CS1231S Cheatsheet

for midterms AY23-24, Sem 1

m. zaidan

Sets

$\mathbb{N}$	natural numbers $\{\mathbb{Z}^+$ and $0\}$
$\mathbb{Z}$	integer
$\mathbb{Q}$	rational numbers
$\mathbb{R}$	real numbers
$\mathbb{C}$	complex numbers

Symbols

$\in$	member of $(x \in \mathbb{Z})$
$\sim$	negation (not)
$\wedge$	conjunction (and)
$\vee$	disjunction (or)
$\equiv$	logically equivalent

Definitions

Tautology	Statement that is always **true**
Contradiction	Statement that is always **false**
Even integers	$even(n) \iff \exists k \in \mathbb{Z}, (n = 2k)$
Odd integers	$odd(n) \iff \exists k \in \mathbb{Z}, (n = 2k+1)$
Divisibility	$d \mid n \iff \exists k \in \mathbb{Z}, (n = dk)$

Theorem 4.3.1: $\forall a, b \in \mathbb{Z}^+, a \mid b \rightarrow a \leq b$
Theorem 4.3.2: The only divisors of 1 are 1 and -1.
Theorem 4.3.3: $\forall a, b, c \in \mathbb{Z}^+, (a \mid b \wedge b \mid c) \rightarrow (a \mid c)$

Rational numbers	$rational(r) \iff \exists a, b \in \mathbb{Z}, (r = \frac{a}{b} \wedge b \neq 0)$

Theorem 4.2.1: Every integer is a rational number
Theorem 4.2.2: The sum of any two rational numbers is rational
Corollary 4.2.3: The double of a rational number is rational

Prime numbers	$prime(n) \iff (n > 1) \wedge \forall r, s \in \mathbb{Z}^+, (n = rs \rightarrow (r = 1 \wedge s = n) \vee (r = n \wedge s = 1))$ ***or*** $((r > 1) \wedge (s > 1) \rightarrow rs \neq n)$
Composite numbers	$composite(n) \iff \exists r, s \in \mathbb{Z}^+, (n = rs \wedge (1 < r < n) \wedge (1 < s < n))$
Congruence $a \equiv b (mod n)$	$\iff a, b \in \mathbb{Z}, n \in \mathbb{Z}^+ (n \mid (a - b))$

Proofs

Existential Statements

Proof by **constructive proof**: Find x in D that makes $Q(x)$ true.

Universal Statements

Proof by **exhaustion** (for finite sets or finite amount of element satisfy the *if* condition.
Proof by **generalizing from the generic particular**: Generic proof
Disproof by **counterexample**

Indirect Proof

Proof by **contraposition**: Prove *contrapositive* with a direct proof.
Proof by **contradiction**: Prove *negation* is false.

Logical Equivalences

Theorem 2.1.1 Logical Equivalences

Commutative	$p \wedge q \equiv q \vee p$	$p \vee q \equiv q \vee p$
Associative	$p \wedge q \wedge r \equiv (p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	$p \vee q \vee r \equiv (p \vee q) \vee r \equiv p \vee (q \vee r)$
Distributive	$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$
Identity	$p \wedge true \equiv p$	$p \vee false \equiv p$
Negation	$p \vee \sim p \equiv true$	$p \wedge \sim p \equiv false$
Double negative	$\sim(\sim p)$	
Idempotent	$p \wedge p \equiv true$	$p \vee p \equiv p$
Universal bound	$p \vee true \equiv true$	$p \wedge false \equiv false$
De Morgan's	$\sim(p \wedge q) \equiv \sim p \vee \sim q$	$\sim(p \vee q) \equiv \sim p \wedge \sim q$
Absorption	$p \vee (p \wedge q) \equiv p$	$p \wedge (p \vee q) \equiv p$
Negation of true & false	$\sim true \equiv false$	$\sim false \equiv true$

