CS1231S Cheatsheet

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

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	$prime(n) \iff (n > 1) \wedge \forall r, s \in \mathbb{Z}^+, (n = rs \to (r = 1 \wedge s = n) \vee (r = n \wedge s = 1))$ ***or*** $((r > 1) \wedge (s > 1) \to rs \neq n)$
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

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

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

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)	$\forall x (P(x) \to Q(x))$
For all x, P(x) is a necessary condition for Q(x)	$\forall x (Q(x) \to P(x))$
For all x, P(x) only if R(x)	$\forall x (P(x) \to Q(x))$

Rules of Inference

Table 2.3.1 Rules of Inference

Modus Ponens	$p \to q$ p $\therefore q$	
Modus Tollens	$p \to q$ $\sim q$ $\therefore \sim p$	
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	$p \to q$ $q \to r$ $\therefore p \to r$	
Proof by division into cases	$p \vee q$ $p \to r$ $q \to r$ $\therefore r$	

Errors

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

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

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

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
$\not\subseteq$	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	$A \setminus B = A \cap \bar{B}$	

Theorems

Theorem 4.4.1: *Quotient-Remainder Theorem*
$\forall n \in \mathbb{Z}, d \in \mathbb{Z}^+, \exists! q, r \in \mathbb{Z}((n = dq + r) \wedge (0 \le r < d))$
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 $\lvert S \rvert$	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)	$x \in \bar{A} \iff x \notin \bar{A}$
$\cup_{i=0}^{n} A_i$	$A_0 \cup A_1 \cup ... \cup A_n$
(procedural)	$\{x \in U \mid x \in A_i, \exists i = [0, n]\}$
$\cap_{i=0}^{n} A_i$	$A_0 \cap A_1 \cap ... \cap A_n$
(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	$\{a \in A : aRb$ *for some* $b \in B\}$
Co-domain of R from A to B	B
Range of R from A to B	$\{b \in B : aRb$ *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 $\mathcal{C}$	$\forall x, y \in A, xRy \iff$ $\exists S$ *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	$a \preccurlyeq b \vee b \preccurlyeq a$
Compatibility	$\exists c \in A(a \preccurlyeq c \wedge b \preccurlyeq c)$
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	$\iff \forall x, y, z \in A(xRy \wedge yRz \Rightarrow xRz)$

Functions

Function Definitions

Function $f : X \to Y$ (F1) $\forall x \in X \exists y \in Y (x, y) \in f$

(F2) $\forall x \in X\ \forall y_1, y_2 \in Y$

$(((x, y_1) \in f \wedge (x, y_2) \in f) \to y_1 = y_2)$

or $f \subseteq X \times Y \iff \forall x \in X\ \exists! y \in Y (x, y) \in F$

or $\forall x \in X\ \exists y \in Y, \{y\} = \{b \mid (x, b) \in f\}$

Given $f : A \to B, f(x) = y$

Argument	x
Output of f input x	$f(x)$
Image of x under f	$f(x)$
x is a preimage of y	$f(x) = y$
Domain $Dom(f)$	A
Co-domain $coDom(f)$	B
Range $Range(f)$	$\{b \in B : b = f(a) \text{ for some } a \in A\}$
Injective	$\iff \forall x_1, x_2 \in A (f(x_1) = f(x_2) \Rightarrow x_1 = x_2)$
(contrapositive)	$\iff \forall x_1, x_2 \in A (x_1 = x_2 \Rightarrow f(x_1) \neq f(x_2))$
Surjective	$\iff \forall y \in B\ \exists x \in A (y = f(x))$
Bijective	$\iff \forall y \in B\ \exists! x \in A (y = f(x))$
Inverse f^{-1}	$\iff \forall x \in A\ \forall y \in B (y = f(x) \iff x = g(y))$

Given $g : B \to C$

Composition of f & g $g \circ f : A \to C$

where $(g \circ f)(x) = g(f(x)) \forall x \in A$

Identity function on A $id_A(x) = x\ \forall x \in A$

Given $f : A \to B, f(x) = y$

Left inverse g $g : B \to A \iff g(f(a)) = a \forall a \in A$

Right inverse h $h : B \to A \iff f(h(b)) = b \forall b \in B$

Assignment 2: Fact 1

A function is injective $\iff$ it has a left inverse.

