CS1231S Discrete Structures
Help Sheet for Final Examinations

Disclaimer: This help sheet does not contain everything. It mainly contains the formulae which I deem important for solving questions for the Finals. I hereby affirm that any mistake found in this document is due to my own human error, and not committed on purpose in order to "snake".

Predicate and Propositional Logic

Logical Equivalences		
Commutative laws	$p \wedge q \equiv q \wedge p$	$p \vee q \equiv q \vee p$
Associative laws	$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	$(p \vee q) \vee r \equiv p \vee (q \vee r)$
Distributive laws	$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$
Identity laws	$p \wedge \text{true} \equiv p$	$p \vee \text{false} \equiv p$
Negation laws	$p \vee \sim p \equiv \text{true}$	$p \wedge \sim p \equiv \text{false}$
Double negative law	$\sim(\sim p) \equiv p$	
Idempotent laws	$p \wedge p \equiv p$	$p \vee p \equiv p$
Universal bound laws	$p \vee \text{true} \equiv \text{true}$	$p \wedge \text{false} \equiv \text{false}$
De Morgan's laws	$\sim(p \wedge q) \equiv \sim p \vee \sim q$	$\sim(p \vee q) \equiv \sim p \wedge \sim q$
Absorption laws	$p \vee (p \wedge q) \equiv p$	$p \wedge (p \vee q) \equiv p$
Negation of true and false	$\sim \text{true} \equiv \text{false}$	$\sim \text{false} \equiv \text{true}$

Conditionals			
Conditional	$p \to q$	if p, then q	p is a **sufficient** condition for q
Contrapositive	$\sim q \to \sim p$	p only if q	
Converse	$q \to p$	p if q	p is a **necessary** condition for q
Inverse	$\sim p \to \sim q$		
Biconditional	$p \leftrightarrow q$	p if, and only if, q	
Note that Conditional Statement ≡ Contrapositive, Converse ≡ Inverse, but Conditional Statement ≢ Converse.			
Implication Law	$p \to q \equiv \sim p \vee q$		

Set Theory

Subsets (≡)		
Subset	$A \subseteq B$	$\forall x\, (x \in A \to x \in B)$
-Not a subset	$A \nsubseteq B$	$\exists x\, (x \in A \wedge x \notin B)$
Equality	$A = B$	$\forall x\, (x \in A \leftrightarrow x \in B)$ $A \subseteq B \wedge B \subseteq A$
Proper Subset	$A \subsetneq B$	$(\forall x \in A, x \in B) \wedge (\exists y \in B, y \notin A)$
Transitivity	$A \subseteq B \wedge B \subseteq C \Rightarrow A \subseteq C$	

Set Operations (=)		
Union	$A \cup B$	$\{x \in \mathcal{U} \mid x \in A \vee x \in B\}$
Intersection	$A \cap B$	$\{x \in \mathcal{U} \mid x \in A \wedge x \in B\}$
Complement	$A - B$	$\{x \in A \mid x \notin B\}$
Union of 3 or more sets	$\bigcup_{i=1}^{n} A_i$	$A_1 \cup A_2 \cup \cdots \cup A_n$
Intersection of 3 or more sets	$\bigcap_{i=1}^{n} A_i$	$A_1 \cap A_2 \cap \cdots \cap A_n$

