Lesson 1: Preliminaries

Theme: Review of some essential mathematical backgrounds.

1 Useful notations and facts from discrete mathematics

Equivalence relations:
A binary relation $R$ over $X$ is called an equivalence relation, if it satisfies the following conditions.

- Reflexive: $(x, x) \in R$, for every $x \in X$.
- Symmetric: $(x, y) \in R$ if and only if $(y, x)$, for every $x, y \in X$.
- Transitive: for every $x, y, z \in X$, if $(x, y) \in R$ and $(y, z) \in R$, then $(x, z) \in R$.

For $x \in X$, the equivalence class of $x$ in $R$ is defined as:

$$[x]_R := \{y \mid (x, y) \in R\}$$

Lemma 1.1 Let $R$ be an equivalence relation over $X$. Then, the following holds:

- $[x]_R = [y]_R$ if and only if $(x, y) \in R$.
- If $[x]_R \neq [y]_R$, then $[x]_R \cap [y]_R = \emptyset$.

Theorem 1.2 Let $R$ be an equivalence relation over $X$. Then, the equivalence classes of $R$ partition $X$, i.e., every member of $X$ belongs to exactly one equivalence class of $R$.

Countable and uncountable sets:
Let $\mathbb{N}$ be the set of natural numbers $\{0, 1, 2, \ldots\}$. A set $X$ is countable, if there is an injective function from $X$ to $\mathbb{N}$. Otherwise, it is called an uncountable set.

Theorem 1.3 The following sets are all countable.

1. The set $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ of integers.
2. The set $\mathbb{N}^k$, for every integer $k \geq 1$.
3. The set $\mathbb{N}^* := \bigcup_{k \geq 1} \mathbb{N}^k$.

Theorem 1.4 The set $2^\mathbb{N}$ is uncountable.

Poset (partially ordered set):
Let $X$ be a set and $R$ be a binary relation on $X$. The set $X$ is a poset (w.r.t. $R$), if $R$ is reflexive, anti-symmetric and transitive.

Definition 1.5 An element $m \in X$ is a maximal element in a poset $X$ (w.r.t. $R$), if for every $x \in X$ and $x \neq m$, $(m, x) \notin R$.

Definition 1.6 A subset $C$ of $X$ is a chain in $X$ (w.r.t. $R$), if for every $x, y \in C$, either $(x, y) \in R$, or $(y, x) \in R$. A chain $C$ is bounded, if there is $z \in X$ such that for every $x \in C$, $(x, z) \in R$.

A binary relation $R$ on $X$ is anti-symmetric, if the following holds: for every $a, b \in X$, if both $(a, b)$ and $(b, a)$ are in $R$, then $a = b$. 
2 Basic propositional calculus (Boolean logic)

Throughout this class, $T$ and $F$ are special symbols denoting true and false, respectively. The symbols $\neg$, $\land$, $\lor$, $\to$ and $\leftrightarrow$ denote the negation, and, or, implication and iff operators on $\{T, F\}$, respectively, which are defined as follows.

<table>
<thead>
<tr>
<th>$p$</th>
<th>$q$</th>
<th>$p \land q$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$T$</td>
<td>$T$</td>
<td>$T$</td>
</tr>
<tr>
<td>$T$</td>
<td>$F$</td>
<td>$F$</td>
</tr>
<tr>
<td>$F$</td>
<td>$T$</td>
<td>$F$</td>
</tr>
<tr>
<td>$F$</td>
<td>$F$</td>
<td>$F$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$p$</th>
<th>$q$</th>
<th>$p \lor q$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$T$</td>
<td>$T$</td>
<td>$T$</td>
</tr>
<tr>
<td>$T$</td>
<td>$F$</td>
<td>$T$</td>
</tr>
<tr>
<td>$F$</td>
<td>$T$</td>
<td>$T$</td>
</tr>
<tr>
<td>$F$</td>
<td>$F$</td>
<td>$F$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$p$</th>
<th>$\neg p$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$T$</td>
<td>$F$</td>
</tr>
<tr>
<td>$F$</td>
<td>$T$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$p$</th>
<th>$q$</th>
<th>$p \to q$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$T$</td>
<td>$T$</td>
<td>$T$</td>
</tr>
<tr>
<td>$T$</td>
<td>$F$</td>
<td>$F$</td>
</tr>
<tr>
<td>$F$</td>
<td>$T$</td>
<td>$T$</td>
</tr>
<tr>
<td>$F$</td>
<td>$F$</td>
<td>$T$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$p$</th>
<th>$q$</th>
<th>$p \leftrightarrow q$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$T$</td>
<td>$T$</td>
<td>$T$</td>
</tr>
<tr>
<td>$T$</td>
<td>$F$</td>
<td>$F$</td>
</tr>
<tr>
<td>$F$</td>
<td>$T$</td>
<td>$F$</td>
</tr>
<tr>
<td>$F$</td>
<td>$F$</td>
<td>$T$</td>
</tr>
</tbody>
</table>

