Notes on
Propositional Calculus

by Charles Lin

1 Introduction

Most of you have taken your share of math courses. Whether you've taken high school algebra or geometry, or courses in calculus, you've probably learned math by solving math problems. Hopefully, you've even liked doing math and are good at it. As abstract as math can be for some, there's some fun in solving problems.

It usually comes as a surprise to students, especially those who've liked math in high school and even college to realize that solving problems is not typically what mathematicians do. In general, mathematicians aren't interested in solving problems once the technique has been established. Instead, they're either interested in looking for new techniques to solve problems or just to *prove* interesting facts about math. Some of those facts are rather profound, and might be nearly impossible to explain to the typical layperson– even a well-educated layperson.

Mathematicians are usually interested in proving theorems, which are facts shown to be true, in some logical system. Mathematics is fascinating in this regard compared to science. In science, theories are validated through observation of the physical world. Even in a highly mathematical field like physics, a theory is only good if there are observations which validate the theory.

Einstein's theory on gravitation was shown to be true based on experimental results on light received from the planet Mercury (I believe). If a physical theory doesn't accurately predict what happens in the physical world based on experiments, then that theory isn't very good. (It's a misconception to say Einstein disproved Newton. He simply produced a theory that had much more accurate results in unusual situations. Newton's theories are still good in many respects).

In fact, what's surprising about physics is that mathematics does such a spectacular job describing physical phenomena such as light, electricity, magnetism, optics, etc. After all, mathematics is very much a human invention. It's a testament to human ingenuity that the physical world can be explained by math symbols and solving certain equations.

Although mathematics has often used physical sciences, especially physics, to drive its theoretical development, many study mathematics on an abstract level. For example, number theory is the study of interesting properties of numbers, such as how often prime numbers appear or prime twins appear (prime twins are two prime numbers separated by 2, e.g. 29 and 31 are prime twins).

Many mathematicians study such problems because they find it interesting in its own right, not because it has any practicality in the real world. Occasionally, some areas

of mathematics that were originally thought to be very abstract (not dealing much with the real world) have been used in physics, years after the mathematics was formally developed. Thus, sometimes even without meaning to, the study of mathematics leads to something that can be "practically" used.

As I said earlier, mathematicians are often in the business of stating and proving theorems. Sometimes the theorems are what's interesting, and sometimes it's the techniques used to prove the theorem that's interesting (because it can serve as the basis to prove other theorems).

If mathematics is abstract, and not always based on physical phenomena, then how do mathematicians convince each other that what they say is true? For example, Fermat's Last Theorem states that for $n \geq 2$, there are no positive integer solutions to the equation $a^n + b^n = c^n$ (note: when $n = 2$, this is the familiar Pythagorean Theorem which has an infinite number of positive integer solutions). How might you prove this? Perhaps the only technique you might think of is brute force substitution.

Even though you could plug in as many numbers as you want, and never find values for a, b, and c, that doesn't prove Fermat's Last Theorem true. (In fact, until this theorem was proved by Andrew Wiles, it was more accurately called Fermat's Last Conjecture. The word *theorem* implies that is has actually been proved). For example, some conjectured that $a^4 + b^4 + c^4 = d^4$ has no positive integer solutions (notice its similarity to Fermat's Last Theorem). However, until recently, no one could prove that either. Then, in the late 1980s, a mathematician proved this conjecture was wrong by providing a counterexample (he found positive values for a, b, c, and d which satisfied the formula).

Even in the face of overwhelming empirical evidence that Fermat's Last Theorem was true, this was still not a proof. No one (until Andrew Wiles, that is) could say, for certain, that this conjecture was true. Mathematicians are generally not interested in whether something is true, most of the times, or true as far as someone can tell. They want to be sure that something is true all of the time. How can they do this without resorting to *brute force* (which is the technique of trying everything exhaustively)?

2 Proofs

Unlike science, where observation is used to validate theories, mathematics doesn't rely on observation. To establish mathematical facts (often called *theorems*), you provide a *proof*. A proof usually starts with some set of assumptions, then given well-established proof rules, it proceeds to derive other facts, eventually working its way to proving the theorem. Because the proof rules are well-established and mathematicians agree that these proof techniques work, they can convince each other of the veracity of a theorem.

Even though mathematicians are more careful about proving things that the average person, and are therefore more sure of what they say, they, too, can get a little lazy. When writing proofs, mathematicians will make statements which they hope other well-read mathematicians will believe based on their knowledge of mathematics, and therefore, they don't have to explain it in excruciating detail. They can "skip steps", and still be sure that a good mathematician can fill in the missing steps.

Of course, humans skips steps all the time. Pick up any cookbook, the recipes will often assume a great deal. For example, they assume you know where to find the vegetables and meats needed and how to select good quality. They assume you know what it means to marinate something or how to grate cheese or how to julienne or sautee. They don't sit and explain "common errors in sauteeing food", even as this might be useful to novice cooks.

Mathematicians make assumptions that their reader knows a lot of math, and can take certain statements as fact. They assume the reader will know what technique is being applied, because all mathematicians should know it. Despite this apparently sloppiness, mathematicians can, in principle, simply fill in the missing steps and double check the work. Of course, sometimes these "obvious steps" which aren't proved are at the root of a proof not really being a proof. For example, when Andrew Wiles first presented with his proof, several mathematicians started going through the steps of his monumental proof (it was said to be around 100 pages long). Wiles apparently applied a technique under the wrong constraints. At first, he thought he could fix the problem with a little work, but it eventually took him almost a year, and going back to an older technique to resolve the difficulties of the proof and fix it so it was kosher.

Proofs are the way that mathematicians convince one another that what they say is true, and because mathematicians know the rules, they can independently verify other people's theorems. (Admittedly, some of the mathematics is *so* difficult, that only a handful of mathematicians can verify it, although the process of verifying a proof is easier than the proof itself). Some mathematicians feel that mathematics is superior to science in that respect. The facts they prove will be good forever, while a physics "proof" may be challenged when some observational data doesn't seem to support the known theories (which is why Einstein's theory of gravity replaced Newton's).

The technique of proofs have lead to the surest body of knowledge, i.e. mathematical theorems, that humans have created. Surprisingly, the basics structure of proofs aren't all that difficult to understand. You don't even have to be a genius to understand proofs nor to prove basic theorems. In fact, you will be learning about the basics in this (and a future) tutorial.

3 Why Prove?

So what? That's probably what you're thinking. I want to be a programmer, you say. Why do *I* need to know any of this math? Let the mathematicians deal with it. I'll just program.

There are several reasons why you should learn how to prove things. First, believe it or not, there are computer scientists who rarely program and are essentially doing math. For example, some computer scientists are interested in developing efficient algorithms (e.g., sorting algorithms). Those algorithms are often put in actual practice because they are so efficient. Others are interested in developing models of computation or interested in the limits of what can be computed. While these are all very theoretical topics, there are occasionally a few students who like this, and we would be remiss in not teaching it.

