What's a good mathematical proof (for CMSC 250 purposes)?

Jason Filippou

June 19, 2016

Contents

Abstract

We describe in some detail what constitutes a formal, quality proof for the purposes of CMSC 250, "Discrete Structures" at the University of Maryland Computer Science department. Proof methodologies encountered in this course include direct, indirect proofs for universal statements as well as constructive and non-constructive proofs for existential statements. Indirect proofs are further subdivided into proofs by contradiction and contrapositive, while direct proofs can be

subdivided into many different categories, for instance proofs by division into cases, proofs by exhaustion if the domain is tractable, and classic universal proofs with generic particulars. We give examples of both good and bad proofs and include an FAQ section.

Disclaimers

- There will always be issues and proofs not addressed by this document. Oftentimes, writing clear, concise proofs is as much of an art as it is a science.
- This text has been written as a resource for undergraduate students and it is therefore assumed to be read by such an audience.
- The author is not a mathematician, but rather identifies more as a Computer Scientist with a waning interest in Logic.
- This text will not cover inductive proofs, since other UMD instructors have covered the matter at length and have posted interesting resources.

1 Basic Definitions

We provide definitions for what we consider a statement, a conjecture, a theorem and a corollary. In the process, we also provide some proofs of certain theorems, alluding to certain characteristics of proofs that will be analyzed in more detail in sections 2 and 3.

1.1 Statements

A (mathematical) **statement** will be defined as any sentence in mathematics that is *syntactically* correct . For instance, $1 + 2 = 3$ is a statement. So is $1 + 2 = 2$. Technically speaking, there does not need to exist a notion of "correctness" in a mathematical statement; only the syntax need be correct. $2\ 5\ (-) => -3$ is thus not a statement.

Statements can be either **true** or **false** given established semantics. Proving (or attempting to prove)

In 250, and, particularly, in Number Theory, the mathematical statements that we care about are **quantified** via the **existential** or **universal** quantifier, leading us to **existential** and **universal** statements, respectively.

1.2 Proofs

A **proof** is a sequential application of logical and algebraic rules that shows, beyond any doubt, that a statement is either false or true. Sometimes, the "flow" or "control structure" of proofs can branch into various different cases; that is acceptable as well.

In section 1.7 we will also begin offering examples of proofs. We will examine two kinds of proofs closely:

(i) Direct proofs (section 3)

(ii) Indirect proofs, (section 3)

1.3 Conjectures

A conjecture is a statement that somebody proposes, yet we don't yet have a proof of truth or falsehood. Examples include the Collatz and Golbach conjectures, both of which we have encountered in class. It is common practice to call interesting mathematical statements conjectures which, once we prove true or false, we can then elevate to *theorem* status (section 1.4).

1.4 Theorems

A **theorem** is an *answered* conjecture that can be re-used to prove more theorems. Examples are too numerous: Fermat's Last Theorem, the Infinitude of Primes, $\sqrt{2}$ is irrational, there is no greatest integer, $\forall n^2 \in Z^{\text{even}} \Rightarrow n \in Z^{\text{even}}$, etc.

We already see that theorems can be stated in various different ways: sometimes textually, sometimes entirely with symbols, and sometimes mixed. For example, the following theorems state the exact same thing:

Theorem 1.1. *Squares of odd integers are also odd.*

Theorem 1.2. *If n is an odd integer, n^2 is also an odd integer.*

Theorem 1.3. $(\forall n \in \mathbb{Z}), n \in \mathbb{Z}^{odd} \Rightarrow n^2 \in \mathbb{Z}^{odd}$

Theorem 1.4. $(\forall n \in \mathbb{Z}^{odd}) n^2 \in \mathbb{Z}^{odd}$

The difference between the last two writings of the theorem can be subtle to detect at first: the first version uses the implication ($\Rightarrow$) in order to say that "if n is such that it satisfies the property of membership in $\mathbb{Z}^{\text{odd}}$, then so should its square", while the second one says: "all squares of members of $\mathbb{Z}^{\text{odd}}$ are also in $\mathbb{Z}^{\text{odd}}$". Yet they mention exactly the same thing!

In the Ancient times, especially before we largely settled upon Arabic numerals $(0, 1, \ldots, 9)$ that describe the decimal system, mathematicians would mostly describe theorems using text. Euclid surely did so in his *Elements* while the philosophers Aristotle and Plato would also "codify" logic still using text. People simply did not have the arsenal of symbols that we have today and, even if they did, there was no way they could reach an agreement on the semantics of symbols (there were no conferences, journals, universities...). This might be why, even to this day, many theorems are stated with a lot of text in them. For instance, here's how Fermat's Last Theorem was stated by Pierre de Fermat himself in his famous work *Arithmetica*:

> It is impossible to separate a cube into two cubes, or a fourth power into two fourth powers, or in general, any power higher than the second, into two like powers.[1]

Today we state the theorem with a mixture of symbols and text:

Theorem 1.5. *(Fermat's last theorem, mixed) Let a, b, c and n be positive integers. The equation $a^n + b^n = c^n$ has no non-trivial solutions for $n > 2$.*

[1] Followed by: "I have discovered a truly marvellous proof of this, which this margin is too narrow to contain.". Thanks, Pierre.

Note that in the theorem above, we could've substituted "positive integers" with "naturals". Most people, though, don't use the term "natural" and stick to "positive integers". One example of these people is our very own Evan Golub; he was not even sure what I meant when I mentioned "natural number" to him one day!