Let $PV = \{p_1, p_2, \ldots\}$ to be a countable set of propositional variables. Sometimes we also write $p$, $q$, or $q_1, q_2, \ldots$ to denotes propositional variables. Elements in $PV$ are also called atomic formulas.

**Definition 1.7** A well formed formula (wff) is a formula built up inductively as follows.

- Every propositional variable $p \in PV$ is a wff.
- If $\alpha$ and $\beta$ are wffs, so are $(\neg \alpha)$, $(\alpha \land \beta)$, $(\alpha \lor \beta)$, $(\alpha \to \beta)$ and $(\alpha \leftrightarrow \beta)$.

Usually we will use the term formula to mean wff.

The negation of a propositional variable $p$ is $\neg p$. A literal is either a propositional variable or its negation. A formula is in conjunctive normal form (CNF), if it is of the form:

$$(\ell_{0,0} \lor \cdots \lor \ell_{0,n_0}) \land (\ell_{1,0} \lor \cdots \lor \ell_{1,n_1}) \land \cdots \land (\ell_{k,0} \lor \cdots \lor \ell_{k,n_k}),$$

where each $\ell_{i,j}$ is a literal.

A formula is in disjunctive normal form (DNF), if it is of the form:

$$(\ell_{0,0} \land \cdots \land \ell_{0,n_0}) \lor (\ell_{1,0} \land \cdots \land \ell_{1,n_1}) \lor \cdots \lor (\ell_{k,0} \land \cdots \land \ell_{k,n_k}).$$

An assignment is a function that maps each propositional variable in $PV$ to either $T$ or $F$. The value of a formula $\alpha$ under an assignment $w$ is defined inductively as follows.

- $w(\alpha) = w(p)$, if $\alpha$ is propositional variable $p$.
- $w(\neg \alpha) = \neg w(\alpha)$.
- $w(\alpha \land \beta) = w(\alpha) \land w(\beta)$.
- $w(\alpha \lor \beta) = w(\alpha) \lor w(\beta)$.
- $w(\alpha \to \beta) = w(\alpha) \to w(\beta)$.
- $w(\alpha \leftrightarrow \beta) = w(\alpha) \leftrightarrow w(\beta)$.

\[\text{†For simplicity, we only consider } PV \text{ a countable set. Although in general such assumption is not necessary, it will simplify our discussions a lot.}\]
Definition 1.8

- An assignment \( w \) is a satisfying assignment for a formula \( \alpha \), denoted by \( w \models \alpha \), if \( w(\alpha) = T \). We also say that \( w \) is a model of \( \alpha \).
- Likewise, \( w \) is a satisfying assignment (or, a model) for a set \( X \) of formulas, denoted by \( w \models X \), if \( w \models \alpha \), for every \( \alpha \in X \).
- A formula \( \alpha \) is satisfiable, if it has a satisfying assignment, and accordingly, a set \( X \) of formulas is satisfiable, if it has a satisfying assignment.
- Two formulas \( \alpha \) and \( \beta \) are equivalent, if for every assignment \( w \), \( w(\alpha) = w(\beta) \).

Sometimes we omit the brackets, when they are irrelevant. For example, \( \alpha \land (\beta \land \gamma) \) and \( (\alpha \land \beta) \land \gamma \) are equivalent, so the brackets can be omitted, and written simply as \( \alpha \land \beta \land \gamma \).

