Discrete Mathematics 16/01/2019

Lecture 3: Well-Ordering and Induction

Instructor: Goutam Paul *Scribe: Soham Das*

Definition 3.1. A relation R on X is called a *partial order* if R is reflexive, transitive and anti-symmetric.
Generic notation for any partial order R is '$\leq$'. Given $(a, b) \in \leq$, we write $a \leq b$. Thus, $\leq$ is a partial order on X if it satifies (i) $x \leq x$ for all $x \in X$, (ii) $x \leq y, y \leq z$ implies $x \leq z$ and (iii) if $x \leq y$ and $y \leq x$ then $x = y$.

If $a \leq b$ and $a \neq b$ then we write $a < b$.

If a partial order $\leq$ is defined on a set X then $(X, \leq)$ is called partial ordered set or *poset*.

Examples:

1. $X = \{a, b, c\}$, $\mathscr{P}(X) = \{\phi, \{a\}, \{b\}, \cdots, \{a, b, c\}\}$. Then $\subseteq$ operation induces a partial order $\leq$ on $\mathscr{P}(X)$: we write $x \leq y$ if $x \subseteq y$. For example, $(\{b\}, \{b, c\}) \in \leq$, but $(\{a\}, \{b, c\}) \notin \leq$.

2. Consider the set of natural numbers $\mathbb{N}$. We write $(a, b) \in \leq$ if $a \mid b$. For example, $(1, 3), (2, 8) \in \leq$, but neither (3,5) nor (5,3) belongs to $\leq$. One can easily check that this $\leq$ is a partial order on $\mathbb{N}$.

Definition 3.2. A partial order relation $\leq$ on X is called a *total order* if for any two elements $x, y \in X$ we have either $x \leq y$ or $y \leq x$.

Examples:

1. The set of real numbers with the usual ordering $\leq$. It is a property of real numbers that for any two $x, y \in \mathbb{R}$, one and exactly one of the following is true: $x < y$, $x = y$ or $y < x$.

2. Consider the set complex numbers $\mathbb{C}$. We can define a dictionary ordering on it as follows: $(a + ib, c + id) \in \leq$ if (i) $a < c$ or (ii) $a = c$ and $b \leq d$. Then $(1 + i, 2 - i), (0, 2 - 3i) \in \leq$. One can easily show that this $\leq$ is a total order on $\mathbb{C}$.

3. Consider the set of natural numbers $\mathbb{N}$. We write $(a, b) \in \leq$ if $a \mid b$. Note that neither (3,5) nor (5,3) belongs to $\leq$. Hence this $\leq$ is not a total order on $\mathbb{N}$.

Definition 3.3. Consider a partial order $\leq$ on X,
(i) x is the *least*(smallest) element, if $\forall\ a \in X$, $x \leq a$.
(ii) x is the *greatest*(largest) element, if $\forall\ a \in X$, $a \leq x$.
(iii) x is a *minimal* element, if $\nexists\ a \in X$, such that $a < x$.
(iv) x is a *maximal* element, if $\nexists\ a \in X$, such that $x < a$.

Example: Consider the partial order $\leq$ on $\mathbb{N}$ defined by $x \leq y$ iff $x \mid y$. Then, note that $1 \leq n$ for all $n \in \mathbb{N}$ as 1 divides every other $\mathbb{N}$; whereas there does not exist any $n < 0$ which could divide 0. Thus, 1 is the least element and 0 is a minimal element of the partially ordered set $(\mathbb{N}, \leq)$. (Note that $(\mathbb{N}, \leq)$ is not a total order. Thus, in order to have a least/greatest element, the set need not be totally ordered.)

Remark. Note that, least (and greatest) element is unique if it exists. However, minimal and maximal element may not be unique. For example, if we define a partial order $\leq$ on $\{a, b\}$ by $\leq = \{(a, a), (b, b)\}$ then a, b are both minimal elements.

Definition 3.4. A set is called *well-ordered* if every non-empty subset of X has a least element.

Remark. (Well-order implies total order but total order does not imply well-order.) Suppose a set X is well-ordered, with respect to the partial order $\leq$. Then, for any $x, y \in X$, the set $\{x, y\}$ must have a least element, which means either $x \leq y$ or $y \leq x$ is true. Thus, if $(X, \leq)$ is well-ordered then $\leq$ must be a total order on X. However, the converse is not true. Suppose we take $\mathbb{Q}$ with the usual ordering $\leq$. Then $\leq$ is a total order on $\mathbb{Q}$ but it does not make $\mathbb{Q}$ an well-ordered set.

Theorem 3.5 (Zermelo's well ordering theorem)**.** Every non-empty set can be well-ordered. That is, given any non-empty set X, there exists a partial order on it which makes X an well-ordered set.

A1. Well-ordering principle (WOP)
Every non-empty subset of $\mathbb{N}$ has a least element.

A2. Principle of weak induction (WIP)
If $B \subseteq \mathbb{N}$ such that $0 \in B$ and $n \in B \Rightarrow n^+ \in B$ then $B = \mathbb{N}$.

