Discrete Structures	Final Exam
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 72 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 $|\Sigma^*| < |Lang|$.

   (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 $\Sigma^* = \{x_0, x_1, x_2, \dots\}$.

2. [4 points] 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 Q, 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) $\forall n.P(2n)$

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.

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.

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 $X_1, \dots, X_n$ 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?

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 $0 < \Pr(E) < 1$.)

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}.

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

   (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?

8. [6 points] Prove that $L = \{0^n 10^n \mid n \in \mathbb{N}\}$ is not regular.

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 corresponding to the regular expression/automaton is what you claim it is (using the definitions).

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.)

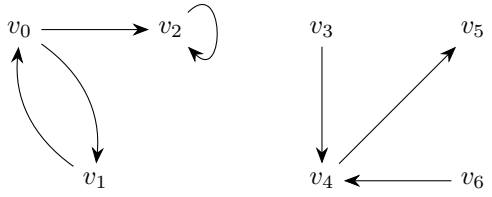
11. [2 points] Suppose that the domain is the natural numbers. Give an interpretation of the binary predicate $L(x, y)$ that makes the following formula true, and give another interpretation that makes it false:

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

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.

    (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.