Discrete Structures *Final Exam—* ***Solutions***
CS2800

Instructions: *This is a 150 minute test. Answer the following questions in the provided booklet. Ensure that your name and netid are on your exam booklet. You may answer the questions in any order, but please mark the questions clearly. Books, notes, calculators, laptops, and carrier pigeons are all disallowed. You may leave mathematical expressions unevaluated (e.g. just write $17 \cdot 3$ instead of 51 and don't bother evaluating $C(17, 3)$). Good luck! There are a total of 70 points*

1. *[7 points: 2+5] Let $\Sigma = \{0, 1\}$, and let Lang denote the set of all languages with alphabet Σ, i.e. $Lang = 2^{\Sigma^*}$.*

   (a) *Identify the first erroneous statement in this proof, and explain why it is incorrect:*

   > ***Claim:*** $|\Sigma^*| < |Lang|$.
   > ***Proof:*** *Let $f : \Sigma^* \to Lang$ be given by $f(x) = \{x\}$. f is not surjective, because there is no string x with $f(x) = \emptyset$. Therefore $|\Sigma^*| \not\geq |Lang|$, so $|\Sigma^*| < |Lang|$.*

   Solution Just because f is not surjective doesn't mean there is *no* surjection.

   (b) *Use diagonalization to prove that $|\Sigma^*| < |Lang|$. If you wish, you may use the fact that Σ^* is countable and can be written as $\Sigma^* = \{x_0, x_1, x_2, \dots\}$.*

   Solution Suppose for the sake of contradiction that $|\Sigma^*| \geq |Lang|$. Then there exists a surjection $f : \Sigma^* \to Lang$.

   We can make a table of f:

x	$x_0 \in f(x)$?	$x_1 \in f(x)$?	$x_2 \in f(x)$?	$\cdots$
x_0	yes	yes	yes	$\cdots$
x_1	yes	no	yes	$\cdots$
x_2	no	no	yes	$\cdots$

   We can form a diabolical set S_D by diagonalizing. Formally, $S_D = \{x \in \Sigma^* \mid x \notin f(x)\}$. Then S_D cannot be $f(x)$ for any x, because if $x \in S_D$ then by definition of S_D, $x \notin f(x) = S_D$, while if $x \notin S_D$ then by definition of S_D, $x \in f(x) = S_D$.

   Thus S_D is not in the image of f, contradicting the assumption that f is surjective.

2. *[4 points: 1+1+2] Suppose $P(n)$ is a predicate on the natural numbers, and suppose that*

$$\forall k.(P(k) \Rightarrow P(k + 2)).$$

   For each of the following propositions, indicate which must be true regardless of P (which is not necessarily true). If you think it's true, explain why in 1–2 sentences. If you think it's false, give an example where P satisfies $\forall k.(P(k) \Rightarrow P(k + 2))$ but the conclusion is false.

   (a) $\forall n.P(n)$

   (b) $P(1) \Rightarrow \forall n.P(2n + 1)$

   (c) $\forall n.P(2n)$

Solution (a) This is not necessarily true. If $P(n)$ says that n is an even number, then $\forall n P(n)$ is false although $\forall k(P(k) \Rightarrow P(k+2))$ is true.

(b) This is true. It follows by induction.

(c) This is not necessarily true. If $P(n)$ says that n is an odd number, then $\forall n P(2n)$ is false although $\forall k(P(k) \Rightarrow P(k+2))$ is true.