Even if you believe you'll never be such a theoretician, it's even good to be aware of the

basics of algorithms and why they work, and for that you need a solid understanding of discrete mathematics. Being a computer science major, even being a college student is not just about training you to be a programmer and getting jobs that pay the big bucks. (And even then, a solid understanding of discrete mathematics can help you be a better programmer–really!).

Academics tries to balance the ideal with the practical. On the one hand, most students attend college because they believe they are being trained for well-paying jobs (or in the case of English, for jobs). The original goals of college, at least, in the past century or so, was to give students a "classical" education, modeled after ancient Greek education. A well-educated person (alas, typically male and probably well-to-do) was expected to master foreign languages, mathematics, sciences, literature and history. This training wasn't meant to get a person a job.

It was just what every educated person was expected to know so they be well-versed in conversation. Later on, it was felt a well-rounded liberal arts training helped you to think, write, and organize your thoughts, and that such training would be good for a wide variety of jobs, even as this kind of education might not train you for job-specific skills. This is still the basis for making students, even computer science, take courses in the humanities.

Similarly, many computer scientists also feel that any well-educated computer scientists need to know the theoretical aspects of computer science. Even if you never get good at discrete math and proofs, at least you're good enough to handle the basics. And hopefully, you learn to think more mathematically, which ultimately to think more precisely and to state assumptions clearly.

There are even several practical reasons to learn theory. Mathematics has achieved a lot throughout the ages. Physicists have used math to explain various phenomena of the world. Chemists, biologists, even social scientists use math as an integral part of their work. But mathematics, in and of itself, has lead to the study of logic.

Logic is the study of reasoning. In the early days of Greek society, philosophers often pondered the meaning of truth. What is truth? How do we determine truth? They even thought that one could determine truth by applying techniques of reasoning in a similar way to applying math to solve problems. Over the years, this evolved to modern day logic.

Logic forms the basis by which mathematical proof is done. Some see it as the foundation of mathematics. We study logic for two reasons. The first is to understand how logic works. Logic gives us a precise way of reasoning. Although logic was often used to reason about statements and determine whether someone was telling the truth or not, it has been applied far more successfully as the foundations for proving mathematical statements.

It turns out that humans, as a whole, reason rather poorly. Logic gives us a sound way to make logical arguments, especially when it comes to mathematics. Furthermore, logic makes a great way to train one's mind in solid, rational reasoning.

Mathematics also has given the world a precise language for expressing ideas. Mathematicians discovered long ago that natural languages, such as English, was ambiguous. A certain sentence could be interpreted in one of many ways. By using mathematical symbols, defined in precise ways, mathematicians could say what they meant far more precisely. Even when mathematicians wrote in a natural language like English, it was a

formal kind of English filled with phrases like “such that”, “there exists”, “if and only if”. Mathematicians try to state their theorems precisely and concisely.

The average computer science student often has a great deal of problems expressing themselves accurately. A typical student will mumble something about their code not working, and something not printing, and the code just is broken. This information is often next to useless. What would be far more useful is to demonstrate exactly what cases were being tested, what worked so far, and what has already been successfully tested, and to phrase that as accurately as possible, without delving into the details of the code itself.

One of the biggest benefits of learning math, especially if you learn it properly is that you are expected to state things precisely and concisely. Ambiguity leads to confusion, and that’s not where you want to be. Even though it’s easy to tell students “learn to be clear, learn to be precise”, it’s skill that many students find incredibly difficult to master.

I’ve met very few students who can clearly state the problem with their program without resorting to “Just look at my program, I can’t explain it”. Students been working on your program for so many hours, and despite that, they can’t tell you exactly what they mean when their program doesn’t work, and worse yet, they often have no idea why it doesn’t work, not have any established methodology to find the errors. (To be fair, even though I think debugging relies on common sense, I suspect this common sense is difficult to learn, because it requires a lot of work that most students aren’t prepared to expend).

Let me give you some advice. *Learn to explain it*. This will be one of the harder things you will ever learn, but that should not stop you. You must try and try to find clearer ways of expressing yourself. This skill is vital if you really want to succeed as a computer scientist, and just to succeed in general.

4 Getting Started

Perhaps that pep talk has convinced you that logic and math is well worth studying. Even if it hasn’t, you don’t have much of a choice. This course is required, so you might as well learn it the best you can. Perhaps time, and some success with writing proofs will open your eyes to this fascinating area of computer science, and perhaps, just maybe, you might be good at theory too. Really.

Usually the study of logic proceeds in two parts. Initially, you learn propositional calculus and having mastered that, you proceed to predicate calculus. This is very similar to learning C, then progressing on to C++. While propositional calculus isn’t nearly as useful as predicate calculus, the basic techniques carry over into predicate calculus, which is why you learn it first.

At this point, you’re probably wondering why I use the word *calculus*. Are you going to compute integrals and derivatives? No. The word “calculus” is actually more general. It only means “a method of calculating”. In fact, you really study *differential* calculus (methods of calculating derivatives) and *integral* calculus (methods of calculating integrals). Thus, propositional calculus is a method to compute with propositions and predicate calculus is a method to compute with predicates.

To begin, we'll study PROP, the language of propositional calculus. It's a simple language, far simpler than C or C++. This language tells us which statements are syntactically valid, and which are not.

The language consists of the following symbols.

propositional variables (also called Boolean variables). These are lowercase, alphabetic letters, possibly with numeric subscripts.

logic connectives This consists of the following connectives: $\wedge$, $\vee$, $\sim$, $\rightarrow$, and $\leftrightarrow$.

parentheses Left and right parentheses.

These are the rules for valid propositional statements. By valid, I mean that if there were such a thing as a propositional statement "compiler", these would compile and be recognized as valid. If the propositional statement is valid (meaning it is syntactically correct), we say it is *well-formed*.

1. All propositional variables are well-formed.
2. If α is well-formed, then so is $\sim \alpha$.
3. If α and β are well-formed, then so are $(\alpha \wedge \beta)$, $(\alpha \vee \beta)$, $(\alpha \rightarrow \beta)$, and $(\alpha \leftrightarrow \beta)$. Notice the use of parentheses.

If you followed the rules exactly, you would discover that some propositions would not be considered well-formed, even though you think they ought to be. For example, $p \wedge q$ is not well-formed, however $(p \wedge q)$ is. Although the language has strict rules as to what is well-formed and what isn't, you are permitted to be "sloppy" as long as you realize there is a well-formed equivalent to the statement you are writing.

You may also note that PROP forces $\sim$ to have the highest precedence (just underneath parentheses), but says nothing about the precedence of any of the other connectives. Thus, in general, you should not assume that $\wedge$ has higher precedence than $\vee$ which has higher precedence than $\rightarrow$ which finally has higher precedence than $\leftrightarrow$. (Realistically, people do make such assumptions about precedence, but not everyone remembers these rules nor do the necessarily believe precedence ought to be ranked in that order, so to avoid problems, you're usually better off adding enough parentheses to make yourself clear).

