CPSC 121 Midterm 2
Monday November 14th, 2016

[15] 1. Consider the theorem

For any integer n, if $2^n - 1$ is a prime, then n is also prime.

[3] a. Translate the theorem statement into predicate logic. You can use the predicate *Prime*(x) which is true when x is a prime.

Solution: $\forall n \in \mathbf{Z}, \mathit{Prime}(2^n - 1) \rightarrow \mathit{Prime}(n)$.

[4] b. Suppose that you decide to prove this theorem using a **direct proof**. Write down what you would assume and what you would need to show. You can use the predicate *Prime*(x). **Do not prove the theorem.**

Solution: You would consider an unspecified integer n, and assume that $2^n - 1$ is prime. You would need to prove that n is prime.

[4] c. Suppose that you decide to prove this theorem using a **proof by contrapositive**. Write down what you would assume and what you would need to show. You can use the predicate *Prime*(x). **Do not prove the theorem.**

Solution: You would consider an unspecified integer n, and assume that n is **not** prime. You would need to prove that $2^n - 1$ is not prime.

[4] d. Suppose that you decide to prove this theorem using a **proof by contradiction**. Write down what you would assume and what you would need to show. You can use the predicate *Prime*(x). **Do not prove the theorem.**

Solution: You would assume that some integer n is not prime, but that $2^n - 1$ is prime. Then you would need to prove a contradiction (any contradiction will work).

[15] 2. Your friend designed an algorithm whose execution requires $4n^3 + 2n^2$ steps where n is the size of the input.

Hint: Suppose that an algorithm runs in $f(n)$ steps where n is the size of the input. Recall that the number of steps of this algorithm is in $O(g)$ if the following proposition is true:

$$\exists c \in \mathbf{R}^+ \, \exists n_0 \in \mathbf{N} \, \forall n \in \mathbf{N}, n \geq n_0 \rightarrow f(n) \leq cg(n). \qquad (*)$$

[6] a. Prove that the number of steps of your friend's algorithm is in $O(n^4)$.

Solution: Choose n_0 = 1 and $c = 6$, and consider an unspecified positive integer $n \geq n_0$. For this n,

$$\begin{aligned} 4n^3 + 2n^2 &\leq 4n^3 + 2n^3 \qquad \text{because } n \geq 1 \\ &= 6n^3 \\ &\leq 6n^4 \qquad \text{because } n \geq 1 \end{aligned}$$

Therefore $4n^3 + 2n^3 \in O(n^4)$.

[3] b. Negate the proposition in $(*)$ and bring the negation all the way to the right so that there is no negation in front of any quantifier.

Solution : The negation is:

$$\begin{aligned}
&\sim \exists c \in \mathbf{R}^+ \, \exists n_0 \in \mathbf{N} \, \forall n \in \mathbf{N}, n \geq n_0 \rightarrow f(n) \leq cg(n) \\
&\quad \equiv \forall c \in \mathbf{R}^+ \ \sim \exists n_0 \in \mathbf{N} \, \forall n \in \mathbf{N}, n \geq n_0 \rightarrow f(n) \leq cg(n) \\
&\quad \equiv \forall c \in \mathbf{R}^+ \, \forall n_0 \in \mathbf{N} \ \sim \forall n \in \mathbf{N}, n \geq n_0 \rightarrow f(n) \leq cg(n) \\
&\quad \equiv \forall c \in \mathbf{R}^+ \, \forall n_0 \in \mathbf{N} \, \exists n \in \mathbf{N}, \sim (n \geq n_0 \rightarrow f(n) \leq cg(n)) \\
&\quad \equiv \forall c \in \mathbf{R}^+ \, \forall n_0 \in \mathbf{N} \, \exists n \in \mathbf{N}, \sim (\sim (n \geq n_0) \vee f(n) \leq cg(n)) \\
&\quad \equiv \forall c \in \mathbf{R}^+ \, \forall n_0 \in \mathbf{N} \, \exists n \in \mathbf{N}, \sim\sim (n \geq n_0) \wedge \sim (f(n) \leq cg(n)) \\
&\quad \equiv \forall c \in \mathbf{R}^+ \, \forall n_0 \in \mathbf{N} \, \exists n \in \mathbf{N}, (n \geq n_0) \wedge f(n) > cg(n))
\end{aligned}$$

[6] c. **Using the proposition in part b**, prove that the number of steps of your friend's algorithm is **NOT** in $O(n^2)$.

