Math 358 – Foundations of Mathematics **Fall 2008**
8-28-08 Class Notes

Sections 1.3, 1.4
1.3: 41, 43, 52
1.4: 59, 67, 68, 69

Methods of Proof

Recall from Example 1 of the last set of notes the equation $x^2 - 3 = 1$. This is not a proposition because, as written, it is neither true nor false. Once we substitute values in place of x, it then becomes a proposition. So name this equation $P(x)$ (which we will call a **propositional function**). Although $P(x)$ is not a proposition, $P(-2)$ is a proposition (a true one) and $P(4)$ is a proposition (a false one). Another way to change a propositional function into a proposition is to add quantifiers. There are two types of quantifiers: universal and existential.

Definition: The **universal quantifier**, denoted by $\forall$, means "for all" or "for every". The **existential quantifier**, denoted by $\exists$, means "there exists" or "for some".

Using quantifiers is another way to create propositions from the propositional function $P(x)$. While $P(x)$ is *not* a proposition, the statement $\forall x P(x)$ ("for all x, $x^2 - 3 = 1$") is a proposition since it is false. Similarly, the expression $\exists x P(x)$ ("there exists an x such that $x^2 - 3 = 1$") is a proposition since it is true.

Example 1: Define $P(x): x^2 < x$. What are the truth values of $\forall x P(x)$ and $\exists x P(x)$?

Since $\left(\frac{1}{2}\right)^2$ is less than $\frac{1}{2}$, $\exists x P(x)$ is true, but clearly $\forall x P(x)$ is false.

You might have wondered why I allowed x to assume a non-integer value. This is in fact an important point. The **universe of discourse**, denoted by U, is the set of all values the variables can take on. For propositional functions that are algebraic, we assume it to be as large as possible considering the domains of the expressions involved unless otherwise stated. But for propositional functions of an alphabetic nature, we usually have to define our universe.

Example 2: Let U be all undergraduate Nicholls students. Define $P(x): x$ is required to take 42 hours of mathematics. What are the truth values of $\forall x P(x)$ and $\exists x P(x)$?

$\forall x P(x)$ is false (unfortunately) and but $\exists x P(x)$ is true.

This brings us back to the divide between mathematics and the English language. What is the opposite (or negation) of "For all x, $P(x)$ is true?" We might think that it is the other extreme, namely "For all x, $P(x)$ is false." (i.e. "For all x, $-P(x)$ is true.") But that's incorrect. Let's do an example.

Example 3: Let $U = 2\mathbb{Z} = \{\text{all even integers}\}$ and define $P(x): x\,\text{is divisble by}\,4$. What is the negation of $\forall x P(x)$? Recall that by definition, the negation of a statement must have the opposite truth value. But in this example, both $\forall x P(x)$ and $\forall x P(x)$ are false.

Look at this another way, if I claimed "For all x, $P(x)$ is true," how would you be able to contradict me? The opposite (or negation) is "For *some* x, $P(x)$ is false." Or "For some x, $-P(x)$ is true." In symbols,

$$-(\forall x P(x)) \Leftrightarrow \exists x(-P(x)).$$

As you can see, great care must be taken in translating from mathematics to English and vice versa.

Example 4: Let U be all people. Define $P(x)$ as "x loves baseball" and $Q(x)$ as "x hates hot dogs." Translate each of the following into English.

(a) $\forall x(P(x) \to Q(x))$
(b) $\exists x(P(x) \wedge -Q(x))$
(c) $-\exists x(P(x) \wedge Q(x))$
(d) $-\forall x(P(x) \vee Q(x))$

There are several ways to say these things. I'll write what I think is the most clear version.

(a) Everyone who loves baseball hates hot dogs.
(b) Some people love baseball and don't hate hot dogs.
(c) No one loves baseball and hates hot dogs.
(d) It is not true that everyone either loves baseball or hates hot dogs.

Now, we're ready to begin proving statements. Most mathematical statements to prove involve a quantifier (e.g. "There exists an odd perfect number." Or "Every polynomial is differentiable.") and most are implications of the form $p \to q$. In this section, we outline three of the main methods for proving statements.

Method of Proof 1: Direct Proofs

In this method, to prove that $p \to q$ is true, we show directly that q logically follows from p.

Example 5: Prove that the sum of two even integers is even.