5 Arguments

What is an argument? An *argument* consists of statements, written in PROP. Some of these statements are called *premises* and represent the assumptions you make. One statement is referred to as the conclusion. Usually, you write an argument as:

$$\begin{array}{l} q \\ q \rightarrow r \\ \hline \therefore r \end{array}$$

The premises are written above the horizontal line, and the conclusion is written below the line.

An *argument* is said to be valid when the conclusion is true for all possible truth assignments that make the premises true. If there are no truth assignments which make all the premises true, then the premises are said to be inconsistent, and the argument is said to be *vacuously true*.

What does it intuitively mean if the premises are inconsistent and why does that make the argument true? Suppose I told you "If you give me 100,000 dollars, and the weather is 72 degrees on May 1, and the wind is 2 mph heading east, then I will complete Boston marathon in world record time on that day". You might say, "No way, that's not true". However, I would say, but those conditions didn't exist on that day, so you have to give me the benefit of the doubt.

Of course, you might complain and say that you don't have to give me the benefit of the doubt, that even if such conditions were to exist, there would still be no way I could complete the marathon in world record time. However, I could still say, "I don't care. The conditions weren't provided to me, and you can't say I was lying". Logic is like that. It's rather optimistic. If the premises can't be made true, then we optimistically say that the argument is valid.

Perhaps a more compelling argument that is also vacuously true runs like "If one student in the class gets above 150 on the final, then everyone will receive an A in the course". However, suppose I say that the maximum allowed score on the final is 100, and so no one will get 150. If no one received an A, would you say I was lying? You would say, of course not. Yet, it's the same idea as before. The premises can't be satisfied, and therefore I'm not lying by not giving everyone A's.

But you might claim there is indeed a difference between the two arguments. In the second case, you'd say if it were somehow possible that someone did get 150 (say, because we changed our mind and made the test out of 200), then I'd be forced to give everyone A's. That is, it seems reasonable to give everyone A's, in a world where a score of 150 were permissible, while it seems ludicrous to believe, even under perfect conditions that I could break a world record, no matter what.

However, logic doesn't make those distinctions. In both cases, the premises could not be made true, and therefore in both cases, the argument is valid. In logic, there is no notion of "even were the premises true, the conclusion is so preposterous that it could never ever be true". Logic says "when the premises can't be made true, the argument is valid". Thus, we treat every argument just like the second one above (about giving everyone A's). It wouldn't make sense to create a logic that actually looks at the meaning of the sentences and attempts to determine when, say, the conclusion is possibly true and possibly false, versus, false no matter what happens. Logic isn't nearly that flexible, and frankly it doesn't have to be.

At this point, I'm dwelling on a point that probably doesn't need to be dwelled on all that long. After all, most arguments we're interested in will have some truth assignments that make the premises true, and under such circumstances, it will also make the conclusion true too.

6 Proving Arguments Using Truth Tables

How do we tell if an argument is valid or not? There are two ways to show this. The first way, which we'll briefly cover now, is using truth tables. The second way is to use proof rules. We'll spend most of our time using proof rules.

How do you show an argument is valid using truth tables? Here are the steps.

1. Create columns for each of the input variables.
2. Create columns for each of the premises and one for the conclusion.
3. Fill out the truth table.
4. Look for *critical rows*. These are the rows for which all the columns with the premises contain T.
5. Look at the column for the conclusion. If it is always T in the critical rows, then the argument is valid. If there is even one F, then the argument is invalid.

Notice that we only care about critical rows. Only the rows where all the premises are true are considered. If there is a row that contains even one F for a premise, then we ignore that row. It may turn out that there are no critical rows, in which case, the argument is vacuously true. After all, we said an argument is true when every critical row has a T in the conclusion. If there are no critical rows, then the argument is true.

This is analogous to saying "I will give a candy bar to everyone in the room". If no one is in the room and I hand out no candy bars, I could claim that I was telling the truth. Similarly, when I say "A statement is true when every single critical row has a T in the column for the conclusion." If there are are no critical rows (which is analogous to having no students in the room", then it's OK for the conclusion to be either T or F.

The book does a reasonably good job of showing how you can show arguments are valid using truth tables, and so I won't dwell on it anymore. Instead, we'll show you how to show a statement is valid by applying proof rules.

7 Proving Arguments Using Proof Rules

While truth tables give you a nice, easy way to do proofs, they aren't very insightful. You would write a program to fill out truth tables. Furthermore, if there are a large number of variables, the truth table could get very large. Nevertheless, if you're really, really stuck, you might at least verify an argument is true via truth tables.

Mathematicians simply don't write their proofs using truth tables. Instead, they use proof rules. The proof rules have to be *sound*. That is, given a set of premises which are consistent (i.e., which are not contradictory—there is some assignment of truth values to input variables which make all premises true), then the proof rules will only allow you to conclude other facts that are consistent with the premises. On the other hand, if premises

are not consistent (i.e., it contains a contradiction somewhere), the proof rules will prove more contradictions. As bad as that sounds, it actually isn't disastrous. The techniques do work.

We will use the 'T' technique to write proofs. Here is an example of part of a proof.

1	p	Assume
2	$p \to q$	Assume
3	$q \to r$	Assume
3	r	MP (steps 1,2)
	...	
	...	

Each line of a proof is numbered. The statements that appear above the horizontal bar are assumptions. In fact, they are usually just the premises given to us from the argument (recall that an argument consists of premises and a conclusion). Just copy the premises to the top of the horizontal bar, and write in the word "Assume" (or "Given", if you prefer). In the 'T' proof technique, assumptions always appear above the horizontal bar, and represent facts which we accept, without justification. Steps 1, 2, and 3 are listed as assumptions.

Every step below the bar needs to be justified (except statements that are assumed to be true, in a subproof—we'll see this later), meaning we need to provide a reason for why that fact is true. This is the part where you actually prove something, and requires you to think (although once you master the techniques, it's not that bad). Step 4 is a statement which was justified by a rule (in this case, the proof rule was *modus ponens*).

The justification for each statement beneath the horizontal bar can come one of two places: we can apply logical equivalences to rewrite a statement to a logically equivalent form, or we can apply proof rules which permit us to conclude new facts from previous proved (or assumed) facts. For example, *modus ponens* is a proof rule. In both cases, you must refer to previous steps (unless you plan to introduce new assumptions—that will be discussed next section).

Essentially, a proof is a sequence of true statements that follow from the premises. That is, once you assume that the premises are true, then the proof rules (or logical equivalences) guarantee every subsequent fact to be a true *consequence*. Notice I use the word *consequence*. Basically, in logic, there are some facts that are always true. These are called tautologies (for example, $p \vee \wedge p$ is a tautology). Then, there are facts that are proven true, provided other facts are true.

Step i of a proof is true, provided the premises are true. Each step of a proof proves new facts, from facts already proven to be true. Thus, if I claim p is true, then I must justify it by some rule, and then show which previous steps I derived the fact from. The previous steps may come from previously justified steps (earlier in the proof) or from the assumptions above the horizontal bar.