3. *[7 points] Let f_n be the nth Fibonacci number, given by $f_0 = f_1 = 1$ and $f_{n+2} = f_{n+1} + f_n$ for $n \in \mathbb{N}$. Prove inductively that $gcd(f_{n+1}, f_n) = 1$, using ideas from Euclid's algorithm. Hint: the uniqueness of the remainder may be useful.*

Solution We show by induction that $gcd(f_n, f_{n+1}) = 1$ for all $n \geq 0$. For the base case, clearly $gcd(f_0, f_1) = gcd(1, 1) = 1$. Suppose that $gcd(f_n, f_{n+1}) = 1$. We use the fact, proved in class, that $gcd(a, b) = gcd(a, a - b)$. Note that

$$\begin{aligned}
gcd(f_{n+1}, f_{n+2}) &= gcd(f_{n+1}, f_n + f_{n+1}) && \text{(by definition)} \\
&= gcd(f_{n+1}, f_n + f_{n+1} - f_{n+1}) && \text{(by fact above)} \\
&= gcd(f_{n+1}, f_n) \\
&= 1 && \text{(by the induction hypothesis)}
\end{aligned}$$

Thus, we have proved the result by induction.

Here is an alternative solution for the inductive step: Suppose that $gcd(f_{n+1}, f_n) = 1$. We have

$$gcd(f_{n+2}, f_{n+1}) = gcd(f_{n+1}, r),$$

where $r = rem(f_{n+2}, f_{n+1})$. We would be done if $r = f_n$, because the inductive hypothesis says $gcd(f_{n+1}, f_n) = 1$. But in fact, $f_{n+2} = 1 \cdot f_{n+1} + f_n$, and $f_n < f_{n+1}$ (since $n > 0$; we are doing the inductive step), so by the uniqueness of euclidean division, $r = f_n$.

4. *[4 points] Use the pigeonhole principle to show that in any set of 100 integers, there must exist two different integers whose difference is a multiple of 37.*

Solution Let $\mathbb{Z}_{37}$ be the set of holes, and the set of numbers to be the set of pigeons; n goes in hole $[n]_{37}$. Then there must be two "pigeons" in the same "hole": so $[n]_37 = [m]_37$. Thus $[n - m]_{37} = [0]_{37}$, so $n - m$ is a multiple of 37, as required.

5. *[7 points: 1+1+2+1+2] Suppose that a coin has probability .6 of landing heads. You flip it 100 times. The coin flips are all mutually independent.*

   (a) *What is the expected number of heads?*

   (b) *What upper bound does Markov's Theorem give for the probability that the number of heads is at least 80?*

   (c) *What is the variance of the number of heads for a* single *toss? Calculate the variance using either of the equivalent definitions of variance.*

   (d) *What is the variance of the number of heads for 100 tosses? You may use the fact that if $X_1, \ldots, X_n$ are mutually independent, then $\text{Var}(\sum X_i) = \sum \text{Var}(X_i)$; you don't need to prove this.*

   (e) *What upper bound does Chebyshev's Theorem give for the probability that the number of heads is either less than 40 or greater than 80?*

Solution (a) Let X_i be the outcome of the ith coin toss; $X_i = 1$ if the ith coin toss lands heads and 0 otherwise. The total number of heads is $Y = X_1 + \cdots + X_{100}$. We are interested in $E(Y)$. By linearity, $E(Y) = E(X_1) + \cdots + E(X_{100}) = 100(.6) = 60$.

(b) Markov's Theorem says that $\Pr(Y \geq 80) \leq E(Y)/80 = 60/80 = 3/4$.

(c) X_i is a Bernoulli variable with $p = .6$, so as shown in class, its variance is $p(1-p) = .24$. You can also compute this directly, since $X_i^2 = X$, so $E(X_i^2) = .6$ and $E(X_i)^2 = .36$, so $Var(X) = E(X_i^2) - E(X_i)K^2 = .6 - .36 = .24$.

(d) $Var(Y) = Var(X_1) + \cdots + Var(X_{100})$. Since $Var(X_i) = .24$ for $i = 1, \ldots, 100$, $Var(Y) = 100 \times .24 = 24$.

(e) By Chebyshev's Theorem. $\Pr(|Y - E(Y)| \geq 20) \leq \text{Var}(Y)/400$. Since $E(Y) = 60$, $\Pr(Y \geq 80 \cup Y \leq 40) \leq 24/400 = .06$.

