CSE 311: Foundations of Computing I
Sample midterm - *with solutions*

1. **Prime factorization** (4 points) *Compute the prime factorization of* 320 *and* 450. *Compute* $\gcd(320, 450)$ *and* $\text{lcm}(320, 450)$, *expressing your answer as a product of prime factors.*

   $320 = 2^6 \cdot 5$, $450 = 2 \cdot 3^2 \cdot 5^2$. $\gcd(320, 450) = 2 \cdot 5$ and $\text{lcm}(320, 450) = 2^6 \cdot 3^2 \cdot 5^2$.

2. **Sets** (12 points) *Let* $A = \{z \in \mathbb{Z} | 1 \le z \le 8\}$, $B = \{z \in \mathbb{Z} | \, 2 | z\}$ *and let* C *be the set of primes. Fill in the table below with the set that each expression evaluates to:*

Expression	Value
$A \cap B$	$\{2, 4, 6, 8\}$
$B \cap C$	$\{2\}$
$A - (B \cup C)$	$\{1\}$

3. **Primes and predicates** (8 points) *Translate the expression "p is prime" into mathematical notation, i.e. using only* $\forall, \exists, |, \mathbb{Z}$ *and other mathematical symbols.*

   $\forall d \in \mathbb{Z}^+ (d | p \rightarrow (d = 1 \vee d = p))$.

   Other answers are also possible.

4. **Propositional logic** (20 points)

   (a) Show that $\neg(p \oplus q) \equiv (p \rightarrow q) \wedge (\neg p \rightarrow \neg q)$ *using logical equivalences from the table at the back of the exam and the fact that* $p \oplus q \equiv \neg(p \leftrightarrow q)$.

   (b) Construct a truth table for $q \vee (p \rightarrow \neg q)$. *Is this a tautology, contradiction or contingency? Briefly indicate why.*

   (a)

$$\neg(p \oplus q) \equiv \neg(\neg(p \leftrightarrow q)) \quad \text{given} \quad (1)$$
$$\neg(\neg(p \leftrightarrow q)) \equiv p \leftrightarrow q \quad \text{double negation} \quad (2)$$
$$p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p) \quad \text{Table 8, line 1} \quad (3)$$
$$q \rightarrow p \equiv \neg p \rightarrow \neg q \quad \text{Table 7, line 2} \quad (4)$$
$$(p \rightarrow q) \wedge (q \rightarrow p) \equiv (p \rightarrow q) \wedge (\neg p \rightarrow \neg q) \quad \text{Combining (3) and (4)} \quad (5)$$

   (b)

p	q	$\neg q$	$p \rightarrow \neg q$	$q \vee (p \rightarrow \neg q)$
T	T	F	F	T
T	F	T	T	T
F	T	F	T	T
F	F	T	T	T

5. **Predicate logic** (20 points)

(a) *Let $S(x)$ be the predicate "x is a student", $R(y)$ the predicate "y is a road in Seattle" and $V(x,y)$ the predicate "x has visited road y." Express the following statements using $\forall, \exists, \neg$.*

i. *No student has visited all roads in Seattle.*

ii. *At least two roads were visited by all students.*

iii. [0 points] *There exist two roads such that I could not travel both and I took the one less traveled by.*

(b) *Express the negations of each of the following statements in a way such that $\neg$ does not precede a $\forall, \exists$ or (.*

i. $\exists x \forall y (P(x,y) \wedge \exists z \neg Q(x,z))$

ii. $\forall x (P(x) \rightarrow \exists y (Q(x,y)))$.

(a) i. $\neg \exists x \forall y (V(x,y))$

ii. $\exists y_1, \exists y_2 (y_1 \neq y_2 \wedge \forall x (V(x,y_1) \wedge V(x,y_2)))$.

iii. Trick question. Note that the author didn't actually take the road less traveled by: he only imagines that in later retelling the story he'll claim that the road he took was the less popular one.

(b) i. $\forall x \exists y (\neg P(x,y) \vee \forall z (Q(x,z)))$.

ii. $\exists x (P(x) \wedge \forall y (\neg Q(x,y)))$.

6. **Proof** (10 points) *If A and B are sets, then does $A - B = \emptyset$ imply that $A = B$? Prove, or give a counter-example.* No. Consider $A = \{1\}$, $B = \{1,2\}$.

7. **Proof** (10 points) *Prove that $\forall a,b,n \in \mathbb{Z}$ $(4|n \wedge n = ab) \rightarrow (2|a \vee 2|b)$.* We prove the contrapositive.

Assume $\neg(2|a \vee 2|b)$ or, equivalently, that $2 \not| a$ and $2 \not| b$. Use the division algorithm to write

$$a = 2q_1 + r_1 \qquad \text{and} \qquad b = 2q_2 + r_2,$$

for some integers q_1, r_1, q_2, r_2 satisfying $0 \leq r_1, r_2 < 2$. If we had $r_1 = 0$ then it would imply that $2|a$; since we know this is not the case, we must have $r_1 = 1$. The same argument proves that $r_2 = 1$. Thus $ab = (2q_1+1)(2q_2+1) = 2(2q_1q_2 + q_1 + q_2) + 1$. Thus implies that $ab \equiv 1 \pmod 4$ or $ab \equiv 3 \pmod 4$ and that $4 \not| ab$. Therefore either $4 \not| n$ or $n \neq ab$ (or both). QED.