Theorem 1.9 (Distributivity law for \( \land \) and \( \lor \)) For every formulas \( \alpha, \beta, \gamma \), the following holds.

- \( \alpha \land (\beta \lor \gamma) \) and \( (\alpha \land \beta) \lor (\alpha \land \gamma) \) are equivalent.
- \( \alpha \lor (\beta \land \gamma) \) and \( (\alpha \lor \beta) \land (\alpha \lor \gamma) \) are equivalent.

A formula \( \alpha \) using only atomic formulas \( p_1, \ldots, p_n \) defines a function \( f_\alpha : \{T,F\}^n \to \{T,F\} \), where for every \( (v_1, \ldots, v_n) \in \{T,F\}^n \)

\[
f_\alpha(v_1, \ldots, v_n) = v \quad \text{if and only if} \quad \left\{ \begin{array}{l}
\text{under the assignment} \ w \\
\text{where} \ w(p_i) = v_i, \ \text{for each} \ i = 1, \ldots, n, \\
w(\alpha) = v.
\end{array} \right.
\]

Definition 1.10 A set \( \Gamma \) of operators is complete, if for every integer \( n \geq 1 \), for every function \( g : \{T,F\}^n \to \{T,F\} \), there is a formula \( \alpha \) using only operators from \( \Gamma \) such that \( f_\alpha = g \).

Theorem 1.11

(a) For every function \( g : \{T,F\}^n \to \{T,F\} \), there is a formula \( \alpha \) in DNF such that \( f_\alpha = g \).

(b) Similarly, for every function \( g : \{T,F\}^n \to \{T,F\} \), there is a formula \( \alpha \) in CNF such that \( f_\alpha = g \).

Corollary 1.12 The set \( \{\neg, \land, \lor\} \) is complete.
Exercises

(1) Let $\mathbb{R}$ be the set of real numbers. Define a relation $R$, where $(x, y) \in R$ if and only if $x < y$. Prove that $\mathbb{R}$ is a poset w.r.t. $R$.\footnote{The poset $\mathbb{R}$ w.r.t. the relation $\leq$ is usually written as $(\mathbb{R}, \leq)$.}

(2) Give an example of a bounded chain in the poset $(\mathbb{R}, \leq)$ as defined in question 4.

(3) Give an example of an unbounded chain in the poset $(\mathbb{R}, \leq)$.\footnote{The poset $\mathbb{R}$ w.r.t. the relation $\leq$ is usually written as $(\mathbb{R}, \leq)$.}

(4) Let $A$ be a set and $\mathcal{F}$ be a collection of subsets of $A$. Define a relation $R$ on elements of $\mathcal{F}$:

$$(x, y) \in R \text{ if and only if } x \subseteq y$$

Prove that $\mathcal{F}$ is a poset w.r.t. $R$.\footnote{The poset $\mathcal{F}$ w.r.t. the relation $\subseteq$ is usually written as $(\mathcal{F}, \subseteq)$.}

(5) Give an example of a poset $(\mathcal{F}, \subseteq)$ in which every chain is bounded.

(6) Give an example of a poset $(\mathcal{F}, \subseteq)$ in which there is an unbounded chain.

(7) Consider a poset $(\mathcal{F}, \subseteq)$ where $\mathcal{F}$ is a collection of subsets of a set $A$. Suppose that for every chain $C$ in $\mathcal{F}$, the set $\bigcup C$ is in $\mathcal{F}$.

Assuming Zorn’s lemma, prove that there is an element $M \in \mathcal{F}$ such that there is no $X \in \mathcal{F}$ where $M \subseteq X$.

(8) Write down the equivalent formulas for $x \leftrightarrow y$ in DNF and CNF.

(9) Write down the formulas in DNF and CNF for the following function $f(p, q, r)$:

<table>
<thead>
<tr>
<th>$p$</th>
<th>$q$</th>
<th>$r$</th>
<th>$f(p, q, r)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
<td>F</td>
</tr>
</tbody>
</table>

(10) Prove that $\{\neg, \land\}$ and $\{\neg, \lor\}$ are complete.

(11) Define the operators NAND and NOR, denoted by $p \logicnot\land q$ and $p \logicnot\lor q$, respectively, as follows.