Translations

Conditional Statements Translations

	$p \rightarrow q$
contrapositive	$\sim q \rightarrow \sim p$
converse	$q \rightarrow p$
inverse	$\sim p \rightarrow \sim q$

if p then q	$p \rightarrow q$
p implies q	$p \rightarrow q$
p only if q	$\sim q \rightarrow \sim p$ $p \rightarrow q$
p if, and only if, q	$p \leftrightarrow q$
p iff q	$p \leftrightarrow q$
p is sufficient for q	$p \rightarrow q$
p is necessary for q	$q \rightarrow p$ or $\sim p \rightarrow \sim q$

Quantified Statements Translations

Truth set	$x \in D \mid P(x)$
For all x in D, Q(x)	$\forall x \in D, Q(x)$
There is a x in D s.t. Q(x)	$\exists x \in D, Q(x)$
There exists x in D s.t. Q(x)	$\exists x \in D, Q(x)$
There is a unique x in D s.t. Q(x)	$\exists! x \in D, Q(x)$
For all x, P(x) is a sufficient condition for Q(x)	$\forall x (P(x) \rightarrow Q(x))$
For all x, P(x) is a necessary condition for Q(x)	$\forall x (Q(x) \rightarrow P(x))$
For all x, P(x) only if R(x)	$\forall x (P(x) \rightarrow Q(x))$

Rules of Inference

Table 2.3.1 Rules of Inference

Modus Ponens	$p \rightarrow q$ p $\therefore q$	
Modus Tollens	$p \rightarrow q$ $\sim q$ $\therefore \sim p$	
Generalization	p $\therefore p \vee q$	q $\therefore p \vee q$
Specialization	$p \wedge q$ $\therefore p$	$p \wedge q$ $\therefore q$
Conjunction	p q $\therefore p \wedge q$	
Elimination	$p \vee q$ $\sim q$ $\therefore p$	$p \vee q$ $\sim p$ $\therefore q$
Transitivity	$p \rightarrow q$ $q \rightarrow r$ $\therefore p \rightarrow r$	
Proof by division into cases	$p \vee q$ $p \rightarrow r$ $q \rightarrow r$ $\therefore r$	

Errors

Converse Error	$p \rightarrow q$ q $\therefore p$
Inverse Error	$p \rightarrow q$ $\sim p$ $\therefore \sim q$

Quantified Statements

Theorem 3.2.1
$\sim(\forall x \in D, Q(x)) \equiv \exists x \in D, \sim Q(x)$
Theorem 3.2.2
$\sim(\exists x \in D, Q(x)) \equiv \forall x \in D, \sim Q(x)$

	$\forall x \in D (P(x) \rightarrow Q(x))$
contrapositive	$\forall x \in D (\sim Q(x) \rightarrow \sim P(x))$
converse	$\forall x \in D (Q(x) \rightarrow P(x))$
inverse	$\forall x \in D (\sim P(x) \rightarrow \sim Q(x))$

Quantified Rules of Inference

Universal Modus Ponens	$\forall x \in D(P(x) \to Q(x))$ $P(a)$ *for a particular* a $\therefore Q(a)$
Universal Modus Tollens	$\forall x \in D(P(x) \to Q(x))$ $\sim Q(a)$ *for a particular* a $\therefore \sim P(a)$
Universal Transitivity	$\forall x \in D(P(x) \to Q(x))$ $\forall x \in D(Q(x) \to R(x))$ $\therefore \forall x \in D(P(x) \to R(x))$
Universal Instantiation	$\forall x \in D\, P(x)$ $\therefore \forall P(a)$ *if* $a \in D$
Universal Generalization	$P(a)$ *for every* $a \in D$ $\therefore \forall x \in D\, P(x)$
Existential Instantiation	$\exists x \in D\, P(x)$ $\therefore \exists P(a)$ *if* $a \in D$
Existential Generalization	$P(a)$ *for some* $a \in D$ $\therefore \exists x \in D\, P(x)$

Errors

Converse Error	$\forall x \in D(P(x) \to Q(x))$ $Q(a)$ *for a particular* a $\therefore P(a)$
Inverse Error	$\forall x \in D(P(x) \to Q(x))$ $\sim P(a)$ *for a particular* a $\therefore \sim Q(a)$