Set Identities		
Commutative laws	$A \cup B = B \cup A$	$A \cap B = B \cap A$
Associative laws	$(A \cup B) \cup C = A \cup (B \cup C)$	$(A \cap B) \cap C = A \cap (B \cap C)$
Distributive laws	$(A \cup B) \cap C = (A \cup B) \cap (A \cup C)$	$(A \cap B) \cup C = (A \cap B) \cup (A \cap C)$
Identity laws	$A \cup \emptyset = A$	$A \cap \mathcal{U} = A$
Complement laws	$A \cup \overline{A} = \mathcal{U}$	$A \cup \overline{A} = \emptyset$
Double complement law	$\overline{(\overline{A})} = A$	
Idempotent laws	$A \cup A = A$	$A \cap A = A$
Universal bound laws	$A \cup \mathcal{U} = \mathcal{U}$	$A \cap \emptyset = \emptyset$
De Morgan's laws	$\overline{A \cup B} = \overline{A} \cap \overline{B}$	$\overline{A \cap B} = \overline{A} \cup \overline{B}$
Absorption laws	$A \cup (A \cap B) = A$	$A \cap (A \cup B) = A$
Set difference law	$A - B = A \cap \overline{B}$	
Complements of the null and universal set	$\overline{\mathcal{U}} = \emptyset$	$\overline{\emptyset} = \mathcal{U}$

Disjoint Sets		
Sets are **disjoint**	$\Leftarrow$	$A \cap B = \emptyset$
Sets are **pairwise disjoint**	$\Leftrightarrow$	$\forall A, B \in \mathcal{C}$ with $A \neq B$, we have $A \cap B = \emptyset$

Set Definitions (=)		
Cartesian Product	$A \times B$	The set of ordered pairs, $\{(a, b) \mid a \in A, b \in B\}$
Power Set	$\wp(A)$	The set of all subsets of A, $\{X \mid X \subseteq A\}$

Partition of A	
P is a partition of $A \Leftrightarrow$ it is an unordered collection of:	
pairwise disjoint,	$\forall X, Y \in P$ with $X \neq Y$, we have $X \cap Y = \emptyset$
non-empty	$\emptyset \notin P$
subsets of A,	$P \subseteq \wp(A)$
whose union is A.	$\bigcup_{X \in P} X = A$

Counting and Probability

Number of elements in a set
There are $n - m + 1$ integers from m to n inclusive.
Number of elements in a power set
If a set X has n elements, then the power set $\wp(X)$ has 2^n elements.

Permutations	
Number of permutations of a set with n elements	$n!$
Number of r-permutations (ordered selection of r elements) from a set of n elements	$P_r^n = \frac{n!}{(n-r)!}$
Number of permutations of a set with n elements, where $n_1, n_2, \cdots, n_k$ elements indistinguishable from each other	$\frac{n!}{n_1!\, n_2! \cdots n_k!}$

Combinations	
Number of r-combinations (subsets of size r) that can be chosen from a set of n elements	$\binom{n}{r} = \frac{n!}{r!\,(n-r)!} = \frac{P_r^n}{r!}$
Number of multisets of size r (r-combinations with repetition allowed) that can be selected from a set of n elements	$\binom{r+n-1}{r}$

Pigeonhole Principle	
Function	For any function f
Domain	From a finite set X with n elements
Codomain	To a finite set Y with m elements
Positive integer	For any positive integer k
If $k < \frac{n}{m}$, then there is some $y \in Y$ such that y is the image of at least k+1 distinct elements of X.	
If for each $y \in Y$, $f^{-1}(\{y\})$ has at most k elements, then X has at most km elements, i.e. $n \leq km$.	
Implication on the Function	
$\lvert Domain \rvert > \lvert Codomain \rvert$	f is not injective
$\lvert Domain \rvert = \lvert Codomain \rvert$	f is injective if, and only if, it is surjective.

Pascal's Formula	
$\binom{n+1}{r} = \binom{n}{r-1} + \binom{n}{r}$	$\binom{n}{r} = \binom{n}{n-r}$

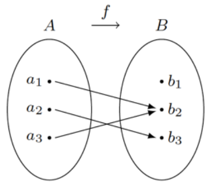
Binomial Theorem

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$$
$$= a^n + \binom{n}{1} a^{n-1} b^1 + \binom{n}{2} a^{n-2} b^2 + \cdots + \binom{n}{n-1} a^1 b^{n-1} + b^n$$

