Name Student ID

# CSE 311: Foundations of Computing I
# Spring 2011

## Final exam - *with solutions*

1. **Logic, proofs, sets and functions.** (25 points; 5+10+10)

   (a) *Prove or disprove:* $\exists x \in \mathbb{R}^+, \forall y \in \mathbb{R}(y \geq x \rightarrow y^2 \geq 2y)$.

   (b) *Let* $P(S)$ *denote the power set of* $S$*; i.e.* $P(S) = \{T : T \subseteq S\}$. *Prove that* $A \subseteq B$ *if and only if* $P(A) \subseteq P(B)$.

   (c) *Let* $S$ *and* $T$ *be subsets of a universal set* $U$*, and define* $A_{0,0} = S \cap T$, $A_{0,1} = S \cap \bar{T}$, $A_{1,0} = \bar{S} \cap T$ *and* $A_{1,1} = \bar{S} \cap \bar{T}$. *Express* $S \cup T$ *as a union of some or all of the* $\{A_{0,0}, A_{0,1}, A_{1,0}, A_{1,1}\}$. *You do not need to prove your answer.* Hint: You may find a Venn diagram helpful, although it is not required.

   (a) Choose $x = 2$. Then we use a direct proof to show that $y \geq x \rightarrow y^2 \geq 2y$. Assume that $y \geq x = 2$. Since $y \geq 0$, we can multiply both sides by $y$ and still have a valid inequality: $y^2 \geq 2y$. QED

   (b) For one direction, assume that $A \subseteq B$. We will use a direct proof to show that $\forall S\,(S \in P(A) \rightarrow S \in P(B))$.

| | |
|---|---|
| $S \in P(A)$ | by assumption |
| $S \subseteq A$ | by the definition of a power set |
| $S \subseteq B$ | using the fact that $A \subseteq B$ |
| $S \in P(B)$ | by the definition of a power set |

   Since $\forall S\,(S \in P(A) \rightarrow S \in P(B))$, we have that $P(A) \subseteq P(B)$.
   For the other direction, assume that $P(A) \subseteq P(B)$.

| | | |
|---|---|---|
| $P(A) \subseteq P(B)$ | by assumption | (1) |
| $A \subseteq A$ | set identity (this step could be skipped) | (2) |
| $A \in P(A)$ | definition of power set | (3) |
| $A \in P(B)$ | by (1) and (3) | (4) |
| $A \subseteq B$ | definition of power set | (5) |

   (c) $S \cup T = A_{0,0} \cup A_{0,1} \cup A_{1,0}$.

2. **Number theory.**(25 points; 5+10+10)

   (a) *Use Euclid's algorithm to compute the gcd of 328 and 432. Write down the numbers you obtain at the intermediate steps.*

   (b) *Prove that if* $a, b \in \mathbb{Z}$ *and* $b > 0$*, then there exist unique* $q, r \in \mathbb{Z}$ *satisfying* $a = bq - r$ *(note the* $-$ *here) and* $0 \leq r < b$.

   (c) *One type of cicada living in the Eastern US has a lifecycle of 17 years, has appeared in 1970, 1987, 2004, and next will appear in 2021. Suppose that a parasite that attacks the cicadas has an* $n$*-year lifecycle, and also appeared in 1970, then* $1970 + n$, $1970 + 2n$, *etc. Assume that* $1 \leq n \leq 16$. *If the cicadas and parasites both appeared in the same year in 1970, in what year will they next both appear?*

(a)

$$\begin{aligned}
432 &= 1 \cdot 328 + 104 \\
328 &= 3 \cdot 104 + 16 \\
104 &= 6 \cdot 16 + 8 \\
16 &= 2 \cdot 8 + 0
\end{aligned}$$

The GCD is 8.

(b) First we prove existence. Use the (conventional) division algorithm to obtain integers $q', r'$ such that $a = bq' + r'$ and $0 \leq r' < b$. Define $r = b - r'$ and $q = q' + 1$. Since $0 \leq r' < b$, we also have $0 \leq r < b$. Also $bq - r = b(q' + 1) - (b - r') = bq' + r' = a$, so $q, r$ are a valid solution. For uniqueness, we can either prove it directly (e.g. showing that two different valid pairs of $q, r$ must be the same) or we can use the fact that this process can be run in reverse. To do this, suppose we are given some $q, r$ satisfying $a = bq - r$ and $0 \leq r < b$. Then define $r' = b - r$ and $q' = q - 1$. These satisfy $0 \leq r' < b$ and $a = bq' + r'$, and so by the (conventional) division algorithm, the pair $q', r'$ are unique. Since the map from $(q, r)$ to $(q', r')$ is one-to-one, this implies that $q, r$ must be unique as well.

(c) $1970 + 17n$.

3. **Induction and recursion.** (30 points; 10+20)

*(a) Prove using induction that* $\sum_{k=1}^{n} k^2 = n(n+1)(2n+1)/6$ *for all positive integers* $n$.