If we wanted to state the theorem purely symbolically, we would write something like:

Theorem 1.6. *(Fermat's last theorem, purely symbolically)* $\forall n \in \{2, 3, \dots\} \sim \exists\ a, b, c \in \mathbb{N} : a^n + b^n = c^n$

which reads: "For all n in the set $\{2, 3, \dots\}$ (or: for all n that are integers greater than or equal to 2), there do not exist positive integers a, b, c such that $a^n + b^n = c^n$. [2]

As a rule of thumb, we suggest that **you always translate theorems into purely symbolic statements**. Doing so allows you to perform operations such as contraposition and negations necessary to apply proof by contradiction in a manner that minimizes errors. Furthermore, by having you look over the theorem at least once very carefully, in order to translate it symbolically, this process forces you to examine the theorem closely and make sure you've understood what is stated by it.

1.5 Definitions

A **definition** is a kind of **theorem** that usually introduces an operation or an interesting set of numbers. Since an operation or a set of numbers has to be "well-defined", i.e adhere to some rigorous semantics and some rules (e.g commutativity, associativity, closure, etc), *only theorems can be definitions, not conjectures.* In other words: **Not every mathematical statement out there can be a definition.** Examples:

Definition 1.7. *(Parity of integers) We say that an integer n has **odd parity** (or, simply, that n is **odd**) if and only if there exists an integer k such that $n = 2 \cdot k + 1$. Equivalently, we state that an integer s has **even parity** (or, simply, that s is **even**) if and only if there exists an integer k' such that $n = 2 \cdot k'$.*

Definition 1.8. *(Divisibility) A non-zero integer d **divides** another integer k (denoted $d|k$) if and only if there exists an integer r such that $k = d \cdot r$.*

Definition 1.7 is an example of a definition that hasn't been stated particularly nicely. Theorems should be **court**: they should get to the point without any fuss, like Ancient Spartans did. To that end, adverbs such as "simply" or "equivalently" are to be omitted from theorems. Furthermore, the theorem uses more variables than are absolutely necessary to convey its essence. In fact, it is often the case that mathematicians prefer having *corollaries* (see section 1.6) attached to theorems instead of making the theorems more "verbose" than necessary.

Here's how an Ancient Spartan mathematician would define parity:

Definition 1.9. *(Parity of integers, improved) An integer n has **odd parity** if, and only if, there exists an integer k such that $n = 2 \cdot k + 1$. n has **even parity** if, and only if, it does not have odd parity.*

Corollary 1.10. *(Form of even integers) An integer n has even parity if, and only if, there exists an integer k such that $n = 2 \cdot k$.*

[2] Equivalent statements: the equation $a^n + b^n = c^n$ has no solutions in $\mathbb{N}$, or no positive integer solutions, or no natural solutions.

Definition 1.11. *(Definition of even and odd integers) An integer n is called* ***odd*** *if and only if it has odd parity, otherwise it is called* ***even****.*

You can see from those definitions and the sandwiched corollary that there exists a clear bias towards stating theorems in a succinct way. We prefer many, small and succinct mathematical statements (which we tend to number, so that we can clearly distinguish them from their peers and refer to them later!) over few, complicated mathematical statements that don't have clear "sub-statements" and overflow with useless linguistic boilerplate.

1.6 Corollaries

A *corollary* is a straight consequence of a theorem. They are like "mini-theorems", but which are clearly not important enough to even be called such. In fact, a corollary is always kind of "attached" to a theorem. Corollary 1.10 is an example of the co-existence of corollaries and theorems. Here's another:

Definition 1.12. *(Prime numbers) An integer $p \geq 2$ is called* ***prime*** *if, and only if, its only factors are 1 and itself. An integer $p \geq 2$ is called* ***composite*** *if, and only if, it is not prime.*

Corollary 1.13. *2 is the only even prime number.*

Corollary 1.14. *0 and 1 are neither composite nor prime.*

Great care must be made when writing theorems and attaching corollaries to them. Observe an interesting consequence of writing Definition 1.12 in the following manner (make sure to see where the definition is different from 1.12:

Definition 1.15. *(Prime numbers, incorrect) An integer $p \geq 2$ is called* ***prime*** *if, and only if, its only factors are 1 and itself. An integer p is called* ***composite*** *if, and only if, it is not prime.*

This statement of the theorem makes it possible to define 0, 1 and every negative number as composite numbers.

Could we have written another corollary about how primality is not defined for negative integers? Of course! We just chose not to because we only work in the realm of naturals when talking about primes. The study of primes has been around since Ancient Greece, and Ancient Greeks never developed a theory about negative numbers!

1.7 Lemmas

A *lemma* is the application of a theorem to prove another theorem. Often, the relevant proof is shorter than the proof of the theorem that just took place. Consider the following examples:

Theorem 1.16. *(Odd numbers have odd squares) If n is an odd integer, so is n^2.*

Proof. Let a be a generic particular for the set of odd integers. Then, by the definition of odd parity, there exists an integer k such that $a = 2k + 1$. By basic algebra, we have that $a^2 = (2k + 1) \cdot (2k + 1) = 4k^2 + 4k + 1 = 2k(2k + 2) + 1$. Setting $r = k(2k + 2)$, we

observe that clearly r is an integer, since it's a linear combination of integers.[3] Therefore, $a^2 = 2r + 1$. By the definition of odd numbers, this means that a^2 is odd. Since a was chosen arbitrarily from the set of odd integers, the conclusion holds for every odd n and we have proven our theorem. □

Lemma 1.17. *(Even perfect squares have even square roots[4]) If n^2 is even, then so is n.*

Proof. (By contraposition). We will prove that if n is odd, so should n^2. But theorem 1.16 already proves this. We are therefore done. □

Sometimes, lemmas combine more than one theorem to prove another theorem. Here's a famous example:

