Name Student ID

CSE 311: Foundations of Computing I
Spring 2011

Midterm - *with solutions*

1. **Sets** (12 points)

   (a) Let A, B, C be sets. Express $A-(B-C)$ using only symbols from this list: $(,), \cap, \cup, A, B, C, \bar{A}, \bar{B}, \bar{C}$.

   (b) Prove or give a counter-example: for any sets A, B, $|P(A) \times P(B)| = |P(A \times B)|$. Here $P(S)$ is defined to be the power set of S, meaning $P(S) = \{T : T \subseteq S\}$.

   (a) $A \cap (\bar{B} \cup C)$. Equivalent forms are also acceptable.

   (b) $|P(A) \times P(B)| = 2^{|A|+|B|}$ and $|P(A \times B)| = 2^{|A|\cdot|B|}$, so this is false whenever $|A| + |B| \neq |A| \cdot |B|$; for example when $|A| = |B| = 1$.

2. **Quantifiers** (12 points)

   (a) Prove or disprove: $\forall x \in \mathbb{Z}, \exists y \in \mathbb{Z}(x + y = 0)$.

   (b) Prove or disprove: $\exists x \in \mathbb{Z}, \forall y \in \mathbb{Z}(x + y = 0)$.

   (a) For any x, choose y to be $-x$.

   (b) This is false. For any x, we can take y to be something other than $-x$. For example, take $y = 1-x$, so $x + y = 1 \neq 0$.

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

   (a) Show that $(\neg p \to q) \to p \equiv q \to p$ using logical equivalences from the table at the back of the exam. Use at most one equivalence per line.

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

   (a)

$\neg p \to q \equiv \neg(\neg p) \vee q$	Table 7, line 1	(1)
$\neg(\neg p) \equiv p$	Double negation	(2)
$(\neg p \to q) \to p \equiv (p \vee q) \to p$	Combining (1) and (2)	(3)
$\equiv \neg(p \vee q) \vee p$	Table 7, line 1	(4)
$\equiv (\neg p \wedge \neg q) \vee p$	De Morgan's Law	(5)
$\equiv p \vee (\neg p \wedge \neg q)$	Commutative law	(6)
$\equiv (p \vee \neg p) \wedge (p \vee \neg q)$	Distributive law	(7)
$\equiv T \wedge (p \vee \neg q)$	Negation law	(8)
$\equiv (p \vee \neg q) \wedge T$	Commutative law	(9)
$\equiv p \vee \neg q$	Identity law	(10)
$\equiv \neg p \to \neg q$	Table 7, line 1	(11)
$\equiv q \to p$	Table 7, line 2	(12)

(b)

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

This is a contingency, since it is sometimes true and sometimes false.

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

   (a) Let $A(x, y)$ be the predicate "x has read book y", and $B(x, y, z)$ be the predicate "x prefers book y over book z" where the domain of x is the set of all people, and the domain of y and z is the set of all books. Express the following statements using $\forall, \exists, \neg$.

   i. There is a book that no one prefers over any other book.

   ii. Anyone who has read any book has a book that they prefer over all other books.

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

   i. $\forall x(\exists y(A(x, y) \vee \exists z(A(x, z) \wedge \neg B(x, y, z))))$.

   ii. $\exists y(\forall x(A(x, y) \rightarrow \forall z((y \neq z) \rightarrow B(x, y, z))))$.

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

   ii. $\forall x(\exists y(A(x, y)) \rightarrow \exists y \forall z(y \neq z \rightarrow B(x, y, z)))$.

   (b) i. $\exists x(\forall y(\neg A(x, y) \wedge \forall z(\neg A(x, z) \vee B(x, y, z))))$.

   ii. $\forall y(\exists x(A(x, y) \wedge \exists z(y \neq z \wedge \neg B(x, y, z))))$.

5. **Proof** (12 points) *Suppose $x_1, x_2, x_3 \in \mathbb{R}$. Define the mean of these numbers to be*

$$\bar{x} := \frac{x_1 + x_2 + x_3}{3}$$

   Prove that there exists $i \in \{1, 2, 3\}$ such that $x_i \geq \bar{x}$.

   The proof is by contradiction. Assume that for all i, $x_i < \bar{x}$. Then $\sum_{i=1}^{3} x_i < 3\bar{x}$, contradicting our definiton of $\bar{x}$.

6. **Functions** (12 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
$\{0, 1, \ldots, 29\}$	$\mathbb{Z} \times \mathbb{Z}$	$f_1(x) = (x \bmod 5, x \bmod 6)$	N	Y
$\mathbb{R}^+$	$\mathbb{R}^+$	$f_2(x) = \sqrt{x}$	Y	Y
$\mathbb{Z} \times \mathbb{Z}$	$\mathbb{Z} \times \mathbb{Z}$	$f_3(x, y) = (x, y - x^2)$	Y	Y

   f_1 is not surjective because its range is finite and $\mathbb{Z} \times \mathbb{Z}$ is infinite. It is injective by the Chinese Remainder Theorem.

   f_2 is surjective because for any $y > 0$ there exists $x > 0$ such that $\sqrt{x} = y$; namely, choose $x = y^2$. It is injective because $\sqrt{x_1} = \sqrt{x_2}$ implies that $x_1 = x_2$ whenever $x_1, x_2 > 0$.

   f_3 is both surjective and injective because we can construct an inverse: $f_3^{-1}(x, y) = (x, y + x^2)$.

7. **Modular arithmetic** (12 points)

   (a) Calculate $5^{256} \pmod 7$.

   (b) Find the smallest positive integer x *satisfying* $4x \equiv 3 \pmod 9$*, if one exists, or write NONE, if none exists.*

   (c) Find the smallest positive integer x *satisfying* $3x \equiv 4 \pmod 9$*, if one exists, or write NONE, if none exists.*

(a) Repeatedly squaring eight times, we obtain $5, 4, 2, 4, 2, 4, 2, 4, 2$, and so the answer is 2.

(b) The multiplicative inverse of $4 \pmod 9$ can be seen by inspection to be -2, or equivalently 7. We can also obtain this using Euclid's algorithm: $9 = 2 \cdot 4 + 1$ and so $-2 \cdot 4 = 1 - 9$. Thus $x \equiv -6 \pmod 9$, and so $x = 3$.

(c) NONE. $3x$ mod 9 is always divisible by 3 and 4 is not.

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