Assignment 2: Fact 2

A function is surjective $\iff$ it has a right inverse.

Theorem 7.1.1. *Function Equality*

Given $f : A \to B, g : C \to D$,

$f = g \iff (A = C \wedge B = D) \wedge (f(x) = g(x) \forall x \in A)$

Proposition: *Uniqueness of inverses*

If g_1 and g_2 are inverses of $f : X \Rightarrow Y$, then $g_1 = g_2$

Theorem 7.2.3

$f : A \to B$ is a bijection $\iff f^{-1}$ exists.

Theorem 7.3.1: *Composition with an Identity Function*

Given $f : A \Rightarrow B, (f \circ id_A = f) \wedge (id_B \circ f = f)$

Theorem 7.3.2: *Composition of a function with its inverse*

Given $f : A \Rightarrow B$ where f is a bijection with f^{-1},

$(f^{-1} \circ f = id_A) \wedge (f \circ f^{-1} = id_B)$

Theorem: *Associativity of Function Composition*

If $f : A \to B, g : B \to C, h : C \to D, (h \circ g) \circ f = h \circ (g \circ f)$

Theorem 7.3.3

If $f : A \to B, g : B \to C$ and f and g are both injective, $g \circ f$ is injective

Theorem 7.3.4

If $f : A \to B, g : B \to C$ and f and g are both surjective, $g \circ f$ is surjective

Proposition:

Congruence-mod n is an equivalence relation on $\mathbb{Z}\ \forall n \in \mathbb{Z}^+$

$+$ and $\times$ on $\mathbb{Z}_n$

$\sim_n$ is the congruence-mod-n relation on $\mathbb{Z}$

$\mathbb{Z}_n$	$Z/\sim_n$
$+$ on $\mathbb{Z}_n$	$[x] + [y] = [x + y]$
$\times$ on $\mathbb{Z}_n$	$[x] \times [y] = [x + y]$
Well-defined property	$\forall x_1, x_2 \in A\ \forall f : A \to B$
w.r.t Equiv Relation $\sim$	$x_1 \sim x_2 \Rightarrow f(x_1) \sim f(x_2)$
w.r.t Equiv Class $[x]$	$[x_1] = [x_2] \Rightarrow [f(x_1)] \sim [f(x_2)]$

Proposition: *Addition on* $\mathbb{Z}_n$ *is well defined*

$\forall n \in \mathbb{Z}^+, [x_1], [y_1], [x_2], [y_2] \in \mathbb{Z}^+$,

$[x_1] = [x_2] \wedge [y_1] = [y_2] \Rightarrow [x_1] + [y_1] = [x_2] + [y_2]$

Proposition: *Multiplication on* $\mathbb{Z}_n$ *is well defined*

$\forall n \in \mathbb{Z}^+, [x_1], [y_1], [x_2], [y_2] \in \mathbb{Z}^+$,

$[x_1] = [x_2] \wedge [y_1] = [y_2] \Rightarrow [x_1] \times [y_1] = [x_2] \times [y_2]$

String/Sequence

Definitions

Sequence	ordered set with members called terms.
$a_0, a_1, a_2, ...$	represented by a function a
	where $Dom(a) = \mathbb{Z}_{\geq 0}$
	where $a(n) = a_n \forall n \in \mathbb{Z}_{\geq 0}$
Fibonacci sequence	$\forall n \in \mathbb{Z}_{\geq 0} Z$,
$F_0, F_1, F_2, ...$	$F_0 = 0, F_1 = 1, F_{n+2} = F_{n+1} + F_n$
String over A	$a_0, a_1 ... a_{l-1}, l \in \mathbb{Z}_{\geq 0}$
	$a_0, a_1 ... a_{l-1} \in A$
Empty string ε	String of length 0
Summation $\sum_n^{k=m} a_k$	$a_m + a_{m+1} + ... + a_n$
Product $\prod_n^{k=m} a_k$	$a_m \times a_{m+1} \times ... \times a_n$

Equality of Sequences:

Given sequences $A = a_0, a_1, a_2 ...$ and $B = b_0, b_1, b_2 ...$ defined by the functions $a(n) = a_n$ $b(n) = b_n$ respectively for every $n \in \mathbb{Z}_0$, $A = B \iff a(n) = b(n) \forall n \in \mathbb{Z}_0$