Theorem 1.18. *For any integer a and prime p, $p|a \Rightarrow p \nmid (a+1)$*

Proof. (By contradiction) Suppose not. Therefore, there exists an $a \in \mathbb{Z}$ and a $p \in \mathbf{P}$ such that $p|a$ and $p|(a+1)$. By the definition of divisibility (1.8), we have that there exist $k, l \in \mathbb{Z} : a = k \cdot p$ and $a + 1 = l \cdot p \Leftrightarrow k \cdot p + 1 = l \cdot p \Leftrightarrow 1 = p\underbrace{(l-k)}_{r \in \mathbb{Z}} \Leftrightarrow p|1$.
Contradiction, because the only divisors of 1 are 1 and -1, and p, being prime, can be neither. We conclude that the statement can only be true. □

(Observe some interesting things about the proofs we have written so far: They are indirect, and both state their approach in the beginning of their text. This helps the reader follow the proof much easier, and helps the proof author remember to immediately follow up with either a definition of a generic particular for a direct proof, or the form of the contrapositive for a proof by contraposition, or perhaps the statement "suppose not" for a proof by contradiction. Also, because we numbered the theorems those proofs use, we can easily refer to them to keep our proofs shorter. This is standard procedure in all mathematical papers and textbooks; we won't be re-inventing the wheel with every proof.)

After this gentle break on discussing qualitative aspects of proofs, here's the other theorem that we will use:

Theorem 1.19. *Every integer $n > 1$ is divisible by a prime number.*

Proof. (Direct, by division into cases) Let $a \in \{2, 3, \dots\}$ be a generic particular. We consider the cases:

- a is prime. Then, by definition of primality (1.12), $a|a$ and we are done.
- a is composite. By definition of composite numbers (1.12), there exist integers $1 < r_0, s_0 < a$[5] such that $a = r_0 \cdot s_0$. By the definition of divisibility (1.8), this means that $r_0|a$. We have more cases:
  - r_0 is prime. Then, we are done.

[3] A linear combination is any mathematical statement that involves products and sums over constants and variables raised to at most a power 1. So, for example, $2x + y - 3z$ is a linear combination over x, y and z, while $x^3 + y^2 + z$ is not.

[4] Recall the definition of a "perfect square": An integer with an integer square root.

[5] That is a symbolic way of saying the more contrived statement "[...]integers r_0, s_0 between 2 and n-1[..]"

– r_0 is composite. Then, by the definition of composite numbers we have that there exist integers $1 < r_1, s_1 < r_0$ such that $r_0 = r_1 \cdot s_1 \Leftrightarrow r_1 | r_0 \Rightarrow r_1 | a$ because divisibility is transitive.[6] r_1 can then be either prime or composite, so we have the cases [...]

This process can continue indefinitely, until we reach a factor that is prime. This will happen in **finite time**, because every factor is smaller than the number if divides, which means that we will end up with a factor of 1 at some point. Since a was arbitrarily chosen in $\{2, 3, \dots\}$, the conclusion holds for the entire set $\{2, 3, \dots\}$. □

Given theorems 1.18 and 1.19, we can now state the following theorem as their lemma:

Lemma 1.20. *(Infinitude of primes) There are infinitely many primes.*

It is probably mathematical sacrilege to be calling a theorem as important as this a "lemma", but it suits our current purposes. On to the proof:

Proof. (By contradiction) Assume that the statement is false.[7] So the set of primes is assumed to be finite. This means that we can arrange all primes in ascending order and end our arrangement after some finite number of primes, say n primes, like so:

$$p_1, p_2, \dots, p_n$$

Let us now consider the integer $N = p_1 \cdot p_2 \cdot \dots \cdot p_n + 1$. Since the smallest prime $p_1 = 2$, $N > 1$. By this fact, and by theorem 1.19, we deduce that $p_k | N$, for some $k \in \mathbb{N}$.[8] Trivially, $p_k | p_1 \cdot p_2 \cdot \dots \cdot p_n$. By theorem 1.18, this means that $p_i \nmid (p_1 \cdot p_2 \cdot \dots \cdot p_n + 1) = N$. Contradiction. Therefore, the set of primes is infinite. □

(Look at how beautiful this proof is! It is a proof by contradiction which has something of a "constructive" character about it, since, in order to bring a contradiction into the fray, we have to "construct" a particular element. Can you classify the original statement as existential or universal?)

2 Direct proofs

In this section, we outline some points about properly authoring **direct** proofs. Those are typically the hardest proofs we will concern ourselves with, because they usually involve long syllogisms that test our knowledge of existing theorems as well as our deductive capacity and comfort with formal notation. Susanna Epp's book divides them into proofs by exhaustion (when the domain is small enough to do them), proofs by "division into cases" (where we *partition* the domain in non-overlapping parts, which allows us to prove the statement for every sub-domain independently, in a manner often easier than dealing with the entire original domain) and proofs by using the generic particular. We follow this approach to demonstrate some interesting points, but it should be noted that these kinds of proofs are not mutually exclusive: One would typically still encounter generic particulars in a proof by cases, and it's quite likely that a "single-threaded" proof which already operates on one or more generic particulars might branch onto certain "sub-cases" down the road, perhaps introducing new generic particulars for every sub-domain!

[6] We proved that in class.

[7] A fine alternative to "suppose not".

[8] Or, equivalently, "one of the primes, call it p_k, divides N", or "$\exists k \in \mathbb{N} : p_k | N$"

2.1 The Generic Particular

Observe the proof of Theorem 1.16. This proof begins by stating that a is a generic particular for the set of odd integers, and ends by saying that exactly because the statement was proved for a generic particular (that is, a *particular* element of the domain which is *generically*[9] selected), the result has to hold for all the elements of the domain that a represents. Why is this important? Are we being too verbose for the sake of being verbose?

