MATHEMATICS 300 — SPRING 2005

Introduction to Mathematical Reasoning

H. J. Sussmann

INSTRUCTOR'S NOTES

February 3, 2005

Contents

7 Some types of valid propositional inference form steps (continued from the previous set of notes)

We have already presented seven valid rules for inferences (the "in" and "out" rules for $\vee$, $\wedge$ and $\Rightarrow$, and the tautology proof rule). Now we are going to present more rules, namely, the in and out rules for $\Leftrightarrow$, and the rule (or rules) about "proof by contradiction." The rules for $\Leftrightarrow$ are rather trivial. *Proofs by contradiction*, are one one of the most widely used proof techniques in mathematics. So this type of proof will get a special section all for itself, namely, §8.

Let us start with the rules for $\Leftrightarrow$. As before, there will be a rule $\Leftrightarrow_{in}$ and a rule $\Leftrightarrow_{out}$.

7.10 Rules $\Leftrightarrow_{in}$ and $\Leftrightarrow_{out}$

These are the valid propositonal inference step forms

$$(\Leftrightarrow_{in}) \qquad \left\{ \begin{array}{l} P \Rightarrow Q \\ Q \Rightarrow P \\ \hline P \Leftrightarrow Q \end{array} \right. ,$$

$$(\Leftrightarrow_{out}.a) \qquad \left\{ \begin{array}{l} P \Leftrightarrow Q \\ \hline P \Rightarrow Q \end{array} \right. , \qquad \text{and} \qquad (\Leftrightarrow_{out}.b) \qquad \left\{ \begin{array}{l} P \Leftrightarrow Q \\ \hline Q \Rightarrow P \end{array} \right. .$$

These rules are quite trivial: all they say is that

(1) if you prove that P implies Q and Q implies P then you can go to $P \Leftrightarrow Q$,

(2) if you prove that $P \Leftrightarrow Q$ then you can go to P implies Q and to Q implies P.

7.11 Are rules $\Leftrightarrow_{in}$ and $\Leftrightarrow_{out}$ really needed?

Suppose that, for whatever reason, you do not want to use Rules $\Leftrightarrow_{in}$ and $\Leftrightarrow_{out}$. Can you do without them?

The answer is "yes." Let me show you how you can do everything that Rules $\Leftrightarrow_{in}$ and $\Leftrightarrow_{out}$ allow you to do without ever using those rules.

Suppose you find yourself in a situation where you would want to use Rule $\Leftrightarrow_{in}$, and you want to achieve the same result without using the rule. That is, you have $P \Rightarrow Q$ and $Q \Rightarrow P$, and you would like to go to $P \Leftrightarrow Q$ without invoking Rule $\Leftrightarrow_{in}$. Here is how you can do it:

(1)	$P \Rightarrow Q$
(2)	$Q \Rightarrow P$
(3)	$(Q \Rightarrow P) \Rightarrow ((P \Rightarrow Q) \Rightarrow (P \Leftrightarrow Q))$
(4)	$(P \Rightarrow Q) \Rightarrow (P \Leftrightarrow Q)$
(5)	$P \Leftrightarrow Q$

(The justifications of the steps are as follows: (3) is a tautology, (4) follows from (2) and (3) by Modus Ponens, and (5) follows from (1) and (4) by Modus Ponens.)

Next, suppose you find yourself in a situation where you would want to use Rule $\Leftrightarrow_{out}$, but you want to achieve the same thing without using the rule. That is, you have $P \Leftrightarrow Q$, and you would like to go to $P \Rightarrow Q$ or to $Q \Rightarrow P$ without invoking Rule $\Leftrightarrow_{out}$. Here is how you can get to $P \Rightarrow Q$:

(1)	$P \Leftrightarrow Q$
(2)	$(P \Leftrightarrow Q) \Rightarrow (P \Rightarrow Q)$
(3)	$P \Rightarrow Q$

(The justifications of the steps are as follows: (2) is a tautology, and (3) follows from (1) and (2) by Modus Ponens.) Naturally, a very similar technique can be used if you want to get to $Q \Rightarrow P$.