Solution : We use a direct proof using the result of part (b). Consider an unspecified positive real number c, and an unspecified natural number n_0. Choose any natural number n larger than both n_0 and c, for instance $n = \max\{n_0 + 1, \lceil c \rceil + 1\}$. Then

$$\begin{aligned}
4n^3 + 2n^2 &\geq 4n^3 && 4n^3 \text{ is positive} \\
&> n^3 && \text{dividing a positive integer by 4 makes it smaller} \\
&= n \cdot n^2 \\
&> c \cdot n^2 && \text{because } n > c
\end{aligned}$$

Therefore $4n^3 + 2n^2 > cn^2$ as required.

[10] 3. Consider the following theorem:

For any integers a, b and c, if $a^2 + b^2 = c^2$, then at least one of a and b is even. $(*)$

To guide you through proving this theorem, we broke down the proof into 3 steps below.

[3] a. First, prove that for any integers a, b and c, if $a^2 + b^2 = c^2$ and a and b are both odd, then c^2 is even.

Solution : Consider any two unspecified integers a, and b. Assume a and b are both odd, which means we can write $a = 2i + 1$ for some integer i and $b = 2j + 1$ for some integer j. Then $a^2 + b^2 = (2i+1)^2 + (2j+1)^2 = 4i^2 + 4i + 1 + 4j^2 + 4j + 1 = 2(2i^2 + 2j^2 + 2i + 2j + 1)$. Because i and j are integers, so is $2i^2 + 2j^2 + 2i + 2j + 1$, and therefore $a^2 + b^2$ is even.

[3] b. Second, prove that for any integer c, if c^2 is even, then c^2 is divisible by 4.

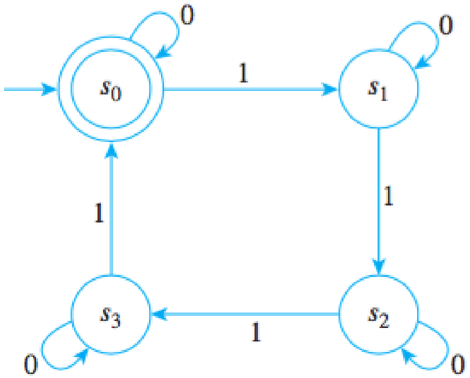
Hint: we proved in class that if the square n^2 of an integer n is even, then n is even.

Solution : Consider an unspecified integer c. If c^2 is even, then by the hint c is even. Thus $c = 2k$ where k is an integer. The integer c^2 is therefore equal to $4k^2$. Since k is an integer, so is k^2, and hence c^2 is divisible by 4.

[4] c. Prove theorem $(*)$ using the results from part (a) and (b) above.
Hint 1: a **proof by contradiction** works well here.
Hint 2: it may be useful to show that $(a^2 + b^2)$ is not divisible by 4.

Solution : We use a proof by contradiction. Suppose that there are integers a, b and c such that $a^2 + b^2 = c^2$ and both a and b are odd. On the one hand, from part (a) we know that c^2 is even, and thus from part (b) it must be divisible by 4. On the other hand, our calculation from part (a) shows that $c^2 = a^2 + b^2 = 4i^2 + 4i + 1 + 4j^2 + 4j + 1 = 4(i^2 + j^2 + i + j) + 2$, and so c^2 is not divisible by 4. These two facts contradict one another, which means that at least one of a or b must be even.

[9] 4. Consider the following deterministic finite-state automaton. Assume that every input is a string of 0's and 1's.



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

Solution :

- **01010** Yes [✓ No]
- **11001** Yes [✓ No]
- **110110** [✓ Yes] No
- **101111** Yes [✓ No]
- **1101101** Yes [✓ No]
- **111101100** Yes [✓ No]

- **110111011** Yes [✓ No]
- **111101111** [✓ Yes] No

[3] b. Describe as simply as possible the set of inputs that will lead you to each state.

