CPSC 121 Midterm 2
Tuesday, March 19th, 2013

[9] 1. Proof Techniques

[3] a. When we use a direct proof for a statement of the form $\forall x \in D, P(x) \rightarrow Q(x)$, we first consider an unspecified element x of the domain, and then assume that $P(x)$ is true. Why do we make this assumption?

Solution : We make this assumption because if $P(x)$ is false for a given x, then the implication $P(x) \rightarrow Q(x)$ is automatically true. Hence the only case where we need to prove something about $Q(x)$ is the case where $P(x)$ is true.

[3] b. One of your friends claims to have proved the theorem

$$\forall n \in \mathbf{Z}^+, \forall x \in \mathbf{Z}^+, \forall y \in \mathbf{Z}^+, \forall z \in \mathbf{Z}^+, P(x, y, z, n)$$

where $P(x, y, z, n)$ is some complicated predicate involving x^n, y^n and z^n. You do not believe him, as you think his "theorem" is false. How would you prove this?

Solution : You would find values of x, y, z and n that make $P(x, y, z, n)$ false.

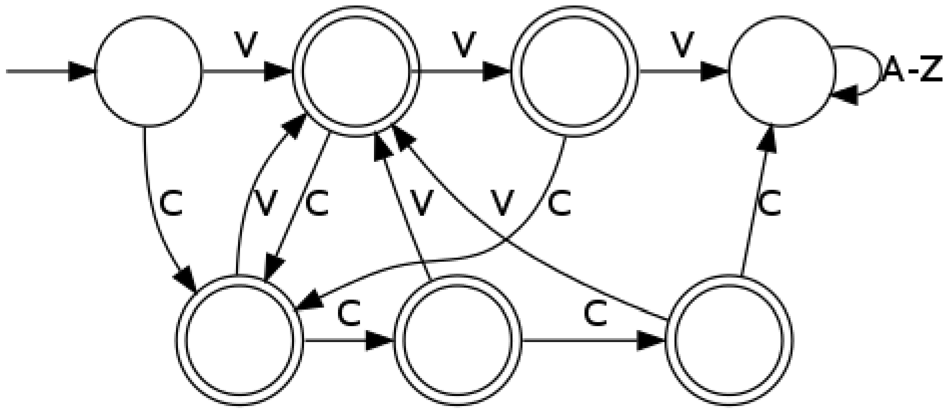
[3] c. In order to prove the theorem

$$\exists x \in \mathbf{Z}^+, \forall y \in \mathbf{Z}^+, Q(x, y)$$

a CPSC 121 instructor from a previous term chooses $x = y^2$ and an unspecified positive integer y, and then proves $Q(y^2, y)$ without making mistakes. Is the intructor's proof valid? Explain why or why not.

Solution : The instructor's proof is invalid: because $\exists x \in \mathbf{Z}^+$ comes before $\forall y \in \mathbf{Z}^+$, he must choose the value of x **first**, and can not select it based on the value of y. The chosen x must work for all possible y's.
Thinking in terms of the challenge method: if the instructor is trying to prove that this theorem is true, he will need to pick x before you choose y, and hence his value of x can not depend on the value of y you have not yet chosen.

[7] 2. Consider the following finite-state automaton, whose inputs are words written using upper-case letters (A through Z) only. The letter "C" on an edge denotes any consonant (B-D,F-H,J-N,P-T,V-Z), whereas the letter "V" denotes any vowel (A,E,I,O,U).



[4] a. Which of the following words will this finite-state automaton accept (circle one of Yes/No for each word)?

Solution :

• **ACQUAINTANCE**	Yes	[No]
• **AVADAKEDAVRA**	[Yes]	No
• **ENTHRONE**	Yes	[No]
• **FRIENDSHIP**	Yes	[No]
• **GOOEY**	Yes	[No]
• **MOTHERHOOD**	[Yes]	No
• **SCHNITZEL**	Yes	[No]
• **TROMBONE**	[Yes]	No

[3] b. Describe as simply as you can the set of words that this finite-state automaton accepts.

Solution : It accepts words that contain at most two consecutive vowels and at most three consecutive consonants.

[4] 3. Sketch a proof of the following theorem, using a proof technique of your choice:

> We can find integers x and y such that $P(x)$ and $P(y)$ and $P(xy + z)$ for some integer z.

As we did not tell you what property P is, you will not be able to write a complete proof. However write as much of it as you can.

Solution: This is a witness proof, because all of the quantifiers are existential ones: we would first choose specific integer values for x, y and z. We would then prove that, for these specific values, $P(x)$, $P(y)$ and $P(xy + z)$ are all true.

[5] 4. Sketch a proof by contradiction of the following theorem:

> You are in a lab section with a total of X students (including yourself). All X+2 of you (both teaching assistants are also present) write down the day of the week on which your birthdays fall this year. Your instructor then walks in and asks you to prove that at least Y of you wrote down the same day of the week.

As we did not tell you what X and Y are you will not be able to write a complete proof. Write as much of it as you can; stop when you reach a point where you would need to know the values of X and Y.

Solution: We would start by assuming that fewer than Y of the people present wrote down the same day of the week. Then we would prove a contradiction using that assumption, and the fact that a week has 7 days (the contradiction would most likely be that we had fewer than $X + 2$ people writing a day of week on their paper).