6. *[7 points] Let E and H be events in a probability space. We say that E is* evidence in favor of H *if* $\Pr(H|E) > \Pr(H)$. *Similarly, E is* evidence against H *if* $\Pr(H|E) < \Pr(H)$. *Show that if E is evidence in favor of H then $\overline{E}$ is evidence against H. (Assume that $0 < \Pr(E) < 1$.)*

Solution Suppose that E is evidence in favor of H. Thus, $\Pr(H \mid E) = \Pr(H \cap E)/\Pr(E) > \Pr(H)$, so $\Pr(H \cap E) > \Pr(H)\Pr(E)$. Now $\Pr(H) = \Pr(H \cap E) + \Pr(H \cap \overline{E})$, so $\Pr(H \cap E) = \Pr(H) - \Pr(H \cap \overline{E})$. It follows that $\Pr(H) - \Pr(H \cap \overline{E}) > \Pr(H)(1 - \Pr(\overline{E}) = \Pr(H) - \Pr(H)\Pr(\overline{E})$. Subtracting $\Pr(H)$ from both sides gives $-\Pr(H \cap \overline{E}) > -\Pr(H)\Pr(\overline{E})$, or equivalently $\Pr(H \cap \overline{E}) < \Pr(H)\Pr(\overline{E})$. Diving both sides by $\Pr(\overline{E})$, we get that $\Pr(H \mid \overline{E}) = \Pr(H \cap \overline{E})/\Pr(\overline{E}) < \Pr(H)$; that is, $\overline{E}$ is evidence against H.

7. *[7 points: 2+2+3] Bob the Bomber wishes to receive encrypted messages from Alice the Accomplice. He generates a public key pair $m = 21$ and $k = 5$. Luckily, you have access to an NSA supercomputer that was able to factor* 21 *into* $7 \cdot 3$.

   (a) *Use this information to find the decryption key k^{-1}.*

   Solution We must find the inverse of 5 mod $\phi(m) = \phi(7 \cdot 4) = (7-1)(4-1) = 12$. Experimentally, $[5 \cdot 5] = [25] = [1]$. Alternatively, you can use the pulverizer. This results in $1 = -2 \cdot 12 + 5 \cdot 5$, giving an inverse of 5.

   (b) *Without changing m, what other possible keys k could Bob have chosen? Find the decryption keys for those keys as well.*

   Solution By inspection, the units of $\mathbb{Z}_{12}$ are [1], [5], [7], and [11] (all other numbers share a factor with 12. Experimentally, they are all their own inverses. Note that [1] is not a smart key choice, but we accepted it.

   (c) *Alice encrypts a secret message msg using Bob's public key ($k = 5$), and sends the ciphertext $c = 4$. What was the original message?*

   Solution We must compute $[4]^{[5]} = [4^5]$. We see $[4^2] = [16]$; squaring this gives $[4^4] = [(4^2)^2] = [64] = [1]_{21}$. Thus $[4^5] = [4 \cdot 4^4] = [4]$.

8. *[6 points] Prove that $L = \{0^n 1 0^n \mid n \in \mathbb{N}\}$ is not regular.*

Solution Suppose that this language is accepted by some deterministic finite automaton with N states. Consider the string $x = 0^n 1 0^n$. Since x is in the language and $|x| \geq N$, by the Pumping Lemma, there exist strings u, v, and w such that $x = uvw$, $|v| \geq 1$, $|uv| \leq N$, and M accepts $uv^i w$ for all $i > 0$. Since $|uv| \leq N$, it must be the case that uv is a string of 0's, and that w contains the 1 in $0^N 1 0^N$. Thus, if $i > 1$, $uv^i w$ has more than N 0s to the left of the 1 and only N 0s to the right of the 1, and thus is not in the language. This contradicts the assumption that the language is accepted by M (since M accepts a string not in the language).