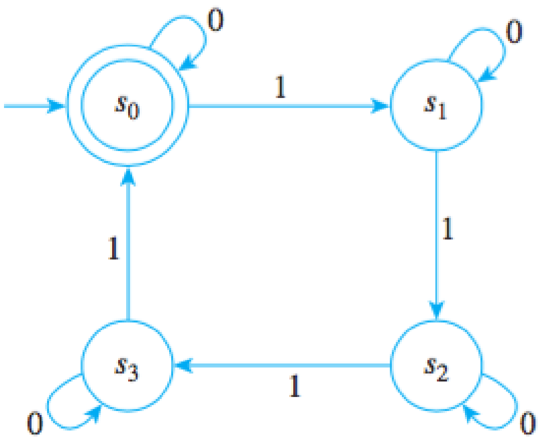
Solution : Let k be the number of 1's in the input string. The states have the following meanings:

- State s0: k is divisible by 4.
- State s1: k divided by 4 has a remainder of 1.
- State s2: k divided by 4 has a remainder of 2.
- State s3: k divided by 4 has a remainder of 3.

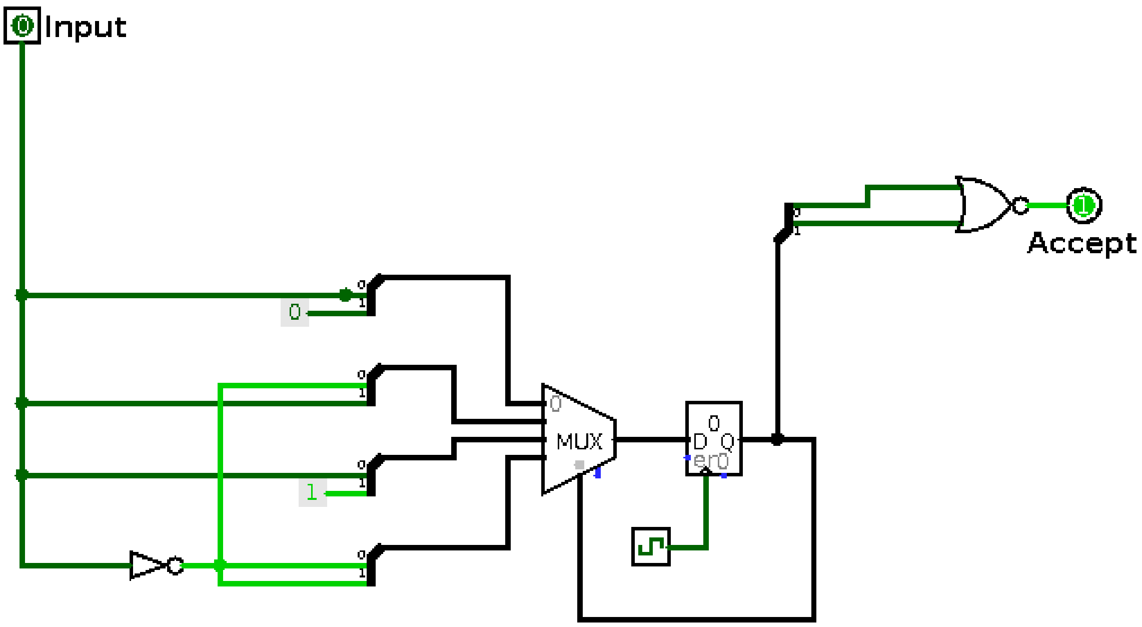
[2] c. Describe as simply as you can the set of strings that this finite-state automaton accepts.

Solution : The DFA accepts any string of bits for which the number of 1's in the string is divisible by 4.

[6] 5. Convert the DFA to a sequential circuit. We have given you several components of the sequential circuit below. Please fill in the missing parts.



Solution :


0
Input
0
1
0
0
1
0
1
0
1
1
0
1
0
MUX
0
D
Q
en
0
0
1
1
Accept