To do this, we need to be able to identify the hypothesis (p) and the conclusion (q). Sometimes this requires rewriting the statement to be proved. In this example we wish to prove that if x and y are even integers, then $x+y$ is an even integer. So p is the statement "x and y are even integers", q is the statement "$x+y$ is an even integer." Direct proofs consist of assuming the proposition p is true, and then deducing that statement q must also then be true. Often this requires translating what the truth of p means and/or what q means.

> **Proof**: Let x and y be even integers. (Assuming p to be true) This means that there exists some integer m such that $x = 2m$ and some integer n such that $y = 2n$. (Translation of the hypothesis) We want to show that $x+y$ is even. (This is just a reminder of the desired conclusion to keep us on track) So we need to find an integer, call it k, such that $x + y = 2k$. (Translating the conclusion) However, since $x + y = 2m + 2n = 2(m + n)$, we can let $k = m + n$ and we are done. ■

Some comments are in order. (1) Often there will be several ways to reach the desired conclusion. So while you might do something different that what I do, it could still be logically correct. (2) In this proof, I actually found the integer needed to show that $x+y$ was even. This is called a constructionist proof. Sometimes, we will just show that it exists (even if we cannot find it). This is called an existential proof. The former is obviously a better type of proof, but it is not always possible. (3) Notice that after I stated the hypothesis, and translated it, I then stated the conclusion and translated it. Then I just needed to bridge the gap.

Example 6: Let x be an integer. Prove that if $7x+5$ is odd, then x is even.

> **Proof**: Since $7x+5$ is odd, there exists an integer n such that $7x+5=2n+1$ (definition of "odd"). So we have,
>
> $$\begin{aligned} 7x+5 &= 2n+1 \\ 7x &= 2n-4 \\ 7x &= 2(n-2). \qquad (*) \end{aligned}$$
>
> To show that x is even, we must show that we can write x as twice an integer (definition of "even").
>
> Now since 2 divides $2(n-2)$, it must also divide $7x$. But 7 is relatively prime to 2 (they have no common factors), so 2 must in fact divide x. Hence x is even.

Method of Proof 2: Contrapositive Proofs

The second method of proving the implication "if p, then q" is called the contrapositive method. We noted in our last set of notes that $p \to q$ and $-q \to -p$ are ***logically equivalent***. If we prove the latter, we are proving by the contrapositive method.

Example 7: Let's re-prove Example 6 using the contrapositive method. The statement was "Let x be an integer. Prove that if $7x+5$ is odd, then x is even."

> **Proof**: Suppose x is not even (this is $-q$). We want to show that $7x+5$ is not odd (this is $-p$). Obviously, if x is not even then x is odd, so there exists a integer n such that $x=2n+1$. Thus we have,
>
> $$7x+5=7(2n+1)+5=14n+12=2(7n+6),$$
>
> which is an even integer. So $7x+5$ is not odd.

Method of Proof 3: Indirect Proofs (a.k.a. Proofs By Contradiction)

> "How often have I said to you that when you have

> eliminated the impossible, whatever remains, however
> improbable, must be the truth."
>
> Sir Arthur Conan Doyle

The third method of proving the implication "if p, then q" is called the indirect method, more commonly called proof by contradiction. The strategy here is to assume both p and $-q$ are true and then arrive at a contradiction or impossible result. This will imply that our assumption was actually false (since it was logically equivalent to a contradiction). Therefore, if p is true, q must also be true. This is a very useful method of proving propositions because it gives you more hypotheses to work with.

Example 8: Let's re-prove Example 5 using contradiction. The statement was "Prove that the sum of two even integers is even."

Proof: Let x and y be even integers and suppose that $x+y$ is odd. (We are assuming p and $-q$.) We can rewrite each of these numbers based on their parity (i.e. their even-ness or odd-ness) as follows: $x=2a$, $y=2b$, and $x+y=2c+1$ for some integers a, b, and c. So we have,

$$\begin{aligned} x+y &= x+y \\ 2c+1 &= (2a)+(2b) \\ 1 &= 2a+2b-2c \\ 1 &= 2(a+b-c) \end{aligned}$$

But this shows that 1 is an even number, which we know is false. So our assumption was false and hence if x and y are even, so is $x+y$.

Proofs by contradiction are in some circles controversial. Essentially, we are showing that a statement cannot be false, therefore it must be true. What this assumes implicitly is that every statement is either true or false but not both. This assumption is called the **Law of the Excluded Middle**. Some people in older days rejected this law.