Set Theory

Symbols

$\subseteq$	subset of
$\subsetneq$	proper subset of
$\nsubseteq$	not subset of

Set Identities

Theorem 6.2.2 Set Identities

Commutative	$A \cup B = B \cup A$	$A \cap B = B \cap A$
Associative	$(A \cup B) \cup C$ $= A \cup (B \cup C)$	$(A \cap B) \cap C$ $= A \cap (B \cap C)$
Distributive	$A \cup (B \cap C)$ $= (A \cup B) \cap (A \cup C)$	$A \cap (B \cup C)$ $= (A \cap B) \cup (A \cap C)$
Identity	$A \cup \emptyset = A$	$A \cap U = A$
Complement	$A \cup \bar{A} = U$	$A \cap \bar{A} = \emptyset$
Double complement	$\bar{\bar{A}} = A$	
Idempotent	$A \cup A = A$	$A \cap A = A$
Universal bound	$A \cup U = U$	$A \cap \emptyset = \emptyset$
De Morgan's	$\overline{A \cup B} = \bar{A} \cap \bar{B}$	$\overline{A \cap B} = \bar{A} \cup \bar{B}$
Absorption	$A \cup (A \cap B) = A$	$A \cap (A \cup B) = A$
Complements of U & $\emptyset$	$\bar{U} = \emptyset$	$\bar{\emptyset} = U$
Set difference law	$A \backslash B = A \cap \bar{B}$	

Theorems

Theorem 4.4.1: *Quotient-Remainder Theorem*
$\forall n \in \mathbb{Z}, d \in \mathbb{Z}^+, \exists! q, r \in \mathbb{Z}((n = dq + r) \wedge (0 \leq r < d))$
Theorem: *Cardinality of Power Set of a Finite Set*
$(|A| = n \wedge n \neq \infty) \to (|\mathcal{P}(A)| = 2^n)$
Theorem 6.3.1:
$|\mathcal{P}(A)| = 2^{|A|}$

Properties

Inclusion of Intersection	$A \cap B \subseteq A$	$A \cap B \subseteq B$
Inclusion of Union	$A \supseteq A \cup B \subseteq A$	$B \supseteq A \cup B$
Transitive Property of Subsets	$A \subseteq B \wedge B \subseteq C \to A \subseteq C$	

Definitions

Cardinality $\|S\|$	number of elements in S
Subset $A \subseteq B$ Superset $B \supseteq A$	$\iff \forall x(x \in a \Rightarrow x \in B)$
Proper subset $A \subsetneq B$	$\iff A \subseteq B \wedge A \neq B$
Ordered pair $(a,b) = (c,d)$	$\iff (a = c) \wedge (b = d)$
Cartesian product $A \times B$	$= \{(a,b) : a \in A \wedge b \in B\}$
Set equality $A = B$	$A \subseteq B \wedge B \subseteq A$ ***or*** $\forall x(x \in A \iff x \in B)$
(procedural)	$(x,y) \in A \times B \iff x \in A \wedge y \in B$
Union $A \cup B$	$\{x \in U : x \in A \vee x \in B\}$
(procedural)	$x \in A \cup B \iff x \in A \vee x \in B$
Intersection $A \cap B$	$\{x \in U : x \in A \wedge x \in B\}$
(procedural)	$x \in A \cap B \iff x \in A \wedge x \in B$
Difference $A \setminus B$	$\{x \in U : x \in A \wedge x \notin B\}$
(procedural)	$x \in A - B \iff x \in A \wedge x \notin B$
Complement $\bar{A}$	$\{x \in U \mid x \notin A\}$
(procedural)	$x \in \bar{A} \iff x \notin \bar{A}$
$\cup_{i=0}^{n} A_i$	$A_0 \cup A_1 \cup \ldots \cup A_n$
(procedural)	$\{x \in U \mid x \in A_i, \exists i = [0,n]\}$
$\cap_{i=0}^{n} A_i$	$A_0 \cap A_1 \cap \ldots \cap A_n$
(procedural)	$\{x \in U \mid x \in A_i, \forall i = [0,n]\}$
Disjoint	$A \cap B = \emptyset$
Mutually disjoint	$\forall i, j(i \neq j \to (A_i \cap A_j = \emptyset))$
Partition of A	all subsets are mutually disjoint all subsets are non empty union of subsets $= A$
Power set $\mathcal{P}(A)$	set of all subsets of A