*(b) Euclid's algorithm for computing the GCD of a pair of positive integers* $a, b$ *is as follows:*

*EUCLID*$(a, b)$*:*
    *If* $(a < b)$ *return EUCLID*$(b, a)$
    *If* $b = 0$ *return* $a$
    *Use the division algorithm to compute* $q, r \in \mathbb{Z}$ *such that* $a = bq + r$ *and* $0 \leq r < b$.
    *Return EUCLID*$(b, r)$

*Define* $P(a)$ *to the predicate that EUCLID*$(a, b)$ *returns gcd*$(a, b)$ *for all* $0 \leq b < a$. *Use strong induction to prove that EUCLID*$(a, b)$ *=gcd*$(a, b)$ *for all positive integers* $a, b$.

(a) Let $P(n)$ be the predicate that the stated identity holds for $n$. The base case is $P(1)$: we verify that $1^2 = 1(1 + 1)(2 + 1)/6$. Assume that $P(k)$ holds for some integer $k \geq 1$. Then

$$\begin{aligned}
\sum_{j=1}^{k+1} j^2 &= (k+1)^2 + \sum_{j=1}^{k} j^2 \\
&= (k+1)^2 + \frac{k(k+1)(2k+1)}{6} && \text{induction hypothesis} \\
&= (k+1)\frac{6(k+1) + k(2k+1)}{6} \\
&= (k+1)\frac{2k^2 + 7k + 6}{6} \\
&= (k+1)\frac{(k+2)(2k+3)}{6} \\
&= \frac{(k+1)((k+1)+1)(2(k+1)+1)}{6} && \text{implying } P(k+1)
\end{aligned}$$

By induction $P(n)$ holds for all positive integers $n$.

(b) Base case: $P(1)$ is the statement that EUCLID(1,0) returns $\gcd(1,0) = 1$, which is true. For the inductive step, assume $P(1) \wedge P(2) \cdots \wedge P(a)$. We will attempt to prove $P(a+1)$. For this, we use a direct proof. Assume that $b$ is an integer satisfying $0 \leq b < a+1$. Consider the behavior of EUCLID when given inputs $(a+1, b)$.

If $b = 0$, then it returns $a+1$, which equals $\gcd(a+1, 0)$, so in this case $P(a+1)$ is true.

If $b > 0$, then the algorithm computes $q, r$ satisfying $a+1 = bq + r$, $0 \leq r < b$ and returns the result of running EUCLID on $(b, r)$. Since $b < a+1$, the inductive hypothesis implies that $P(b)$ holds, and since $r < b$, this means that EUCLID$(b, r)$ returns $\gcd(b, r)$. Next Lemma 1 of Section 3.6 of Rosen implies that $\gcd(b, r) = \gcd(a+1, b)$. This establishes $P(a+1)$, and so by strong induction, EUCLID$(a, b)$ returns $\gcd(a, b)$ whenever $0 \leq b < a$.

If $b > a$, then the first line of EUCLID reduces this to the case when $b < a$.

Finally, if $a = b$, then the division step will obtain $r = 0$, and EUCLID will return the value of EUCLID on $(b, 0)$, which is $b = \gcd(a, b)$.

Thus, EUCLID returns the gcd for all pairs of positive integers $a, b$.

4. **Relations.** (15 points; 5+10)

   *(a) Define the rock-paper-scissors relation on $S = \{r, p, s\}$ by $R = \{(r,r), (p,p), (s,s), (p,r), (r,s), (s,p)\}$. Is this relation a partial order? Why or why not?*

   *(b) Consider the relation $R$ on $\mathbb{R}$ given by $\{(x,y) | x - y \in \mathbb{Z}\}$.*

   *i. Prove that $R$ is an equivalence relation.*

   *ii. What is the equivalence class of 1? What is the equivalence class of 0.5?*

(a) It's not a partial order because it's not transitive: $(p,r) \in R \wedge (r,s) \in R$ but $(p,s) \notin R$. In English, paper beats-or-ties rock and rock beats-or-ties scissors, but paper does not beat or tie scissors.

(b) i. Reflexivity: $x \in \mathbb{R} \rightarrow x - x = 0 \in \mathbb{Z}$. Symmetry: $(x,y) \in R \rightarrow x - y \in \mathbb{Z} \rightarrow y - x \in \mathbb{Z} \rightarrow (y,x) \in R$. Transitivity: $((x,y) \in R \wedge (y,z) \in R) \rightarrow (x - y \in \mathbb{Z} \wedge y - z \in \mathbb{Z}) \rightarrow (x - z \in \mathbb{Z}) \rightarrow ((x,z) \in R)$.

   ii. $\mathbb{Z}$. $\{z + 1/2 : z \in \mathbb{Z}\}$.

