EIDMA
Lecture 6

- Well-orders
- Induction
- Operations modulo *n*

Definition.
A set X is *totally* ordered by an ordering relation $\preccurlyeq$ iff

$$(\forall a, b \in X)(a \preccurlyeq b \vee b \preccurlyeq a).$$

In other words, $\preccurlyeq \cup \preccurlyeq^{-1} = X \times X$, or every two elements are comparable. Such an ordering relation is called a *total order on X*.

Definition.
A *chain* in a poset (X,$\preccurlyeq$) is any subset A which is *totally* ordered by $\preccurlyeq$.

Hasse diagram of a chain looks like a vertical line

(finite or not).

Comprehension. Prove or disprove:

1. Every subset of a chain is a chain.
2. If every proper subset of X is a chain, then X is totally ordered.
3. What are maximal chains in $(\{1,2, \ldots 17\}, |)$?
   ”maximal” means with "maximal with respect to inclusion".
4. What are maximal chains in $(\mathbb{N}, |)$? *This one is fun!*
5. What are maximal chains in $(\mathbb{N}, \leq)$?

Antichains.

Definition.

Let (X,≼) be a poset. A subset A of X is called an *antichain* in (X,≼) iff

$$(\forall x, y \in A)\big(x \neq y \Rightarrow \sim (x \preccurlyeq y \vee y \preccurlyeq x)\big)$$

What it really means is that no two different elements of an antichain are comparable by ≼.

Facts.

- If $(X,\preccurlyeq)$ is a chain (a totally ordered poset) then it only has one-element antichains.
- If $(X,\preccurlyeq)$ is a poset, C is a chain and A is an antichain in $(X,\preccurlyeq)$ then $|A \cap C| \leq 1$.

Theorem (Dilworth).

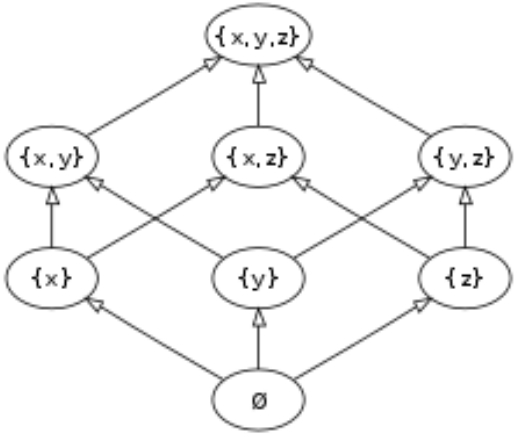
In every finite poset $(X, \preccurlyeq)$ the largest size of an antichain (LSA) is equal to the smallest number of pairwise disjoint chains (SNC) whose union is X.

Comprehension.

This is proved by showing that LSA $\leq$ SNC and LSA $\geq$ SNC. One inequality is easy, the other not so much. Prove the easy one.

Examples.

- Verify Dilworth theorem in the poset $(\{1,2, \ldots, 17\},|)$
- Verify Dilworth theorem in the poset $(2^{\{x,y,z\}},\subseteq)$
  One largest-size antichain is {{x}, {y}, {z}}.



We should be able to partition our set into 3 chains.
For example: {∅, {x},{x,y}}, {{y},{y,z},{x,y,z}}, {{z},{x,z}}

Graph source – Wikipedia

Definition.

A set X is *well-ordered* by an ordering relation $\preccurlyeq$ iff it is totally ordered and every nonempty subset of X has the smallest element.

$\preccurlyeq$ is then called a *well order* (not a *good order*, this is a well as in „every well has a bottom” rather than in „you jump well”.

The fact that $(\mathbb{N}, \leq)$ is a well order is considered one of the axioms of the theory of natural numbers. That, or the *principle of induction* - they can be shown to be equivalent, hence, in a sense, interchangeable.

Examples

Determine which of the posets below are total, which are well, and which are neither:

1. $(\mathbb{N},\leq)$
2. $(\mathbb{Z},\leq)$
3. $(\mathbb{N},|)$
4. $(\mathbb{R},\leq)$
5. $(\mathbb{C},\preccurlyeq)$ where $a+bi \preccurlyeq c+di$ iff $a\leq c \wedge b\leq d$
6. $(\mathbb{C},\preccurlyeq)$ where $a+bi \preccurlyeq c+di$ iff $a<c \vee (a=c \wedge b \leq d)$ (this is known as the *lexicographic* or *dictionary* order)
7. $(\mathbb{R}^n,\preccurlyeq)$ where $(a_1, a_2, \dots, a_n) \preccurlyeq (b_1, b_2, \dots, b_n)$ iff $(\forall i \leq n)(a_i = b_i) \vee (\exists k \leq n)(\forall j < k)(a_j = b_j \wedge a_k < b_k)$ (the lexicographical order on $\mathbb{R}^n$).

The fact that $(\mathbb{N}, \leq)$ is a well order is considered one of the axioms of the theory of natural numbers. That, or the *principle of induction* - they can be shown to be equivalent, hence, in a sense, interchangeable.

Theorem (Principle of induction)

For every propositional function φ defined on $\mathbb{N}$,

if

(1) $\varphi(1)$

(2) $(\forall k \epsilon \mathbb{N})(\varphi(k) \Rightarrow \varphi(k+1))$

then $(\forall n \epsilon \mathbb{N})\varphi(n)$.