7.1 Proof Rules vs. Logical Equivalences

Below the horizontal line, each statement must be justified with either a proof rule or a logical equivalence. What's the difference between the two. If two statements are logically equivalent, then you can substitute one for the other. For example, suppose you have proven $(p \to q) \wedge r$. It turns out that $p \to q$ is logically equivalent to $\sim p \vee q$. So, you can substitute $\sim p \vee q$ into $(p \to q) \wedge r$ to get $(\sim p \vee q) \wedge r$

On the other hand, a proof rule produces facts which follows from other rules. For example, suppose you have $p \vee q$. Then, the rule "Conjunctive Simplification" says that you can conclude p. However, $p \wedge q$ is not logically equivalent to p (to show this, let p by T and q be F. $p \wedge q$ is F while p is T). Even though p is a logical consequence of $p \wedge q$, it is not a logical equivalence, which means you can't substitute p for $p \wedge q$ in a more complicated statement.

To illustrate, suppose you had the following statement: $(p \wedge q) \to r$. p could stand for "I water my plants" and q could stand for "The weather is sunny", and r could mean "my plants will grow". Thus the statement says "If I water my plants and the weather is sunny, then my plants will grow".

Now, p can be proved from $p \wedge q$ using Conjunctive Simplification. p is called a logical consequence of $p \wedge q$. Still, it would be incorrect to substitute $p \wedge q$ with p to get $p \to r$. This new statement says that "If I water my plants, then it will grow". That's not something you can conclude from "If I water my plants and the weather is sunny, then my plants will grow".

That's the key difference between logical equivalence and proof rules. Logical equivalences are much stronger. You can substitute a statement with any logically equivalent statement. However, you can't substitute a statement with a statement derived from a proof rule.

The list of logical equivalences and proof rules are given in a separate handout. You should print that up and learn them

7.2 Goal of Proof

When you are writing a proof, your goal is to eventually reach the conclusion of the argument, and have that conclusion be justified. The conclusion is the last step of the proof (after all, once it's proved, why do any more work afterwards?).

1	p	Assume
2	$p \to q$	Assume
3	$q \to r$	Assume
	...	
	...	
n	r	Justification

Thus, in this example, you want to eventually prove r, which will be the last step of the proof.

Since this is the last step, I often write what I plan to prove near the top, just to remind me where I am headed with the proof.

Prove: r

1	p	Assume
2	$p \to q$	Assume
3	$q \to r$	Assume
	...	
	...	
	...	

Every step below the horizontal must be justified. This includes providing the proof rule/logical equivalence, plus the steps you are applying it on.

1	p	Assume
2	$p \to q$	Assume
3	$q \to r$	Assume
4	q	MP (steps 1, 2)
5	r	MP (steps 3, 4)

Steps 4 and 5 were justified. In both cases, the proof rule *modus ponens* was applied, and the steps on which they were applied were shown. If you want to save some writing, you can omit the word "step" from the justification. For example, you can write "MP (1, 2)" as the justification for step 4 of the proof, which means *modus ponens* applied on steps 1 and 2. It also doesn't matter which order you list the numbers (although we could have created rules that were nitpicky and forced you to write the numbers in a particular order). Thus, "MP (2, 1)" would have been a valid justification too.

7.3 Some Terminology

Let's define some terminology so I can easily refer to them later on.

Proof header These are the statements written above the horizontal line. They are the assumptions, and only have to be justified with the word "Assume" (or "Given").

Proof body These are the statements written below the horizontal line. They are statements which need to be justified with reasons using either proof rules or logical equivalences.

8 Introducing New Assumptions—Subproofs

Suppose you wanted to make more assumptions, in addition to the premises that you can already assume to be true. Is this permitted? The proof technique allows you to introduce assumptions—*any assumption*—you want, provided it appears in its own 'T' (which I will

draw as more of an 'E'). For example, suppose you wanted to assume q, you would write it as:

1	p	Assume
2	$p \to q$	Assume
3	$q \to r$	Assume
4	q	MP (steps 1, 2)
5	$\sim r$	Assume
i	...	...
	...	...
j	...	...
k	r	Justification

In order to introduce a *new* assumption, you create a new E. Above the horizontal bar, you add the new assumption (see step 5 above). Why introduce a new assumption? Why introduce an E? When you are asked to prove something, you are given premises. Those are your only assumptions. You have to expect that, to make new assumptions, requires some restrictions. There are no restrictions to when you can make an assumption, but there are restrictions to what you can conclude from this new assumption. (If there weren't, you'd simply assume what you had to prove, and you'd be done—obviously, it isn't that simple).

When you introduce a new assumption, you are allowed to use any previous assumptions (although there are restrictions). In particular, you can always use the premises, which were the original assumptions.

What have you done? You are starting of a *subproof*. This allows you to introduce new assumptions, and derive new conclusions.

8.1 Levels of a Proof

In order to explain subproofs, I need to introduce the idea of *levels of a proof*. When you start a proof, you begin with level 1 assumptions (which are the premises) and start proving facts below the horizontal line. If you do not introduce any new assumptions, these facts will be called *level 1 statements*.

Key observation *The* ***conclusion*** *of a proof must appear as a level 1 statement*

Suppose you are in the middle of level 1 statements, and you wish to introduce a new assumption. This means you are starting a new subproof (we'll shortly discuss what can be proved when you begin a new subproof). When you create a new subproof, you start at a proof at one level higher than the current one you're working on. Thus, if you were in a level 1 proof, then introducing a new 'E' creates a level 2 subproof.

Just like the level 1 proof, the level 2 subproof consists of assumptions (which appear above the horizontal line) and statements that need justification. In the previous example, a

subproof was started at step 5 and the subproof concludes at step j. The assumption appear at step 5. Everything between line i and j must be justified. You are allowed to use the assumptions in step 4 (a level 2 assumption) as well as the assumptions in the premises (level 1 assumptions). In fact, you are also allowed to use any level 1 statements proved earlier on. For example, since q was proved in step 4 (a level 1 statement), you may use that fact in steps i through j.

In general, suppose you are in the middle of a level n proof. You want to start a new assumption, which means you begin a new subproof (with the 'E'). This subproof is called a level $n+1$ subproof.

When you start a level $n+1$ subproof, you are nested in a level n subproof, which is nested in a level $n-1$ subproof etc. Thus, at level $n+1$ subproof, there are n active subproofs from level 1 up to level n.

You may use any assumptions in the active subproofs, as well as any statements proved earlier. However, a subproof may become inactive, in which case you can no longer use the statements. Here's an example.

1	p	Assume
2	$p \to q$	Assume
3	$q \to r$	Assume
4	q	Assume
i	...	...
	...	...
j	$s \wedge t$	...
j + 1	s	...
k	r	Assume
k + 1	...	...
	...	...
m	...	...
n	s	Justification

Step 4 began a level 2 subproof. This ended at step j. A subproof ends whenever you want it to (although, again, I'll provide rules that let you know when you would want to stop a subproof). Once a subproof ends, you go back to an outer proof. For example, step j was the last statement of a level 2 proof. Step $j+1$ returns back to level 1 proof and is therefore a level 1 statement. Thus, closing off a proof at level $n+1$ returns you back to a level n proof.