7.12 Which propositional rules are really needed?

So far, we have seen ***nine*** propositional rules, namely, the "in" and "out" rules for $\vee$, $\wedge$, $\Rightarrow$ and $\Leftrightarrow$, and the tautology proof rule. However, we have also seen that three of those rules (rules $\vee_{out}$, $\Leftrightarrow_{in}$ and $\Leftrightarrow_{out}$) can be avoided if you want to, because anything you can do with them can also be done without them. So it would seem that we can manage with just six rules. It turns out that three more of these six rules can also be completely avoided if you want to. *You can avoid using Rules $\wedge_{out}$, $\wedge_{in}$, and $\vee_{in}$.* Here is how.

How to avoid using Rule $\wedge_{in}$. Suppose you find yourself in a situation where you would want to use Rule $\wedge_{in}$, and you want to achieve the same thing without using the rule. That is, you have P and Q, and you would like to go to $P \wedge Q$ without invoking Rule $\wedge_{in}$. Here is how you can do it:

(1)	P
(2)	Q
(3)	$P \Rightarrow (Q \Rightarrow (P \wedge Q))$
(4)	$Q \Rightarrow (P \wedge Q)$
(5)	$P \wedge Q$

(The justifications of the steps are as follows: (3) is a tautology, (4) follows from (1) and (3) by Modus Ponens, and (5) follows from (2) and (4) by Modus Ponens.)

How to avoid using Rule $\wedge_{out}$. Now suppose you find yourself in a situation where you would want to use Rule $\wedge_{out}$, and you want to achieve the same thing without using the rule. That is, you have $P \wedge Q$, and you would like to go to P, or to Q, without invoking Rule $\wedge_{out}$. Here is how you can get to P.

(1)	$P \wedge Q$
(2)	$(P \wedge Q) \Rightarrow P$
(3)	P

(The justifications of the steps are as follows: (2) is a tautology, and (3) follows from (1) and (2) by Modus Ponens.) Naturally, a very similar method can be used if you want to get to Q.

How to avoid using Rule $\vee_{in}$. Suppose you are in a situation where you would want to use Rule $\vee_{in}$, and you want to achieve the same thing without using the rule. That is, you have P (or maybe Q), and you would like to go to $P \vee Q$, without invoking Rule $\vee_{in}$. Here is how you can get to $P \vee Q$ from P:

(1)	P
(2)	$P \Rightarrow (P \vee Q)$
(3)	$P \vee Q$

(The justifications of the steps are as follows: (2) is a tautology, and (3) follows from (1) and (2) by Modus Ponens.) Naturally, a very similar method can be used if you want to get to $P \vee Q$ from Q.

Summarizing, ***of the nine rules we have seen so far, three suffice; all you need is Rules*** $\Rightarrow_{in}$ ***and*** $\Rightarrow_{out}$***, and the tautology rule.***

7.13 Is it better to have few rules or to have many?

I have given you nine propositional rules, but I have also told you that there are three of them that suffice, and you do not need the other six. Is it better to just remember and use all nine rules, or to forget the six "unnecessary" ones and remember and use just three?

The answer is that ***each of the two approaches has its own advantages and disadvantages.*** So all I am going to do is tell you about the pros and cons of each approach, and let you choose whichever one you prefer.

8 Proofs by contradiction

As we explained earlier, you can always "assume" anything you want, in order to find out what would be the case "under that assumption." In other words, you imagine that something is true because you want to know what would have to happen in that case. There is not need for your assumption to be true, because you are only trying to understand what would happen if it was true.

Actually, **one of the most common reasons for assuming something is to prove it cannot be true.** In other words, you set out to explore the consequences of something in order to prove it is impossible. This is called "proof by contradiction."

The structure of a proof by contradiction is as follows:

$$\left\{\begin{array}{l} \text{Assume } \sim P \\ \vdots \\ C \quad \text{(a contradiction)} \\ \hline P \end{array}\right. ,$$

or

$$\left\{\begin{array}{l} \text{Assume } P \\ \vdots \\ C \quad \text{(a contradiction)} \\ \hline \sim P \end{array}\right. .$$

(These two are basically the same, since you can pass from the second one to the first one by plugging $\sim P$ for P [1].)

