Discrete Structures	Homework 2 Hints
CS2800 Fall 2013	Monday, September 16, 2013

Here are some tips on Homework 2 for those still struggling.

1. The purpose of this exercise is *not* to have you memorize the names of the rules of inference in Table 1, p. 72 and Table 2, p. 76. I do not care about that. I *do* care if you understand how quantification works.

   The real purpose of this exercise is to understand that a correct proof written in English represents a sequence of applications of rules of inference, and that in principle, we can take it down to the level of Example 13, p. 77 if we wish, although this is rarely done in practice. In most cases, small, obvious steps are not mentioned explicitly. Nevertheless, those steps are there, and every inference in a proof must be justified.

   A well-crafted proof, like a well-crafted program, is like poetry. The English proof given in the exercise is a good example. It is crisp, clear, and elegant. It says what it needs to say in a clear and precise way, no more and no less. You should always strive for this level of elegance in your proofs. Reread and revise them with your reader in mind. Make sure that all inferences are sound and that all ambiguities are removed.

2. You should restate the theorem stated in Rosen Ex. 16 p. 91 in a formal way, using quantifiers. If you do this correctly, you should get an implication whose premise is a single universal formula and whose conclusion is a disjunction of two universal formulas. This suggests that a good approach would be to prove the contrapositive (see p. 83), which would be an implication whose premise consists of two existential formulas and whose conclusion is an existential formula.

3. In this exercise, p and q are not propositional variables. They are metavariables ranging over all propositions. The theorem is a metatheorem about propositional logic. It is a universal statement; that is, there is an implicit universal quantification over all propositions p and q.

   To prove the equivalence of (i)–(iii), it is important to recall the definitions before doing anything. To say that p is a tautology means that p has value T under all truth assignments. Note that this is also a universal statement. It can be expressed with a universal quantifier that ranges over all truth assignments to propositional variables; equivalently, over all rows of a truth table. To say that $p \equiv q$ means that p and q have the same truth value under all truth assignments. Again, this is a universal statement, where the quantification ranges over all truth assignments.

   To show that (i) $\rightarrow$ (ii), you should start off by saying, "Suppose $p \rightarrow q$ is a tautology. Then..." Then follow it with what you know about tautologies. Use that assumption to prove that $p \equiv p \wedge q$ must hold.

4. For part (a), we have deliberately left unspecified what proof method you should use. The choice is up to you. You have several proof methods at your disposal, so use what you know.

   For part (b), you need to come up with a counterexample. All you need to do is specify a domain of discourse and a particular P for which the converse is not true.

5. You do not have to prove the algebraic rules being used, just say what they are. Here we are relying on you knowledge of the properties of the natural numbers. We will get into some basic number theory later in the course.

6. The line $N = p_1 p_2 \cdots p_n + 1 \implies (p_1|N) \vee (p_2|N) \vee \cdots (p_n|N)$ seems to be giving people a lot of trouble. The writer has not made clear the line of thought that leads to this inference. Note that this is a proof by contradiction. We have made the (erroneous) assumption that there are only finitely many primes $p_1, \ldots, p_n$. Then $N = p_1 \cdots p_n + 1$ cannot be one of them (Why not?). If N is not prime, then it must be composite, therefore must be divisible by one of the p_i.