CS1231 Cheatsheet

for midterms, by ning

Appendix A of Epp is not covered. Theorems, corollaries, lemmas, etc. not mentioned in the lecture notes are marked with an asterisk (*).

Proofs

Basic Notation

- $\mathbb{R}$: the set of all real numbers
- $\mathbb{Z}$: the set of integers (includes 0)
- $\mathbb{Q}$: the set of rationals
- $\exists$: there exists...
- $\exists!$: there exists a unique...
- $\forall$: for all...
- $\in$: member of...
- $\ni$: such that...

Proof Types

- **By Construction**: finding or giving a set of directions to reach the statement to be proven true.
- **By Contraposition**: proving a statement through its logical equivalent contrapositive.
- **By Contradiction**: proving that the negation of the statement leads to a logical contradiction.
- **By Exhaustion**: considering each case.
- **By Mathematical Induction**: proving for a base case, then an induction step.

Order of Operations

First $\sim$ (also represented as $\neg$). No priority within $\wedge$ and $\vee$, so $p \wedge q \vee r$ is ambiguous and should be written as $(p \wedge q) \vee r$ or $p \wedge (q \vee r)$. The implication, $\rightarrow$ is performed last. Can be overwritten by parenthesis.

Universal & Existential Generalisation

'All boys wear glasses' is written as

$$\forall x(\text{Boy}(x) \rightarrow \text{Glasses}(x))$$

If conjunction was used, this statement would be falsified by the existence of a 'non-boy' in the domain of x.

'There is a boy who wears glasses' is written as

$$\exists x(\text{Boy}(x) \wedge \text{Glasses}(x))$$

If implication was used, this statement would true even if the domain of x is empty.

Valid Arguments as Tautologies

All valid arguments can be *restated* as tautologies.

Rules of Inference

Modus ponens

$$p \rightarrow q$$
$$p$$
$$\therefore q$$

Modus tollens

$$p \rightarrow q$$
$$\neg q$$
$$\therefore \neg p$$

Generalization

$$p$$
$$\therefore p \vee q$$

Specialization

$$p \wedge q$$
$$\therefore p$$

Elimination

$$p \vee q$$
$$\neg q$$
$$\therefore p$$

Transitivity

$$p \rightarrow q$$
$$q \rightarrow r$$
$$\therefore p \rightarrow r$$

Proof by Division into Cases

$$p \vee q$$
$$p \rightarrow r$$
$$q \rightarrow r$$
$$\therefore r$$

Contradiction Rule

$$\neg p \rightarrow \mathbf{c}$$
$$\therefore p$$

Universal Rules of Inference

Only modus ponens, modus tollens, and transitivity have universal versions in the lecture notes.

Implicit Quantification

The notation $P(x) \implies Q(x)$ means that every element in the truth set of $P(x)$ is in the truth set of $Q(x)$, or equivalently, $\forall x, P(x) \rightarrow Q(x)$.

The notation $P(x) \iff Q(x)$ means that $P(x)$ and $Q(x)$ have identical truth sets, or equivalently, $\forall x, P(x) \leftrightarrow Q(x)$.

Implication Law

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

Universal Instantiation

If some property is true of everything in a set, then it is true of any particular thing in the set.

Universal Generalization

If $P(c)$ must be true, and we have assumed nothing about c, then $\forall x, P(x)$ is true.

Regular Induction

$$P(0)$$
$$\forall k \in \mathbb{N}, P(k) \rightarrow P(k+1)$$
$$\forall$$

Epp T2.1.1 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

$$p \wedge \mathbf{t} \equiv p$$
$$p \vee \mathbf{c} \equiv p$$

Negation Laws

$$p \vee \neg p \equiv \mathbf{t}$$
$$p \wedge \neg p \equiv \mathbf{c}$$

Double Negative Law

$$\neg(\neg p) \equiv p$$

Idempotent Laws

$$p \wedge p \equiv p$$
$$p \vee p \equiv p$$

Universal Bound Laws

$$p \vee \mathbf{t} \equiv \mathbf{t}$$
$$p \wedge \mathbf{c} \equiv \mathbf{c}$$

