'll be making an *awful lot* of exacting mathematical arguments in the weeks ahead.) So before we start into mathematics, we need to investigate the problem of how to talk about mathematics.

To get around the ambiguity of English, mathematicians have devised a special mini-language for talking about logical relationships. This language mostly uses ordinary English words and phrases such as "or", "implies", and "for all". But mathematicians endow these words with definitions more precise than those found in an ordinary dictionary. Without knowing these definitions, you could sort of read this language, but you would miss all the subtleties and sometimes have trouble following along.

Surprisingly, in the midst of learning the language of logic, we'll come across the most important open problem in computer science— a problem whose solution could change the world.

7.1 Combining Propositions

In English, we can modify, combine, and relate propositions with words such as "not", "and", "or", "implies", and "if-then". For example, we can combine three propositions into one like this:

If all humans are mortal **and** all Greeks are human, **then** all Greeks are mortal.

For the next while, we won't be much concerned with the internals of propositions— whether they involve mathematics or Greek mortality— but rather with how propositions are combined and related. So we'll frequently use variables such as P and Q in place of specific propositions such as "All humans are mortal" and "$2 + 3 = 5$". The understanding is that these variables, like propositions, can take on only the values **T**(true) and **F**(false). Such true/false variables are sometimes called ***Boolean variables*** after their inventor, George— you guessed it— Boole.

7.1.1 "Not", "And" and "Or"

We can precisely define these special words using ***truth tables***. For example, if P denotes an arbitrary proposition, then the truth of the proposition "not P" is defined by the following truth table:

P	not P
T	**F**
F	**T**

The first row of the table indicates that when proposition P is true, the proposition "not P" is false (F). The second line indicates that when P is false, "not P" is true. This is probably what you would expect.

In general, a truth table indicates the true/false value of a proposition for each possible setting of the variables. For example, the truth table for the proposition "P and Q" has four lines, since the two variables can be set in four different ways:

P	Q	P and Q
T	T	T
T	F	F
F	T	F
F	F	F

According to this table, the proposition "P and Q" is true only when P and Q are both true. This is probably reflects the way you think about the word "and".

There is a subtlety in the truth table for "P or Q":

P	Q	P or Q
T	T	T
T	F	T
F	T	T
F	F	F

This says that "P or Q" is true when P is true, Q is true, or *both* are true. This isn't always the intended meaning of "or" in everyday speech, but this is the standard definition in mathematical writing. So if a mathematician says, "You may have cake or your may have ice cream", then you *could* have both.

7.1.2 "Implies"

The least intuitive connecting word is "implies". Mathematicians regard the propositions "P implies Q" and "if P then Q" as synonymous, so both have the same truth table. (The lines are numbered so we can refer to the them later.)

	P	Q	P implies Q, if P then Q
1.	T	T	T
2.	T	F	F
3.	F	T	T
4.	F	F	T

Let's experiment with this definition. For example, is the following proposition true or false?

"If Goldbach's Conjecture is true, then $x^2 \geq 0$ for every real number x."

Now, we told you before that no one knows whether Goldbach's Conjecture is true or false. But that doesn't prevent you from answering the question! This proposition has the form $P \longrightarrow Q$

where P is "Goldbach's Conjecture is true" and Q is "$x^2 \geq 0$ for every real number x". Since Q is definitely true, we're on either line 1 or line 3 of the truth table. Either way, the proposition as a whole is *true*!

One of our original examples demonstrates an even stranger side of implications.

"If pigs fly, then you can understand the Chernoff bound."

Don't take this as an insult; we just need to figure out whether this proposition is true or false. Curiously, the answer has *nothing* to do with whether or not you can understand the Chernoff bound. Pigs do not fly, so we're on either line 3 or line 4 of the truth table. In both cases, the proposition is *true*!

In contrast, here's an example of a false implication:

"If the moon shines white, then the moon is made of white cheddar."

Yes, the moon shines white. But, no, the moon is not made of white cheddar cheese. So we're on line 2 of the truth table, and the proposition is false.

The truth table for implications can be summarized in words as follows:

An implication is true when the if-part is false or the then-part is true.