Well... maybe. Or maybe not. Thing is, there exist some fundamental rules that come to us from Predicate Logic and about which we've talked in class: The rules of **Universal Instantiation** and **Universal Generalization**, reminded to us through Table 1.

Universal Instantiation	**Universal Generalization**
$(\forall d \in D)\ P(d)$ $\therefore P(A)$ for any $A \in D$	$(P(A)$ for an arbitrarily chosen $A \in D.$ $\therefore (\forall d \in D)\ P(d)$

Table 1: The Predicate Logic rules of Universal Instantiation and Generalization.

The wording in those rules might appear subtle at first, but you should not let that confuse you. What they are essentially saying can be described by an example. Imagine that one day you wake up and you prepare breakfast. Being late for class or work, you decide to be efficient about it and prepare a bowl of cereal, let's say classic Corn Flakes. Then you pour yourself a healthy dose of milk, and give them a good stir with your spoon such that you soak every flake in the milk.

Universal instantiation tells you: Since **every** flake is soaked in milk, no matter which one you pick with your spoon (provided you had the time to go ahead and examine **all flakes**, with or without repetitions of flakes you've already examined) then it will still be soaked in milk. In this case, the predicate P describes the relationship "soaked in milk". The domain is the entirety of the Corn Flakes in your bowl. We can, in fact, adapt Universal Instantiation to our example, like so:

$$(\forall f \in Flakes)\ Soaked(f, Milk)$$
$$\therefore\ Soaked(Flake, Milk)\ for\ any\ Flake \in Flakes$$

Conversely, at the end of an argument that uses a generic particular, we (implicitly) make use of the rule of Universal Generalization. Since we did, in fact, prove a desired property P for an *arbitrarily* selected element A of the domain, Universal Generalization tells us that we can *generalize* the result to *all* elements of the domain. That is why sometimes people call the application of Universal Generalization as the method of **generalizing from the generic particular**.

In our example, this is how we might adapt the "template" of Universal Generalization:

$$Soaked(Flake, Milk)\ for\ an\ arbitrarily\ selected\ Flake \in Flakes$$
$$\therefore (\forall f \in Flakes)\ Soaked(f, Milk)$$

[9] Alternative characterizations: *Uniformally at random, arbitrarily, agnostically...*

A *non-arbitrary* (*"directed", "planned"*) selection of an element A from the domain *breaks* the rule of Universal Generalization. Suppose that we wanted to prove Theorem 1.19 and started the proof as follows:

Proof. (Direct, by division into cases) Let $a \in \{2, 4, \dots\}$ be a generic particular. Then [...] □

We've already lost. Our generic particular is not generic at all: it's the equivalent of examining our cereal closely, picking out some corn flakes because of, say, some intricate pattern that they have on their surface, pouring them into some other bowl, soaking them in milk and then make the statement that all our flakes are thus soaked.

Such unsafe generalizations happen **all the time**, and not just in mathematics! The validity of public surveys greatly depends upon the sample being what we call *representative* of the population you are *generalizing* the statement of the survey for. George Gallup famously predicted the winner of the 1936 Presidential Election to be the incumbent Franklin Delano Roosevelt instead of the challenger Alf Landon, despite the fact that the prestigious poll *America Speaks* of the popular magazine *Literary Digest* predicted a Landon victory.[10] It did so because it polled people through the phone, often finding their phone numbers from car registration papers. Only wealthy folk could afford phones or cars back then! So the *Digest's* sample was highly **biased**, and the generalization it made was unsafe!

Can you find other such cases of unsafe generalizations in the mainstream media? Try it, and you might be surprised at certain unfounded claims that are often made and believed without much hesitation by the general public.

But back to mathematics. When considering generic particulars, there are additional pitfalls that we can fall into. One of the more common ones concern a misunderstanding about what it means for a *particular* element to also be *generic* or a failure to acknowledge functional relationships between variables. For instance, consider the following two proof segments:

Proof. Let $p, q \in \mathbb{Q}$ be generic particulars. Let also $a, c \in \mathbb{Z}$ and $b, d \in \mathbb{Z}^*$ be generic pariculars such that $p = a/b$ and $q = c/d$ [...] □

Proof. Suppose m, n are generic particulars for the set of odd integers. Then, by definition of odd parity, $m = 2k + 1$ and $n = 2k + 1$ for some integer k. Then [...] □

In the first proof, we are stating that a, c, b and d are generic particulars, but they are clearly not! To be precise, only one of $\{a, b\}$ and one of $\{c, d\}$ can be considered a generic particular. This is because when p and a are given, b is fully defined by them (equiv. for q, c and d). So the statement that those 4 are generic particulars is false.

But those problems don't appear as if they are *big* problems, right? I mean, it seems as if the proof writer just let something slip in terms of *language*, but the fact that he called a variable something that it isn't can probably be forgiven if the result is otherwise sound. Well, in the case of the second proof, the violation that occurs digs deep into the scope of the proof. We can not let the fact that n is constrained to be the **exact same value** as m slide. m and n are declared as generic particulars, but once k is defined as a function of m, it fully defines n, essentially making m be the only generic particular in the problem. Any results to be drawn then will not represent arbitrary pairs of odd integers, but pairs of the same odd integer!

[10] Full story here: http://www.uh.edu/engines/epi1199.htm

2.2 Proof by division into cases and "without loss of generality" statements

Let us consider the following theorem.

Theorem 2.1. *Any consecutive integers have opposite parity.*

We will prove Theorem 2.1 with a direct proof, which follows the principle of **domain partitioning** or, in simpler jargon, **"division into cases"**.

Proof. (Direct, by division into cases) Let a be a generic particular for the set of integers. We distinguish between two cases [11].