Equality of Strings:

Given sequences $s_1 = a_0, a_1, a_2 ..., a_{l-1}$ and $s_2 = b_0, b_1, b_2 ..., b_{l-1}, l \in \mathbb{Z}_{\geq 0}$,

$s_1 = s_2 \iff a_i = b_i \forall i \in \{0, 1, 2, ..., l - 1\}$

Theorem 5.1.1

If a_m, a_{m+1}, a_{m+2} and b_m, b_{m+1}, b_{m+2} are sequences of real numbers and c is a real number,

$\sum_n^{k=m} a_k + \sum_n^{k=m} b_k = \sum_n^{k=m} (a_k + b_k)$

$c \times \sum_n^{k=m} a_k = \sum_n^{k=m} c \times a_k$ (generalised distributive law)

$(\prod_n^{k=m} a_k) \times (\prod_n^{k=m} b_k) = (\prod_n^{k=m} (a_k \times b_k))$

Common Sequences

Arithmetic	$a_k = a_{k+1} + d\ \forall k \in \mathbb{Z}^+$
	$a_n = a_0 + dn\ \forall n \in \mathbb{N}$
Geometric	$a_k = r a_{k-1}\ \forall k \in \mathbb{Z}^+$
	$a_n = a_0 r^n\ \forall n \in \mathbb{N}$

Mathematical Induction

Weak MI

1. Let $P(n) \equiv$ statement to be proved
2. **Basis step** : Prove $P(a)$ is true (a is the base case)
3. **Inductive hypothesis** : Let $P(k)$ be true for some $\mathbb{Z}_{\geq k}$
4. **Inductive step** : To prove $P(k + 1)$, show $P(k) \Rightarrow P(k + 1)\ \forall k \in \mathbb{Z}^+$
5. $\therefore P(n)$ is true $\forall n \in \mathbb{N}$

Strong MI

1. Let $P(n) \equiv$ statement to be proved
2. **Basis step** : Prove $P(a) \wedge P(a + 1) \wedge ... \wedge P(k)$ is true (a to k are base cases)
3. **Inductive hypothesis** : Let $k, m \in \mathbb{N}$. Assume $P(m)$ is true for $\forall\ m < k$ for some k
4. **Inductive step** : To prove $P(k + 1)$, show $(P(a) \wedge P(a + 1) \wedge ... \wedge P(k)) \Rightarrow P(k + 1)\ \forall k \in \mathbb{Z}^+$
5. $\therefore P(n)$ is true $\forall n \in \mathbb{N}$

Definitions

Well-Ordered Principle: Every nonempty subset of $\mathbb{N}$ has a smallest element.

Recurrence Relation: A formula that relates each term a_k to its predecessors $a_{k-1}, ... a_{k-i}$ where $(k - 1) \in \mathbb{N}$

Recursively Defined Sets

1. (Define **founders**) $a \in S$	*base clause*
2. (Define **constructors**) If $x \in S$, then $g(x) \in S$.	*recursion clause*
3. (Specify nothing more) Membership of S	*minimality clause*

can always be demonstrated by (finitely many) successive applications of the clauses above.

Structural Induction

To prove $\forall x \in S\ P(x)$ is true,

Basis step	show that $P(c)$ is true for every founder c
Induction step	show $\forall x \in S (P(x) \Rightarrow P(f(x)))$ is true $\forall f$

Cardinality

Pigeonhole Principle

Let A and B be finite sets. If the injection $f : A \to B$ exists, then $|A| \leq |B|$.

Contrapositive: Let $m, n \in \mathbb{Z}^+ with m > n$. If m pigeons are put into n pigeonholes, then there must be at least one pigeonhole with at least two pigeons.

Dual Pigeonhole Principle

Let A and B be finite sets. If the surjection $f : A \to B$ exists, then $|A| \leq |B|$.

Contrapositive: Let $m, n \in \mathbb{Z}^+ with m > n$. If m pigeons are put into n pigeonholes, then there must be at least one pigeonhole with at least no pigeons.

