CSCE 222
Discrete Structures for Computing

Review for Exam 1

Dr. Hyunyoung Lee
Topics

- Propositional Logic (Sections 1.1, 1.2 and 1.3)
- Predicate Logic (Sections 1.4 and 1.5)
- Rules of Inferences and Proofs (Sections 1.6, 1.7 and 1.8)
- Sets (Sections 2.1, 2.2, and 2.5)
- Functions (Section 2.3)
- Asymptotic Notations (Section 3.2)
Strategy for Exam Preparation

- Start studying now (unless have already started)!
- Study class notes and make sure you know your definitions!
- Review your quizzes and in-class exercises
- Review your homework
- Study the examples in the textbook
- Do odd numbered exercises in the textbook
Logical Connectives - Summary

Let $B=\{t,f\}$. Assign to each connective a function $M: B \rightarrow B$ that determines its semantics.

<table>
<thead>
<tr>
<th>$P$</th>
<th>$M_\land(P)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$f$</td>
<td>$t$</td>
</tr>
<tr>
<td>$t$</td>
<td>$f$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$P$</th>
<th>$Q$</th>
<th>$M_\land(P, Q)$</th>
<th>$M_\lor(P, Q)$</th>
<th>$M_\oplus(P, Q)$</th>
<th>$M_\rightarrow(P, Q)$</th>
<th>$M_\leftrightarrow(P, Q)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$f$</td>
<td>$f$</td>
<td>$f$</td>
<td>$f$</td>
<td>$f$</td>
<td>$t$</td>
<td>$t$</td>
</tr>
<tr>
<td>$f$</td>
<td>$t$</td>
<td>$f$</td>
<td>$t$</td>
<td>$t$</td>
<td>$t$</td>
<td>$f$</td>
</tr>
<tr>
<td>$t$</td>
<td>$f$</td>
<td>$f$</td>
<td>$t$</td>
<td>$t$</td>
<td>$f$</td>
<td>$f$</td>
</tr>
<tr>
<td>$t$</td>
<td>$t$</td>
<td>$t$</td>
<td>$t$</td>
<td>$f$</td>
<td>$t$</td>
<td>$t$</td>
</tr>
</tbody>
</table>
Informally, we can summarize the meaning of the connectives in words as follows:

1. The **and** connective $(a \land b)$ is true if and only if both $a$ and $b$ are true.

2. The **or** connective $(a \lor b)$ is true if and only if at least one of $a$, $b$ is true.

3. The **exclusive or** $(a \oplus b)$ is true if and only if precisely one of $a$, $b$ is true.

4. The **implication** $(a \rightarrow b)$ is false if and only if the premise $a$ is true and the conclusion $b$ is false.

5. The **biconditional** $(a \leftrightarrow b)$ is true if and only if the truth values of $a$ and $b$ are the same.
Conditional

Perhaps the most important logical connective is the conditional, also known as implication:

\[ p \rightarrow q \]

The statement asserts that \( q \) holds on the condition that \( p \) holds. We call \( p \) the hypothesis or premise, and \( q \) the conclusion or consequence. Typical usage in proofs:

“If \( p \), then \( q \”; “p implies \( q \”; “q only if \( p \”; “q when \( p \”; “q follows from \( p \”

“p is sufficient for \( q \”; “a sufficient condition for \( q \) is \( p \”; “a necessary condition for \( p \) is \( q \”; “q is necessary for \( p \”
Logical Equivalence
of propositions

Two propositions $p$ and $q$ are called logically equivalent if and only if $v[[p]] = v[[q]]$ holds for all valuations $v$ on Prop.

In other words, two propositions $p$ and $q$ are logically equivalent if and only if $p \leftrightarrow q$ is a tautology.

We write $p \equiv q$ if and only if $p$ and $q$ are logically equivalent.

We have shown that $(\neg p \lor q) \equiv (p \rightarrow q)$. In general, we can use truth tables or logical derivations to establish logical equivalences.
A proposition $p$ is called a **tautology** if and only if $v[[p]] = t$ holds for all valuations $v$ on Prop.

In other words, $p$ is a tautology if and only if in a truth table it always evaluates to true regardless of the assignment of truth values to its variables.