- a is even. Then, from the definition of even integers, there exists an integer k such that $a = 2k \Rightarrow a + 1 = 2k + 1$. But this means that the consecutive integer of a, $a + 1$, is odd (by the definition of odd integers). Done.
- a is odd. Through the same argument, there exists an integer k[12] such that $a = 2k + 1 \Rightarrow a + 1 = 2k + 2 = 2(k + 1)$. Let $k + 1 = r$. Clearly, r is an integer. Therefore, $a + 1 = 2r$ and by the definition of even parity, a is even. Done.

So in both cases, we have proven the result for an arbitrarily chosen integer a. This means that the result holds for all consecutive integers. End of proof. □

This proof is straightforward, correct, and showcases a clear application of the logical rules outlined in Table 1. However, it is somewhat tedious. After reading through the first bullet, a person with some comfort with mathematics will likely not go through the second bullet, since he will've already been convinced about the validity of the argument *irrespective of whether a is even or odd*. This is where the popular statement **without loss of generality** (abbrv. **WLOG**) can help out. Let's examine an alternative proof of Theorem 2.1.

Proof. (Direct, by division into cases and WLOG statement)[13]
Let a be a generic particular for the set of integers. **Without loss of generality**, assume that a is even. Then ...

□

You can think of the use of WLOG in the proof above in the following way:

> *"The statement I'm trying to prove would require me to perform a partition of the domain of integers into even and odd integers. However, it is clearly the case that even if I choose a to be odd, then the same algebra will give me the same conclusion. So I might as well save time and use a WLOG statement, because I am indeed not losing* ***any*** *"generality" in my argument. My statement is trivially true*[14] *even in the domain of odds, so I can abbreviate my proof."*

[11] You could also say: "There are two cases", or "Let us then consider some cases", or something of the sort.

[12] Note that you can re-use k here without a "name conflict". Think about k as a "local variable" and cases as "local scopes", as with a high-level programming language.

[13] You don't need to be *that* explicit in your opening proof statements. In fact, please don't. Just stating "Direct", or "Indirect, by contradiction/contraposition" is sufficient.

[14] *Trivial because I made it so, by using algebra that can be applied to evens as much as odds!*

Let us see a case where the WLOG argument might be a bit problematic. Consider our proof of Theorem 1.19. In that proof, every time we examine a dividend (initially, n, then, r_0 and so on), we split our proof into two more cases, depending on whether we assume the dividend to be prime or not.

Using WLOG to say something along the lines of "without loss of generality, we assume that n, (or r_0, or $r_1, \dots$) is composite" would probably not be appropriate here. This is because the two different cases are treated in *radically different manners*: one ends the proof, because a factor divides the dividend by definition of divisibility, and the other one continues it. Using WLOG here would be a statement on your part that tries to say the following:

> *"Ok, so clearly my proof ends whenever I reach a factor that is prime, so in order to push the proof to its more interesting parts, I can say that without loss of generality, my factor is composite."*

The "interesting parts" are only obvious to **you**, because you've written the proof! The reader has no idea what the "interesting parts" are! So don't confuse him by assuming an algebraic symmetry that simply is not there!

If this was indeed your line of thinking about how WLOG ought to be used, don't be disappointed! When you're starting out in Formal Proofs, it is entirely logical and understandable to not be sure about what constitutes symmetry and what does not. In this case, the two pathways that we branch off at every factor are not sufficiently "symmetric" to justify a WLOG argument. At least, that's what the author believes! After all, the arrival at a prime factor is the termination condition for our proof, and we need to give the reader the understanding that this is guaranteed to happen in finite time.

You might think that it might not be obvious to a reviewer of your proof when a WLOG statement "skims over" partitions of the domain that need exactly the same treatment to produce the desired conclusion. This can lead you towards a general rejection of WLOG. Please do not reject this statement on that basis. It is true that in courses such as 250, you should err towards more detail than less, which would make an explicit proof by cases a more attractive option than the use of a WLOG argument. However, as you gain more experience, you will find out that whenever you are sure that a WLOG statement would make your proof more court, you should use one. Writing short proofs and theorems is a highly sought after virtue for mathematicians and Computer Science theorists.

3 Indirect proofs

In this section, we will make some remarks on how to formulate a proof by **contradiction** and **contraposition**, the two kinds of **indirect proof** that we consider in this course.

3.1 Proof by contradiction

Typically, in a proof by contradiction, you will always begin by assuming the negation of the statement that you're trying to prove. Some of those statements will be *"if.... then"* statements, which are described via the implication operator ($\Rightarrow$). Recall that,

when proving implication relationships, it suffices to only prove that the conclusion is true when the premise is true, because of the truth table of implication:

p	**q**	**p ⇒ q**
F	F	T
F	T	T
T	F	F
T	T	T

Table 2: The truth table of implication.

This is exactly what is changed in a proof by contradiction. In such statements, since we want to prove them by contradiction, i.e, by contradicting what it's saying, by *challenging* it, **we have to assume a true premise and a false conclusion**.

This is a point where students confuse themselves a lot. They think that, in order to perform a proof by contradiction of an implication relationship, they need to formulate the statement to be proven in propositional logic, and then "negate" that entire implication. This is simply not true; by the truth table of implication (Table 2, assuming a true premise and a false conclusion is the only way to go. Hopefully, through valid rules of logic or algebra, we will then reach a contradiction c, and we will done. Why? But, because of the propositional logic **law of contradiction**:

$$\sim p \Rightarrow c$$
$$\therefore p$$

The contradiction might show up in something that has to do with the premise which we assume to be true or not, in which case the premise is usually leveraged to build the logic that leads us towards the contradiction. A good example is the proof of Theorem 1.18: the premise is used to derive a multiplicative relationship which, in conjunction with a similar relationship derived by our (assumed true) conclusion, leads us to a contradiction that has to do with the primality of p.

