# CS1231(S) Cheatsheet

for Mid-term of AY 19/20 Semester 1, by Howard Liu

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
- $\mathbb{N}$: the set of natural numbers (include 0, i.e. $\mathbb{Z}_{\geq 0}$)
- $\mathbb{Q}$: the set of rationals
- $\exists$: there exists...
- $\exists!$: there exists a unique...
- $\forall$: for all...
- $\in$: member of...
- $\ni$: such that...
- $\sim$: not ...

### 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.
  1. $P(a)$
  2. $\forall k \in \mathbb{Z}, k \geq a\ (P(k) \to P(k+1))$
  3. $\cdot \forall n \in \mathbb{Z}, n \geq a\ (P(n))$
- **By Strong Induction**: mathematical induction assuming $P(k), P(k-1), \cdots, P(a)$ are all true.
- **By Structural Induction**: MI assuming $P(x)$ is true, prove $P(f(x))$ is true ($f(x)$ is the recursion set rule, i.e. if $x \in S, f(x) \in S$)

### Order of Operations

In the ascending order (1 executes first, 3 is the latest, can be overwritten by parenthesis)

1. **Negation**: $\sim$ (also represented as $\neg$)
2. **Logic AND & OR**: $\wedge$ and $\vee$
3. **Implication**: $\to$

### Universal & Existential Generalisation

*'All boys wear glasses'* is written as

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

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

$$p \to q$$
$$p$$
$$\cdot\ q$$

Modus tollens

$$p \to q$$
$$\sim q$$
$$\cdot\ \sim p$$

Generalization

$$p$$
$$\cdot\ p \vee q$$

Specialization

$$p \wedge q$$
$$\cdot\ p$$

Elimination

$$p \vee q$$
$$\sim q$$
$$\cdot\ p$$

Transitivity

$$p \to q$$
$$q \to r$$
$$\cdot\ p \to r$$

Proof by Division into Cases

$$p \vee q$$
$$p \to r$$
$$q \to r$$
$$\cdot\ r$$

Contradiction Rule

$$\sim p \to \textbf{c(ontradiction)}$$
$$\cdot\ p$$

### 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, $\forall x, P(x) \to Q(x)$.

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

$$p \to q \equiv \sim p \vee q$$

### 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

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

### 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

$$p \wedge \textbf{true} \equiv p$$
$$p \vee \textbf{false} \equiv p$$

Negation Laws

$$p \vee \sim p \equiv \textbf{true}$$
$$p \wedge \sim p \equiv \textbf{false}$$

Double Negative Law

$$\sim(\sim p) \equiv p$$

Idempotent Laws

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

Universal Bound Laws

$$p \vee \textbf{true} \equiv \textbf{true}$$
$$p \wedge \textbf{false} \equiv \textbf{false}$$

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

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

Negations of **true** and **false**

$$\sim \textbf{true} \equiv \textbf{false}$$
$$\sim \textbf{false} \equiv \textbf{true}$$

### 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 $p \to q$. 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 $p \to q$ is $\sim q \to \sim p$. Note: one will always be equivalent to the other.

### Definition 2.2.3 (Converse)

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

### Definition 2.2.4 (Inverse)

The inverse of $p \to q$ is $\sim p \to \sim q$.

### 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 $r \to s$, "$r$ is necessary for $s$" means $\sim r \to \sim s$ or equivalently $s \to r$.

### Definition 2.3.2 (Sound & Unsound Arguments)

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

### Definition 3.1.2 (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 3.1.3 (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 3.1.6 (Equivalent Forms of Universal and Existential State.)

By narrowing $\mathcal{U}$ to be the domain $D$ consisting of all values of the variable $x$ that makes $P(x)$ **true**,

$$\forall_{x \in \mathcal{U}}, P(x) \implies Q(x) \equiv \forall_{x \in D}, Q(x)$$

Similarly,

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

### 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

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

### 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

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

Note: for negation of $\exists!$, consider

$\exists! x$ s.t. $P(x) \equiv \exists x$ s.t. $(P(x) \wedge (\forall_{y \in \mathcal{U}} P(y) \to (y = x))$

**Theorem 3.2.4 (Vacuous Truth of Universal State.)**
In general, a statement of the form

$$\forall_{x \in D}, P(x) \to Q(x)$$

is called **vacuously true/true by default** iff $P(x)$ is **false** for every $x$ in $D$

