CS 201 Formal Foundations of Computer Science **Fall Semester, 2000**

Additional Material on Quantifiers (and Proofs)

September 25, 2000 *Handout 5*

In this handout we'll go over some additional examples on quantifiers. These examples were selected based on some of the common mistakes seen on Homework 2. First, here are some warnings about common mistakes that we've seen.

- Be very careful to NOT use something like $P(x)$ as a proposition — It is not a proposition since its truth value depends on x.
- In each problem there is a universe of discourse for each predicate. Also, if you have the statement $\forall x\ P(x) \vee Q(x)$, then P and Q must have the same universe of discourse – otherwise you could not write this statement. If you are asked whether

  $$\forall x\ (P(x) \vee Q(x)) \Longleftrightarrow (\forall x\ P(x)) \vee (\forall y\ Q(y))$$

  then clearly the predicate P used on both sides is the same and thus has the same universe of discourse on both sides. Likely, the predicate Q used on both sides is the same and thus has the same universe of discourse. Further, since we have the statement $\forall x\ P(x) \vee Q(x)$ on the left hand side, then we know that P and Q have the same universe of discourse. The fact that we use $Q(x)$ on the left and $Q(y)$ on the right is not what makes these two statements not logically equivalent.
- You cannot prove that a statement is a tautology by giving one example where it is true. For example, let $P(x)$ be that x is divisible by 6 and let $Q(x)$ be that x is divisible by 5. Consider the following claim: $\forall x\ P(x) \rightarrow Q(x)$. I could say, "Let $x = 30$, note that 30 is divisible by 6 and so $P(30)$ is true. Also, 30 is divisible by 5, and so $Q(30)$ is true. Thus we have $T \rightarrow T$ which means that the proposition $\forall x\ P(x) \rightarrow Q(x)$ is true.

  I hope everyone sees the flaw in the above "proof". What if I change $Q(x)$ to be that x is divisible by 3? Now it is the case that $\forall x\ P(x) \rightarrow Q(x)$ is true. But still if we gave the above as a proof it would not be a valid proof since all it shows is that $P(30) \rightarrow Q(30)$ is true. If you have ANY questions at all about this, please ask us.
- To prove that a statement is not a tautology you need just give a single example, called a *counterexample* for which it fails. However, do be sure what you give is a counterexample. Let's return to $\forall x\ P(x) \rightarrow Q(x)$ where $P(x)$ is x is divisible by 6 and $Q(x)$ is x is divisible by 5. Saying that $x = 15$ is a counterexample is wrong. Notice that $P(15) = F$ and $Q(15) = T$ and since $F \rightarrow T \Longleftrightarrow T$ this is not a counterexample. (Letting $x = 12$ is a valid counterexample.) Another thing that is not acceptable, is to begin a proof and then when you cannot go further, say that it must be false. If it is really false, then you should be able to find a counterexample. If you cannot find a counterexample, then it may be that the statement holds and you just have not yet determined how to prove it.

Here are several example problems (of various types) to help everyone understand how to work with quantifiers. The most important thing to remember is to think about the meaning and not try to convert everything into "symbol pushing." Let's begin with a sequence of examples to provide an alternate way for you to understand what is happening as you move quantifiers. We will assume that the universe of discourse for all the predicates is $x_1, x_2, x_3, \ldots$. If you want to apply the rules of logic to understand how quantified statements can be rewritten than you can replace $\forall x\ P(x)$ by $(P(x_1) \wedge P(x_2) \wedge \cdots)$ and replace $\exists x\ P(x)$ by $(P(x_1) \vee P(x_2) \vee \cdots)$. Let's start with an example that was done in class and then we can do some more complex examples. You will not be asked on the exam to do problems in this way but for those who are having trouble understanding what holds and what does not, this may be a good method for you to use.

Example 1

$$\begin{aligned}
(\forall x\ P(x)) \wedge (\forall x Q(x)) &\iff (P(x_1) \wedge P(x_2) \wedge \cdots) \wedge (Q(x_1) \wedge Q(x_2) \wedge \cdots) \\
&\iff (P(x_1) \wedge Q(x_1)) \wedge (P(x_2) \wedge Q(x_2)) \wedge \cdots \\
&\iff \forall x\ (P(x) \wedge Q(x))
\end{aligned}$$