Cardinality Definitions

Finite set	$\iff$ S is empty, or $\exists$ bijection $f: S \to \mathbb{Z}_n$ for some $n \in \mathbb{Z}^+$
Infinite set	If S is not finite.
Cardinality of S $\lvert S \rvert$	(i) 0 if $S = \emptyset$ or (ii) n if $f: S \to \mathbb{Z}_n$ is a bijection
Cardinal number $\aleph_0$	$\lvert \mathbb{Z}^+ \rvert$
Countably infinite	$\lvert S \rvert = \lvert \aleph_0 \rvert$
Countable set	$\iff$ finite or countably infinite
Uncountable	Non-countable set

Theorem: *Equality of Cardinality of Finite Sets*:
Let A and B be any finite sets.
$(|A| = |B|) \iff \exists$ bijection $f : A \to B$.
Same Cardinality (Cantor)
Given any two sets A and B,
$(|A| = |B|) \iff \exists$ bijection $f : A \to B$.
Theorem 7.4.1: *Properties of Cardinality*
The same-cardinality relation is an equivalence relation.
For all sets A, B, C,
Reflexive: $|A| = |A|$
Symmetric: $(|A| = |B|) \to (|B| = |A|)$
Transitive: $(|A| = |B|) \wedge (|B| = |C|) \to (|A| = |C|)$
Theorem: $\mathbb{Z}^+ \times \mathbb{Z}^+$ is countable
Theorem: *(Cartesian Product)*
If sets A and B are both countably infinite, then so is $A \times B$
Corollary: *(General Cartesian Product)*:
Given $n \in \mathbb{Z}_{\geq 2}$ countably infinite sets $A_1, .., A_n$,
the Cartesian product $A_1 \times ... \times A_n$ is also countably infinite.
Theorem: *Unions*
If $A_1, ...$ are all countable sets and the amount of sets are countable, $\bigcup_{i=1}^{\infty} A_i$ is also countable.
Proposition 9.1
An infinite set B is countable $\iff$ there is a sequence $b_0, ... \in B$ in which every element of B appears exactly once.
Lemma 9.2:*Countability via Sequence*
An infinite set B is countable $\iff$ there is a sequence $b_0, ... \in B$ in which every element of B appears.
Theorem 7.4.2: (Cantor)
$(0, 1) = \{x \in \mathbb{R} \mid 0 < x < 1\}$ is countable.
Theorem 7.4.3: Any subset of any countable set is countable.
Corollary 7.4.4 *(contrapositive of 7.4.3)*: Any set with an uncountable subset is uncountable.
Proposition 9.3: Every infinite set has a countably infinite subset.
Lemma 9.4: *Union of Countably Infinite Sets*
$(|A| = |\aleph_0|) \wedge (|B| = |\aleph_0|) \to (A \cup B)$ is countable

Counting

General Rules

Theorem 9.1.1: *The Number of Elements in a List*
$n - m + 1$ integers from m to n inclusive. $(m, n \in \mathbb{Z}, m \leq n)$
Theorem 9.2.1: *The Multiplication/Product Rule*
If an operation consists of k steps, and the amount of ways the k^{th} step can be performed is n_k, the amount of possible ways for the operation $= n_1 \times .... \times ...n_k$.
Theorem 9.3.2: *The Addition/Sum Rule*
Suppose a finite set A is the union of k distinct mutually disjoint subsets $A_1, ..., A_k$, $|A| = |A_1| + ...|A_k|$
Theorem 9.3.3: *The Difference Rule*
If A is a finite set, and $B \subseteq A$, $|A \backslash B| = |A| - |B|$
Theorem 9.3.3: *The Inclusion/Exclusion Rule for 2 or 3 sets*
If A, B, C are finite sets,
$|A \cup B| = |A| + |B| - |A \cap B|$
$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$
Theorem 9.7.2: *Binomial Formula*
$(a + b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$
$= a^n + \binom{n}{1} a^{n-1} b^1 + ... + \binom{n}{n-1} a^1 b^{n-1} + b^n$
Theorem 6.3.1: *Number of elements in a Power Set*
If $|X| = n \in \mathbb{Z}^+$, $|\mathcal{P}(A)| = 2^n$