## Sets

**Definition 6.1.1 (Subsets & Supersets)**
$S$ is a subset of $T$ if all the elements of $S$ are elements of $T$, denoted $S \subseteq T$. Formally,

$$S \subseteq T \longleftrightarrow \forall x \in S(x \in T)$$

**Definition 6.2.1 (Empty Set)**
An empty set has no element, and is denoted $\varnothing$ or $\{\}$. Formally, where $\mathcal{U}$ is the universal set:

$$\forall Y \in \mathcal{U}(Y \notin \varnothing)$$

**Epp T6.24**
An empty set is a subset of all sets.

$$\forall S,\ S \text{ is a set, } \varnothing \subseteq S$$

**Definition 6.2.2 (Set Equality)**
Two sets are equal iff they have the same elements.

**Proposition 6.2.3**
For any two sets $X, Y$, $X$ and $Y$ are subsets of each other iff $X = Y$. Formally,

$$\forall X, Y((X \subseteq Y \wedge Y \subseteq X) \longleftrightarrow X = Y)$$

**Epp C6.2.5 (Empty Set is Unique)**
It's what it says.

**Definition 6.2.4 (Power Set)**
The power set of a set $S$ denoted $\mathcal{P}(S)$, or $2^S$; is the set whose elements are all possible subsets of $S$. Formally,

$$\mathcal{P}(S) = \{X \mid X \subseteq S\}$$

**Theorem 6.3.1**
If a set $X$ has $n$ elements, $n \geq 0$, then $\mathcal{P}(X)$ has $2^n$ elements.

**Definition 6.3.1 (Union)**
Let $S$ be a set of sets. $T$ is the union of sets in $S$, iff each element of $T$ belongs to some set in $S$. Formally,

$$T = \bigcup S = \bigcup_{X \in S} X = \{y \in \mathcal{U} \mid \exists X \in S(y \in X)\}$$

**Definition 6.3.3 (Intersection)**
Let $S$ be a non-empty set of sets. $T$ is the intersection of sets in $S$, iff each element of $T$ also belongs to all the sets in $S$. Formally,

$$T = \bigcap S = \bigcap_{X \in S} X$$
$$= \{y \in \mathcal{U} \mid \forall X((X \in S) \to (y \in X))\}$$

**Definition 6.3.5 (Disjoint)**
Let $S, T$ be sets. $S$ and $T$ are disjoint iff $S \cap T = \varnothing$.

**Definition 6.3.6 (Mutually Disjoint)**
Let $V$ be a set of sets. The sets $T \in V$ are mutually disjoint iff every two distinct sets are disjoint. Formally,

$$\forall X, Y \in V(X \neq Y \to X \cap Y = \varnothing)$$

**Definition 6.3.7 (Partition)**
Let $S$ be a set, and $V$ a set of non-empty subsets of $S$. Then $V$ is a partition of $S$ iff

1. The sets in $V$ are mutually disjoint
2. The union of sets in $V$ equals $S$

**Definition 6.3.8 (Non-symmetric Difference)**
Let $S, T$ be two sets. The (non-symmetric) difference of $S$ and $T$ denoted $S - T$ or $S \setminus T$ is the set whose elements belong to $S$ and do not belong to $T$. Formally,

$$S - T = \{y \in \mathcal{U} \mid y \in S \wedge y \notin T\}$$

This is analogous to subtraction for numbers.

**Definition 6.3.10 (Set Complement)**
Let $A \subseteq \mathcal{U}$. Then, the complement of A denoted $\overline{A}$ is $\mathcal{U} - A$.

**Set Properties**
Let $A, B, C$ be sets, some properties are:

- $\bigcup \varnothing = \bigcup_{A \in \varnothing} A = \varnothing$
- $\bigcup\{A\} = A$
- **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**: $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$, $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
- **Identity Laws**: $A \cup \varnothing = A$, $A \cap \mathcal{U} = A$
- **Complement Laws**: $A \cup \overline{A} = \mathcal{U}$, $A \cap \overline{A} = \varnothing$
- **Double Complement Law**: $\overline{(\overline{A})} = A$
- **Idempotent Laws**: $A \cup A = A$, $A \cap A = A$
- **Universal Bound Laws**: $A \cup \mathcal{U} = \mathcal{U}$, $A \cap \varnothing = \varnothing$
- **De Morgan's Laws**: $\overline{A \cup B} = \overline{A} \cap \overline{B}$, $\overline{A \cap B} = \overline{A} \cup \overline{B}$
- **Adsorption Laws**: $A \cup (A \cap B) = A$, $A \cap (A \cup B) = A$
- **Set Difference Law**: $A - B = A \cap \overline{B}$
- $\overline{\mathcal{U}} = \varnothing$, $\overline{\varnothing} = \mathcal{U}$
- $A \subseteq B \leftrightarrow A \cup B = B \leftrightarrow A \cap B = A$