This sentence is worth remembering; a large fraction of all mathematical statements are of the if-then form!

7.1.3 "If and Only If"

Mathematicians commonly join propositions in one additional way that doesn't arise in ordinary speech. The proposition "P if and only if Q" asserts that P and Q are logically equivalent; that is, either both are true or both are false.

P	Q	P if and only if Q
T	T	T
T	F	F
F	T	F
F	F	T

The following if-and-only-if statement is true for every real number x:

"$x^2 - 4 \geq 0$ if and only if $|x| \geq 2$"

For some values of x, *both* inequalities are true. For other values of x, *neither* inequality is true . In every case, however, the proposition as a whole is true.

The phrase "if and only if" comes up so often that it is often abbreviated "iff".

7.2 Propositional Logic in Computer Programs

Propositions and logical connectives arise all the time in computer programs. For example, consider the following snippet, which could be either C, C++, or Java:

```
if ( x > 0 || (x <= 0 && y > 100) )
    ⋮
    (further instructions)
```

The symbol `||` denotes "or", and the symbol `&&` denotes "and". The *further instructions* are carried out only if the proposition following the word `if` is true. On closer inspection, this big expression is built from two simpler propositions. Let A be the proposition that `x > 0`, and let B be the proposition that `y > 100`. Then we can rewrite the condition this way:

$$A \text{ or } ((\text{not } A) \text{ and } B)$$

A truth table reveals that this complicated expression is logically equivalent to "A or B".

A	B	A or $((\text{not } A)$ and $B)$	A or B
T	**T**	**T**	**T**
T	**F**	**T**	**T**
F	**T**	**T**	**T**
F	**F**	**F**	**F**

This means that we can simplify the code snippet without changing the program's behavior:

```
if ( x > 0 || y > 100 )
    (further instructions)
```

Rewriting a logical expression involving many variables in the simplest form is both difficult and important. Simplifying expressions in software might slightly increase the speed of your program. But, more significantly, chip designers face essentially the same challenge. However, instead of minimizing `&&` and `||` symbols in a program, their job is to minimize the number of analogous physcial devices on a chip. The payoff is potentially enormous: a chip with fewer devices is smaller, consumes less power, has a lower defect rate, and is cheaper to manufacture.

7.3 A Cryptic Notation

Programming languages use symbols like && and ! in place of words like "and" and "not". Mathematicians have devised their own cryptic symbols to represent these words, which are summarized in the table below.

English	**Cryptic Notation**
"not P"	$\neg P$ (alternatively, $\overline{P}$)
"P and Q"	$P \wedge Q$
"P or Q"	$P \vee Q$
"P implies Q" or "if P then Q"	$P \longrightarrow Q$
"P if and only if Q"	$P \longleftrightarrow Q$

For example, using this notation, "If P and not Q, then R" would be written:

$$(P \wedge \neg Q) \longrightarrow R$$

This symbolic language is helpful for writing complicated logical expressions compactly. But in most contexts ordinary words such as "or" and "implies" are much easier to understand than symbols such as $\vee$ and $\longrightarrow$. So we'll use this symbolic language sparingly, and we advise you to do the same.

7.4 Logically Equivalent Implications

Are these two sentences saying the same thing?

If I am hungry, then I am grumpy.
If I am not grumpy, then I am not hungry.

We can settle the issue by recasting both sentences in terms of propositional logic. Let P be the proposition "I am hungry", and let Q be "I am grumpy". The first sentence says "P implies Q" and the second says "(not Q) implies (not P)". We can compare these two statements in a truth table:

P	Q	P implies Q	(not Q) implies (not P)
T	T	T	T
T	F	F	F
F	T	T	T
F	F	T	T

Sure enough, the two statements are precisely equivalent. In general, "(not Q) implies (not P)" is called the ***contrapositive*** of "P implies Q". And, as we've just shown, the two are just different ways of saying the same thing. This equivalence is mildly useful in programming, mathematical arguments, and even everyday speech, because you can always pick whichever of the two is easier to say or write.