And there is a third version, which is what the book calls "proof by contradiction":

$$\left\{\begin{array}{ll} \text{Assume } \sim P & \\ \vdots & \\ Q & \\ \vdots & \\ \sim Q & \\ Q\wedge(\sim Q) & \quad [\text{by Rule } \wedge_{in}] \\ \hline P & \end{array}\right.$$

You can think of these three formats for proofs as "rules." But you can also view them as methods for proof, which can always be justified by using the other rules that we already know. (For example, take the book's version if a "proof by contradiction." If assuming $\sim P$ you prove Q, and then you also prove $\sim Q$, then Rule $\wedge_{in}$ tells you that you can go to $Q\wedge(\sim Q)$, always under the assumption that $\sim P$ holds. But then Rule $\Rightarrow_{in}$ tells you that you can go to $(\sim P) \Rightarrow (Q\wedge(\sim Q))$. On the other hand, $((\sim P) \Rightarrow (Q\wedge(\sim Q))) \Rightarrow P$ is a tautology[2]. So you can bring it in, and then use Modus Ponens, from $(\sim P) \Rightarrow (Q\wedge(\sim Q))$ and $((\sim P) \Rightarrow (Q\wedge(\sim Q))) \Rightarrow P$, to get P.)

8.1 A non-mathematical example: a purported proof that time travel to the past is impossible, using the famous "killing your grandmother" technique

Let us "prove" that it is impossible to travel backwards in time. Let us do it by contradiction. Suppose you could travel backward in time. Then you could go back to the time three years before your mother was born, find your mother's mother, and kill her. This way, your mother would never be born and then of course you would not exist either, contradicting the fact that you exist. Therefore it is impossible to travel backwards in time. $\diamondsuit$

COMMENTS AND REMARKS. You probably haven't found this "proof" very convincing. If so, you are in good company, because I don't find it

[1] To be completely precise, if you take the second version and plug in $\sim P$ for P, then you end up with $\sim(\sim P)$. But then you can easily get P, because $(\sim(\sim P)) \Rightarrow P$ is a tautology, and from $(\sim(\sim P)) \Rightarrow P$ and $\sim(\sim P)$ you get P by Modus Ponens.

[2] You are asked to prove this in one of the homework problems. It's very easy!

convincing either. But let us forget about this for a minute, and focus on the logical structure of the proof. I want to make sure you understand that, **as far as its logical structure goes, this is a perfect example of a proof by contradiction.** We want to prove that something cannot happen, and to do that we imagine a world in which it happens, and show that something impossible (say "absurd," or "contradictory") would have to happen in that imaginary world. We then conclude that this thing we imagined is itself impossible.

Now let us look at the proof. Is it convincing? Do you really believe that traveling backwards in time is impossible *because of this proof*? Frankly, I do not trust this proof at all. Here is my main reason. Once you have assumed that traveling backwards in time is possible, it does not follow that *every way of traveling backwards in time is possible.* For all we know, there may be some other physical laws that make some particular forms of travel backwards in time impossible, in particular when they allow you affect the present by killing your grandmother[3].

8.2 A first mathematical example: proof that the equation $x^2 = -1$ does not have a real solution

THEOREM. *There does not exist a real number x such that $x^2 = -1$.*

PROOF. We are going to prove our result by contradiction. Suppose a real number x such that $x^2 = -1$ exists. Pick one and call it c. Then $c^2 = -1$, so $c^2 + 1 = 0$. But in the universe of real numbers it is true that the square of any number is ≥ 0. So $c^2 \geq 0$. Furthermore, $1 > 0$, so $c^2 + 1 > 0$. But $c^2 + 1 = 0$, so we have shown that $0 > 0$, which is not true. This tells us that c cannot exist, and our proof is complete. $\diamondsuit$

QUESTION. You probably know that there are numbers (called "complex numbers") such that in the universe of those numbers the equation $x^2+1 = 0$ does have a solution. (Actually, it has two solutions, namely, i and $-i$.) It follows that the proof we just gave cannot work in thw world of complex numbers. *Which step or steps of the proof go wrong if we deal with complex numbers rather than real numbers?*

[3]If you are a science-fiction reader, you must have read at least one novel or short story where the plot depends on this. For example, somebody travels to the past and tries to kill his grandmother but something always happens that prevents him. The 1995 movie "Twelve Monkeys" deals with this issue, by showing a scenario of time travel to the past which does not lead to anything impossible or contradictory.