Here's an example of a proof where the contradiction encountered is "tied" to the premise:

Theorem 3.1. *If a is irrational, so is $-a$.*

Proof. (By contradiction) Assume not. So $-a$ is rational. This means that $\exists k, l \in \mathbb{Z}, l \neq 0$, such that $-a = \frac{k}{l}$. But this would mean one of two things:

(i) $a = \frac{-k}{l} \Rightarrow a \in \mathbb{Q}$ by definition of rationals $\Rightarrow a \notin \mathbb{R} - \mathbb{Q}$. Contradiction.

(ii) $a = \frac{k}{-l}$. **Through an argument similar to the one made above**, we reach a contradiction.

So $-a$ cannot be rational, and the statement has been proven. □

Note how we cut the division into cases short here. We have already been sufficiently formal and precise in the first case; there's no need to repeat the exact same argument just

because the minus sign was moved to the denominator! That would be useless boilerplate now, wouldn't it?

In the proof of Theorem 3.1, the contradiction that we reach is essentially a statement that the premise would have to be false if the conclusion were fals as well. Take a minute to understand what this says: what's it telling us is that, in all possible worlds where the conclusion is false, then so is the premise! In other words, *it is not possible for a world to exist where the conclusion is false and the premise is true*: so, in all possible worlds, the implication holds (Table 2)! For all these reasons, when attempting a proof by contradiction, we must negate *just the conclusion*. Not the premise, not the entire implication.

3.2 Proof by contraposition

Proofs by contraposition are definitely more rare than proofs by contradiction. They are only applicable in statements that can be formulated as statements of form "If p, then q", since those are logically equivalent to their **contrapositive**: "If not q, then not p."

The only real challenge in such a proof is negating one's statements properly. This might be tricky to do when theorems are stated verbosely. Let's consider two examples:

Theorem 3.2. *For all integers m and n, if $m + n$ is even, then m and n are either both even or both odd.*

First of all, and just to get it out of the way, it is possible to prove this statement directly via a division into cases, like so:

Proof. (**Direct** proof of Theorem 3.2) Since the theorem assumes all integers m, n such that $m + n$ is even, let us assume generic particulars a, b such that $a + b$ is even. By the definition of even parity, this means that there exists an integer k such that:

$$a + b = 2k \Rightarrow a = 2k - b \tag{1}$$

We distinguish between the following cases:

(i) b is even. Then, there exists an integer r such that $b = 2r$. Substituting this result into (1) we retrieve: $a = 2\underbrace{(k - r)}_{s\in\mathbb{Z}} = 2s$, which means that a is also even.

(ii) b is odd. Then, there exists an integer ℓ such that $b = 2\ell+1$. Substituting this result into (1) we retrieve: $a = 2\underbrace{(k - \ell)}_{s\in\mathbb{Z}} - 1 = 2s - 1 = 2s - 2 + 1 = 2\underbrace{(s - 1)}_{q\in\mathbb{Z}} + 1 = 2q + 1$, which means that a is also odd.

We conclude that a and b **must** have the same parity. The conclusion was drawn for arbitrarily selected integers a, b, so it holds for all integer pairs m, n. We are done. □

*Note how meticulous we have to be in case (b), where we have to bring a exactly to the format of an odd number. We haven't proven that an odd number is odd if we can write it in the format $2k \pm 1$, but only in the format $2k + 1$; we must therefore strive to bring our expression for a in **exactly** that format.*

So now that we have established that the theorem is provable in a direct setting, let us examine the indirect setting, via contraposition. To use proof by contraposition, it

might help if we translated some of the facts stated as propositional symbols. Let p be a propositional symbol that denotes the fact "$m + n$ is even". Let us also come up with propositional symbols z and q that denote the facts "m (resp. n) is even". Then, we can refactor our statement as: $p \Rightarrow (z \Leftrightarrow q)$.

We can now start thinking about how we can prove this by contraposition. The negation of the bi-conditional is the "exclusive OR" operator $\oplus$, therefore, the contrapositive can be written as: $(z \oplus q) \Rightarrow \sim p$

Now things are becoming somewhat clearer. We want to prove that if one of m or n is even and the other is odd, then their sum is guaranteed to be **odd**. **Not even**, don't confuse yourselves (that would be the **converse error**)! So I will constrain one of m or n to be odd, and the other to be even. Does it really matter which is which? Not really, since integer addition is commutative! Therefore:

Proof. (Proof of Theorem 3.2 by contraposition) **Without loss of generality**, assume that m is odd and n is even. Let $a \in \mathbb{Z}^{\text{odd}}$ and $b \in \mathbb{Z}^{\text{even}}$ be generic particulars. By definition of odd and even parity respectively, there exist integers k, ℓ such that $a = 2k+1$ and $b = 2\ell$. Ergo, $a + b = 2\underbrace{(k + \ell)}_{s \in \mathbb{Z}} + 1 = 2s + 1$, which means that $a + b$ is odd. Since a and b were arbitrarily chosen from their respective domains, the result holds for every single odd and even integer, respectively. □

You might have noticed that the proof by contraposition was smaller than the direct proof. Why do you think this is? Our thought is that it's probably because the symmetry that required to be explicitly shown by cases in the direct proof could be simplified through a generality argument in the indirect proof. Indeed, it does not matter which one among m and n is the even and odd integer respectfully; while, on the direct proof, there's a bit more algebra in the case where b is assumed to be odd, which makes it mathematically necessary to write down both cases.