Example 2

$$\begin{aligned}
(\forall x\ P(x)) \vee (\forall x Q(x)) &\iff (P(x_1) \wedge P(x_2) \wedge \cdots) \vee (Q(x_1) \wedge Q(x_2) \wedge \cdots) \\
&\iff (P(x_1) \vee (Q(x_1) \wedge Q(x_2) \wedge \cdots)) \wedge (P(x_2) \vee (Q(x_1) \wedge Q(x_2) \wedge \cdots)) \wedge \cdots \\
&\iff (P(x_1) \vee Q(x_1)) \wedge (P(x_1) \vee Q(x_2)) \wedge (P(x_1) \vee Q(x_3)) \wedge \cdots \\
&\qquad (P(x_2) \vee Q(x_1)) \wedge (P(x_2) \vee Q(x_2)) \wedge (P(x_2) \vee Q(x_3)) \wedge \cdots \\
&\qquad (P(x_3) \vee Q(x_1)) \wedge (P(x_3) \vee Q(x_2)) \wedge (P(x_3) \vee Q(x_3)) \wedge \cdots \\
&\iff \forall x\ \forall y\ (P(x) \vee Q(y))
\end{aligned}$$

Note that $(P(x_1) \vee (Q(x_1) \wedge Q(x_2) \wedge \cdots)) \wedge (P(x_2) \vee (Q(x_1) \wedge Q(x_2) \wedge \cdots)) \wedge \cdots$ (which is the second line in the above derivation) can be written as $\forall x\ (P(x) \vee \forall y\ Q(y)))$ and hence we've shown by the distributive property

$$(\forall x\ P(x)) \vee (\forall x Q(x)) \iff \forall x\ (P(x) \vee \forall y\ Q(y))) \iff \forall x\ \forall y\ (P(x) \vee Q(y))$$

Example 3

$$\begin{aligned}
\forall x\ \exists y\ (P(x) \rightarrow Q(y)) &\iff \forall x\ \exists y\ (\neg P(x) \vee Q(y)) \\
&\iff \forall x\ [(\neg P(x) \vee Q(x_1)) \vee (\neg P(x) \vee Q(x_2)) \vee \cdots] \\
&\iff \forall x\ (\neg P(x) \vee (Q(x_1) \vee Q(x_2) \vee \cdots)) \\
&\iff \forall x\ (\neg P(x) \vee \exists y\ Q(y)) \\
&\iff \forall x\ (P(x) \rightarrow \exists y\ Q(y))
\end{aligned}$$

Thus, we have shown that $\forall x\ \exists y\ (P(x) \rightarrow Q(y)) \iff \forall x\ (P(x) \rightarrow \exists y\ Q(y))$. However, we do not need to stop there. Let's go back to second to last step and continue our derivation.

$$\begin{aligned}\forall x\ \exists y\ (P(x) \to Q(y)) &\iff \forall x\ (\neg P(x) \vee \exists y\ Q(y)) \\ &\iff (\neg P(x_1) \vee \exists y\ Q(y)) \wedge (\neg P(x_2) \vee \exists y\ Q(y)) \wedge \cdots \\ &\iff (\neg P(x_1) \wedge \neg P(x_2) \wedge \cdots) \vee (\exists y\ Q(y)) \\ &\iff (\forall x\ \neg P(x)) \vee (\exists y\ Q(y)) \\ &\iff (\neg \exists x\ P(x)) \vee (\exists y\ Q(y)) \\ &\iff (\exists x\ P(x)) \to (\exists y\ Q(y)) \\ &\iff (\exists x\ P(x)) \to (\exists x\ Q(x))\end{aligned}$$

So we have shown that

$$\forall x\ \exists y\ (P(x) \to Q(y)) \iff \forall x\ (P(x) \to \exists y\ Q(y)) \iff (\exists x\ P(x)) \to (\exists x\ Q(x)).$$

Let's think through this. Let's start with the expression on the left hand side above. Suppose there is some $a \in U$ for which $Q(a)$ is true. Then $\forall x\ \exists y\ (P(x) \to Q(y))$ will be true. Otherwise (that is if $Q(a)$ is false for each $a \in U$), the only way that it could be true is if for all $a \in U$, $P(a)$ is false. In other words we are saying that

$$\forall x\ \exists y\ (P(x) \to Q(y)) \iff (\exists y\ Q(y)) \vee (\forall x\ \neg P(x)) \iff (\forall x\ \neg P(x)) \vee (\exists y\ Q(y))$$

Then like above we can then rewrite the rightmost expression above as $(\exists x\ P(x)) \to (\exists y\ Q(y))$. I strongly recommend that you make sure that you understand why

$$\forall x\ (P(x) \to \forall y\ Q(y)) \text{ and } (\forall x\ P(x)) \to (\forall y\ Q(y))$$

are NOT logically equivalent. If you don't please come talk to us about it.

Example 4

Finally, let's do one example where an indirect proof is used to prove that a quantified statement is a tautology. For each of the following suppose you are asked to prove whether or not it is a tautology.