De Morgan's Laws

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

Absorption Laws

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

Negations of $\mathbf{t}$ and $\mathbf{c}$

$$\neg \mathbf{t} \equiv \mathbf{c}$$
$$\neg \mathbf{c} \equiv \mathbf{t}$$

Definition 2.2.1 (Conditional)

If p and q are statement variables, the conditional of q by p is "if p then q" or "p implies q", denoted $p \rightarrow q$. It is false when p is true and q is false; otherwise it is true. We call p the *hypothesis* (or *antecedent*), and q the *conclusion* (or *consequent*).

A conditional statement that is true because its hypothesis is false is called *vacuously true* or *true by default.*

Definition 2.2.2 (Contrapositive)

The contrapositive of $p \rightarrow q$ is $\neg q \rightarrow \neg p$.

Definition 2.2.3 (Converse)

The converse of $p \rightarrow q$ is $q \rightarrow p$.

Definition 2.2.4 (Inverse)

The inverse of $p \rightarrow q$ is $\neg p \rightarrow \neg q$.

Definition 2.2.6 (Biconditional)

The biconditional of p and q is denoted $p \leftrightarrow q$ and is true if both p and q have the same truth values, and is false if p and q have opposite truth values.

Definition 2.2.7 (Necessary & Sufficient)

"r is sufficient for s" means $r \rightarrow s$, "r is necessary for s" means $\neg r \rightarrow \neg s$ or equivalently $s \rightarrow r$.

Definition 2.3.2 (Sound & Unsound Arguments)

An argument is called *sound*, iff it is valid and all its premises are true.

Definition 3.1.3 (Universal Statement)

A *universal statement* is of the form

$$\forall x \in D, Q(x)$$

It is defined to be true iff $Q(x)$ is true for every x in D. It is defined to be false iff $Q(x)$ is false for at least one x in D.

Definition 3.1.4 (Existential Statement)

A *existential statement* is of the form

$$\exists x \in D \text{ s.t. } Q(x)$$

It is defined to be true iff $Q(x)$ is true for at least one x in D. It is defined to be false iff $Q(x)$ is false for all x in D.

Theorem 3.2.1 (Negation of Universal State.)

The negation of a statement of the form

$$\forall x \in D, P(x)$$

is logically equivalent to a statement of the form

$$\exists x \in D \text{ s.t. } \neg P(x)$$

Theorem 3.2.2 (Negation of Existential State.)

The negation of a statement of the form

$$\exists x \in D \text{ s.t. } P(x)$$

is logically equivalent to a statement of the form

$$\forall x \in D, \neg P(x)$$

Number Theory

Representation of Integers

Given any positive integer n and base b, repeatedly apply the Quotient-Remainder Theorem to get,

$$\begin{aligned} n &= bq_0 + r_0 \\ q_0 &= bq_1 + r_1 \\ q_1 &= bq_2 + r_2 \\ &\cdots \\ q_{m-1} &= bq_m + r_m \end{aligned}$$

The process stops when $q_m = 0$. Eliminating the quotients q_i we get,

$$n = r_m b^m + r_{m-1} b^{m-1} + \cdots r_1 b + r_0$$

Which may be represented compactly in base b as a sequence of the digits r_i,

$$n = (r_m r_{m-1} \cdots r_1 r_0)_b$$

Properties (of Numbers)
Closure, i.e.

$$\forall x, y \in \mathbb{Z},\ x + y \in \mathbb{Z},\ \text{and } xy \in \mathbb{Z}$$

Commutativity, i.e.

$$a + b = b + a \text{ and } ab = ba$$

Distributivity, i.e.

$$a(b + c) = ab + ac \text{ and } (b + c)a = ba + ca$$

Trichotomy, i.e.

$$(a < b) \oplus (b < a) \oplus (a = b)$$

(Can be used without proof)

Definition 1.1.1 (Colorful)
An integer n is said to be colorful if there exists some integer k such that $n = 3k$.