<table>
<thead>
<tr>
<th>$p$</th>
<th>$q$</th>
<th>$p \land q$</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$p$</th>
<th>$q$</th>
<th>$p \lor q$</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
</tbody>
</table>

That is, $p \land q$ is equivalent to $\neg(p \land q)$ and $p \lor q$ is equivalent to $\neg(p \lor q)$. Prove that $\{\land\}$ and $\{\lor\}$ are complete.

(12) Prove part (b) of Theorem 1.11.
Appendix

A Basic set theoretic notations

Sets:

• A set is a collection of things, which are called its members or elements.
  $a \in X$ (read: $a$ is in $X$, or $a$ belongs to $X$) means $a$ is a member or an element of $X$. $a \notin X$ means that $a$ is not a member of $X$.

• An empty set is denoted by $\emptyset$.

• $X$ is a subset of $Y$, denoted by $X \subseteq Y$, if every element of $X$ is also an element of $Y$.

• $X$ is a proper subset of $Y$, denoted by $X \subset Y$, if $X \neq Y$ and $X \subseteq Y$.

• For two sets $X$ and $Y$, we write $X \cap Y$ and $X \cup Y$ to denote their intersection and union, respectively.

• Let $X$ be a set whose elements are also sets. Then, $\bigcup X$ and $\bigcap X$ denote the following.

\[
\bigcup X := \{a \mid a \text{ belongs to an element in } X\}
\]

\[
\bigcap X := \{a \mid a \text{ belongs to every element in } X\}
\]

• The cartesian product between two sets $X$ and $Y$ is the following.

\[
X \times Y := \{(a, b) \mid a \in X \text{ and } b \in Y\}.
\]

We write $X^n$ to denote $X \times \cdots \times X$ ($X$ appears $n$ times).

Relations:

• A relation $R$ over two sets $X, Y$ is a subset of $X \times Y$.

• A binary relation $R$ over $X$ is a subset of $X \times X$.

• An $n$-ary relation $R$ over $X$ is a subset of $X^n$.

Functions:

• A relation $R$ over $X, Y$ is a function or a mapping, if for every $x \in X$, there is exactly one $y \in Y$ such that $(x, y) \in R$.
  In this case, we will say $R$ is a function from $X$ to $Y$, or $R$ maps $X$ to $Y$. We denote it by $R : X \rightarrow Y$.

• We will usually use the letters $f, g, h, \ldots$ to represent functions. As usual, we write $f(x)$ to denote the element $y$ in which $(x, y) \in f$.

• A function $f : X \rightarrow Y$ is an injective function, if for every $y \in Y$, there is at most one $x \in X$ such that $f(x) = y$. An injective function is also called an injection.

• A function $f : X \rightarrow Y$ is a surjective function, if for every $y \in Y$, there is at least one $x \in X$ such that $f(x) = y$.

• A function $f : X \rightarrow Y$ is a bijection, if it is both injective and surjective.
B Axiom of choice, Zorn’s lemma and Well-ordering theorem

The three statements below are equivalent and they are usually taken as “axioms” in mathematics.

**Axiom of choice:** Let $I$ be a set such that each $i \in I$ is associated with a set $A_i$. There is a function $f : I \rightarrow \bigcup A_i$ such that for every $i \in I$, $f(i) \in A_i$.

**Zorn’s lemma:** Let $(A, R)$ be a poset such that every chain in $A$ is bounded. There is an element $m \in A$ such that for every $x \in A$ and $x \neq m$, $(m, x) \notin R$.

**Well-ordering theorem:** Every set can be well-ordered. That is, for every set $A$, there is a total order relation $R$ on $A$, that is, it satisfies the following conditions:

- Antisymmetry: for every $a, b \in A$, if $(a, b), (b, a) \in R$, then $a = b$;
- Transitive: if $(a, b), (b, c) \in R$, then $(a, c) \in R$;
- Totality: for every $a, b \in A$, either $(a, b) \in R$ or $(b, a) \in R$,

such that for every nonempty subset $B \subseteq A$ has a minimal element (w.r.t. $R$).

There is a kind of contradiction here: the axiom of choice is viewed as obviously “correct,” while the well-ordering theorem is obviously “false,” and there are mixed opinions about Zorn’s lemma.