Combinations, Permutations

	Order	Without order
Repetition	n^k	$\binom{k+n-1}{k}$ *(9.6.1)*
No repetition	$P(n, k)$ *(9.2.3)*	$\binom{n}{k}$ *(9.5.1)*

Permutations

Theorem 9.2.2: *Permutations*
Permutations of a set with $n \in \mathbb{Z}^+$ elements is $n!$
Theorem 9.2.3: *r-permutations from a set of n elements*
$r \in \mathbb{Z}^+ \wedge r \leq n$, $P(n, r) = \frac{n!}{(n-r)!}$

Combinations

r-combination: A subset of r of the n elements.
Theorem 9.5.1: *Formula of* $\binom{n}{r}$
$\binom{n}{r} = \frac{n!}{r!(n-r)!}$
Theorem 9.5.2: *Permutations with sets of indistinguishable objects*
$\binom{n}{r}\binom{n-n_1}{n_2}..\binom{n-...-n_{k-1}}{n_k} = \frac{n!}{n_1!n_2!..n_k!}$
Theorem 9.7.1: *Pascal's Formula*
$\binom{n+1}{r} = \binom{n}{r-1} + \binom{n}{r}$

Multiset

Multiset of size r: r-combination with repetition allowed
Theorem 9.6.1: *Number of r-combinations with repetition allowed*
$\binom{r+n-1}{r}$

Pigeonhole Principle

Pigeonhole Principle (PHP)
Given a function from one finite set to a smaller finite set, there must be at least 2 elements in the domain that have the same image in the co-domain.
Generalised Pigeonhole Principle
$\forall f : X \to Y$ where X, Y are finite and $|X| = n, |Y| = m$ and $\forall k \in \mathbb{Z}^+$, if $k < n/m$, $\exists y \in Y$ that y is the image of at least $k + 1$ distinct elements of X.
Generalised Pigeonhole Principle *(Contrapositive)*
$\forall f : X \to Y$ where X, Y are finite and $|X| = n, |Y| = m$ and $\forall k \in \mathbb{Z}^+$, if $\forall y \in Y, f^{-1}(\{y\})$ has at most k elements, X has at most km elements - $n \leq km$

Probability

Axioms

Let S be the sample space, $\forall$ events A and B in S.
1. $0 \leq P(A) \leq 1$
2. $\mathcal{P}(\emptyset) = 0$ and $P(S) = 1$
3. $(A \cap B = \emptyset) \to (P(A \cup B) = P(A) + P(B))$

Equally Likely Probability Formula:
If S is a finite sample space where all outcomes are equally likely and E is an event in S, $P(E) = \frac{|E|}{|S|}$
Probability of the Complement of an Event
$P(\bar{A}) = 1 - P(A)$
Probability of General Union of Two Events
$P(A \cup B) = P(A) + P(B) - P(A \cap B)$

Expected Value

$\sum_{k=1}^{n} a_k p_k = a_1 p_1 + ... + a_n p_n$

Linearity of Expectation
For random variables X and Y, $E[X + Y] = E[X] + E[Y]$
For random variables $X_1, ...X_n$,
$E[\sum_{i=1}^{n} c_i \times X_i] = \sum_{i=1}^{n} c_i \times E[X_i]$

Conditional Probability

The conditional probability of B given $A = P(B|A)$
$P(B|A) = \frac{P(A \cap B)}{P(A)}$ *(9.9.1)*
$\therefore P(A \cap B) = P(B|A) \times P(A)$ *(9.9.2)*
$\therefore P(a) = \frac{P(A \cap B)}{P(B|A)}$ *(9.9.3)*
Theorem 9.9.1: *Bayes' Theorem*
Suppose $S = B_1 \cup ... \cup B_n$ where the events are disjoint.
Suppose A is an event in S.
$P(B_k|A) = \frac{P(A|B_k) \times P(B_k)}{P(A|B_1) \times P(B_1) + ... + P(A|B_n) \times P(B_n)}$

Independent Events A and B are independent
$\iff P(A \cap B) = P(A) \times P(B)$
Pairwise Independent A, B, C are pairwise independent
$\iff P(A \cap B) = P(A) \times P(B) \wedge$
$P(A \cap B) = P(A) \times P(C) \wedge$
$P(A \cap B) = P(B) \times P(C)$
Mutually Independent A, B, C are mutually independent
$\iff$ they are pairwise independent $\wedge$
$P(A \cap B \cap C) = P(A) \times P(B) \times P(C)$