**Example:**

<table>
<thead>
<tr>
<th>$p$</th>
<th>$\neg p$</th>
<th>$p \lor \neg p$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$F$</td>
<td>$T$</td>
<td>$T$</td>
</tr>
<tr>
<td>$T$</td>
<td>$F$</td>
<td>$T$</td>
</tr>
</tbody>
</table>
A function $P$ from a set $D$ to the set $\text{Prop}$ of propositions is called a \textit{predicate}. The set $D$ is called the domain of $P$.

For example,

$E: \mathbb{Z} \rightarrow \{t,f\}$ with $E(x)=x$ is an even integer; $E(6)$ is true.

$O: \mathbb{Z} \rightarrow \{t,f\}$ with $O(x)=x$ is an odd integer; $O(6)$ is false.
Universal Quantifier

Let $P$ be a predicate with domain $D$.

The statement “$P(x)$ holds true for all $x$ in $D$” can be written shortly as $\forall x P(x)$.

Suppose that $P(x)$ is a predicate over a finite domain, say $D=\{1,2,3\}$. Then $\forall x P(x)$ is equivalent to $P(1) \land P(2) \land P(3)$.

Put differently, $\forall x P(x)$ is false if and only if $P(x)$ is false for some $x$ in $D$. 
Existential Quantifier

The statement \( P(x) \) holds for some \( x \) in the domain \( D \) can be written as \( \exists x \ P(x) \)

Example: \( \exists x \ (x>0 \land x^2 = 2) \)

is true if the domain is the real numbers
but false if the domain is the rational numbers.
Logical Equivalence
- involving quantifiers and predicates

Two statements involving quantifiers and predicates are **logically equivalent** if and only if they have the same truth values no matter which predicates are substituted into these statements and which domain is used.

We write $A \equiv B$ for logically equivalent $A$ and $B$.

You use logical equivalences to derive more convenient forms statements.

Example: De Morgan’s laws.
De Morgan’s Laws

\[ \neg \forall x P(x) \equiv \exists x \neg P(x) \]

\[ \neg \exists x P(x) \equiv \forall x \neg P(x) \]

\[ \neg (p \land q) \equiv \neg p \lor \neg q \]

\[ \neg (p \lor q) \equiv \neg p \land \neg q \]
Valid Arguments

An argument in propositional logic is a sequence of propositions that end with a proposition called conclusion. The argument is called valid if the conclusion follows from the preceding statements (called premises).

In other words, in a valid argument it is impossible that all premises are true but the conclusion is false.
Modus Ponens

The tautology \((p \land (p \rightarrow q)) \rightarrow q\) is the basis for the rule of inference called “modus ponens”.

\[
\begin{align*}
\text{p} \\
\text{p} \rightarrow \text{q} \\
\hline
\therefore \quad \text{q}
\end{align*}
\]
Modus Tollens

\[-q, p \rightarrow q\]

\[\therefore \neg p\]

"The University will not close on Wednesday."

"If it snows on Wednesday, then the University will close."

Therefore, "It will not snow on Wednesday"
Simplification

\[ p \land q \]

\[ \rightarrow \]

\[ p \]
Example Formal Argument

\[
\neg p \land q \\
r \rightarrow p \\
\neg r \rightarrow s \\
s \rightarrow t
\]

\[
\begin{align*}
1) & \quad \neg p \land q & \text{Hypothesis} \\
2) & \quad \neg p & \text{Simplification of 1)} \\
3) & \quad r \rightarrow p & \text{Hypothesis} \\
4) & \quad \neg r & \text{Modus tollens using 2) and 3)} \\
5) & \quad \neg r \rightarrow s & \text{Hypothesis} \\
6) & \quad s & \text{Modus ponens using 4) and 5)} \\
7) & \quad s \rightarrow t & \text{Hypothesis} \\
8) & \quad t & \text{Modus ponens using 6) and 7)}
\end{align*}
\]
Proofs

Review carefully the two styles of proof:

- Direct proof

- Proof by contradiction

In addition, we discussed some variations of these basic styles of proofs such as proof by contrapositive which is a variation of direct proof. Review them also.
Sets and Functions
The set builder notation describes all elements as a subset of a set having a certain property.

\[ Q = \{ \frac{p}{q} \in \mathbb{R} \mid p \in \mathbb{Z}, q \in \mathbb{Z}, \text{ and } q \neq 0 \} \]

\[ [a,b] = \{ x \in \mathbb{R} \mid a \leq x \leq b \} \]

\[ [a,b) = \{ x \in \mathbb{R} \mid a \leq x < b \} \]

\[ (a,b] = \{ x \in \mathbb{R} \mid a < x \leq b \} \]

\[ (a,b) = \{ x \in \mathbb{R} \mid a < x < b \} \]
Equality of Sets

Two sets $A$ and $B$ are called equal if and only if they have the same elements.