(a) $[\ (\exists x\ P(x))\ \wedge\ (\exists x\ Q(x))\ ]\ \to\ [\ \exists x\ (P(x) \wedge Q(x))\ ]$

(b) $[\ \exists x\ (P(x) \wedge Q(x))\ ]\ \to\ [\ (\exists x\ P(x))\ \wedge\ (\exists x\ Q(x))\ ]$

For ease of exposition let me define the following three propositions:

r is $\exists x\ P(x)$
s is $\exists x\ Q(x)$
t is $\exists x\ (P(x) \wedge Q(x))$

For proposition P and Q, I will assume that the universe of discourse for x is $\{x_1, x_2, \ldots\}$. Hence each x_i represents one value permitted for the *variable* x.

If you have are given that $\forall x\ P(x)$ is true, then you know that for any x_i, $P(x_i)$ is true. However, if you are given that the statement $\exists x\ P(x)$ is true then you just know that for some object, say x_1, that $P(x_1)$ is true. Be very careful! If you are given that $(\exists x\ P(x)) \wedge (\exists x\ Q(x))$ is true then you CANNOT assume that for a single value of x, say x_1, that both $P(x_1)$ and $Q(x_1)$ are true. The *strongest* statement you can make is that for some x, say x_1, we have that $P(x_1)$ is true, and for some potentially different x, say x_2, $Q(x_2)$ is true.

Let's now consider the two problems given. I'll begin with (a) which is to prove whether or not $(r \wedge s) \rightarrow t$ is a tautology. You might begin by attempting to use a direct proof to show that it is a tautology. Hence, you would assume that $\exists x\ P(x)$ is true and $\exists x\ Q(x)$ is true. However, as we just discussed above, this does not give us that both $P(x)$ and $Q(x)$ are true for the same x. Hence, we can construct the following *counterexample* to *prove* that this is NOT a tautology. This is what the solution you would submit should look like. (Everything up to now was just discussion to help guide you.)

Part (a) is not a tautology. Here is a counterexample. Let $\{x_1, x_2\}$ be the universe of discourse. Consider when $P(x_1) = T$, $Q(x_1) = F$, $P(x_2) = F$, $Q(x_2) = T$. Since $P(x_1) = T$, $\exists x\ P(x)$ is true. Likewise, since $Q(x_2) = T$, $\exists x\ Q(x)$ is true. Hence $(\exists x\ P(x)) \wedge (\exists x\ Q(x))$ is true. Now let's consider $\exists x\ (P(x) \wedge Q(x))$. For x_1, we have that $Q(x_1) = F$ and hence $P(x_1) \wedge Q(x_1)$ is false. Likewise, for x_2, we have that $Q(x_2) = F$ and hence $P(x_2) \wedge Q(x_2)$ is false. Hence $\exists x\ (P(x) \wedge Q(x))$ is false. This completes the proof that part (a) is not a tautology.

We now prove that Part (b) is a tautology using an indirect proof. Recall that Part (b) is $t \rightarrow (r \wedge s)$. Hence we prove that the contrapositive, $\neg(r \wedge s) \rightarrow \neg t$ is a tautology. Thus we assume that $\neg(r \wedge s) \Longleftrightarrow \neg r \vee \neg s$ is true and we must show that

$$\neg t \Longleftrightarrow \neg \exists x\ (P(x) \wedge Q(x)) \Longleftrightarrow \forall x\ \neg(P(x) \wedge Q(x)) \Longleftrightarrow \forall x\ (\neg P(x) \vee \neg Q(x))$$

is true.
Assume that $\neg r \vee \neg s$ which is $(\neg\exists x\ P(x)) \vee (\neg\exists x\ Q(x))$ is true. Hence at least one of $\neg\exists x\ P(x)$ or $\neg\exists x\ Q(x)$ are true. First, let's assume that $\neg\exists x\ P(x) \Longleftrightarrow \forall x\ \neg P(x)$ is true. (That is, for each x_i, $P(x_i) = F$.) So for each x_i, $\neg P(x_i) \vee \neg Q(x_i) \Longleftrightarrow T \vee \neg Q(x_i) \Longleftrightarrow T$ and hence $\forall x\ (\neg P(x) \vee \neg Q(x))$ is true. Now suppose that $\neg\exists x\ Q(x) \Longleftrightarrow \forall x\ \neg Q(x)$ is true. (That is, for each x_i, $Q(x_i) = F$.) So for each x_i, $\neg P(x_1) \vee \neg Q(x_i) \Longleftrightarrow P(x_i) \vee T \Longleftrightarrow T$ and hence $\forall x\ (\neg P(x) \vee \neg Q(x))$ is true. Thus we have shown that (b) is a tautology.