Graphs

Undirected Graph:
V: set of vertices, E: set of edges.
Edge $e \in E = \{v, w\}, v, w \in V$
Directed Graph/Digraph:
V: set of vertices, E: set of edges.
Edge $e \in E = (v, w), v, w \in V$
Simple Graph Undirected graph that does not have any loops or parallel edges.
Complete Graph Simple graph K_n with n vertices and only one edge connecting each pair of distinct vertices.
Bipartite Graph Simple graph whose vertices can be divided into two disjoint sets U and V such that every edge connects a vertex in U to one in V
Complete Bipartitite Graph Bipartite graph on disjoint sets U and V such that every vertex in U connects to every vertex in V. $|U| = m, |V| = n, K_{m,n}$
Subgraph of a Graph H is a subgraph of $G \iff$
$\forall$ vertex $v \in H(v \in G) \wedge$
$\forall$ edge $e \in H(e \in G) \wedge$
$\forall$ edge $e \in H$, (endpoint in H = endpoint in G).
Degree of Vertex and Total Degree of an Undirected Graph
$deg(v)$ = number of edges incident on v (if edge is v to v, counted twice).
Total degree of G = sum of degrees of all vertices in G.
Indegree and Outdegree of a Vertex of a Directed Graph Let $G = (V, E), v \in V$
Indegree of $vdeg^-(v)$ = Number of directed edges that have v as endpoint.
Outdegree of $vdeg^+(v)$ = Number of directed edges that have v as startpoint.
$\sum_{v \in V} deg^-(v) = |E| = \sum_{v \in V} deg^+(v)$

Theorems

Theorem 10.1.1: *The Handshake Theorem*
Total degree of $G = 2\times$ number of edges of G.
Corollary 10.1.2: Total degree of a graph is even.
Proposition 10.1.3: In any graph there are an even number of vertices of odd degree.
Tutorial 11: Q5(a) If $G = (V, E)$ is a simple undirected graph and is connected, $|E| \geq |V| - 1$.
Tutorial 11: Q6(a) If $G = (V, E)$ is a simple undirected graph and is acyclic, $|E| \leq |V| - 1$.
Tutorial 11: Q7 $G = (V, E)$ is a simple undirected graph. G is a tree $\iff$ there is exactly one path between every pair of vertices.

Trails, Paths & Circuits

Let $G = (V, E)$ be a graph, $w, v \in V$
Walk from v to w: Finite alternating sequence of adjacent vertices and edges of G. $ve_1v_1....e_nw$.
Length of walk: Number of edges in walk.
Trivial walk: v
Trail from v to w: Walk from v to w that does not contain a repeated edge.
Path from v to w: Trail that does not contain a repeated vertex.
Closed walk: Walk that starts and ends at same vertex.
Circuit/cycle: Closed walk of length ≥ 3 without a repeated edge.
Simple circuit/cycle: Circuit without any repeated vertex except first and last.
Triangle: Simple circuit of length 3.
Cyclic graph: Contains loop or a cycle.
Acyclic graph: Not cyclic.
Connectedness:
v, w are connected $\iff$ there is a walk from v to w.
G is connected $\iff \forall$ vertices $v, w \in V, \exists$ a walk from v to w.
Connected Component: H is a connected component $\iff$
1. H is a subgraph of G.
2. H is connected.
3. No connected subgraph of G has H as a subgraph and contains vertices or edges not in H.

Lemma 10.2.1:
a. If G is connected, any two distinct vertices of G can be connected by a path.
b. If v, w are part of a circuit in G and one edge is removed from the circuit, there still exists a trail from v to w in G.
c. If G is connected and contains a circuit, then an edge of the circuit can be removed without disconnecting G.
Lemma 10.5.5. Let G be a simple, undirected graph. If there are two distinct paths from a vertex v to a different vertex w, then G contains a cycle (and hence G is cyclic).

Hamiltonian

Hamiltonian Circuit: A simple circuit that includes every vertex of G.
Hamiltonian Graph: A graph that contains a Hamiltonian circuit.
Proposition 10.2.6: If G has a Hamiltonian circuit, G has a subgraph H where:
1. H contains every vertex of G.
2. H is still connected.
3. H has the same number of edges as vertices.
4. Every vertex of H has degree 2.