$A = B$ if and only if $\forall x (x \in A \leftrightarrow x \in B)$

[To prove $A=B$, it is sufficient to show that both $\forall x (x \in A \rightarrow x \in B)$ and $\forall x (x \in B \rightarrow x \in A)$ hold. Why?]
A set $A$ is a **subset** of $B$, written $A \subseteq B$, if and only if every element of $A$ is an element of $B$.

Thus, $A \subseteq B$ if and only if $\forall x(x \in A \rightarrow x \in B)$
Cardinality of a Set

Let $S$ be a set with a finite number of elements. We say that the set has **cardinality** $n$ if and only if $S$ contains $n$ elements. We write $|S|$ to denote the cardinality of the set.

For example, $|\emptyset| = 0$. 
Power Sets

Given a set $S$, the power set $P(S)$ of $S$ is the set of all subsets of $S$.

Example: $P( \{1\} ) = \{ \emptyset, \{1\} \}$

$P( \{1,2\} ) = \{ \emptyset, \{1\}, \{2\}, \{1,2\} \}$

$P(\emptyset) = \{ \emptyset \}$ since every set contains the empty set as a subset, even the empty set.

$P(\{\emptyset\}) = \{ \emptyset, \{\emptyset\} \}$. 
Let $A$ and $B$ be sets. The \textbf{Cartesian product} of $A$ and $B$, denote $A \times B$, is the set of all pairs $(a,b)$ with $a \in A$ and $b \in B$.

$$A \times B = \{ (a,b) \mid a \in A \land b \in B \}$$
Set Operations

Given two sets A and B. You should know

- the union of A and B
- the intersection of A and B
- the set difference between A and B
- the complement of A
De Morgan’s Laws

\[ A \cap B = \overline{A \cup B} \]

**Proof:**

\[ A \cap B = \{ x \mid x \notin A \cap B \} \] by definition of complement

\[ = \{ x \mid \neg(x \in A \cap B) \} \]

\[ = \{ x \mid \neg(x \in A \land x \in B) \} \] by definition of intersection

\[ = \{ x \mid \neg(x \in A) \lor \neg(x \in B) \} \] de Morgan’s law from logic

\[ = \{ x \mid (x \notin A) \lor (x \notin B) \} \] by definition of \( \notin \)

\[ = \{ x \mid x \in \overline{A} \lor x \in \overline{B} \} \] by definition of complement

\[ = \{ x \mid x \in \overline{A \cup B} \} \] by definition of union

\[ = \overline{A \cup B} \]
Function Terminology

Let $f: A \to B$ be a function.

We call

- $A$ the **domain** of $f$ and
- $B$ the **codomain** of $f$.

The **range** of $f$ is the set

$f(A) = \{ f(a) \mid a \in A \}$
A function \( f: A \to B \) is called **injective** or **one-to-one** if and only if \( f(a) = f(b) \) implies that \( a = b \).

In other words, \( f \) is injective if and only if different arguments have different values. [Contrapositive!]
A function $f: A \rightarrow B$ is called **surjective** or **onto** if and only if $f(A)=B$.

In other words, $f$ is surjective if and only if for each element $b$ in the codomain $B$ there exists an element $a$ in $A$ such that $f(a)=b$. 
A function is called a **bijection** or **one-to-one correspondence** if and only if it is injective and surjective.