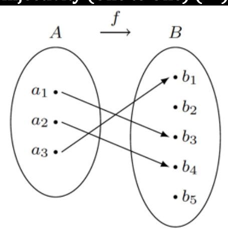
Expected value	
$a_1 p_1 + a_2 p_2 + \cdots + a_k p_k$	$a_1, a_2, \cdots, a_k$ are the possible outcomes, $p_1, p_2, \cdots, p_k$ are their associated probabilities

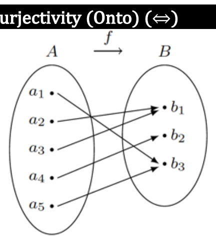
Probability	
Conditional Probability	$P(B \mid A) = \frac{P(A \cap B)}{P(A)}$
Baye's Theorem	$P(B_k \mid A) = \frac{P(A \mid B_k) \cdot P(B_k)}{P(A \mid B_1) \cdot P(B_1) + \cdots + P(A \mid B_n) \cdot P(B_n)}$
Independent Events	$P(A \cap B) = P(A) \times P(B)$
Pairwise Independent	$P(A \cap B) = P(A) \times P(B)$ $P(B \cap C) = P(B) \times P(C)$ $P(A \cap C) = P(A) \times P(C)$
Mutually Independent	A, B and C are pairwise independent, and $P(A \cap B \cap C) = P(A) \times P(B) \times P(C)$

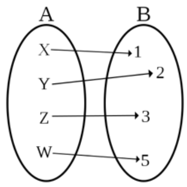
Functions

Functions	
	Each element $a \in A$ is a assigned a **unique** element $f(a) \in B$, and is denoted by $f: A \to B;\ a \mapsto f(a).$
	Every element in the domain A has **one and only one** arrow originating from it.
Identity function on A	$I_A: A \to A;\ a \mapsto a$
Inclusion map of B($\subseteq A$) in A	$\iota_B^A: B \to A;\ b \mapsto b$

Images and Preimages	
Set of images, $f(X)$	$\{f(x) \mid x \in X\} = \{b \in B \mid \exists x \in X, f(x) = b\}$
Set of pre-images, $f^{-1}(X)$	$\{f(x) \mid x \in X\}$
Range, $\mathcal{R}(f)$	$\{f(a) \mid a \in X\} = f(A)$

Injectivity (One to One) (⇔)	
	Distinct elements of A have distinct images under f. $\forall a_1, a_2 \in A\ (f(a_1) = f(a_2) \to a_1 = a_2)$
	No two arrows terminate in the same point in the codomain.
	Take two general elements $a_1, a_2 \in A$ and assume that $f(a_1) = f(a_2)$. Work towards the conclusion that $a_1 = a_2$.
Composition of Functions	f and g are injective → $g \circ f$ is injective
	$g \circ f$ is injective → f is injective

Surjectivity (Onto) (⇔)	
	Range is equal to the codomain, $\mathcal{R}(f) = B$. $\forall b \in B, \exists a_b \in A, f(a_b) = b$
	Every element in the codomain has at least one arrow terminating there.
	Take a general element $b \in B$ and find an element $a_b \in A$ such that $f(a_b) = b$.
Composition of Functions	f and g are surjective → $g \circ f$ is surjective
	$g \circ f$ is surjective → g is injective

Bijectivity (⇔)	
	Both injective and surjective. $\forall b \in B, \exists!\, a_b \in A, f(a_b) = b$
	Every arrow coming out of the domain terminates at a unique element in the codomain, and every element in the codomain has an arrow pointing to it.
Composition of Functions	f and g are bijective → $g \circ f$ is bijective
	$g \circ f$ is bijective → f is injective and g is surjective

Inverses	
Checking if a function has an inverse	f has an inverse ⇔ f is bijective.
Obtaining an inverse	$f: A \to B$, then an inverse of f is $g: B \to A$ such that $g \circ f = I_A$ and $f \circ g = I_B$.

Cantor-Bernstein Theorem
Let $f: A \to B$ and $g: B \to A$ be injective functions. Then there exists a bijective function $h: A \to B$.