[5] 5. Sketch a proof by mathematical induction of the following theorem:

> For every positive integer n, the product of the first n numbers with property P is equal to $f(n)$.

As we did not tell you what property P is, or what $f(n)$ is, you will not be able to write a complete proof. However write as much of it as you can.

Solution: First we would prove the base case (the case $n = 1$). Then we would prove the induction step. That is, we would consider an unspecified integer $n > 1$, and assume that the product of the first $n - 1$ numbers with property P is $f(n - 1)$. We would then express the product of the first n integers with property P as the product of the first $n - 1$ integers with property P times the n^{th} integer x with property P. This would give us $f(n-1)$ times x, which we would then somehow prove is equal to $f(n)$.

[11] 6. Consider the following theorem:

> Every odd integer is the sum of two integers whose difference is equal to 5.

We can easily verify that this theorem holds for $n = 19$, for instance, since $19 = 7 + 12$. It also holds for 15, since $15 = 5 + 10$.

[3] a. Translate this theorem into predicate logic (that is, using predicates and quantifiers). The only non-standard predicate you can use is *Odd* (things like $=$ and $\leq$ are allowed, however). Hint: try to only use two variables.

Solution : $\forall n \in \mathbf{Z}, Odd(n) \rightarrow \exists x \in \mathbf{Z}, n = x + (x + 5)$

[8] b. Prove the theorem using a *direct proof*. Some of the marks for this proof will be given for the structure of your proof; others will be given for the contents.

Solution : Consider an unspecified integer n. Since n is odd, we can write $n = 2k + 1$ where k is another integer. Now, observe that

$$2k + 1 = (k - 2) + (k + 3)$$

Therefore we can choose $x = k - 2$, and n is indeed equal to $x + (x + 5)$ as required.

[9] 7. Recall that Euclid's algorithm to compute the greatest common divisor (GCD) of two positive integer works as follows:

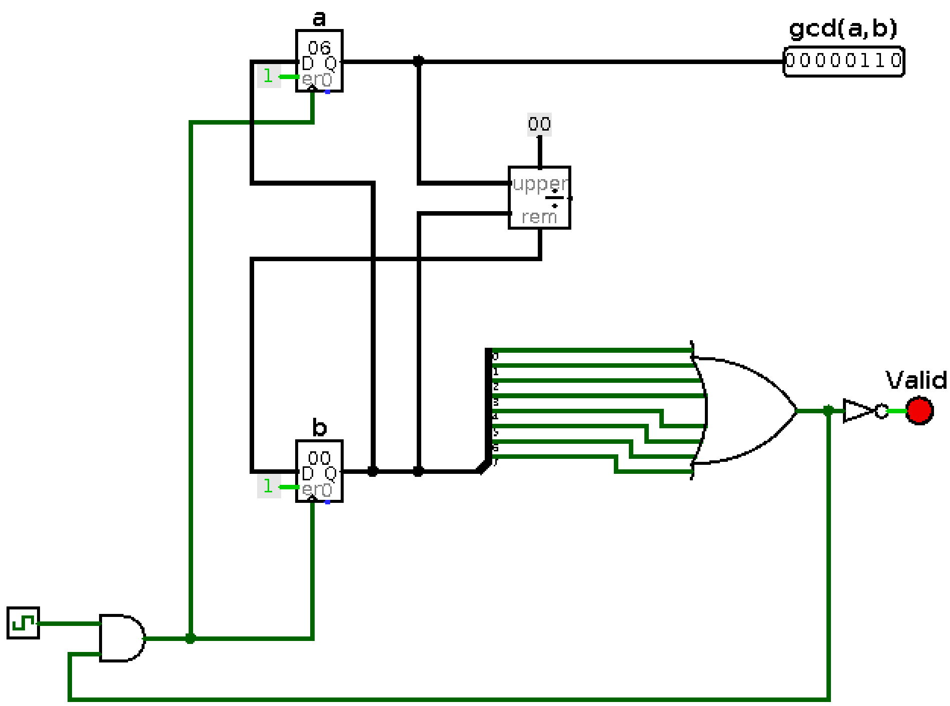
```
(define (gcd a b)
    (if (= b 0)
        a
        (gcd b (remainder a b))))
```

The following is an incomplete sequential circuit to compute the GCD of a pair of positive integers. The computation should start once the initial values of a and b have been entered into the two 8-bit registers `a` and `b`. A number of clock cycles later, the LED labeled `Valid` will be ON, and the output labeled `gcd(a,b)` will contain the GCD of a and b.

Complete the implementation of this circuit. The component labeled "upper" and "rem" is a Divider subcircuit: it takes one 16-bit input x (the 8 bits from the top input, and the 8 bits from the upper-left input) and one 8-bit input y (the 8 bits from the bottom-left input). It produces the quotient x/y (the value obtained by writing `(quotient x y)` in Dr. Racket) on the right output, and the remainder (`(remainder x y)`) on the bottom output.

Hint: consider the correspondence between the parameters in one recursive call and the parameters of the next one.

Solution : Note that the AND gate next to the clock is used to prevent a division by 0 once the answer has been found ($b = 0$) even if the clock keeps ticking.


a
06
D Q
1
en0
gcd(a,b)
00000110
00
upper
rem
b
00
D Q
1
en0
Valid