8.3 A second example: proof that $\sqrt{2}$ is irrational

Recall that a ***rational number*** is a real number r having the property that there exist integers m, n such that $n \neq 0$ and $r = \frac{m}{n}$. An ***irrational number*** is a real number that is not rational.

We want to prove that there does not exist a rational number r such that $r^2 = 2$. In other words, we want to prove that there do not exist integers m, n such that $n \neq 0$ and $(\frac{m}{n})^2 = 2$. Equivalently, we must prove that there do not exist integers m, n such that $n \neq 0$ and $m^2 = 2n^2$. We do the proof by contradiction. Suppose such integers exist. Pick m, n such that $m^2 = 2n^2$, and call them μ, ν, so μ, ν are integers, $\nu \neq 0$, and $\mu^2 = 2\nu^2$. (If you want to call them m and n that's O.K. with me. I don't like it very much, but I will accept it.) If μ is negative, we can change μ to $-\mu$, and the condition $\mu^2 = 2\nu^2$ will still hold with the new μ. So we can assume that $\mu \geq 0$. Simiarly, if ν is negative, we can change ν to $-\nu$, and the condition $\mu^2 = 2\nu^2$ will still hold with the new ν. So we can assume that $\nu > 0$. If both μ and ν are even, then we can divide both of them by 2 (that is, replace μ by $\frac{\mu}{2}$ and ν by $\frac{\nu}{2}$) and we get smaller μ and ν for which the equation $\mu^2 = 2\nu^2$ still holds. If these new μ, ν are still even, we can divide by 2 again, and we can keep doing this until we get μ and ν that are not both even. (That is, one of them is odd, or both are odd.)

Now, if μ was odd, then μ^2 would be odd, which is not the case, because $\mu^2 = 2\nu^2$. So μ has to be even.

But then we can pick an integer k such that $\mu = 2k$. It folows that

$$2\nu^2 = \mu^2 = 4k^2 \,.$$

So $\nu^2 = 2k^2$. So ν^2 is even. So ν is even, because if ν was odd then ν^2 would have to be odd.

So now we have found that (a) μ and ν are not both even, and (b) μ and ν are both even. These two things together are impossible. So the assumption that there exist integers m, n such that $n \neq 0$ and $m^2 = 2n^2$ has led us to an impossible conclusion. Hence m and n do not exist. **END OF PROOF**

8.4 A third example: proof that $\sqrt{3}$ is irrational

Again, we write a proof by contradiction.

Suppose $\sqrt{3}$ was rational. Then we would have $\sqrt{3} = \frac{m}{n}$, where m, n are integers such that $n \neq 0$. If m and n are both divisible by 3, we can cancel the common factor 3 and produce smaller m and n for which $\sqrt{3} = \frac{m}{n}$ is still true. If these new m, n are still both divisible by 3, we can cancel the common factor 3 again, and produce even smaller m and n for which $\sqrt{3} = \frac{m}{n}$ is true. Continue this process until no further cancellation is possible. Then $\sqrt{3} = \frac{m}{n}$, m, n are integers, $n \neq 0$, and m, n are not both divisible by 3. If $n < 0$ then m would have to be < 0 as well, because the quotient $\frac{m}{n}$ is positive. If this is the case, we replace m by $-m$ and n by $-n$, and now we have m, n with all the properties listed above, plus the fact that $m > 0$ and $n > 0$. Since $\sqrt{3} = \frac{m}{n}$, we have $3 = \frac{m^2}{n^2}$, so $3n^2 = m^2$. Now, we need the fact that *if a product $a.b$ of integers is divisible by 3, then one of them must be divisible by 3*. (This is easy to prove; see the remark at the end of this subsection.) Applying this fact, we see that "$3n^2 = m^2$" tells us that m^2 is divisible by 3, so m is divisible by 3. Write $m = 3s$, with $s \in \mathbb{Z}$. Then $3n^2 = m^2 = 9s^2$, so $n^2 = 3s^2$. Therefore n^2 is divisible by 3, so n is divisible by 3. Hence we have shown that both m and n are divisible by 3, But we know that they are not both divisible by 3. Hence we have reached a contradiction and our proof is complete.