Proof. (by contradiction)

Suppose that for some propositional function φ conditions (1) and (2) hold while the set $C(\varphi) = \{n \epsilon \mathbb{N}: \sim\varphi(n)\}$ is nonempty. Then $C(\varphi)$ has the smallest element *p*. Due to (1) $p \neq 1$, hence $p - 1$ is also a natural number and $\varphi(p-1)$ holds. But then condition (2) fails for $k = p - 1$. QED

Principle of induction is often used as a tool for proving theorems about natural numbers. Sometimes it works even if no natural number is explicitly mentioned in the theorem. For example

For every finite set X, $|2^X|=2^{|X|}$

does not look much like a theorem about natural numbers until you rephrase it as

$$(\forall n \epsilon \mathbb{N})(\forall X)(|X| = n \Rightarrow |2^X| = 2^n)$$

Some theorems can be proved with or without induction. It is a matter of taste or simplicity which method we choose.

Notice that the induction theorem is a 'proper' theorem. It has an *assumption* (also called a *premise*), frankly two of those:

(1) $\varphi(1)$

and

(2) $(\forall k \epsilon \mathbb{N})(\varphi(k) \Rightarrow \varphi(k+1))$

and an assertion (sometimes called a *conclusion*):

$(\forall n \epsilon \mathbb{N})\varphi(n)$

which is a logical consequence of the premises.

People often talk about "two induction steps". Each of these "steps" is just verification that one of the assumptions of the induction theorem is fulfilled. There is no reason why checking (1) first and (2) second should be considered better than checking (2) first, every conjunction is commutative.

A common pitfall.
People who do not understand the idea of the *range of a quantifier* sometimes phrase the "second step" of their induction proofs like this:

"Suppose that for every k, $\varphi(k)$ holds. We will prove that $\varphi(k+1)$ holds as well".

LOL, If one "supposes that for every k, $\varphi(k)$ holds" they in fact suppose that the theorem is true, which means you are proving that if a theorem is true then the theorem is true. Which is true but beside the point.
What we really do is this: "We take a number k (any k, but just a single one) and assuming φ holds for this particular k we attempt to prove that it holds for $k+1$".

Example.

For every finite set X, $|2^X|=2^{|X|}$.

Proof by induction on $n=|X|$.

We begin with the smallest possible value of n, $n = 0$. There is only one set X satisfying $|X| = 0$, the empty set. Obviously, $2^X = \{\emptyset\}$, so $|2^X| = 1 = 2^0 = 2^{|X|}$. We have verified assumption (1).

Now, suppose our theorem is true for some k. This means that for every k-element set X, $|2^X| = 2^k$. Consider a $k + 1$ element set Y and proclaim one of its elements, say y_1, king. Subsets of Y can be split into those who do and those who do not contain the king. Each of these two families of subsets has 2^k elements hence, in total we have $2^k + 2^k = 2 \cdot 2^k = 2^{k+1} = 2^{|Y|}$ subsets of Y. QED

Theorem (Strong induction principle)

For every propositional function φ defined on $\mathbb{N}$,

if

(1) $\varphi(1)$

and

(2) $(\forall k \epsilon \mathbb{N})[(\varphi(1) \wedge \varphi(2) \wedge \cdots \wedge \varphi(k)) \Rightarrow \varphi(k+1)]$

then $(\forall n \epsilon \mathbb{N})\varphi(n)$.

It can be proved that the *strong induction principle* is equivalent to the (ordinary) *induction principle*, which means it is not *really stronger* than the ordinary one. But often easier to apply.

Example.

Every natural number $n, n \geq 2$ is a product of primes (we consider a prime a "degenerate product of primes" i.e. a product with just one factor).

Again, we begin our induction not from 1 but from the smallest possible value of *n*, here $n = 2$. Since 2 is a prime – we are done. Now, suppose for some $k + 1 > 2$ every natural number between 2 and *k* is a product of primes (i.e., "2 is a product of primes AND 3 is …. AND *k* is a product of primes") . We must show that so is *k*+1. If *k*+1 happens to be a prime – we are done. If not, $k + 1 = pq$ for some p, q between 2 and *k*. By our assumption, both *p* and *q* are products of primes, hence their product is, too. QED

Arithmetic modulo *n*

Let n be a positive natural number. For any two integers p and q we define

$p \oplus q = (p+q) \bmod n$

$p \otimes q = (pq) \bmod n$

In both cases the result is between 0 and n-1 (inclusive) which means in particular that the operations have no identity elements:

If you take p>n then, whatever your choice of q, $p \oplus q < n < p$, i.e. $(\forall\, q)\ p \oplus q \neq p$

The same argument applies to $\otimes$.

Theorem.

For every natural number *n* the operations $\oplus$ and $\otimes$ are commutative, associative and $\otimes$ is distributive with respect to $\oplus$.

Proof.

Notice that

(1) $(\forall p)\ ((p\ mod\ n)\ mod\ n =\ p\ mod\ n\ )$ and

(2) $(\forall p, q)\ ((p + q) mod\ n\ =\ (p\ mod\ n\ +\ q\ mod\ n)\ mod\ n).$

So, $(p \oplus q) \oplus r\ =\ ((p + q) mod\ n\ +\ r)\ mod\ n$ = (*by* (2))

$(((p + q) mod\ n) mod\ n\ +\ r\ mod\ n)\ mod\ n$ = (*by* (1))

$((p + q) mod\ n\ +\ r\ mod\ n)\ mod\ n\ =\ ((p + q)\ +\ r)\ mod\ n.$

Now we transform p $\oplus$ (q $\oplus$ r) in the same way.

Comprehension test.

1. Prove (1) and (2) from the previous slide.
2. Prove that $\otimes$ is associative.
3. Prove that $\otimes$ is distributive with respect to $\oplus$.