CPSC 121 Midterm 2
Tuesday March 15th, 2016

[10] 1. For each of the following statements, write down ALL of the proof strategies (from the list given below), that are appropriate to use to prove the statement. Just write down the LETTER for each strategy (do not write the full name):

A. Constructive or non-constructive direct proof of existence.

B. Exhaustive proof.

C. Direct proof by generalizing from a generic particular (i,e, let x be any non particular (unspecified)…).

D. Proof by cases.

E. Contrapositive proof.

F. Antecedent assumption (called direct proof by Epp).

G. Proof by contradiction.

Note that you must **NOT** prove the statement. You just need to suggest all the proof strategies which can be used to prove it. In some cases, translating the statement into predicate logic first might be useful (although it is not required).

[2] a. Every CPSC 121 student who plays tennis knows a student who enjoys swimming.

**Solution :** The only possible proof strategy is $B$. We did not deduct marks for students who also wrote C, although it seems unlikely that we could prove this statement by making an argument about an unspecified CPSC 121 student…

[2] b. If an integer $x$ can be written as $x = 5y + 7z$ for some integers $y$ and $z$, then $x + 1$ can be written as $x + 1 = 5y' + 7z'$ for some integers $y'$ and $z'$.

**Solution :** Possible proof strategies are C ($x$ is universally quantified), F (the statement contains an implication) and possibly D.

[2] c. An hexagon (6-sided polygon) can not have more than 3 angles that measure more than $200°$ each.

**Solution :** A possible proof strategy is $G$ (proving this directly would be difficult).

[2] d. At least four UBC Computer Science instructors went to the $46^{\text{th}}$ ACM Symposium on Computer Science Education, held from March $2^{\text{nd}}$ to March $5^{\text{th}}$ 2016 in Memphis, Tennessee.

**Solution :** A possible proof strategies is $A$ (all you need to do is name the four instructors and ask them to confirm they went to this conference).

[2] e. Every positive integer larger than 1 can be written as a sum of one or more, not necessarily distinct, primes.

**Solution :** A possible proof strategy is $C$ (the integer is universally quantified), and possibly $D$ (I can see two cases, depending on whether the integer is even or odd).

[5] 2. Provide a formal proof (by using one formal rule of inference at a time and explicitly stating the rule that is used on the right side) for the following argument. You don't need to rewrite the premises in the proof. Just continue with step 3.

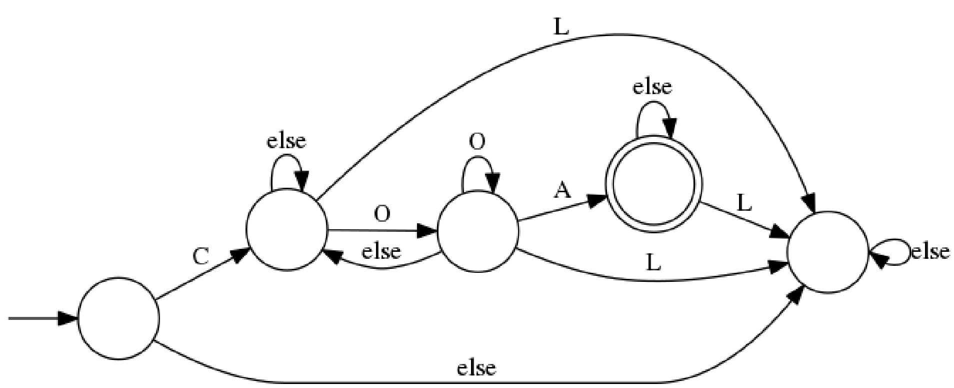
1. $\exists x \in D, \forall y \in D, \sim Q(x,y)$
2. $\forall x \in D, \exists y \in D, \sim P(x) \to Q(x,y)$

$\therefore\ \exists x \in D, P(x)$

**Solution :**

| | | |
|---|---|---|
| 3. | $\forall y \in D, \sim Q(a,y)$ | Existential instantiation from (1). a is a new unspecified element of D. |
| 4. | $\exists y \in D, \sim P(a) \to Q(a,y)$ | Universal instantiation from (2). |
| 5. | $\sim P(a) \to Q(a,b)$ | Existential instantiation from (4). b is a new unspecified element of D. |
| 6. | $\sim Q(a,b)$ | Universal instantiation from (3). |
| 7. | $\sim\sim P(a)$ | Modus tollens from (5) and (6). |
| 8. | $P(a)$ | Double negative law from (7). |
| 9. | $\exists x \in D, P(x)$. | Existential generalization from (8). |

[7] 3. Consider the following deterministic finite-state automaton:




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

**Solution :**

- **CROSSROAD** $\boxed{\text{Yes}}$ No
- **COLGATE** Yes $\boxed{\text{No}}$
- **BLOOD** Yes $\boxed{\text{No}}$
- **COCOON** Yes $\boxed{\text{No}}$
- **LOATH** Yes $\boxed{\text{No}}$
- **COCOA** $\boxed{\text{Yes}}$ No
- **OATMEAL** Yes $\boxed{\text{No}}$
- **COAXAL** Yes $\boxed{\text{No}}$

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

**Solution :** The DFA accepts any word that starts with `C`, does not contain the letter `L`, and contains the substring `OA`.

[5] 4. Prove the following logical argument **using a proof by contradiction**:

1. $p \vee r$
2. $p \to q$
3. $r \to t$
4. $\sim(t \vee u)$

---

$\therefore\ q$

**Solution :** Assume that the conclusion is false, that is

5. $\sim q$

We can then deduce the following argument:

| | | |
|---|---|---|
| 6. | $\sim p$ | Modus tollens from (2) and (5). |
| 7. | $r$ | Elimination from (1) and (6). |
| 8. | $t$ | Modus ponens from (3) and (7). |
| 9. | $\sim t \wedge \sim u$ | De Morgan's law from (4) |
| 10. | $\sim t$ | Simplification from (9). |
| 11. | $t \wedge \sim t$ | Conjunction from (8) and (10). |

and we have thus reached a contradiction. Note that the theorem can be proved using a direct proof, but you were asked specifically to use a proof by contradiction.