9. *[6 points] Let r be a regular expression. Show that there exists a regular expression r' with $L(r') = \overline{L(r)}$ (the complement of $L(r)$). If your proof involves the construction of a regular expression or automaton, you must prove that the language of the regular expression/automaton is what you claim it is (using the definitions).*

   Solution First, note that $L(r)$ is a language, which means that it's a set of strings. So its complement consists of all the strings in $L(r)$ that are not in Σ^*. (Many of you took "complement" to mean the result of switching the 0s and 1s in the strings in $L(r)$. This is not what complement means in this context; moreover, this approach fails if $\Sigma \neq \{0,1\}$. Unfortunately, you typically got 0, 1, or 2 out of 6 if you did this, depending on what else you did.)

   By Kleene's theorem, there is a DFA $M = (Q, \Sigma, \delta, q_0, F)$ with $L(M) = L(R)$. We can form a new automaton M' by flipping the accept and reject states of M: $M' = (Q, \Sigma, \delta, q_0, Q \setminus F)$.

   I claim $L(M') = \overline{L(M)}$. Indeed,

$$\begin{aligned} x \in L(M') &\iff \hat{\delta}(q_0, x) \in Q \setminus F \\ &\iff \hat{\delta}(q_0, x) \notin F \\ &\iff x \notin L(M) \end{aligned}$$

   (You typically lost 1 point if you didn't give a proof.)

   Applying Kleene's theorem again tells us that since there is a DFA with $L(M') = \overline{L(r)}$ there must be a regular expression r' with $L(r') = \overline{L(r)}$.

10. *[3 points] Translate the following sentence into first-order logic: "Everyone knows someone who has a cell phone." (Think of the domain as the students in the class.) Make clear what the predicates you use stand for. For example, if you use a binary predicate $L(x,y)$, you might say "$L(x,y)$ means x likes y". (Although you probably don't want to use $L(x,y)$ defined this way, you may well want to use a predicate that's similar in spirit.)*

    Solution Let $HC(x)$ stand for x has a cell phone and let $K(x,y)$ stand for x knows y. Then $\forall x \exists y (K(x,y) \wedge HC(y))$ says everyone knows someone who has a cell phone.

11. *[2 points] Suppose that the domain is the natural numbers. Give an interpretation of the binary predicate $L(x,y)$ that makes the following formula true, and give another interpretation that makes it false:*

$$\exists x. \forall y. L(x,y)$$

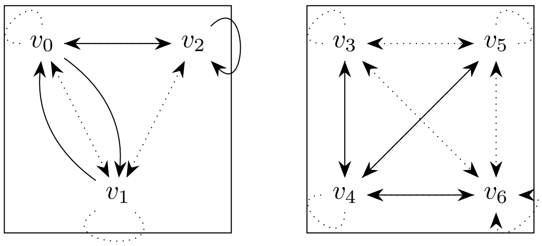
    Solution If $L(x,y)$ says "x is less than y", then $\exists x forally L(x,y)$ is false: it's not the case that there is a natural number that is less than every other integer (0 is not less than itself). If $L(x,y)$ says x is less than or equal to y", then $\exists x forally L(x,y)$ is true: 0 is less than or equal to every natural number. (You could also just take $L(x,y)$ to be **true** for the first part and $L(x,y)$ to be **false** for the first part.)

12. (a) *[3 points] Is it possible for an insect to crawl along the edges of a cube so as to travel along each edge exactly once? Explain why or why not.*

    Solution It is not possible. Each vertex in a cube has degree 3. Thus, there are more than two vertices of odd degree, so by Euler's Theorem, there is no Eulerian path, so the insect cannot travel along each edge exactly once.

(b) *[3 points] Show that if G is a graph with no self loops and if all vertices in G have odd degree k, then (i) the total number of edges must be a multiple of k and (ii) the number of vertices must be even.*

(c) *[4 points] Consider the following graph, which represents a relation R:*



Add as few edges as possible to R to make it into an equivalence relation, and then circle the equivalence classes of R.

Solution (b) The number of edges is the sum of the degrees of the vertices divided by 2. Since each edge has degree k, the sum of the degrees is nk, where n is the number of vertices. Thus, the number of edges is $nk/2$. Since this is an integer and k is odd, n must be even and $nk/2$ is a multiple of k.