Relations

Relations	
$R \subseteq A \times B$	$(a, b) \in R \Rightarrow aRb$
	$(a, b) \notin R \Rightarrow a \not R b$
Domain of R	$\{a \in A \mid \exists b \in B\ aRb\}$
Range of R	$\{b \in B \mid \exists a \in A\ aRb\}$

Inverse of R		$R^{-1} = \{(b, a) \in B \times A \mid aRb\}$
Types of Relations		
Reflexive	⇔	$\forall x \in A\ (xRx)$
Symmetric	⇔	$\forall x, y \in A\ (xRy \Rightarrow yRx)$
Transitive	⇔	$\forall x, y, z \in A\ (xRy \wedge yRz \Rightarrow xRz)$
Equivalence Relation	⇔	Reflexive, symmetric and transitive
Anti-Symmetric	⇔	$\forall x, y \in A\ (xRy \wedge yRx \Rightarrow x = y)$

Equivalence Classes	
Equivalence class of an element a	$[a]_R = \{x \in A \mid aRx\}$.
	$xRy \Rightarrow [x] = [y]$
	$x \not R y \Rightarrow [x] \cap [y] = \emptyset$
Equivalence class of a relation R	The subset $S \subseteq A$ is an equivalence class of R if, and only if, $S = [a]$ for some $a \in A$.
Set of equivalence classes of R	The set of equivalence classes of R is $A/R \subseteq \mathcal{P}(A)$.
	A/R is a partition of A, and every partition is a set of equivalence classes.
Properties of Equivalence Classes	
1. Any two distinct equivalence classes of an equivalence relation are disjoint. 2. The set of equivalence classes of R, is $A/R \subseteq \mathcal{P}(A)$, is a partition of A.	

Partial Orders		
A partial order on A, $\preccurlyeq$, is a relation on A that is reflexive, anti-symmetric and transitive.		
Properties of elements of a set that is partially ordered		
x and y are comparable		$x \preccurlyeq y$ or $y \preccurlyeq x$
x and y are incomparable		$x \not\preccurlyeq y$ or $y \not\preccurlyeq x$
a is minimal		$\forall x \in A\ (x \preccurlyeq a \to x = a)$
a is smallest		$\forall x \in A\ (a \preccurlyeq x)$
a is maximal		$\forall x \in A\ (a \preccurlyeq x \to x = a)$
a is largest		$\forall x \in A\ (x \preccurlyeq a)$
Properties of Partial Orders		
1. If R is a partial order on A, then so is R^{-1}. 2. A has at most one largest element and one smallest element.		
$\preccurlyeq$ is a total order on A	⇔	Every two elements of A are comparable, $\forall x, y \in A\ ((x \prec y) \vee (x = y) \vee (y \prec x))$
Subset $B \subseteq A$ is a chain	⇔	Every two elements of B are comparable, $\forall x, y \in B\ ((x \prec y) \vee (x = y) \vee (y \prec x))$

Number Theory

Division Algorithm	
$a = qb + r$	$q = a \text{ div } b = \lfloor \frac{a}{b} \rfloor$
	$r = a \bmod b$
$a = q\lvert b\rvert + r = q(-b) + r = (-q)b + r$	$a \text{ div } b = -(a \text{ div } \lvert b\rvert)$
	$a \bmod b = a \bmod \lvert b\rvert$

b-adic Expansion
$n = a_0b^0 + a_1b^1 + \cdots + a_kb^k = (a_ka_{k-1}\cdots a_0)_b$
To obtain a *b*-adic expansion of *n*, 1. Write down *n*. 2. Divide *n* by *b*, and write down the remainder at the right of *n*, and the quotient below *n*. 3. Repeat step (2) for the quotient by dividing it by *b*, until you reach 0 at the bottom of the left column. 4. Read the right column from top to bottom, and these are the coefficients of $b^0, b^1, \cdots b^k$.