Here is another example theorem that proves the necessity of properly parsing the theorem to form a valid contrapositive:

Theorem 3.3. *If the product of two positive real numbers is greater than 100, then one of those numbers is greater than 10.*

Observe an important point about the wording of this theorem; it needs you to prove that one of the numbers in question is greater than 10. Does this mean that exactly one ought to be such? Of coutse not; they could both be! Consider, for instance, 20 and 11; their product is 220, which is greater than 100.

Proving Theorem 3.3 by contraposition would first require that we parse the theorem symbolically, in the form of an implication:

Theorem 3.4. $\forall r_1, r_2 \in \mathbb{R}^+,\ r_1 r_2 > 100 \Rightarrow (r1 > 10) \vee (r_2 > 10)$

We can do work now. The contrapositive of this theorem would then be:

Theorem 3.5. $\forall r_1, r_2 \in \mathbb{R}^+,\ (r_1 \leq 10) \wedge (r_2 \leq 10) \Rightarrow r_1 r_2 \leq 100$

Proof. Let a, b be generic particulars for the interval $(0, 10)$. [15] Then, since both a and b are positive, we can multiply the respective sides of the two inequalities like so:

[15] If you're not familiar with interval notation, this interval covers all reals between 0 and 10, including neither 0 nor 10.

$$\left.\begin{array}{l} a \leq 10 \\ b \leq 10 \end{array}\right\} \Rightarrow ab < 10^2 = 100.$$

□

Some students are sometimes confused and think that, with contraposition and the negation of the premise, the universal quantifier should change to an existential one because we are also negating it. **But we're not!** The contrapositive of a universal statement is still a universal statement; after all, it's a *logically equivalent statement*. The equivalences that we established in class, summarized in Table 3, concern logical equivalences that connect the negation of *entire universal and existential statements*.

$$\sim(\forall x \in D)\ P(x) \equiv \exists x \in D\ (\sim P(x))$$
$$(\sim\exists x \in D)\ P(x) \equiv \forall x \in D\ (\sim P(x))$$

Table 3: Logical equivalences between universal and existential statements on a predicate P, and variables $\mathbf{x}$ with joint domain D.

4 F.A.Q

4.1 Should I use text or symbols?

Some text is guaranteed to be in your proofs. For instance, in proofs by contradiction, you are going to at least write "contradiction". But, depending on your style of proving things, you might opt for more symbols than text. For example, the statement "For every pair of odd integers" can be translated into : $\forall a, b \in \mathbb{Z}^{\text{odd}}$.

In fact, it is often very useful to translate text into symbols. This makes sure that we understand the statement better! Consider the following example:

Theorem 4.1. *Even perfect squares have even square roots.*

Upon looking at this theorem, a student might get a little nervous, thinking that they might have to delve into machinations that involve the ugly square root sign. Not really! Consider the symbolic translation of this theorem:

Theorem 4.2. $\forall n \in \mathbb{Z},\ n^2$ *is even* $\Rightarrow n$ *is even.*

Since n is guaranteed to be an integer, we trivially cover the fact that n^2 is a perfect square.

The symbolic translation makes the use of contraposition as a proof methodology very straightforward.[16] On the other hand, the theorem now looks kind of ugly. Even its mental translation: *For all n in the integers, if "n squared" is even, that implies that n is even*, can be characterterized as overly verbose when compared to the textual version shown at 4.1. Each approach has its pros and cons.

The author has a small preference for writing symbol-heavy proofs. This has been a result of using many symbols back in his highschool number theory courses, in order to acquire familiarity with them. Using symbols is also probably a better approach when dealing with Set Theory problems, since we avoid the repetitive expression: "[...] the set of [...]". In fact, the statement of Russel's Paradox:

[16] The theorem can also be proven **directly**: can you find a direct proof?

Theorem 4.3. *(Russel's Paradox, textual) Does the set of all sets that don't contain themselves contain itself?*

The textual description of this paradox, while court, is very confusing. The only way in which we can possibly begin to understand what's going on is to translate it into symbolic algebra:

Theorem 4.4. *(Russel's Paradox, symbolic) Let* $S = \{x | x \notin x\}$. *Then,* $S \in S \Leftrightarrow S \notin S$.

However, when **reading** proofs, it's probably more pleasing to read them in textual form! Consider, for instance, the statement of Theorem 1.20. Is it more interesting and eye-opening to read *"There are infinitely many prime numbers"*, *"The set* $\mathbf{P}$ *has infinite cardinality?"* or $|\mathbf{P}| = \aleph_0$? When reading proofs, the author tends to appreciate textual proofs more. However, when encountering a theorem or a lemma that doesn't appear to be very obvious, he likes to translate the statement into symbols in order to understand it better, perhaps followed by attempting a proof.

4.2 How much text?

Not much at all. **You should use as much text as is absolutely necessary to prove your logical statements**. Recall our critique of definition 1.7. In that definition, there existed english words that conveyed an "informal", elementary school - like essense to the proof. We would like to avoid those.

But the important question with regard to text is: "Have I used enough text to convince the reviewer of my proof that it is valid?" The answer to this question for 250 is easy: **always opt for more detail**. For instance, when dealing with a composite number n, always state that it can be written in the form $n = k \cdot l$ for some integers k and l between 2 and $n - 1$[17], **by the definition of composite numbers**. By doing so, you train your brain in recognizing the theorems that you depend on, and you can also weed out any mistakes that you might be making. It is probably safe to say that, in 250, the only facts that we don't prove are quite elementary, for instance the closure of integers under addition[18] (which, of course, straightforwardly leads to closure under multiplication) or the irrationality of $\sqrt{2}$ (which we prove after we assume true, since it requires some familiarity with proof by contradiction). So those might, in fact, be the only things that are trivial enough for you to not have to mention in your proofs.