8.2 There's a Catch

Once a subproof is closed off, it is considered inactive, and you can no longer use any results within the subproof (there is an exception, which we'll discuss soon) outside of the subproof. For example, in step j, $s \wedge t$ was "proven". However, you can't use that step to justify step $j+1$ since step $j+1$ is a level 1 proof. A level 1 proof can't use steps from an

inactive subproof.

Why not? $s \wedge t$ (see step j) was derived *assuming* step 4 was true. Thus, we derived $s \wedge t$ with *additional assumptions* beyond the premises (steps 1–3). When the subproof ended at step j, the assumption at step 4 also ended. We return back to a level 1 proof, using the premises as our only assumptions.

Every level 1 statement is derived using *only* the premises and no other assumptions. Level 2 statements are proved using Level 1 assumptions *and* any assumptions made when the level 2 subproof was introduced. In general, a level n subproof assumes every assumption from level 1 to level $n-1$ that the proof is nested in.

> ***Key observation*** *A level n proof is always nested inside an active level $n-1$ proof which is nested inside an active $n-2$ proof, etc., which is finally nested in a level 1 proof. The level n proof may use all assumptions from level 1 to level n that is is nested in, as well as any statements proved within any of these outer enclosing proofs in earlier steps.*

Notice that once a proof is closed off, any results can't be used later on (at least, not yet). Thus, at step $k+1$, you can't use any of the steps from steps i to j because i to j appear in a proof that was closed off at step j (and thus became an inactive proof). You can use the results at step $j+1$ in the subproof starting at step $k+1$ because that is a level 1 statement and level 1 statements are always part of an active proof. In general, if you are in a level n proof, you may use any previously proved statements at level $n-1$ or lower. You must be nested within such a proof, however (which means those proofs must still be active).

At this point, you might wonder, why use subproofs at all? The conclusion must be a level 1 statement. If you start a level 2 subproof, you are not allowed (in general) to use any statements inside that level 2 subproof outside of the subproof. So, why bother? Isn't this like saying, "you can have as much money as you want, but you can't spend it."? Why do a subproof when it appears that you can't use any of the results outside the subproof? (And you need the results outside, because the conclusion has to be a level 1 statement).

8.3 Using Proof Rules With Assumptions

Obviously, if you couldn't conclude anything outside a subproof, then there would be no reason to have subproofs at all. It would be a silly exercise that would lead nowhere. *Fortunately*, there are three proof rules that allow you to write subproofs at level $n+1$ and conclude something at level n. Subproofs will therefore be useful, after all.

These are the list of the three proof rules which allow you to make assumptions at level $n+1$, prove facts within level $n+1$, and yet be able to conclude facts at level n.

- $\rightarrow$ Addition
- $\leftrightarrow$ Addition
- Proof by contradiction

Refer to the separate handout on logical equivalences and proof rules to read more about them.

9 When To Make Assumptions

9.1 Proving Implications

Perhaps the biggest source of confusion for students learning to write proofs with assumptions. In particular, students wonder when they should use $\rightarrow$ Addition, $\leftrightarrow$ Addition, and Proof by Contradiction, which are the only three proof rules which allow you to write a subproof, and conclude something was the subproof is closed off (i.e., made inactive).

Let's begin with a very useful strategy.

> *Whenever you're asked prove an implication (i.e., a statement of the form $\alpha \rightarrow \beta$, assume the hypothesis (i.e., assume α) and try to prove β.*

For example, suppose you're asked to prove $\sim p \rightarrow q$. This is an implication, so we can apply this strategy. You will create an 'E' (which starts at step i below and ends at step j). You will assume the hypothesis (at step i) above the horizontal line. Since you wish to prove q, the conclusion, you anticipate this by placing it as the last line of the subproof (at step j). Finally, at step $j + 1$ (after the subproof) fill in what you were planning to prove, namely, $\sim p \rightarrow q$. It looks like the following:

i - 1	...	
i	$\sim p$	Assume
	...	...
	...	...
j	q	Must justify
k	$\sim p \rightarrow q$	$\rightarrow$ Add (steps ...)

When you are asked to prove an implication, you should *automatically* do the following steps. It should almost be done with no hesitation at all. If you are having to think about these steps, then you wasting time. So, if asked to prove an implication (say, of the form $\alpha \rightarrow \beta$), do the following, which are the steps used in a $\rightarrow$ Rule proof:

1. Draw an E (which creates a subproof).
2. Put α in the proof header (i.e., above the middle horizontal bar)
3. Put β as the last step of the proof body
4. Put $\alpha \rightarrow \beta$ just after the E, and fill in, as justification, $\rightarrow$ Addition. You will fill out the step numbers later on once you know how many steps are involved.
5. Fill in the steps of the proof body (this is the part that requires you to think)

Only one part of writing a $\rightarrow$ Addition proof is difficult and that's the last step, which is filling in the missing steps needed to show β. The first four steps should be automatic. You should be able to do it without thinking.

Look at how we applied the steps to the example on the previous page. The E was drawn, then $\sim p$ was assumed (and written above the bar), then we added q as the last step of the

proof, and then added $\sim p \rightarrow q$ just after the subproof and justified it with $\rightarrow$ Addition. After that, it's your job to figure out how to prove q as well as to justify q. That is, you need to fill out the ... using proof rules and logical equivalences.

Perhaps you believe that there are other ways to prove implications, and you would prefer not to use the assumptions as shown above. Yes, you *could* write a proof without these assumptions. For example, instead of proving $\sim p \rightarrow q$, you might prove the logically equivalent $p \vee q$, and not use assumptions. Or you might use a proof by contradiction.

However, I strongly suggest that all implications be used, using this technique. Once you have mastered it, then feel free to explore the other proof techniques available to you, so you see how other methods work. Doing the above technique should always be your first choice, and only when it doesn't seem to lead you anywhere should you consider an alternative.

9.2 Proving If And Only If

If you want to prove bi-implications (e.g., $p \leftrightarrow q$) then you should attempt to use $\leftrightarrow$ Addition. This involves writing two subproofs. You prove $\alpha \rightarrow \beta$ then you prove $\beta \rightarrow \alpha$. When proving $\alpha \rightarrow \beta$, you are proving an implication, so assume α and prove β. When proving $\beta \rightarrow \alpha$, you are proving an implication, so assume β and prove α.

These are the steps.

1. Draw an E (which creates a subproof).
2. Put α in the proof header (i.e., above the middle horizontal bar)
3. Put β as the last step of the proof body (you will need to fill in the steps to prove β)
4. Draw a second E (which creates a second subproof).
5. Put β in the proof header (i.e., above the middle horizontal bar)
6. Put α as the last step of the proof body (you will need to fill in the steps to prove β)
7. Put $\alpha \leftrightarrow \beta$ just after the second E, and fill in, as justification, $\leftrightarrow$ Addition. You will fill out the step numbers later on once you know how many steps are involved.
8. Fill in the steps of the proof body for the first and second subproof bodies.