Relations

Theorems/Lemmas/Propositions

Proposition (lecture 6, pg 18): *Composition is Associative*
Proposition (lecture 6, pg 18): *Inverse of Composition*
$(S \circ R)^{-1} = R^{-1} \circ S^{-1}$
Theorem 8.3.1: *Relation Induced by a Partition*
If R is a relation induced by the partition of a set A,
R is reflexive, symmetric and transitive.
Lemma Rel. 1: *Equivalence Classes*
If $\sim$ is a equivalence relation on A, $\therefore \forall x, y \in A$,
$x \sim y = ([x] = [y]) = ([x] \cap [y] \neq \emptyset)$
Theorem 8.3.4: *Partition Induced by an Equivalence Relation*
If R is an equivalence relation on A, the distinct equivalence classes of R form a partition of A; union of equivalence classes is A and the intersection of any two distinct classes is $\emptyset$
Proposition (lecture 6, pg 54): *Congruence-mod n is equivalence relation on $\mathbb{Z}$ for every $n \in \mathbb{Z}^+$*
Theorem Rel.2: *Equivalence classes form partition*
$A/\sim$ is a partition of A
Proposition (lecture 6, pg 83): *A smallest element is minimal on a partial order $\preccurlyeq$ on A*

Definitions

xRy	$\iff (x,y) \in R$
Domain of R from A to B	$\{a \in A : aRb \textit{ for some } b \in B\}$
Co-domain of R from A to B	B
Range of R from A to B	$\{b \in B : aRb \textit{ for some } a \in A\}$
Composition of R with S $(S \circ R)$	$\forall x \in A, \forall z \in C$ $(xS \circ Rz \iff (\exists y \in B(xRy \wedge ySz)))$
Inverse R^{-1}	$\{(y,x) \in B \times A : (x,y) \in R\}$
Relation on A	Relation from A to A
Transitive Closure R^t	R^t is transitive $R \subseteq R^t$ if S transitive and contains R, $R^t \subseteq S$
Partition $\mathcal{C}$	$\forall S \in \mathcal{C}(\emptyset \neq S \subseteq A)$ $\forall x \in A\ \exists! S \in \mathcal{C}(x \in S)$
Relation induced by Partition $\mathcal{C}$	$\forall x, y \in A, xRy \iff$ $\exists S \textit{ of } \mathcal{C}(x, y \in S)$
Equivalence Relation	$\iff R$ is reflexive, **symmetric** and transitive.
Equivalence Class $[a]_\sim$	$\{x \in A : a \sim x\}$
Set of Eq. Class $A/\sim$	$\{x_\sim : x \in A\}$

$[A/\sim = \mathcal{C}]$ Set of eq. class is a partition **(Tut. 4 Q9(b))**

(procedural)	$\forall x \in A(x \in [a]_\sim \iff a \sim x)$
Partial Order Relation	$\iff R$ is reflexive, **antisymmetric** and transitive.
Comparability	$a \preccurlyeq b \vee b \preccurlyeq a$
Comparability	$\exists c \in A(a \preccurlyeq c \wedge b \preccurlyeq c)$
Maximal Element	$\forall x \in A(c \preccurlyeq x \Rightarrow c = x)$
Minimal Element	$\forall x \in A(x \preccurlyeq c \Rightarrow c = x)$
Largest Element	$\forall x \in A(c \preccurlyeq x)$
Smallest Element	$\forall x \in A(x \preccurlyeq c)$
Total Order Relation	$\iff R$ is partial order $\wedge$ $x, y \in A(xRy \vee yRx)$

iff R is a partial order and all elements are comparable to each other

Linearisation $\preccurlyeq^*$	$\forall x, y \in A(x \preccurlyeq y \Rightarrow X \preccurlyeq^* y)$
Well Ordered Set	$\forall S \in \mathcal{P}(A), S \neq \emptyset \iff$ $(\exists x \in S\ \forall y \in S(x \preccurlyeq y))$

iff every non empty subset of A contains a smallest element.