**Bijectons**
Floor Function

The floor function \( \lfloor x \rfloor : \mathbb{R} \rightarrow \mathbb{Z} \) assigns to a real number \( x \) the largest integer \( \leq x \).

\[ \lfloor 3.2 \rfloor = 3 \]

\[ \lfloor -3.2 \rfloor = -4 \]

\[ \lfloor 3.99 \rfloor = 3 \]
Ceiling Function

The ceiling function \( \lceil \cdot \rceil : \mathbb{R} \rightarrow \mathbb{Z} \) assigns to a real number \( x \) the smallest integer \( \geq x \).

\[ \lceil 3.2 \rceil = 4 \]

\[ \lceil -3.2 \rceil = -3 \]

\[ \lceil 0.5 \rceil = 1 \]
Basic Facts

We have ⌈x⌉ = n if and only if n <= x < n+1.

We have ⌊x⌋ = n if and only if n-1 < x <= n.

We have ⌈x⌉ = n if and only if x-1 < n <= x.

We have ⌊x⌋ = n if and only if x <= n < x+1.
Example

Prove or disprove:

$$\lfloor \sqrt{\lfloor x \rfloor} \rfloor = \lfloor \sqrt{x} \rfloor$$
Let \( m = \lfloor \sqrt{[x]} \rfloor \)

Hence, \( m \leq \sqrt{[x]} < m + 1 \)

Thus, \( m^2 \leq [x] < (m + 1)^2 \)

It follows that \( m^2 \leq x < (m + 1)^2 \)

Therefore, \( m \leq \sqrt{x} < m + 1 \)

Thus, we can conclude that \( m = \lfloor \sqrt{x} \rfloor \)

This proves our claim.
Asymptotic Notations
Let $f, g: \mathbb{N} \rightarrow \mathbb{R}$ be functions from the natural numbers to the set of real numbers.

We write $f \in O(g)$ if and only if there exists some real number $n_0$ and a positive real constant $U$ such that

$$|f(n)| \leq U|g(n)|$$

for all $n$ satisfying $n \geq n_0$. 
Set Interpretation

We have interpreted $f(n) = O(g(n))$ as a relation between the two functions $f(n)$ and $g(n)$.

We can give $O(g(n))$ a meaning by interpreting it as the set of all functions $f(n)$ such that $f(n) = O(g(n))$, that is,

$$O(g) = \{ f: \mathbb{N} \rightarrow \mathbb{R} \mid \text{there exists a constant } U \text{ and a natural number } n_0 \text{ such that } |f(n)| \leq U|g(n)| \text{ for all } n \geq n_0 \}$$
Example $O(n^2)$
Upper Bound

The big Oh notation provides an upper bound on a function \( f \).

\[ f(n) = O(n) \text{ means that } f(n) \leq Un \]

for some constant \( U \) and for all \( n \geq n_0 \)

The notation does not imply that \( f \) has to grow that fast.

E.g. \( f(n) = 1 \) satisfies \( f(n) = O(n) \).

so \( f(n) = O(1) \) would have been a better bound.

\[ \Rightarrow \text{We need lower bounds as well} \Rightarrow \text{Big } \Omega \]
Big $\Omega$

We define $f(n) \in \Omega(g(n))$ if and only if there exist a positive real constant $L$ and a natural number $n_0$ such that

$$L |g(n)| \leq |f(n)|$$

holds for all $n \geq n_0$.

In other words, $f(n) = \Omega(g(n))$ if and only if $g(n) = O(f(n))$. 
We define \( f(n) \in \Theta(g(n)) \) if and only if there exist positive real constants \( L \) and \( U \) and a natural number \( n_0 \) such that

\[
L |g(n)| \leq |f(n)| \leq U |g(n)|
\]

holds for all \( n \geq n_0 \).

In other words, \( f(n) = \Theta(g(n)) \) if and only if \( f(n) = \Omega(g(n)) \) and \( f(n) = O(g(n)) \).
Informal Summary

\[ f(n) = O(g(n)) \text{ means that } |f(n)| \text{ is upper bounded by a constant multiple of } |g(n)| \text{ for all large } n. \]

\[ f(n) = \Omega(g(n)) \text{ means that } |f(n)| \text{ is lower bounded by a constant multiple of } |g(n)| \text{ for all large } n. \]

\[ f(n) = \Theta(g(n)) \text{ means that } |f(n)| \text{ has the same asymptotic growth as } |g(n)| \text{ up to multiplication by constants.} \]