5. **Graphs and trees.** (15 points; 5+10)

   *(a) Define the complete graph $K_n$ to be the undirected graph on $n$ vertices with no self-loops and with all possible edges present. Prove by induction that $K_n$ has $\sum_{k=1}^{n-1} k$ edges.*

   *(b) Draw a directed graph with four vertices such that the edges form a partial order. Your score on this question will be 1 point per edge that you draw, or 0 if what you draw isn't a partial order.*

(a) Let $P(n)$ be the claim about $K_n$. $P(1)$ is true because $K_0$ has no edges. Assume $P(k)$ is true for some $k \geq 1$. Consider an arbitrary vertex of $K_k$. It has $k-1$ edges to the other $k-1$ vertices. Remove this vertex and the $k-1$ edges and we are left with $K_{k-1}$, which by the inductive hypothesis has $\sum_{j=1}^{k-2} j$ edges. Thus $K_k$ has $\sum_{j=1}^{k-2} j + (k-1) = \sum_{j=1}^{k-1} j$ edges.

(b) Consider the graph with vertices $\{1,2,3,4\}$ and edges $\{(1,1), (1,2), (1,3), (1,4), (2,2), (2,3), (2,4), (3,3), (3,4), (4,4$

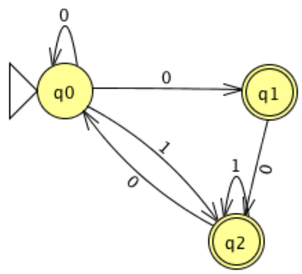


Figure 1: A non-deterministic finite automaton.

6. **Circuits and boolean algebra.** (15 points) *The goal of this problem is to prove that AND and OR are not functionally complete. Let $x_1, \ldots, x_n$ be boolean variables for some $n \geq 1$. We say that a boolean function $F(x_1, \ldots, x_n)$ is monotone if*

$$\forall x_1, \ldots, x_n \in \{0,1\}, \forall i \in [n]\, (F(x_1, \ldots, x_n) = 1 \rightarrow F(x_1, \ldots, x_{i-1}, 1, x_{i+1}, \ldots, x_n) = 1).$$

*In other words, if $F$ equals 1 for some input, then changing one of those inputs to 1 will not change $F$.*

  *(a) Suppose that $F(x_1, \ldots, x_n)$ is a boolean function constructed from AND and OR gates. Prove, using structural induction, that $F$ is monotone.*

  *(b) Give an example of a boolean function that is not monotone.*

  (a) The base case is to consider a circuit that outputs simply $x_j$ for some $j \in [n]$. This is monotone because if $x_j = 1$ then setting some $x_i$ to 1 (whether or not $i = j$) will not change this. For the inductive step, we note that an AND-OR circuit can be constructed from smaller AND-OR circuits by combining their output with an AND or an OR. Call the new AND-OR circuit $F$ and the smaller ones $G$ and $H$, so that either $F = G + H$ or $F = GH$. By the inductive hypothesis, we assume that $G$ and $H$ are monotone. Then changing one of the $x_i$'s to 1 will not change either $G$ or $H$ from 1 to 0, which will not change $F$ from 1 to 0.

  To make this more formal, we define $f = F(x_1, \ldots, x_n)$, $f' = F(x_1, \ldots, x_{i=1}, 1, x_{i+1}, \ldots x_n)$ $g = G(x_1, \ldots, x_n)$, $g' = G(x_1, \ldots, x_{i=1}, 1, x_{i+1}, \ldots x_n)$ $h = H(x_1, \ldots, x_n)$, $h' = H(x_1, \ldots, x_{i=1}, 1, x_{i+1}, \ldots x_n)$. The first case is that $F = GH$ so that $f = gh$ and $f' = g'h'$. In this case, $f = 1$ if and only $g$ and $h$ are both 1, and by the inductive hypothesis, this implies that $g'$ and $h'$ are both 1, which means that $f' = 1$. The second case is that $F = G + H$ so that $f = g + h$ and $f' = g' + h'$. In this case, $f = 1$ implies that $g = 1$ or $h = 1$. By the inductive hypothesis, $g' = 1$ or $h' = 1$, and thus $f' = 1$.

  (b) $F(x_1) = \bar{x}_1$.

7. **Turing Machines and Finite state machines.** (25 points)

  *(a) Draw a DFA that accepts the same strings as the NFA in Figure 1.*

  *(b) Construct a Turing machine that takes as input a binary string, and halts in an accepting state with the entire tape filled with blank symbols and with the tape head in its starting position.*

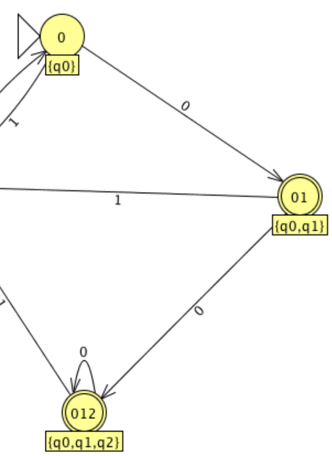


Figure 2: 7a: A DFA corresponding to the NFA above. States with no incoming transitions have been omitted.

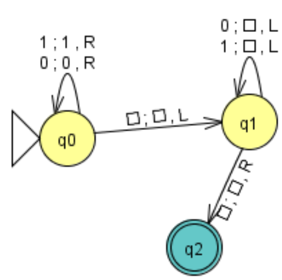


Figure 3: 7b: A Turing machine that erases a binary string and leaves the tape head where it started.