For example, suppose you were asked to prove $\sim p \leftrightarrow q$. Your proof would look like the following after doing the first 7 steps.

i - 1	$\ldots$	
i	$\sim p$	Assume
	$\ldots$	$\ldots$
	$\ldots$	$\ldots$
j	q	Must justify
j + 1	q	Assume
	$\ldots$	$\ldots$
	$\ldots$	$\ldots$
k	$\sim p$	Must justify
k + 1	$\sim p \leftrightarrow q$	$\rightarrow$ Add (steps $\ldots$)

At this point, you would actually have to do some thinking, and fill out all the steps with $\ldots$. Notice that this proof is simply two $\rightarrow$ Addition proofs. This makes perfect sense $\alpha \leftrightarrow \beta$ is logically equivalent to $\alpha \rightarrow \beta$ and $\beta \leftrightarrow \alpha$, so it should be no surprise that you just do these two $\rightarrow$ subproofs. This proof rule saves you three steps, namely, concluding $\alpha \rightarrow \beta$, concluding $\beta \rightarrow \alpha$, putting them together using $\wedge$ Addition to get $(\alpha \rightarrow \beta) \wedge (\beta \rightarrow \alpha)$ and using $\leftrightarrow$ rule to get $\alpha \leftrightarrow \beta$, all of which seems awfully tedious. Thus, the $\leftrightarrow$ Addition proof rule!

9.3 Proving Anything Else

For any other kinds of proof which do not use either $\rightarrow$ or $\leftrightarrow$ as the *main connective*, then you can use proof by contradiction. For example, if you're asked to prove p prove $p \vee q$ or even $\sim (p \rightarrow q)$ which do not have $\rightarrow$ or $\leftrightarrow$ as the *main* connective, you ought to attempt a proof by contradiction.

In a proof by contradiction, you *assume the negation* of what you wish to prove. Please, please, please just write the negation by simply putting a $\sim$ in front of the expression (adding parentheses if needed). Stop using DeMorgan's on it, because it makes it that much harder to decipher what you are doing.

Let's see how this works. Assume you wish to prove $p \vee q$. Neither $\rightarrow$ nor $\leftrightarrow$ appear as the main connective, so you start a proof by contradiction. Thus, assume the negation of what you want to prove, i.e., assume $\sim (p \vee q)$ (don't assume $\sim p \wedge \sim q$ even though this is logically equivalent—it makes harder to tell you are doing a proof by contradiction—keep it simple).

i - 1	$\ldots$	
i	$\sim (p \vee q)$	Assume
	$\ldots$	$\ldots$
	$\ldots$	$\ldots$
j	$\ldots$	$\wedge$ Addition
k	$p \vee q$	Proof by contradiction (steps i–j)

Here are the steps to take when starting a proof by contradiction. Assume you are trying to prove α. (If you want to prove $\sim \alpha$, you can assume α, and then prove a contradiction.)

1. Draw an E (which creates a subproof).
2. Put $\sim \alpha$ in the proof header (i.e., above the middle horizontal bar).
3. Put α just after the E, and fill in, as justification, Proof by Contradiction. You will fill out the step numbers later on once you know how many steps are involved.
4. Fill in the steps of the proof body and attempt to find any contradiction that can be justified. The last step (step j) will be the contradiction itself, usually written in the form $\beta \wedge \sim \beta$.

In a proof by contradiction, you may find any contradiction that works, provided you can justify the reasons. Once you have the contradiction, then the assumption you originally made (in this case, $\sim (p \vee q)$ had to be false, and so $p \vee q$ had to be true.

10 Why Proof By Contradiction Works

Here's the intuition. Suppose you're trying to prove α and you believe that it can indeed be proved. Then, certainly, if you assume $\sim \alpha$, the negation of α, you will get a contradiction. Namely, you will get $\alpha \wedge \sim \alpha$.

It turns out that if you introduce $\sim \alpha$ to try and get a contradiction with α, usually other contradictions will also appear. The goal of proof by contradiction is to find any one of these contradictions, not just finding α to contradict $\sim \alpha$.

Proof by contradiction also works because the proof rules don't create contradictions if they weren't any contradictions in the original premises. Thus, if you kept producing fact after fact from proof rules, and the premises were consistent (meaning there was at least one truth assignment that makes all the premises true), then you can only generate other facts that keep its consistency. Thus, the only way the contradiction arises is when the contradictory fact is assumed (namely, $\sim \alpha$ is assumed).

Let's see how this works. Here are a list of statement letters and their meaning.

- a stands for "Ali is at the store"
- t stands for "Tina is at the store"
- s stands for "Sandip is at the store"
- c stands for "Chamique is at the store"

Suppose you make the following argument:

$$\begin{array}{l} a \leftrightarrow t \\ t \leftrightarrow s \\ s \leftrightarrow c \\ c \\ \hline \therefore a \vee s \end{array}$$

If you look carefully at the argument, the first three premises basically say that all four people are either at the store or they not at the store. There's never part of the group there. The last premise (i.e., c) says Chamique is at the store, and in combination with the other premises, it means everyone is at the store.

This argument then concludes that either Ali or Sandip are at the store, which makes senses given what the statement variables mean.

In a proof by contradiction, you begin by assuming the opposite of what you want to prove. You assume $\sim (a \vee s)$. By DeMorgan's theorem, this is equivalent to $\sim a \wedge \sim s$, which states that neither Ali nor Sandip is at the store. We want to eventually show $a \vee s$ to get a contradiction, but we'll see other contradictions come up soon.

Let's start the proof to see how this happens.

1	$a \leftrightarrow t$	Assume
2	$t \leftrightarrow s$	Assume
3	$s \leftrightarrow c$	Assume
4	c	Assume
5	$\sim (a \vee s)$	Assume
6	$\sim a \wedge \sim s$	DeMorgan's (step 5)
7	$\sim s$	$\wedge$ Simp (step 6)
8	$c \rightarrow s$	$\leftrightarrow$ Simp (step 3)
9	s	MP (step 4, 8)
10	$s \wedge \sim s$	$\wedge$ Add (step 7, 9)
11	$a \vee s$	Proof by Contradiction (steps 5–10)

Although we were trying to prove $a \vee s$ to create the contradiction, we found another contradiction, namely $s \wedge \sim s$, i.e., that Sandip was at the store and wasn't at the store at the same time.

This happens a lot in a proof by contradiction. You are trying to contradict the assumption (in this example, you try to contradict $\sim (a \vee s)$—see step 5), but you find a different contradiction much sooner. Thus, instead of showing $a \vee s$ which would contradict $\sim (a \vee s)$, the contradiction $s \wedge \sim s$ appeared earlier, and you use that.