Euler

Euler Circuit: A circuit that contains every vertex and traverses every edge of G exactly one.
Eulerian Graph: A graph that contains an Euler circuit.
Euler Trail from v to w: A sequence of adjacent edges that start at v, ends at w and passes through every vertex of G at least once, and traverses every edge of G exactly one.
Theorem 10.2.2: If a graph has an Euler circuit, every vertex of the graph has a positive even degree.
Contrapositive: If some vertex of a graph has odd degree, then the graph does not have an Euler circuit.
Theorem 10.2.3: If G is connected and the degree of every vertex of G is a positive even integer, then G has an Euler circuit.
Theorem 10.2.4: G has an Euler circuit $\iff$ G is connected and every vertex of G has a positive even degree.
Corollary 10.2.5: There is an Euler trail from v to w $\iff$ G is connected, v, w have odd degree, and all other vertices of G have positive even degree.

Matrix Representation

$m \times n$ matrix A over set S: Rectangular array of elements of S arranged into m rows and n columns. $A = (a_{ij})$
Matrix equality: $A = B \iff$ size(A) = size$(B) \wedge$
$a_{ij} = b_{ij} \forall i = 1, 2, ..., m \wedge j = 1, 2, ..., n$
Square matrix: $m = n$
Main diagonal: $a_{11}, a_{22}....a_{nn}$ for a square matrix.
Adjacency Matrix of a Directed Graph: Let G be a directed graph with ordered vertices $\{v_1, .., v_n\}$.
Adjacency matrix of G is the $n \times n$ matrix $A = (a_{ij})$ over set of non negative integers such that a_{ij} = number of arrows from v_i to v_j $\forall i, j = 1, 2, ..n$
Symmetric Matrix: $n \times n$ square matrix is symmetric $\iff$
$a_{ij} = a_{ji} \; \forall i, j = 1, 2, ..., n$
Scalar Product: $A \cdot B = a_{i1}b_{ij} + ... + a_{in}b_{nj}$
Matrix Multiplication: $A \times B = (c_{ij})$ where
$c_{ij} = a_{i1}b_{1j} + ... + a_{ik}b_{kj}$
Identity Matrix: $I_n = (\delta_{ij})$ where
$\delta_{ij} = 1$ if $i = j$,
$\delta_{ij} = 0$ if $i \neq j \; \forall i, j = 1, 2, ..., n$
n^{th} Power of a Matrix
$A^0 = I_n$
$A^n = A \times A^{n-1}$
Theorem 10.3.2 If G is a graph with vertices $v_1, v_2, ..., v_m$ and A is the adjacency matrix of G, $\forall n \in \mathbb{Z}^+$ and $\forall i, j = 1, 2, .., m$, the ij-th entry of A^n is the number of walks of length n from v_i to v_j.

Isomorphism and Planar Graphs

Isomorphic Graph

Let $G = (V_G, E_G), G' = (V_{G'}, E_{G'})$
$G \cong G' \iff$ there exist bijections $g : V_G \to V_{G'}$ and $h : E_G \to E_{G'}$ that preserve the edge-endpoint functions of G and G' that $\forall v \in V_G, e \in E_G$.
v is endpoint of $e \iff g(v)$ is endpoint of $h(e)$
alternatively:
$G \cong G' \iff$ exists a permutation $\pi : V_G \to V_{G'}$ such that $\{u, v\} \in E_G \iff \{\pi(u), \pi(v)\} \in E_{G'}$
Complement of G $\bar{G}$
The vertex set of $\bar{G}$ is identical to the vertex set of G. However, two distinct vertices v, w of $\bar{G}$ are connected by an edge $\iff v, w$ are not connected by an edge in $\bar{G}$.
Self-complementary A graph isomorphic with its complement.
Theorem 10.4.1: *Graph Isomorphism is an Equivalence Relation* Let $\cong$ be the relation of graph isomorphism on set of graphs S. $\cong$ is an equivalence relations.