REMARK. Here is a proof that "if a product $a.b$ of integers is divisible by 3, then one of them must be divisible by 3." Suppose a is not divisible by 3 and b is not divisible by 3. Then there exist integers k, r, k', r' such that $a = 3k + r$, $b = 3k' + r'$, $r = 1$ or $r = 2$, and $r' = 1$ or $r' = 2$. Then

$$a.b = (3k + r)(3k' + r') = 9kk' + 3kr' + 3k'r + rr' = 3\ell + rr' ,$$

where $\ell = 3kk' + kr' + k'r$. Now, if $r = 1$ or $r = 2$ and $r' = 1$ or $r' = 2$, then $rr' = 1$ or $rr' = 2$ or $rr' = 4$. In each of the three cases, rr' is not divisible by 3. So $a.b$ is not divisible by 3 either, because if it was then rr' would also be, since $rr' = a.b - 3\ell$. $\diamondsuit$

8.5 A fourth example: Euclid's proof that there are infinitely prime numbers

If we want to be able to prove that there are infinitely many prime numbers, we need to know what a "prime number" is a what it means to say that "there are infinitely many" of them.

DEFINITION. A *prime number* is an integer p such that

(1) $p > 1$,

and

(2) there do not exist integers m, n such that $1 < m < p$, and $m.n = p$. $\diamondsuit$

DEFINITION. The statement *"there are infinitely many prime numbers"* means "there does not exist a positive integer N such that there are exactly N primes." ♢

Now that we know the meaning of the statement we would like to prove, we can state our result and prove it.

THEOREM. *There are infinitely many prime numbers.*

PROOF. We want to prove that a positive integer N with the properties of the previous definition does not exist. We do this by contradiction. Suppose N exists. Then there are exactly N primes, and one can list them all and label them $p_1, p_2, \ldots, p_N$. Now introduce a new integer M by letting

$$M = 1 + p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_N\,.$$

(That is, we construct M by multiplying together all the primes and adding 1 to the result.)

We now use one basic result about integers. (We will show later how to prove this fact.) *If n is an arbitrary integer such that $n > 1$, then n is divisible by a prime.* That is, *if n is an arbitrary integer such that $n > 1$, then there exist integers p, q such that p is prime and $n = p \cdot q$.*

We apply this to the integer M, and conclude that we can pick a prime number p such that M is divisible by p. Could p be one of the prime numbers $p_1, p_2, \ldots, p_N$? The answer is "no," because if we divide M by any one of these numbers the remainder is 1. So p is a new prime number, not one of the numbers $p_1, p_2, \ldots, p_N$.

Hence we have shown that **there exists a prime number which is not one of $p_1, p_2, \ldots, p_N$.** But on the other hand **there does not exist a prime number which is not one of $p_1, p_2, \ldots, p_N$,** because we have picked N such that $p_1, p_2, \ldots, p_N$ are *all* the primes.

Together, the two boldfaced assertions add up to a contradiction. (More precisely, if you wish: let A be the first of the two boldfaced assertions; we have proved A and $\sim A$. Using Rule $\wedge_{in}$ we get $A \wedge (\sim A)$, which is a contradiction.)

So N does not exist, and we are done. ♢

8.6 A fifth example: studying the intersection of two lines in space.

As you have seen in one of your Calculus courses, each of the two systems of parametric equations

$$(L_1) \qquad \begin{cases} x = 2t + 1 \\ y = t - 2 \\ z = 3t + 7 \end{cases}$$

and

$$(L_2) \qquad \begin{cases} x = t + 2 \\ y = 5t + 1 \\ z = t + 7 \end{cases}$$

defines a straight line in 3-dimensional space. Each of these two system is a *system of parametric equations.* The letter "t" that occurs in each system is a *parameter*, meaning that if we give to this letter all possible values then we get all possible points of the corresponding line. This means that, if x, y, z are arbitrary real numbers, then

$$(x, y, z) \in L_1 \Leftrightarrow (\exists t \in \mathbb{R})(x = 2t + 1 \wedge (y = t - 2 \wedge z = 3t + 7))$$

and

$$(x, y, z) \in L_2 \Leftrightarrow (\exists t \in \mathbb{R})(x = t + 2 \wedge (y = 5t + 1 \wedge z = t + 7))\,.$$

(We read "$(x, y, z) \in L_1$" as "the point with coordinates x, y, z belongs to the line L_1.")