Let's review. You wish to prove α. Suppose α were indeed true. Now, you assume $\sim \alpha$ (as part of the proof by contradiction). If α were indeed true, then $\sim \alpha$, its negation, would contradict it, because both α and its negation $\sim \alpha$ can't both be true. Thus, we claim if α *weren't* true, we would never have had a contradiction with $\sim \alpha$. But we *did* get a contradiction, and we believe $\sim \alpha$ caused it, and it caused it because α was true. Thus, α must be true (otherwise, the contradiction should never have happened with $\sim \alpha$). It sounds weird, but makes some sense if you think about it.

If you think that proof by contradiction isn't used in day-to-day life, you're probably wrong. Someone might claim "If I had been in charge of the job, then I would have made sure such-and-such happened, and that would avoided this entire mess". What's implied is that the

mess occurred, and therefore (by contradiction) the person couldn't have been in charge.

This also happens in court cases when people come up with alibis. They try to bring in witnesses that will claim that they are at some location at some particular time, and therefore there's no way they could have been at the location of some crime, because one can't be at two places at the same time. Again, this is a kind of proof by contradiction.

11 Inconsistent Premises—Prove Anything!

There is an odd result that falls out of a proof by contradiction. Suppose the premises were inconsistent. That is, suppose you could show a contradiction within the premises itself. Then, you could prove anything. Thus, the phrase "contradiction proves anything" (though it's more accurate to say "contradictory assumptions prove anything").

Let's see why this happens. First, create a simple argument with a contradiction in the premises.

$$\begin{array}{l} p \\ \sim p \\ \hline \therefore q \end{array}$$

We want to show that when p and $\sim p$ are true, then we can prove q. A person that's just learning about proofs might say "That's impossible! The conclusion has nothing to do with the premises! q doesn't even appear in the premises!". This is all true. Nevertheless, proof by contradiction will allow us to prove this seemingly unrelated fact.

1	p	Assume
2	$\sim p$	Assume
3	$\sim q$	Assume
4	$p \wedge \sim p$	$\wedge$ Add (step 1, 2)
5	q	Proof by Contradiction (steps 3–4)

As usual, we begin a proof by contradiction by assuming the negation of what we want to prove. In this case, we assume $\sim q$ (step 3). The contradiction doesn't even use this assumption at all. It uses the contradiction from the premises from steps 1 and 2.

In fact, with very little modification, we can even prove $\sim q$, and we can prove $q \wedge \sim q$. You can prove anything you want! This makes most students quite uncomfortable. Why does contradiction allow you to prove whatever you want? Wouldn't it be more reasonable to conclude nothing once you have contradictory premises?

Perhaps it would, but you might not discover the contradiction for quite a while, and therefore be proving line after line of facts. Should those facts then no longer hold once the contradiction shows up? This would make the proof rules complicated. It would suggest that proof rules work, but when contradictions appear, let's not make it work.

Or you might suggest that if the premises are contradictory, we shouldn't allow anything more to be proved. However, that would mean again creating a special case that says

"If the premises are contradictory, you can't use that in the subproof's body". It turns out that it's unnecessary to make these special rules. As long as your prepared to allow contradictions to prove anything, then we can keep the rules simple.

And what rules is that? When you are trying to do a proof by contradiction, you assume $\sim \alpha$, then show a contradiction from the known facts. Whether this contradiction arises because the premises were contradictory or whether they arise because $\sim \alpha$ caused contradictory facts, it doesn't matter. And it turns out, once you accept this weird fact about contradictions, you can still prove legitimate things. In this case, once the contradiction is shown, you can conclude α out of the subproof.

In general, you're not going to be asked to prove anything with inconsistent premises, because such proofs are pretty boring. They don't really amount to much. In a typical proof by contradiction, it's the assumption that causes the contradiction to occur, so the unusual case where the premises are already contradictory is just that—unusual.

11.1 Can't Prove Everything by Proof By Contradiction

When I say "contradiction proves everything", I need to be careful. It's more accurate to say "inconsistent premises prove everything". On the other hand, proof by contradiction does *not* prove everything.

The rule is this. Assume $\sim \alpha$. Show a contradiction occurs with that assumption. Then, you can conclude α. Or assume α and show a contradiction occurs, then conclude $\sim \alpha$.

Let's illustrate this:

i		$\sim \alpha$	Assume
i + 1		...	...
		...	...
j		$\beta \wedge \sim \beta$	$\wedge$ Add (steps ...)
j + 1	α		Proof by Contradiction (steps i–j)

At step i, we assumed $\sim \alpha$. Then, this eventually lead to the contradiction at step j. Once you have that contradiction, you can prove anything else you want. Admittedly, to do so requires that you do yet another proof by contradiction. For example, if you wanted to prove, say $p \wedge s$, you would begin a proof by contradiction (this would be a level 3 proof, which is occuring within the level 2 proof that you're doing right now). This would mean assuming $\sim (p \wedge s)$ which is the negation of what you want to prove, then basically repeating step j where the contradiction occurred, the concluding (at level 2), $p \wedge s$.

But again, there's a catch. While you can prove anything with the contradiction in step j and any more steps you might have within the subproof (done at level 2), you *can't* conclude anything more than the opposite of the assumption *outside of the subproof*! Thus, at step $j + 1$, which is back at level 1, you can only conclude α (OK, technically, you could also prove $\alpha \rightarrow (\beta \wedge \sim \beta)$ by $\rightarrow$ Addition), at least if you use proof by contradiction. Remember, when you start a subproof, you can only conclude certain facts outside the subproof. Thus, in a proof by contradiction, assuming $\sim \alpha$ only allows you to conclude α

once the contradiction has been established.

12 Other Proof Strategies

You have three proof strategies you can use, and the proof strategy you pick is guided whatever you're proving. For example,

- If you are asked to prove $p \to q$, then use $\to$ Addition. That is, assume p, try to prove q. Once you see an implication of the form $\alpha \to \beta$ you should automatically think of $\to$ Addition for your proof.
- If you are asked to prove $p \leftrightarrow q$, then use $\leftrightarrow$ Addition. This requires two subproofs since essentially you are trying to prove both $p \to q$ and $q \to p$. Thus, you assume p, try to prove q. Then, you assume q, try to prove p. This is a very standard proof technique to prove bi-implication (i.e., if and only if).
- If you are asked to prove $p \to (q \to r)$, then use $\to$ Addition. That is, assume p, try to prove $q \to r$.

i	p	Assume
	...	...
	...	...
m	$q \to r$	Need to Justify
m + 1	$p \to q$	$\to$ Add (steps i–m)

But since you need to prove $q \to r$ (see step m), you should start yet another subproof, and assume q and prove r. That would look something like:

i	p	Assume
j	q	Assume
	...	...
	...	...
k	r	Justify
m	$q \to r$	$\to$ Add (steps j–k)
m + 1	$p \to q$	$\to$ Add (steps i–m)

The key to this more complicated proof is to recognize that when you write down step m, that too needs to be proved, and thus you fill in the subproof starting from j to k.