[16] 5. Prove each of the three following theorems using a proof technique of your choice.

a. Let us say that an integer $x$ is *almost divisible* by an integer $y$ if dividing $x$ by $y$ leaves a remainder that is either 1 or $y-1$. For instance, both 15 and 20 are almost divisible by 7.

**Theorem**: If an integer $x$ is almost divisible by an integer $y$, then dividing $x^2$ by $y$ always leaves a remainder of 1.

**Solution :** We use a proof by cases. Consider unspecified integer $x$ and $y$. Assume that $x$ is almost divisible by $y$.

**Case 1** : If $x$ divided by $y$ leaves a remainder of 1, then we can write $x = ay + 1$ for some integer $a$. Hence

$$x^2 = (ay+1)^2 = a^2y^2 + 2ay + 1 = y(a^2y + 2a) + 1$$

and hence dividing $x^2$ by $y$ leaves a remainder of 1.

**Case 2** : If $x$ divided by $y$ leaves a remainder of $y-1$, then we can write $x = ay + (y-1)$ for some integer $a$. Hence

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

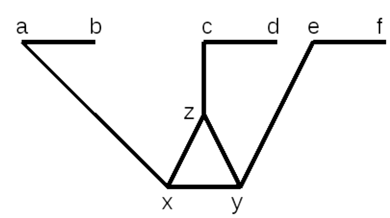
and hence dividing $x^2$ by $y$ leaves a remainder of 1.

This completes the proof of the theorem.

b. **Theorem**: There are primes whose product is one less than another prime.

**Solution :** Choose $x = 2$ and $y = 3$. Then $xy + 1 = 7$, which is also a prime. Note that there are many other possible choices of $x$ and $y$ that work; all of them require 2 to be one of the primes selected.

c. Suppose that we have an art gallery that is shaped (rather strangely) as follows:




Each line segment is a corridor; corners are labeled $a$, $b$, $c$, $d$, $e$, $f$, $x$, $y$ and $z$. We want to place guards at some of the corners, in order to guard the art work displayed in each of the corridors, and we'd like to use as few guards as possible (they're expensive).

Observe that either corner $a$ or corner $b$ must have a guard (otherwise the corridor joining them isn't guarded). Similarly, either corner $c$ or corner $d$ must have a guard, and either corner $e$ or corner $f$ must have a guard.

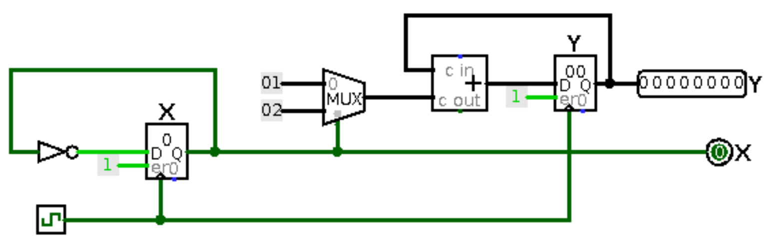
**Theorem**: If we placed a guard at at least one of corners $a$, $c$ and $e$, then we will only need to place guards at TWO of corners $x$, $y$ and $z$.

**Solution :** There are two possible approaches to this problem. First, we can divide the proof into three cases: one where there is a guard at $a$ (there may or may not be guards at $c$ and $e$), one where there is a guard at $c$ (there may or may not be guards at $a$ and $e$), and one where there is a guard at $e$ (there may or may not be guards at $a$ and $c$). However the problem is symmetrical with respect to $a$, $c$ and $e$, which means only one case really needs to be considered.

So, assume without loss of generality that there is a guard at corner $a$. We then place guards at $y$ and $z$. These guards will cover all of the corridors $ax$, $cy$, $ez$, $xy$, $xz$ and $yz$. A guard at $x$ would not cover any new corridor, and is thus unnecessary.

Note that we will need guards at either $d$ or $e$, and either $e$ of $f$, but these are not mentioned on the right-hand side of the implication in the theorem, and hence the proof does not need to worry about them.

[7] 6. Consider the following sequential circuit:




Please observe that the registers labeled X and Y initially contain the value $0$.

[3] a. Fill in the following table indicating the contents of registers X and Y after $1$, $2$, $3$, $4$ and $5$ clock cycles.

**Solution :** Please note that a clock cycle consists of the clock going from LOW to HIGH and then back to LOW, and that the two registers take in new values AT THE SAME TIME (so the new value of X does not contribute to the new value of Y).

| Clock cycles | X | Y |
|---|---|---|
| 1 | 1 | 1 |
| 2 | 0 | 3 |
| 3 | 1 | 4 |
| 4 | 0 | 6 |
| 5 | 1 | 7 |

[4] b. The following sequential circuit will output `1` if the sequence of bits it receives as input contains three **consecutive** 1 bits. Unfortunately the instructor designing the circuit made **two mistakes**, and **left out a small part of the circuit**. Fix the mistakes and add the part of the circuit that was left out.

**Solution :** The two mistakes were (1) the wires connected to the clock and D inputs of the second flip-flop from the left were reversed and (2) the OR gate should have been an AND. The missing part of the circuit uses feedback from the rightmost flip-flop to set its D input to TRUE if either it was already true, or the output of the AND gate (three consecutive 1 bits) is true. The complete circuit is shown below.