Properties of General Relations

Reflexive	$\iff \forall x \in A(xRx)$
Symmetric	$\iff \forall x, y \in A(xRy \Rightarrow yRx)$
Antisymmetric	$\iff \forall x, y \in A(xRy \wedge yRx \to x = y)$
Asymmetric	$\iff \forall x, y \in A(xRy \Rightarrow y \not{R} x)$

Asymmetric relations must be antisymmetric **(Tut. 5 Q6(c))**

Transitive	$\iff \forall x, y, z \in A(xRy \wedge yRz \Rightarrow xRz)$

Properties of Real Numbers

(Appendix A)
Domain is $\mathbb{R}$ unless stated otherwise.

Field Axioms

F1: *Commutative laws*
$a + b = b + a$, $ab = ba$
F2: *Associative laws*
$(a + b) + c = a + (b + c)$, $(ab)c = a(bc)$
F3: *Distributive laws*
$a(b + c) = ab + ac$, $(b + c)a = ba + ca$
F4: *Existence of Identity Elements*
$0 + a = a + 0 = a$, $1 \times a = a \times 1 = a$
F5: *Existence of Additive Inverses*
$a + (-a) = (-a) + a = 0$
F6: *Existence of Reciprocals*
$a \times \frac{1}{a} = \frac{1}{a} \times a = 1$

Derived Algebraic Properties

T1: *Cancellation Law for Addition*
$(a + b = a + c) \to (b = c)$
T2: *Possibility of Subtraction*
$\exists! x(a + x = b)$, where $x = b - a$
T3: $b - a = b + (-a)$
T4: $-(-a) = a$
T5: $a(b - c) = ab - ac$
T6: $0 \times a = a \times 0 = 0$
T7: *Cancellation Law for Multiplication*
$(ab = ac \wedge a \neq 0) \to (b = c)$
T8: *Possibility of Division*
$\exists! x \in \mathbb{R} \backslash \{0\}(ax = b)$, where $x = \frac{b}{a}$
T9: $a \neq 0 \to \frac{b}{a} = b \times a^{-1}$
T10: $a \neq 0 \to (a^{-1})^{-1} = a$
T11: *Zero Product Property*
$ab = 0 \to (a = 0 \vee b = 0)$
T12: *Rule for Multiplication with Negative Signs*
$(-a)b = a(-b) = -(ab)$, $(-a)(-b) = ab$, $-\frac{a}{b} = -\frac{-a}{b} = \frac{a}{-b}$
T13: *Equivalent Fractions Property*
$(b \neq 0 \wedge c \neq 0) \to (\frac{a}{b} = \frac{ac}{bc})$
T14: *Rule for Addition of Fractions*
$(b \neq 0 \wedge d \neq 0) \to (\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd})$
T15: *Rule for Multiplication of Fractions*
$(b \neq 0 \wedge d \neq 0) \to (\frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd})$
T16: *Rule for Division of Fractions*
$(b \neq 0 \wedge c \neq 0 \wedge d \neq 0) \to (\frac{\frac{a}{b}}{\frac{c}{d}} = \frac{ad}{bc})$

Order Axioms

Ord1: $\forall a, b \in \mathbb{R}, (a > 0 \wedge b > 0) \to (a + b > 0 \wedge ab > 0)$
Ord2: $\forall a \in \mathbb{R} \backslash \{0\}, (a > 0 \vee -a > 0 \wedge \sim (a > 0 \wedge -a > 0))$
Ord3: 0 *is not positive.*

Derived Rules for Calculating with Inequalities

T17: *Trichotomy Law*
$a < b \vee b < a \vee a = b$
T18: *Transitive Law*
$(a < b \wedge b < c) \to a < c$
T19: $(a < b) \to (a + c < b + c)$
T20: $(a < b \wedge c > 0) \to ac < bc$
T21: $(a \neq 0) \to (a^2 = 0)$
T22: $1 > 0$
T23: $(a < b \wedge c < 0) \to ac > bc$
T24: $(a < b) \to (-a > -b)$
T25: $(ab > 0) \to (a > 0 \wedge b > 0) \vee (a < 0 \wedge b < 0)$
T26: $((a < c) \wedge (b < d)) \to (a + b < c + d)$
T27: $((0 < a < c) \wedge (0 < b < d)) \to 0 < ab < cd$