Planar Graph

A graph that can be drawn on a 2D-plane without edges crossing.
Kuratowski's Theorem A finite graph is planar $\iff$ it does not contain a subgraph that is a subdivision of the complete graph K_5 or the complete bipartite graph $K_{3,3}$.
Faces of a planar graph The regions that is split by the edges.
Other useful observations (not definitions):
In a planar graph, 1 edge will border 2 faces.
In a planar graph, 1 face will have at least 3 edges.
Euler's Formula $G = (V, E), e = |E|, v = |V|, f =$ no. of faces $f = e - v + 2$
Tutorial 11: Q2(a) $3f \leq 2e$
Tutorial 11: Q2(b) $e \leq 3v - 6$

Trees

Circuit-free $\iff$ has no circuits
Tree $\iff$ circuit-free and connected.
Trivial tree graph consisting of a single vertex.
Forest $\iff$ circuit-free and not connected.
Terminal vertex Vertex of degree 1.
Internal vertex Vertex of degree > 1
Lemma 10.5.1 Any non-trivial tree has at least one vertex of degree 1.
Theorem 10.5.2 Any tree with n vertices ($n > 0$) has $n - 1$ edges.
Lemma 10.5.3 If G is any connected graph, C is any circuit in G and one of the edges of C is removed from G, then the graph that remains is still connected.
Theorem 10.5.4 If G is a connected graph with n vertices and $n - 1$ edges, then G is a tree.

Rooted Trees

Rooted Tree One vertex that is distinguished from the others and called the root.
Level is the number of edges along the unique path between it and the root.
Height is the maximum level of any vertex on the tree.
Children of v are vertices adjacent to v and one level farther away from the root than v.
Parent If w is a child of v, v is the parent of w.
Siblings Two distinct vertices which are children of the same parent.
Ancestor If v lies on the unique path between w and the root, v is an ancestor.
Descendant If v lies on the unique path between w and the root, w is an descendant.

Binary Tree

Binary Tree Rooted tree which every parent has at most two children, the **left** and **right** child.
Full Binary Tree Binary tree where each parent has exactly two children.
Subtree of v is the left/right child of v whose vertices consist of the left/right child of v and all its descendants, and whose edges consist of all those edges of T that connect the vertices of the left/right subtree.
Theorem 10.6.1: *Full Binary Tree Theorem* If T is a full binary tree with k internal vertices, then T has a total of $2k + 1$ vertices and has $k + 1$ terminal vertices.
Theorem 10.6.2: For non-negative integers h, if T is any binary tree with height h and t terminal vertices, then $t \leq 2^h = log_2 t \leq h$

Binary Tree Traversal

Breadth-first search starts at root, visits adjacent vertices, then moves to the next level.
Depth-first search:
Pre-order:
- Print the data of the root (or current vertex)
- Traverse left
- Traverse right

In-order:
- Traverse left
- Print the data of the root (or current vertex)
- Traverse right

Post-order:
- Traverse left
- Traverse right
- Print the data of the root (or current vertex)

Spanning Path

Spanning Path for a graph G is a subgraph that contains every vertex of G and is a tree.
Weighted Graph is a graph where every edge has a weight.
Minimum spanning tree is a spanning tree with the least possible total weight of all spanning trees of the graph.
$w(G)$ denotes the total weight of G
Proposition 10.7.1
1. Every connected graph has a spanning tree.
2. Any two spanning trees for a graph have the same number of edges.

Algorithm 10.7.1 (Kruskal)

1. Initialise T with all the vertices of G and no edges.
2. Let E be the set of all edges of G, and let $m = 0$.
3. While $(m < n - 1)$:

   3a. Find an edge e in E of least weight.
   3b. Delete e from E
   3c. If addition of e to the edge set of T does not produce a circuit, add e to T and set $m = m + 1$

Algorithm 10.7.2 (Prim)

1. Pick a vertex v in G and let T be the graph with this vertex only.
2. Let V be the set of all vertices of G except v.
3. For $i = 1$ to $n - 1$

   3a. Find an edge e in G such that e connects T to one of the vertices in V and e has the least weight of all edges connecting T to a vertex in V. Let w be the endpoint of e.
   3b. Add e to the edge set of T and w to the edge set of T, and remove w from V.

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: $((0<a<c) \wedge (0<b<d)) \to 0<ab<cd$