A3. Principle of strong induction (SIP)
If $B \subseteq \mathbb{N}$ such that $0 \in B$ and $\forall a \leq n,\ a \in B \Rightarrow n^+ \in B$ then $B = \mathbb{N}$.

Theorem 3.6. A1, A2, A3 are equivalent.

WOP $\Rightarrow$ WIP: Assume WOP holds. Suppose $B \subseteq \mathbb{N}$ such that $0 \in B$ and if $n \in B$ then $n^+ \in B$.

Let if possible, $B \neq \mathbb{N}$ then $\mathbb{N} \backslash B \neq \phi$.

Define $J = \{x \in \mathbb{N} : x \notin B\} \neq \phi$. By WOP, J has a least element say, l.

Now, $l \neq 0$ since $0 \in B$. Then, l has a predecessor, i.e. $\exists m \in \mathbb{N}$ such that $l = m^+$.

Since we assumed l is the smallest member of J, so $m \notin J$. Hence $m \in B$.

But $m \in B$ implies $l = m^+ \in B$, which contradicts that $l \notin B$.

Thus, our initial assumption that $B \neq \mathbb{N}$ is wrong. Hence proved. $\square$

WIP $\Rightarrow$ SIP: Consider $B \subseteq \mathbb{N}$ such that $0 \in B$ and if for all $a \leq n$, $a \in B$ then $n^+ \in B$. Assume that WIP holds. We shall show that $B = \mathbb{N}$.

Construct C as follows: $n \in C$ iff $a \in B$ for all $a \leq n$.

First note that $0 \in B$, so $0 \in C$. Next, $n \in C \Rightarrow a \in B \; \forall \; a \leq n \Rightarrow n^+ \in B$ as per the definition of B. This in turn implies that $n^+ \in C$.

Thus, $0 \in C$ and $n \in C \Rightarrow n^+ \in C$. Therefore WIP allows us to conclude that $C = \mathbb{N}$. This yeilds $B = \mathbb{N}$ since $C \subseteq B \subseteq \mathbb{N}$. □

SIP ⇒ WOP: Assume that SIP holds. Consider B to be a non-empty subset of $\mathbb{N}$. Let if possible, B does not have any least element.

Define $J = \{x : x \notin B\}$. Note, $0 \notin B$ otherwise 0 will be the least element of B, so $0 \in J$. Suppose, $0, 1, \ldots, n \in J$. Now if $n + 1 \in B$, then again it will be the least element in B, and hence $n + 1$ must belong to J.

Thus, $0 \in J$ and $\forall \; a \leq n, a \in J$ implies $n^+ \in J$. Hence, by SIP, $J = \mathbb{N} \Rightarrow B = \phi$ which is a contradiction.

Therefore, B must have a least element. □

Definition 3.7 (Transfinite induction)**.** Consider a well-ordered set X and a non-empty subset $B \subseteq X$. If for any $x \in X$, $\alpha < x$ and $\alpha \in B \Rightarrow x \in B$, then $X = B$.

In a well-ordered set, every non-empty subset contains a distinct smallest element. Given the axiom of dependent choice, this is equivalent to just saying that the set is totally ordered and there is no infinite decreasing sequence, something perhaps easier to visualize. In practice, the importance of well-ordering is justified by the possibility of applying transfinite induction, which says, essentially, that any property that passes on from the predecessors of an element to that element itself must be true of all elements (of the given well-ordered set). If the states of a computation (computer program or game) can be well-ordered in such a way that each step is followed by a "lower" step, then the computation will terminate.

It is inappropriate to distinguish between two well-ordered sets if they only differ in the "labeling of their elements", or more formally: if the elements of the first set can be paired off with the elements of the second set such that if one element is smaller than another in the first set, then the partner of the first element is smaller than the partner of the second element in the second set, and vice versa. Such a one-to-one correspondence is called an order isomorphism and the two well-ordered sets are said to be order-isomorphic, or similar (obviously this is an equivalence relation).

Definition 3.8 (Order isomorphism)**.** Two posets $(X, \leq)$ and $(X', \leq')$ are called *order isomorphic* if and only if $\exists$ a bijection between X and X' that preserves the order, i.e., $\exists f : X \to X'$ such that if $(x_1, x_2) \in \leq$ then $(f(x_1), f(x_2)) \in \leq'$. That is, $x_1 \leq x_2 \implies f(x_1) \leq' f(x_2)$.

Example: Define $\leq$ on $X = \mathbb{N}$ as: $x \leq y$ iff $x \mid y$. Take $X' =$ set of all natural numbers which are perfect squares, with the ordering $\leq'$ defined as: $x \leq' y$ iff $x \mid y$. Then $f(x) = x^2$ sets up an order isomorphism between $(\mathbb{N}, \leq)$ and $(X', \leq')$.

Note that, if there exists an order isomorphism between two well-ordered sets, the order isomorphism is unique: this makes it quite justifiable to consider the two sets as essentially identical, and to seek a "canonical" representative of the isomorphism type

(class). This is exactly what the ordinals provide, and it also provides a canonical labeling of the elements of any well-ordered set.