Definition 1.3.1 (Divisibility)
If n and d are integers and $d \neq 0$,

$$d|n \iff \exists k \in \mathbb{Z} \text{ s.t. } n = dk$$

Proposition 1.3.2 (Linear Combination)

$$\forall a, b, c \in \mathbb{Z},\ a|b \wedge a|c \rightarrow \forall x, y \in \mathbb{Z},\ a|(bx + cy)$$

If a divides b and c, then it also divides their linear combination $(bx + cy)$.

Theorem 4.1.1 (Linear Combination)

$$\forall a, b, c \in \mathbb{Z},\ a|b \wedge a|c \rightarrow \forall x, y \in \mathbb{Z}, a|(bx + cy)$$

Epp T4.3.3 (Transitivity of Divisibility)

$$\forall a, b, c \in \mathbb{Z},\ a|b \wedge b|c \rightarrow a|c$$

Theorem 4.4.1 (Quotient-Remainder Theorem)
Given any integer a and any positive integer b, there exist unique integers q and r such that

$$a = bq + r \text{ and } 0 \leq r < b$$

Definition 4.2.1 (Prime number)

$$\begin{aligned} n \text{ is prime } &\iff \forall r, s \in \mathbb{Z}^+ \\ &\quad\ n = rs \rightarrow \\ &\quad\ (r = 1 \wedge s = n) \vee (r = n \wedge s = 1) \\ n \text{ is composite } &\iff \exists r, s \in \mathbb{Z}^+ \text{ s.t.} \\ &\quad\ n = rs \wedge \\ &\quad\ (1 < r < n) \wedge (1 < s < n) \end{aligned}$$

Proposition 4.2.2
For any two primes p and p',

$$p \mid p' \rightarrow p = p'$$

Theorem 4.2.3
If p is a prime and $x_1, x_2, \cdots, x_n$ are any integers s.t. $p \mid x_1 x_2 \cdots x_n$, then $p \mid x_i$ for some $x_i, i \in \{1, 2, \cdots, n\}$.

Epp T4.3.5 (Unique Prime Factorisation)
Given any integer $n > 1$

$$\begin{gathered} \exists k \in \mathbb{Z}^+, \\ \exists p_1, p_2, \cdots, p_k \in \text{ primes}, \\ \exists e_1, e_2, \cdots, e_k \in \mathbb{Z}^+, \end{gathered}$$

such that

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

and any other expression for n as a product of prime numbers is identical, except perhaps for the order in which the factors are written.

Epp Proposition 4.7.3
For any $a \in \mathbb{Z}$ and any prime p,

$$p \mid a \rightarrow p \nmid (a + 1)$$

Epp T4.7.4 (Infinitude of Primes)
The set of primes is infinite.

Definition 4.3.1 (Lower Bound)
An integer b is said to be a *lower bound* for a set $X \subseteq \mathbb{Z}$ if $b \leq x$ for all $x \in X$.

Does not require b to be in X.

Theorem 4.3.2 (Well Ordering Principle)
If a non-empty set $S \subseteq \mathbb{Z}$ has a lower bound, then S has a least element.

Note three conditions: $|S| > 0$, $S \subseteq \mathbb{Z}$, and S has lower bound.

Likewise, if ... upper bound ... has a greatest element.

Proposition 4.3.3 (Uniqueness of least element)
If a set S has a least element, then the least element is unique.

Proposition 4.3.4 (Uniqueness of greatest e.)
If a set S has a greatest element, then the greatest element is unique.

Theorem 4.4.1 (Quotient-Remainder Theorem)
Given any integer a and any positive integer b, there exist unique integers q and r such that

$$a = bq + r \text{ and } 0 \leq r < b$$

Definition 4.5.1 (Greatest Common Divisor)
Let a and b be integers, not both zero. The *greatest common divisor* of a and b, denoted $\gcd(a, b)$, is the integer d satisfying

1. $d \mid a$ and $d \mid b$
2. $\forall c \in \mathbb{Z}\ ((c \mid a)\ \wedge (c \mid b) \rightarrow c \leq d)$

Proposition 4.5.2 (Existence of gcd)
For any integers a, b, not both zero, their gcd exists and is unique.