- If you are asked to prove $(p \to q) \to r$, then use $\to$ Addition. That is, assume $p \to q$, try to prove r. Notice that the difference between this example and the previous one is the parentheses. Thus, you are now trying to prove r. One way to do that is by contradiction.

i	$p \to q$	Assume
j	$\sim r$	Assume
	...	...
k	...	...
m	r	Proof by Contradiction (steps j–k)
m + 1	$(p \to q) \to r$	$\to$ Add (steps i–m)

You don't need to make the assumption at step j if you don't want to, but generally it is easier to work with more assumptions, and when all else fails, a contradiction proof will give you one additional assumption.

- If you are asked to prove $\sim p$, then you can basically rule out $\to$ Addition and $\leftrightarrow$ Addition as proof methods. The only proof method left that allows you to make an assumption is proof by contradiction. So, you assume the negation of $\sim p$, which is p, and attempt to find some contradiction.
- If you are asked to prove $\sim (p \to q)$, you can't really use $\to$ Addition (not unless you try to rewrite this statement somehow). That's because $\to$ is not the main connective: $\sim$ is. So, that means you're left with doing a proof by contradiction if you want to use an assumption. Thus, you would assume the negation of what you want to prove, namely, assume $p \to q$, and then find a contradiction. At this point, you *already* have assumed $p \to q$ so there's no need to assume p and show q. You do that *only* if you need to *prove* $p \to q$.

So, the basic strategies are very simple. If you see an implication, begin a proof using $\to$ Addition. If you see a bi-implication, begin a proof using $\leftrightarrow$ Addition. If you see neither, then begin a proof by Contradiction. If you use these three rules whenever you can, you will find your proofs are much easier to solve, because you get to use far more assumptions and you get to prove far simpler conclusions.

12.1 Then What?

In a proof by contradiction, the goal is to establish any sort of contradiction. Typically, this will mean proving a variable and its negation. For example, $p \wedge \sim p$. To do this kind of proof, you want to establish as many facts as possible.

Here are the strategies:

If you see	Try To Get	So You Conclude	By Using
$\alpha \to \beta$	α	β	Modus ponens
$\alpha \to \beta$	$\sim \beta$	$\sim \alpha$	Modus tollens
$\alpha \vee \beta$	$\sim \alpha$	β	Disjunctive Syllogism
$\alpha \vee \beta$	$\sim \beta$	α	Disjunctive Syllogism

Also, if you're getting stuck, try using DeMorgan's, Double Negative, and Distributive to rearrange terms. Finally, if worse gets to worse, start an arbitrary Proof by contradiction. Try to prove something like p or $\sim p$ and see if that will lead you anywhere.

It turns out the more you practice these proofs, the more you become attuned to what you need to do. The great thing about doing Proof by Contradiction is that your strategy is quite simple. Try to prove as many small facts as possible (e.g. $p, \sim p, q, \sim q$, etc). The more facts you have, the easier it is to establish a contradiction.

12.2 Avoiding Pitfalls

One of the more common pitfalls is trying to prove something that doesn't need to be proved because it's already assumed true. Let's see how this happens. Suppose you have the following argument.

$$\begin{array}{l} (\sim p \vee r) \rightarrow t \\ \sim p \vee t \\ \sim t \wedge s \\ \hline \therefore t \rightarrow s \end{array}$$

You are expected to *prove* $t \rightarrow s$. Thus, you should assume t, then try to prove s. However, it's easy to get confused. You might, for example, focus your attention to the first premise: $(\sim p \vee r) \rightarrow t$.

At this point, you see an implication. You might think, "That's an implication! I better assume the hypothesis (i.e., $(\sim p \vee r)$) then prove its conclusion (i.e., t)". But if you think about it, where will that lead you? You will prove $(\sim p \vee r) \rightarrow t$. So what? It's already *given*. When it's given, you don't prove it.

Here's an analogy: you want to host a party. You think it would be neat to have candles. Someone gives you candles. Do you go out and buy candles? If you're happy with the ones that you were *given*, you don't buy more. Of course, this seems silly. No one would buy candles if they already had it (assuming they had enough and were happy with them). But when it comes to proofs, students see an implication and try to prove it, when it's already given in the premises, and thus assumed to be true. This is like trying to buy candles when you have been given them.

It's very important, when you see an implication, to know whether you are being asked to prove it (for example, you prove the conclusion) or whether you have been given it as a premise. Simply ask yourself, "Is this implication a premise?" If the answer is yes, don't prove it—it's given! If it isn't (i.e., it's a conclusion) then prove it using proof rules, etc.

> *When you need to **prove** an implication of the form $\alpha \rightarrow \beta$, start a subproof, where you **assume** α and then try to **prove** β. However, when the implication is **given** (as a premise), don't start a subproof.*

What do you do instead? Since you have been already *given* an implication, your goal is to either use *modus ponens* or *modus tollens*. Remember the strategy chart on the previous page? When you have $(\sim p \vee r) \rightarrow t$, either try to get $\sim p \vee r$, so you can apply modus ponens to get t, or try to get $\sim t$, so you can apply modus tollens to get $\sim (\sim p \vee r)$.

To repeat this strategy:

*When you are **given** an implication of the form $\alpha \to \beta$, don't start an assumption. Either you try to prove α (but don't assume it—unless it's a premise), and then use modus ponens to get β, or you try to prove $\sim \beta$ (but don't assume it—unless it's a premise) to get $\sim \alpha$ by modus tollens.*

If you can distinguish between an implication which is a premise and an implication which is something you're asked to prove, then you won't redundantly prove something that's already assumed to be true.

12.3 Modus Ponens, Modus Tollens, etc.

When writing justifications for proof rules such as *modus ponens*, *modus tollens*, etc. some students only justify it with a single step. For example, some will write MP (step 3). Modus ponens requires *two* steps, not one. If you don't write both steps, you might be applying modus ponens incorrectly.

Some students look at $p \vee q$ and want to conclude p (using some kind of $\wedge$ simplification), even though there's no rule that allows you to do this. If you had $p \wedge q$, you could conclude p, but you can't do it with $p \vee q$. There's a difference between $\wedge$ and $\vee$—that's why two different symbols are used! In order to get p from $p \vee q$, you must have $\sim q$, then you can apply disjunctive syllogism to get p.

Similarly, some students try to get $p \wedge q$, but have only proved p. They simply tack on q and justifying it by $\wedge$ addition. q must either have been previously proved or assumed, in order to use $\wedge$ addition. $\wedge$ Addition requires TWO steps. Such students are confusing $\vee$ addition with $\wedge$ addition. In $\vee$ addition, you can have p and derive $p \vee q$. Make sure you know the rules, and don't apply one just because it is convenient to do so (though incorrect).

Some students have assumed that if $p \to q$ is true, then sure p is true. This is not the case. In fact, there are no rules to let you conclude this. Yes, you would need p so you can use modus ponens with it, but you aren't allowed to claim p is true, if $p \to q$ is true. This is why it's so important that you know the rules, and not make up rules just because you are having a difficult time with the proofs. Most of the students who understand proofs have memorized most of the rules, and know exactly how to apply the rules. Do you?