Essentially, an ordinal is intended to be defined as an isomorphism class of well-ordered sets: that is, as an equivalence class for the equivalence relation of "being order-isomorphic". There is a technical difficulty involved, however, in the fact that the equivalence class is too large to be a set in the usual Zermelo-Fraenkel (ZF) formalization of set theory. But this is not a serious difficulty. The ordinal can be said to be the order type of any set in the class. Rather than defining an ordinal as an equivalence class of well-ordered sets, it will be defined as a particular well-ordered set that (canonically) represents the class. Thus, an ordinal number will be a well-ordered set; and every well-ordered set will be order-isomorphic to exactly one ordinal number.

Definition 3.9 (Ordinal numbers)**.** Representation of the equivalence classes of order-isomorphism.

Each of equivalent classes is assigned an ordinal number ordered like

$$\phi \equiv 0, \{\phi\} \equiv \{0\} \equiv 1, \{\phi, \{\phi\}\} \equiv \{0, 1\} \equiv 2, \cdots .$$

In this way we can assign ordinal numbers to the sets of different order-type. Each set is union of the set of previous order and the set containing it. If we continue in this way, at some place we have the set of natural numbers $\mathbb{N}$. We assign ω to it and assign $\omega+1$ for the next ordinal set, namely $\mathbb{N}^+ = \mathbb{N} \cup \{\mathbb{N}\}$. In this way, the hierarchy of ordinal numbers looks like

$$\phi, \{\phi\}, \{\phi, \{\phi\}\}, \cdots, \omega = \mathbb{N}, \omega+1 = \mathbb{N}^+, \omega+2 = (\mathbb{N}^+)^+, \cdots, 2\omega = \omega+\omega, \cdots, \omega^2, \cdots .$$

Now, someone has proved that there is a class of uncountable sets in this list. Hence, the ordinal numbers being well-ordered, there is a least ordinal number which is uncountable, we call it Ω. Thus the list of ordinal numbers looks like:

$$\phi, \{\phi\}, \{\phi, \{\phi\}\}, \cdots, \omega, \omega+1, \omega+2, \cdots, 2\omega, \cdots, \omega^2, \cdots, \omega^3, \cdots, \omega^\omega, \cdots, \Omega, \cdots .$$

It is interesting that all the ordinal numbers preceding Ω are countable, and suddenly Ω becomes uncountable.

Now, recall that we defined cardinality of sets as

Definition 3.10 (Cardinality)**.** For any set S, we associate a number card S such that card $X <$ card Y iff $X \prec Y$ and card $X =$ card Y iff $X \sim Y$.

Example: We set card $\phi = 0$. If $X \sim n \equiv \{0, 1, 2, \cdots, n-1\}$ we denote card X by n. Thus, card $\phi = 0$, card $\{\phi\} = 1$, card $\{\phi, \{\phi\}\} = 2$ etc.

What is the difference between cardinality and ordinal numbers? Ordinal number of an well-ordered set denotes the *position* of that set in the hierarchy of the equivalence classes of order-isomorphism. Whereas, cardinality is related to the *size* of the set. For instance, the set $\mathbb{N}^+$ has same cardinality as $\mathbb{N}$, but their ordinal numbers are different. The reason is that, although there exists a bijection between them, there does not exist a bijection preserving the ordering (the ordering which makes them well-ordered sets). In fact, many ordinals have the same cardinality.

Definition 3.11 (Cardinal numbers)**.** A cardinal number α is an ordinal number such that if there exists another ordinal number β with card α = card β then $\alpha \leq \beta$.

A cardinal number represents the equivalence class of all sets that can be put in one-to-one correspondence (bijection) with each other.

It can be proved that the cardinal $\aleph_0$ ($\aleph$ is the first letter in the Hebrew alphabet) of the set of natural numbers is the smallest infinite cardinal, i.e. that any infinite set has a subset of cardinality $\aleph_0$. The next larger cardinal (which corresponds to Ω) is denoted by $\aleph_1$ and so on. For every ordinal α there is a cardinal number $\aleph_\alpha$, and this list exhausts all infinite cardinal numbers. Since there exists a bijection between $\mathscr{P}(\mathbb{N})$ and $\mathbb{R}$, we denote the cardinal number of $\mathbb{R}$ by $2^{\aleph_0}$.

Remark 3.12. The continuum hypothesis (CH) states that there are no cardinals strictly between $\aleph_0$ and $2^{\aleph_0}$. The latter cardinal number is also often denoted by $\mathfrak{c}$; it is the cardinality of the continuum (the set of real numbers). Thus, continuum hypothesis states that $2^{\aleph_0} = \aleph_1$.

The generalized continuum hypothesis (GCH) states that there are no cardinals strictly between $\aleph_\alpha$ and $2^{\aleph_\alpha}$. It has been proved that the continuum hypothesis is independent of the usual axioms of set theory, i.e., the Zermelo-Fraenkel axioms together with the axiom of choice (ZFC).