4.3 In proof by cases, do I need lists?

We suggest that you do, for the following reasons:

- It makes the partitioning of the domain clear to both you and your proof reader. In outlining your proof in list form, you can discover errors in your partitioning (overlaps or subsets of the domain you missed).
- As you're writing your second list-item, you might discover that the argument you're making is symmetric to the first one, which would make the application of a WLOG statement appropriate.

[17] Technically, the interval is $\{2, 3, \ldots, \lfloor \sqrt{n} \rfloor\}$, but we haven't discussed this in class.
[18] There actually exists a **direct** proof of this, using Modular Arithmetic!

- Nobody likes a lot of text, particularly in mathematical documents, which are usually filled with them. It feels good towards the eye to be able to break the sequential flow of sentences and paragraphs and have something else to deal with for a while.

For instance, consider the proof of Theorem 1.19. Here's what the proof would look like if we didn't use a list format and opted exclusively for text:

Proof. (Alternative style proof of Theorem 1.19) Let $a \in \{2, 3, \dots\}$ be a generic particular. Then, a will be either prime or composite. If a is prime, then we are done, since clearly $a|a$, by divisibility primitives. If a is composite, by definition of composite numbers (1.12), there exist integers $1 < r_0, s_0 < n$ such that $n = r_0 \cdot s_0$. By the definition of divisibility (1.8), this means that $r_0|a$. If r_0 is prime, we are done. If not, by definition of composite numbers, we have that there exist integers $1 < r_1, s_1 < r_0$ such that $r_0 = r_1 \cdot s_1 \Leftrightarrow r_1|r_0 \Rightarrow r_1|a$ because divisibility is transitive. r_1 can then be either prime or composite. If it is prime [...]. □

It's not hard to see that, while it is true that this proof might take less lines of text to write, it is also much harder to parse! For this reason, we recommend lists, numbered or bulleted.

4.4 Is it really important to end my proof?

Yes.

4.5 How much "self-containment" do I want?

Refer to question 4.2 above.

4.6 Underbraces: When to use them?

You should probably avoid the use of underbraces; it's just a technique that the author uses in order to save whiteboard and notebook space. The problem with underbraces is that, while they avoid somewhat superfluous phrases of type *"Let x be* — whatever an underbrace would otherwise 'hug' — ", they cause some problems with typesetting. In LaTeX, for instance, the line underneath the line that uses an underbrace (if not empty) will have to be automatically moved down by a small amount, in order to account for the space for the underbrace, even if the underbrace itself has no text underneath it. This, of course, happens in all WYSIWYG editors (such as MS Word) as well; the line spacing will have to locally adjust itself despite the global settings set by the user.

Furthermore, if you follow a flowing, textual style of proof, letting go of it temporarily in favor of using a rather contrived symbol is probably not the way to go. So, while we choose to follow this approach, e.g in the proof of Theorem 1.18, you should also practice the more textual approach of explicitly setting new variables to some construct.

4.7 If I beat down a man in a soundproof torture hall, does he make any noise?

That would depend on whether you are within the torture hall or outside of it (since the torture hall is soundproof, we can reasonably assume that it is a sealed space surrounded

by some walls or glass panes and can therefore make a clear division between "inside" and "outside"). If you are outside of it, then you will not perceive the man making any noise. If you are inside it, there exist two cases: either the man is making noise or he is not. In the latter case, presumably the man is dead. So there does not exist an answer to this question.

5 Recap

We can recap the entire discussion by agreeing on the following "rules" about what a good proof should be and what it should (and shouldn't) contain. For 250 grading purposes, you can assume that if your proof does not adhere to one of these requirements, it can only get partial credit! In fact, if your proof does not adhere to the first requirement, it probably won't even get *any* credit!

(i) A proof should be **correct**. That is, even if the theorem one is trying to prove holds, it is still possible to write an incorrect proof (see common pitfalls in Section 2). If a proof is incorrect, any discussion about other aspects of it go out the window. Correctness is of **paramount importance**.

(ii) It should also be **self-contained**. That is, it should not make unreasonable assumptions about the reader's knowledge. For instance, consider the proof of lemma 1.20. Would the proof steps be clear to you if it did not mention its heavy dependence on theorems 1.19 and 1.18?

You might then make the reasonable question: *"When do I know that I've mentioned enough?"* This is a problem that comes up even in the best Theoretical Computer Science or Mathematics conferences! Authors assume that their proofs depend upon stuff that is general knowledge, and sometimes reviewers either don't know that stuff or are not comfortable with authors assuming that they *should* know that stuff (that's Academia for you, folks). So you might ask questions such as: *"Is it really necessary for me to mention that an odd integer a can be written in the form $a = 2 \cdot k + 1$ for some k in a proof **by definition of odd numbers**", or should I just say 'a is odd, so $a = 2k + 1$ for some k [...]' and be done with it?*

In 250, you should always err towards greater detail. Later on, as you get more experience with both mathematical proofs as well as submitting proofs for peer review, you will be able to find a nice balance.

(iii) You should **always** state your proof strategy **at the beginning of the proof**. A small statement such as "by contradiction / contraposition" or "directly" suffices.

(iv) In proofs by contradiction, you should **always clearly state the fact that a certain statement you reached produces a contradiction**. Simply saying "Contradiction", followed or preceded by the reason for which the statement is contradicting, suffices.

(v) You should always **clearly end your proof**. Using phrases such as "We have thus proved/disproved the statement" or "This concludes our proof", or "QED", or the use of the "QED" symbol (□) suffice.

(vi) You should **avoid useless boilerplate**, particularly when going for a more "flowing", text-heavy style of proof. Not only do superfluous statements make your proof harder to parse, but they also allow you room for error, which might make the reviewer of your proof believe that you have misunderstood something, negatively predisposing him towards your proof, your manuscript, and perhaps even your person.