8. **Functions** (18 points) *In each row, f is a function from $A \rightarrow B$. Mark Y/N to indicate whether f is surjective or injective. Briefly justify your answers.*

A	B	f	surjective	injective
$\mathbb{Z}$	{0,1,2}	$f(x) = x \bmod 3$	Y	N
$\mathbb{Z}$	$\mathbb{Z}^+$	$f(x) = \lvert x-1 \rvert$	Y	N
$\mathbb{Z} \times \mathbb{Z}$	$\mathbb{Z}$	$f(x,y) = 3x + 7y$	Y	N

For the first function, we see that f is surjective by considering inputs 0,1,2, which together get sent to the entire codomain; we see it is not injective by considering inputs 0,3, which both get mapped to 0. For the second function, f is surjective because for any $y \in \mathbb{Z}^+$, $y+1 \in \mathbb{Z}$ and $f(y+1) = y$. f is not injective because $f(0) = f(2)$. For the third function, f is surjective because $\gcd(3,7) = 1$. Using the extended Euclid's algorithm (or guess-and-check) we see that $3 \cdot (-2) + 7 = 1$. Therefore, for any $z \in \mathbb{Z}$, $f(-2z, z) = 3 \cdot (-2z) + 7z = z$. f is not injective because $f(7,0) = f(0,3) = 21$.

TABLE 6 **Logical Equivalences.**

Equivalence	*Name*
$p \wedge \mathbf{T} \equiv p$ $p \vee \mathbf{F} \equiv p$	Identity laws
$p \vee \mathbf{T} \equiv \mathbf{T}$ $p \wedge \mathbf{F} \equiv \mathbf{F}$	Domination laws
$p \vee p \equiv p$ $p \wedge p \equiv p$	Idempotent laws
$\neg(\neg p) \equiv p$	Double negation law
$p \vee q \equiv q \vee p$ $p \wedge q \equiv q \wedge p$	Commutative laws
$(p \vee q) \vee r \equiv p \vee (q \vee r)$ $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	Associative laws
$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$ $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	Distributive laws
$\neg(p \wedge q) \equiv \neg p \vee \neg q$ $\neg(p \vee q) \equiv \neg p \wedge \neg q$	De Morgan's laws
$p \vee (p \wedge q) \equiv p$ $p \wedge (p \vee q) \equiv p$	Absorption laws
$p \vee \neg p \equiv \mathbf{T}$ $p \wedge \neg p \equiv \mathbf{F}$	Negation laws

TABLE 7 **Logical Equivalences Involving Conditional Statements.**

$p \rightarrow q \equiv \neg p \vee q$

$p \rightarrow q \equiv \neg q \rightarrow \neg p$

$p \vee q \equiv \neg p \rightarrow q$

$p \wedge q \equiv \neg(p \rightarrow \neg q)$

$\neg(p \rightarrow q) \equiv p \wedge \neg q$

$(p \rightarrow q) \wedge (p \rightarrow r) \equiv p \rightarrow (q \wedge r)$

$(p \rightarrow r) \wedge (q \rightarrow r) \equiv (p \vee q) \rightarrow r$

$(p \rightarrow q) \vee (p \rightarrow r) \equiv p \rightarrow (q \vee r)$

$(p \rightarrow r) \vee (q \rightarrow r) \equiv (p \wedge q) \rightarrow r$

TABLE 8 **Logical Equivalences Involving Biconditionals.**

$p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$

$p \leftrightarrow q \equiv \neg p \leftrightarrow \neg q$

$p \leftrightarrow q \equiv (p \wedge q) \vee (\neg p \wedge \neg q)$

$\neg(p \leftrightarrow q) \equiv p \leftrightarrow \neg q$

TABLE 1 Rules of Inference.

Rule of Inference	*Tautology*	*Name*
p $p \to q$ $\therefore q$	$[p \land (p \to q)] \to q$	Modus ponens
$\neg q$ $p \to q$ $\therefore \neg p$	$[\neg q \land (p \to q)] \to \neg p$	Modus tollens
$p \to q$ $q \to r$ $\therefore p \to r$	$[(p \to q) \land (q \to r)] \to (p \to r)$	Hypothetical syllogism
$p \lor q$ $\neg p$ $\therefore q$	$[(p \lor q) \land \neg p] \to q$	Disjunctive syllogism
p $\therefore p \lor q$	$p \to (p \lor q)$	Addition
$p \land q$ $\therefore p$	$(p \land q) \to p$	Simplification
p q $\therefore p \land q$	$[(p) \land (q)] \to (p \land q)$	Conjunction
$p \lor q$ $\neg p \lor r$ $\therefore q \lor r$	$[(p \lor q) \land (\neg p \lor r)] \to (q \lor r)$	Resolution

TABLE 2 Rules of Inference for Quantified Statements.

Rule of Inference	*Name*
$\forall x P(x)$ $\therefore P(c)$	Universal instantiation
$P(c)$ for an arbitrary c $\therefore \forall x P(x)$	Universal generalization
$\exists x P(x)$ $\therefore P(c)$ for some element c	Existential instantiation
$P(c)$ for some element c $\therefore \exists x P(x)$	Existential generalization