PROBLEM. Prove that the lines L_1 and L_2 do not intersect.

SOLUTION. We prove that L_1 and L_2 do not intersect. by contradiction.

Assume that L_1 and L_2 intersect. Pick a point (ξ, η, ζ) that belongs to both lines. Since $(\xi, \eta, \zeta) \in L_1$, there exists a t such that $\xi = 2t+1$, $\eta = t-2$, and $\zeta = 3t+7$. Pick one such t and call it t_1. Since $(\xi, \eta, \zeta) \in L_2$, there exists a t such that $\xi = t + 2$, $\eta = 5t + 1$, and $\zeta = t + 7$. Pick one such t and call it t_2. (IMPORTANT NOTE: We cannot give this second t the same name as the first t, because there is no reason for this second t to be the same as the first t, and if we called both ts by the same name we would be introducing the unwarranted hypothesis that they are the same.)

So now we have five real numbers $\xi, \eta, \zeta, t_1, t_2$, such that

$$\begin{aligned} \xi &= 2t_1 + 1\,, \\ \eta &= t_1 - 2\,, \\ \zeta &= 3t_1 + 7\,, \\ \xi &= t_2 + 2\,, \\ \eta &= 5t_2 + 1\,, \\ \zeta &= t_2 + 7\,. \end{aligned}$$

The first and fourth equation imply

$$2t_1 + 1 = t_2 + 2\,,$$

from which we conclude that

$$t_2 = 2t_1 - 1\,.$$

The second and fifth equation imply

$$t_1 - 2 = 5t_2 + 1\,,$$

from which we conclude that

$$t_1 = 5t_2 + 3\,.$$

The third and sixth equation imply

$$3t_1 + 7 = t_2 + 7\,,$$

so that

$$3t_1 = t_2\,.$$

So we have shown that

$$t_2 = 2t_1 - 1\,, \qquad t_1 = 5t_2 + 3\,, \qquad \text{and} \qquad 3t_1 = t_2\,.$$

We now show that these three equations together cannot hold. The third equation says that $3t_1 = t_2$, so we can plug in $3t_1$ for t_2 in the first two equations, and get

$$3t_1 = 2t_1 - 1 \qquad \text{and} \qquad t_1 = 15t_1 + 3\,.$$

The first equation implies $t_1 = -1$ and the second one implies $14t_1 + 3 = 0$, that is, $t_1 = -\frac{14}{3}$. So the number t_1 has to be equal both to -1 and to $-\frac{14}{3}$. But this is impossible, because $-1 \neq -\frac{14}{3}$.

So the assumption that the two lines intersect has led us to a contradiction, and we are done.

8.7 A sixth example: the Dirichlet pigeon-hole principle

THEOREM. Let N, M be positive integers such that $M > N$. Suppose we have N boxes and M toys, and put each toy in one of the boxes. Then at least one box will contain two or more toys.

PROOF. We do a proof by contradiction. Suppose it is not true that there is a box that contain two or more toys. This means that every box has either one toy or no toys at all. Then the total number of toys is equal to the number of boxes that contain one toy, which is not larger than the total n umber of boxes. That is, $M \geq N$. But this contradicts the fact that $M > N$. So we have reached a contradiction, ♢

8.8 A seventh example: proving that a string is not a well-formed formula

Let us prove that the string

$$P \wedge Q \vee R$$

is not a well-formed formula of the propositional calculus.

Proof by contradiction. Suppose $P \wedge Q \vee R$ was well formed. Then, by Rule PF8, this string would be obtainable by a sequence of steps, each of which is an application of one of the Rules PF1, PF2, PF3, PF4, PF5, PF6, PF7.

Let us ask which rule was the one that was applied last, leading directly to $P \wedge Q \vee R$. Could it have been Rule PF1? No!, because Rule PF1 only produces one-letter strings, and our string has four letters. Also, it couldn't have been Rule PF2 or Rule PF3, because those rules produce strings that start with a $\sim$, and our string does not start with a $\sim$. How about Rule PF4? That one is also impossible, because Rule PF4 only produces strings with three symbols, and our string has five. Finally, Rules PF5, PF6 and PF7 are also impossible, because the produce strings with parentheses, and our string has no parentheses.