Divisibility	
$a \mid b$ *if, and only if*, $\exists k \in \mathbb{Z}$ *such that* $b = ak$.	
Properties of Divisibility	
Negative dividend / divisor	$(a\mid b) \Leftrightarrow (-a\mid b) \Leftrightarrow (a\mid -b) \Leftrightarrow (-a\mid -b)$
If commutative	$(a\mid b) \wedge (b\mid a) \Rightarrow (a = b \vee a = -b)$
Transitivity	$(a\mid b) \wedge (b\mid c) \Rightarrow (a\mid c)$
Constant multiplication	$(a\mid b) \Rightarrow (ac\mid bc)$
	$(ac\mid bc) \wedge (c \neq 0) \Rightarrow (a\mid b)$
Divisor has smaller absolute value	$(a\mid b) \wedge (b \neq 0) \Rightarrow (\lvert a\rvert \le \lvert b\rvert)$

Common Divisors	
d *is a common divisor of* a *and* b *if and only if* $(d\mid a) \wedge (d\mid b)$.	
Properties of Common Divisors	
Divides linear combinations	$d\mid(ax + by)$

Greatest Common Divisor	
The greatest common divisor is denoted as $gcd(a, b)$.	
Euclidean Algorithm 1. Find the quotient and remainder of *a* and *b* and write down an equation in the form $a = qb + r$. 2. Treat *q* and *r* as your new *a* and *b* and repeat step (1). 3. Repeat until you obtain a 0 as your *r*. In the last line, the *q* is your $gcd(a, b)$.	
Properties of the Greatest Common Divisor	
Subtracting a multiple of *b* from *a*	$gcd(a, b) = gcd(b, a - bx)$
	$gcd(a, b) = gcd(b, a \bmod b)$
Divisible by other common divisors	$d \mid gcd(a, b)$

Bezout's Identity
$\exists x, y \in \mathbb{Z}$ *such that* $ax + by = gcd(a, b)$ In fact, $gcd(a, b)$ is the minimum positive integer linear combination of a and b.
Extended Euclidean Algorithm Manipulate the 1st to penultimate equations formed in the Euclidean Algorithm such that you eventually express $gcd(a, b)$ as an integer linear combination of *a* and *b*.

Prime Integers	
Prime	$n \ge 2$ and *n* is not composite.
Composite	There exist positive integers a, b that are strictly between 1 and *n*, such that $n = ab$.
Properties of Prime Integers p and q	
If two prime integers divide each other	If $p \mid q$ then $p = q$.
Set of prime integers	There are infinitely many prime integers.
Greatest common divisor involving a prime	$gcd(p, n) = \begin{cases} p, & if\ p\mid n; \\ 1, & otherwise \end{cases}$
If an integer is divisible by a prime, it must be due to one of the factors.	If $p \mid ab$ then $p \mid a$ or $p \mid b$.
	If $p \mid a_1a_2\cdots a_n$ then $p \mid a_i$ for some *i* between 1 and n.

Fundamental Theorem of Arithmetic	
Every $n \in \mathbb{Z}_{\ge 2}$ can be factorized uniquely up to order into primes. $a = {p_1}^{a_1}{p_2}^{a_2}\cdots{p_k}^{a_k}$ $b = {p_1}^{b_1}{p_2}^{b_2}\cdots{p_k}^{b_k}$	
Things you can do with the Fundamental Theorem	
Comparing constituent primes to check equality	$a = p_1p_2\cdots p_k, b = q_1q_2\cdots q_k$. If $a = b$, then $p_1 = q_1, \cdots, p_k = q_k$.
Comparing exponents to check divisibility	$a\mid b$ if and only if $a_1 \le b_1, a_2 \le b_2, \cdots, a_k \le b_k$.