Theorem 4.5.3 (Bézout's Identity)
Let a, b be integers, not both zero, and let $d = \gcd(a, b)$. Then there exists integers x, y such that

$$ax + by = d$$

Or, the gcd of two integers is some linear combination of the said numbers, where x, y above have multiple solution pairs once a solution pair (x, y) is found. Also solutions, for any integer k,

$$(x + \frac{kb}{d}, y - \frac{ka}{d})$$

***Epp T8.4.8 (Euclid's Lemma)**
For all $a, b, c \in \mathbb{Z}$, if $\gcd(a, c) = 1$ and $a \mid bc$, then $a \mid b$.

***Epp Lemma 4.8.2**
If $a, b \in \mathbb{Z}^+$, and $q, r \in \mathbb{Z}$ s.t. $a = bq + r$, then

$$\gcd(a, b) = \gcd(b, r)$$

Definition 4.5.4 (Relatively Prime)
Integers a and b are *relatively prime* (or *coprime*) iff $\gcd(a, b) = 1$.

Proposition 4.5.5
For any integers a, b, not both zero, if c is a common divisor of a and b, then $c \mid \gcd(a, b)$.

Definitoin 4.7.1 (Congruence modulo)
Let $m, z \in \mathbb{Z}$ and $d \in \mathbb{Z}^+$. We say that m is *congruent* to n *modulo* d and write

$$m \equiv n \pmod{d}$$

iff

$$d \mid (m - n)$$

More concisely,

$$m \equiv n \pmod{d} \iff d \mid (m - n)$$

Epp T8.4.1 (Modular Equivalences)
Let $a, b, n \in \mathbb{Z}$ and $n > 1$. The following statements are all equivalent,

1. $n \mid (a - b)$
2. $a \equiv b \pmod{n}$
3. $a = b + kn$ for some $k \in \mathbb{Z}$
4. a and b have the same non-negative remainder when divided by n
5. $a \bmod n = b \bmod n$

Epp T8.4.3 (Modulo Arithmetic)
Let $a, b, c, d, n \in \mathbb{Z}$, $n > 1$, and suppose

$$a \equiv c \pmod{n} \text{ and } b \equiv d \pmod{n}$$

Then

1. $(a + b) \equiv (c + d) \pmod{n}$
2. $(a - b) \equiv (c - d) \pmod{n}$
3. $ab \equiv cd \pmod{n}$
4. $a^m \equiv c^m \pmod{n}$, for all $m \in \mathbb{Z}^+$

Epp Corollary 8.4.4
Let $a, b, c, d, n \in \mathbb{Z}$, $n > 1$, then

$$ab \equiv [(a \bmod n)(b \bmod n)] \pmod{n}$$

or equivalently,

$$ab \bmod n = [(a \bmod n)(b \bmod n)] \bmod n$$

In particular, if m is a positive integer, then

$$a^m \equiv [(a \bmod n)^m] \pmod{n}$$

Definition 4.7.2 (Multiplicative inv. modulo n)
For any integers a, n with $n > 1$, if an integer s is such that $as \equiv 1 \pmod{n}$, then s is the *multiplicative inverse of a modulo n*. We may write s as a^{-1}.

Because the commutative law still applies in modulo arithmetic, we also have

$$a^{-1} a \equiv 1 \pmod{n}$$

Multiplicative inverses are not unique. If s is an inverse, then so is $(s + kn)$ for any integer k.

Theorem 4.6.3 (Existence of multiplicative inverse)
For any integer a, its multiplicative inverse modulo n where $n > 1$, a^{-1}, exists iff a and n are coprime.

Corollary 4.7.4 (Special case: n is prime)
If $n = p$ is a prime number, then all integers a in the range $0 < a < p$ have multiplicative inverses modulo p.

Epp T8.4.9 (Cancellation Law for mod. arith.)
For all $a, b, c, n \in \mathbb{Z}$, $n > 1$, and a and n are coprime,

$$ab \equiv ac \pmod{n} \rightarrow b \equiv c \pmod{n}$$