So we have seen that our string, was (a) obtained by a last step in which one of the rules PF1, PF2, PF3, PF4, PF5, PF6, PF7 was applied, and (b) not obtained by a last step in which one of the rules PF1, PF2, PF3, PF4, PF5, PF6, PF7 was applied,

These two facts together add up to a contradiction. Hence $P \wedge Q \vee R$ is not well formed. ♢

8.9 An eighth example, on the intersection of two curves

Prove that the circles with equations

$$x^2 + y^2 = 1 \qquad \text{and} \qquad (x-4)^2 + y^2 = 2$$

do not intersect.

Proof by contradiction. Suppose they intersect. Pick a point (ξ, η) that belongs to both. This means that the numbers ξ, η satisfy

$$\xi^2 + \eta^2 = 1 \qquad \text{and} \qquad (\xi - 4)^2 + \eta^2 = 2\,.$$

But

$$(\xi - 4)^2 = \xi^2 - 8\xi + 16\,.$$

So the second equation says that

$$\xi^2 - 8\xi + 16 + \eta^2 = 2\,.$$

On the other hand, $\xi^2 + \eta^2 = 1$. Hence $1 - 8\xi + 16 = 2$, that is, $17 - 8\xi = 2$, and then $8\xi = 15$, so $\xi = \frac{15}{8}$. But then $\xi > 1$, so $\xi^2 > 1$, and then $\xi^2 + \eta^2 > 1$, contradicting the fact that $\xi^2 + \eta^2 = 1$. $\diamondsuit$

8.10 How important are proofs by contradiction?

In my personal opinion, **most proofs mathematicians write are proofs by contradiction or, at least, are originally conceived as proofs by contradiction, even if the author later figures out how to rewrite them as direct proofs.**

The reason, I believe, is quite simple. Suppose you want to prove a statement S, and you do not know what to do. In a direct proof, you would think of all the things that you know are true, and would try to find a way to use them to get to S. In a proof by contradiction, you place yourself in an imaginary world where S is false, so you can use all the things that you know are true in the "real" world, *and in addition you can use* $\sim S$ *as well.* So you have more information that you can use, and this makes it easier to get something done. In other words, the imaginary world that you set out to explore in a proof by contradiction is *richer* than the real world, in the sense that more interesting things are happening in it. Therefore, it's easier to work in this world.

9 Homework assignment No. 3, due on Thursday February 10

1. Prove that the product of two irrational numbers is irrational.

2. Prove that $\sqrt{5}$ is irrational.

3. Prove that $\sqrt{6}$ is irrational.

4. Consider the lines L_1, L_2 defined by the parametric equations

$$(L_1) \qquad \begin{cases} x = 2t+1 \\ y = t-2 \\ z = 3t+7 \end{cases}$$

and

$$(L_2) \qquad \begin{cases} x = t+6 \\ y = 5t-4 \\ z = t+15 \end{cases}$$

4.a Assign a grade (and justify your decision) to the following

Proof that the lines do not intersect. To find the intersection, we solve the system of equations

$$\begin{cases} x = 2t+1 \\ y = t-2 \\ z = 3t+7 \\ x = t+6 \\ y = 5t-4 \\ z = t+15 \end{cases} .$$

From the first and fourth equations we get $2t+1 = t+6$, so $t = 5$. From the second and fifth equations we get $t-2 = 5t-4$, so $4t = 2$, and then $t = \frac{1}{2}$. So $5 = \frac{1}{2}$, which is false. So we have reached a contradiction, and the lines do not intersect.

4.b Do the lines intersect? If they do intersect, prove it. If they do not intersect, prove it.

5. Prove that $((\sim P) \Rightarrow (Q \wedge (\sim Q))) \Rightarrow P$ is a tautology.

6. Prove that the string $(\sim P) \Rightarrow (Q \wedge R) \Rightarrow P$ is not well formed. *(Note: this is in principle easy, but it requires some work.)*

7. Book, §1.5 (page 44), Problem 12, items (a), (c), (d).

8. Book, §1.6 (pages 52-53) Problem 8, items (c), (e), (f), (g), (h), (i).