Constructing $gcd(a, b)$ from the prime factorization	$gcd(a, b) = {p_1}^{min\{a_1,b_1\}}{p_2}^{min\{a_2,b_2\}}\ldots{p_k}^{min\{a_k,b_k\}}$

Coprime Integers	
a and *b* are coprime if, and only if, $gcd(a, b) = 1$	
Properties of Coprime Integers a and b	
Multiplying two coprime integers	If *a* and *c* are coprime, then *a* and *bc* are also coprime, since $(a \nmid b)$ and $(a \nmid c)$.
Coprime integers cannot divide each other	If $a \mid bc$, then $a \mid c$ since $a \nmid b$.
Two integers divided by their gcd are coprime	$gcd(\frac{a}{gcd(a,b)}, \frac{b}{gcd(a,b)}) = 1$

Congruences

Congruences	
$a \equiv b \ (mod\ n)$ if and only if $n \mid (a - b)$.	$a = b + kn$
	$a \bmod n = b \bmod n$
Properties of Congruence Relations	
Reflexive	$a \equiv a \ (mod\ n)$
Symmetric	$a \equiv b \ (mod\ n) \Rightarrow b \equiv a \ (mod\ n)$
Transitive	$[a \equiv b \ (mod\ n)] \wedge [b \equiv c \ (mod\ n)] \Rightarrow [a \equiv c \ (mod\ n)]$
Closure Properties	
Suppose that $a \equiv b \ (mod\ n)$ and $c \equiv d \ (mod\ n)$,	
Addition	$a + c \equiv b + d \ (mod\ n)$
Subtraction	$a - c \equiv b - d \ (mod\ n)$
Multiplication	$ac \equiv bd \ (mod\ n)$
Suppose that $a \equiv b \ (mod\ n)$,	
Addition	$a + c \equiv b + c \ (mod\ n)$
Multiplication	$ac \equiv bc \ (mod\ n)$
Adding a "*mod n*" anyhowly and somehow they still congruent	
$a \pm b \equiv (a \bmod n) \pm b \equiv a \pm (b \bmod n) \equiv (a \bmod n) \pm (b \bmod n) \ (mod\ n)$	$ab \equiv (a \bmod n)b \equiv a(b mod n) \equiv (a \bmod n)(b \bmod n) \ (mod\ n)$
Other Properties	
Eliminating a factor	If $ac \equiv bc \ (mod\ n)$, if you want to eliminate the *c*, then $a \equiv b \ (mod\ \frac{n}{gcd(c,n)})$.

Congruence Equations	
$ax \equiv b \ (mod\ n)$	
Properties of Congruence Equations	
Checking if there is a solution	$x \in \mathbb{Z}$ exists to satisfy the above equation if, and only if, $gcd(a, n) \mid b$.
Dividing throughout by $gcd(a, n)$	$\frac{a}{gcd(a,n)}x \equiv \frac{b}{gcd(a,n)} \ (mod\ \frac{n}{gcd(a,n)})$

Multiplicative Inverse Modulo n	
x is a multiplicative inverse of $a \bmod n$ if, and only if, $ax \equiv 1 \ (mod\ n)$	
Properties of multiplicative inverse modulo n	
Given a congruence equation $ax \equiv b \ (mod\ n)$, let a' be the multiplicative inverse modulo *n*.	
Checking if there is a solution	a' exists if, and only if, $gcd(a, n) = 1$.
Multiplying throughout by a'	$x \equiv a'b \ (mod\ n)$
Dividing throughout by $gcd(a, n)$	$x \equiv a'\frac{b}{gcd(a,n)} \ (mod\ \frac{n}{gcd(a,n)})$
Finding other multiplicative inverses modulo n	
x is a multiplicative inverse of $a \bmod n$ if, and only if, $x \equiv a' \ (mod\ n)$.	
Finding the Multiplicative Inverse Modulo n	
Since $gcd(a, n) = 1$, make use of the Extended Euclidean Algorithm to obtain integers x and y such that $ax + ny = 1$, and x will be the multiplicative inverse of a modulo n.	