Midterm Exam

Instructions: Some notation: N for the natural numbers, Z for the integers, Q for the rationals, R for the reals, $\lg x$ for $\log_2 x$, and $[a, b]$ for $\{x \in \mathsf{R} : a \le x \le b\}$. If you don't understand what something means, please ask.

Good luck, gentle students!

— Phil Rogaway

Your Name (write neatly):

Your E-mail address (write neatly):

On problem	you got	out of
1		50
2		50
3		30
4		20
Σ		150

1 True or False [50 points]

Put an **X** through the **correct** box. No justification required. Grading: *+5 for a correct answer; -5 for an incorrect answer; 0 for no answer.*

A. The logical connectives $\{\vee, \neg\}$ are logically complete. **True** **False**

B. The power set of the emptyset, $\mathcal{P}(\emptyset)$, is the emptyset, $\emptyset$. **True** **False**

C. If a language is finite, it is regular. **True** **False**

D. If $A \cup B = A \cup C$ then $B = C$. **True** **False**

E. Let $f : A \to B$ be an injective function, and suppose that $|A| = |B|$. Then f is surjective. *H*int: $A = B = \mathsf{N}$? **True** **False**

F. There is a bijective function from $\{a, b\}^*$ to Z. **True** **False**

G. Define $R \subseteq \mathsf{Z} \times \mathsf{Z}$ by $R(a, b)$ iff $a \leq b$. Then R is an equivalence relation. **True** **False**

H. $n^2 \lg n + 100n \in O(n^2)$. **True** **False**

I. If $f \in \Theta(n^2)$ then $f \in O(n^3)$. **True** **False**

J. The n-ring Tower of Hanoi problem can be solved in $2^n - n$ moves (using a more sophisticated algorithm than the one we saw in class). **True** **False**

2 Short Answer [50 points: 5 points each]

A. Make a truth table for the Boolean formula: $P \to (Q \land P)$.

B. Describe an infinite set S, where $S \subseteq \mathsf{N}$, having the property that, for any $n \in \mathsf{N}$, $\{(x, y) \in S \times S : 0 < |x - y| \leq n\}$ is finite.

C. Draw a DFA (deterministic finite automaton) that recognizes the language $L = \{aa, abb\}$.

D. Give a regular expression for all strings $x \in \{0, 1\}^*$ such that x has a substring of '01' or a substring of '10' (that is, there is a '01' or a '10' occurring somewhere within x).

E. Give a surjective function from R to Q.

F. Give the common name for the equivalence relation on $\mathsf{R} \times \mathsf{R}$ such that the equivalence classes are $\{\{a\} : a \in \mathsf{R}\}$.

G. Use Euclid's algorithm to find $\gcd(72, 156)$. Show your work.

H. Define what is a **partition** of a nonempty set A:

K. Let $p = 2^{19} - 1$. This number is prime. What is $2^{(2^{19})} \bmod p$?

L. List the elements of the group Z_6 (the group of integers modulo 6), and then list the elements of Z_6^* ("the multiplicative subgroup of integers modulo 6"), and then tell me what is the inverse of 5 in Z_6^*.

3 Look Familiar? [30 points: 10 points each]

The first couple should!

A. Prove that there exist irrational numbers a and b such that a^b is rational. You may assume that $\sqrt{2}$ is irrational, since we proved that in class, but you may not assume that any other number is irrational without proving it.

B. Draw a Boolean circuit (use 2-input logic gates: AND, OR, or NOT gates) which realizes the function "if s then p else q." That is, your circuit has three input wires, p, q, and s, and one output wire, y.

C. Let $n \geq 1$ be an integer. Then the number of bits in the binary representation of n is: (write a formula)

4 A Little Proof [20 points]

Let $S \subseteq \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$ where $|S| = 7$. Prove that there exist $x, y \in S$ such that $x + y = 13$.