In contrast, the ***converse*** of "P implies Q" is the statement "Q implies P". In terms of our example, the converse is:

If I am grumpy, then I am hungry.

This sounds like a rather different contention, and a truth table confirms this suspicion:

P	Q	P implies Q	Q implies P
T	T	T	T
T	F	F	T
F	T	T	F
F	F	T	T

Thus, an implication *is* logically equivalent to its contrapositive, but is *not* equivalent to its converse.

One final relationship: an implication and its converse together are equivalent to an if and only if statement, specifically, to these two statements together. For example,

If I am grumpy, then I am hungry.
If I am hungry, then I am grumpy.

are equivalent to the single statement:

I am grumpy if and only if I am hungry.

Once again, we can verify this with a truth table:

P	Q	(P implies Q) and (Q implies P)	Q if and only if P
T	**T**	**T**	**T**
T	**F**	**F**	**F**
F	**T**	**F**	**F**
F	**F**	**T**	**T**

8 Logical Deductions

Logical deductions or *inference rules* are used to prove new propositions using previously proved ones.

A fundamental inference rule is *modus ponens*. This rule says that a proof of P together with a proof of $P \longrightarrow Q$ is a proof of Q.

Inference rules are sometimes written in a funny notation. For example, *modus ponens* is written:

Rule.

$$\frac{P, \quad P \longrightarrow Q}{Q}$$

When the statements above the line, called the *antecedents*, are proved, then we can consider the statement below the line, called the *conclusion* or *consequent*, to also be proved.

A key requirement of an inference rule is that it must be *sound*: any assignment of truth values that makes all the antecedents true must also make the consequent true. So it we start off with true axioms and apply sound inference rules, everything we prove will also be true.

There are many other natural, sound inference rules, for example:

Rule.

$$\frac{P \longrightarrow Q, \quad Q \longrightarrow R}{P \longrightarrow R}$$

Rule.

$$\frac{\neg P \longrightarrow Q, \quad \neg Q}{P}$$

Rule.

$$\frac{\neg P \longrightarrow \neg Q}{Q \longrightarrow P}$$

SAT

A proposition is **satisfiable** if some setting of the variables makes the proposition true. For example, $P \wedge \neg Q$ is satisfiable because the expression is true when P is true and Q is false. On the other hand, $P \wedge \neg P$ is not satisfiable because the expression as a whole is false for both settings of P. But determining whether or not a more complicated proposition is satisfiable is not so easy. How about this one?

$$(P \vee Q \vee R) \wedge (\neg P \vee \neg Q) \wedge (\neg P \vee \neg R) \wedge (\neg R \vee \neg Q)$$

The general problem of deciding whether a proposition is satisfiable is called ***SAT***. One approach to SAT is to construct a truth table and check whether or not a **T** ever appears. But this approach is not very efficient; a proposition with n variables has a truth table with 2^n lines. For a proposition with just 30 variables, that's already over a billion!

Is there an *efficient* solution to SAT? Is there some ingenious procedure that *quickly* determines whether any given proposition is satifiable or not? No one knows. And an awful lot hangs on the answer. An efficient solution to SAT would immediately imply efficient solutions to many, many other important problems involving packing, scheduling, routing, and circuit verification. This sounds fantastic, but there would also be worldwide chaos. Decrypting coded messages would also become an easy task (for most codes). Online financial transactions would be insecure and secret communications could be read by everyone.

At present, though, researchers are completely stuck. No one has a good idea how to either solve SAT more efficiently or to prove that no efficient solution exists. This is the outstanding unanswered question in computer science.

On the other hand,

Rule.

$$\frac{\neg P \longrightarrow \neg Q}{P \longrightarrow Q}$$

is not sound: if P is assigned **T** and Q is assigned **F**, then the antecedent is true and the consequent is not.

Problem 2. Prove that a propositional inference rule is sound iff the conjunction (AND) of all its antecedents implies its consequent.

As with axioms, we will not be too formal about the set of legal inference rules. Each step in a proof should be clear and "logical"; in particular, you should state what previously proved facts are used to derive each new conclusion.