## Functions

**Definition 7.1.1 (Function)**
Let $f$ be a relation such that $f \subseteq S \times T$. Then $f$ is a function from $S$ to $T$ denoted $f : S \to T$ iff

$$\forall x \in S, \exists! y \in T(x\ f\ y)$$

(Intuitively, this means that every element in $S$ must have exactly one 'outgoing arrow', **AND** the 'arrow' must land in $T$.)

**Definitions 7.1.[2-5]**
Let $f : S \to T$ be a function, $x \in S$ and $y \in T$ such that $f(x) = y$; $U \subseteq S$, and $V \subseteq T$.

$x$ is a pre-image (7.1.2) of $y$.

The inverse image of the element (7.1.3) $y$ is the set of all its pre-images, i.e. $\{x \in S \mid f(x) = y\}$.

The inverse image of the set (7.1.4) $V$ is the set that contains all the pre-images of all the elements of $V$, i.e. $\{x \in S \mid \exists y \in V(f(x) = y)\}$.

The restriction (7.1.5) of $f$ to $U$ is the set $\{(x, y) \in U \times T \mid f(x) = y\}$.

**Definition 7.2.1 (Injective, or One-to-one)**
Let $f : S \to T$ be a function. $f$ is injective (or one-to-one) iff

$$\forall y \in T, \forall x_1, x_2 \in S((f(x_1) = y \wedge f(x_2) = y) \to x_1 = x_2)$$

(Intuitively, this means that every element in $T$ has **at most** one 'incoming arrow'.)

**Definition 7.2.2 (Surjective, or Onto)**
Let $f : S \to T$ be a function. $f$ is surjective (or onto) iff

$$\forall y \in T, \exists x \in S(f(x) = y)$$

(Intuitively, this means that every element in $T$ has **at least** one 'incoming arrow'.)

**Definition 7.2.3 (Bijective)**
A function is bijective (or is a bijection) iff it is injective and subjective.
(Intuitively, this means that every element in $T$ has exactly one incoming arrow.)

**Definition 7.2.4 (Inverse)**
Let $f : S \to T$ be a function and let $f^{-1}$ be the inverse relation of $f$ from $T$ to $S$. Then $f$ is bijective iff $f^{-1}$ is a function.
(Note: $f^{-1}$ is defined but not necessary a function. When $A \subseteq T$, $f^{-1}(A)$ means finding all the preimages of each image in $A$, and this is not a function if the $f$ is not bijective.)

**Definition 7.3.1 (Composition)**
Let $f : S \to T$, $g : T \to U$ be functions. The composition of $f$ and $g$ denoted $g \circ f$ is a function from $S$ to $U$.

**Definition 7.3.2 (Identity)**
The identity function on a set $A$, $\mathcal{I}_A$ is defined by,

$$\forall x \in A(\mathcal{I}_A(x) = x)$$

**Proposition 7.3.3**
Let $f : A \to A$ be an injective function of A. Then $f^{-1} \circ f = \mathcal{I}_A$.

**Inclusive Map**
Let $B$ be a subset of A. Then function $\iota_B^A : B \to A; b \mapsto b$ is called the **inclusive map** of $B$ in $A$
**Equality of Functions** Two functions $f$ and $g$ are **equal**, denoted $f = g$, iff:

- the domains of $f$ and $g$ are equal;
- the codomains of $f$ and $g$ are equal;
- $f(x) = g(x)$ for all $x$ in their domains

**Properties of Composite Functions**
Let $f : A \to B, g : B \to C$ and $h : C \to D$ to be functions. Then

- $h \circ (g \circ f) = (h \circ g) \circ f$
- If $f$ and $g$ are injective, $g \circ f$ is injective.
- If $f$ and $g$ are surjective, $g \circ f$ is surjective.
- If $g \circ f$ is injective, then $f$ is injective.
- If $g \circ f$ is surjective, then $g$ is surjective.

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