CS/SE 2FA3: Discrete Math with Applications II

Winter 2017

J. Zucker

Technical assistance by:

Eric Le Fort

1 Math Preliminaries

[Linz § 1.1]

Definition:

$\mathbb{N}$ = set of **natural numbers** = $\{0, 1, 2, ...\}$

$\mathbb{Z}$ = set of **integers** = $\{..., -2, -1, 0, 1, 2, ...\}$

$\mathbb{Q}$ = set of **rationals**

$\mathbb{R}$ = set of **reals**

$\mathbb{B}$ = set of **booleans** or truth values = $\{\mathsf{T}, \mathsf{F}\}$

Two ways to define sets:

by **listing**: e.g. $\{2, 4, 6, 8, 10\}$
by **description**: $\{x \in \mathbb{N} \mid \underline{\boldsymbol{x\ is\ even\ \wedge\ 2 \leq x \leq 10\}}}$

Given 2 sets, S_1, S_2: define:

$S_1 \cup S_2 = \underline{\boldsymbol{\{x \mid x \in S_1\ \vee\ x \in S_2\}}}$

$S_1 \cap S_2 = \underline{\boldsymbol{\{x \mid x \in S_1\ \wedge\ x \in S_2\}}}$

$S_1 \backslash S_2 = \underline{\boldsymbol{\{x \mid x \in S_1 \;\wedge\; x \notin S_2\}}}$

Assume **universal set**, U

$$\boldsymbol{S_1, S_2, \ldots \;\subseteq\; U}$$

Then define the **complement**:

(Linz uses $U - S$, we will be using $U \setminus S$)

$$\boldsymbol{\overline{S} = U \setminus S = \{x \in U \mid x \notin S\}}$$

Empty set $\varnothing$, then:

$S \cup \varnothing = \underline{\boldsymbol{S}}$

$S \cap \varnothing = \underline{\boldsymbol{\varnothing}}$

$\overline{\varnothing} = \underline{\boldsymbol{U}}$

$\overline{U} = \underline{\boldsymbol{\varnothing}}$

$\overline{\overline{S}} = \underline{\boldsymbol{S}}$

<u>De Morgan's Laws</u>

$\overline{S_1 \cap S_2} = \underline{\boldsymbol{\overline{S_1} \cup \overline{S_2}}}$

$\overline{S_1 \cup S_2} = \underline{\boldsymbol{\overline{S_1} \cap \overline{S_2}}}$

Subset: $S_1 \subseteq S_2 \iff \forall x(x \in S_1 \to x \in S_2)$

Proper Subset: $S_1 \subset S_2 \iff S_1 \subseteq S_2 \wedge S_1 \neq S_2$

Disjoint Sets: $S_1 \cap S_2 = \varnothing$

If S is finite, say $S = \{a_1, ..., a_n\}$, then the **size** of $S = |S| = n$

Unordered pair $\{a, b\} = \{b, a\} = \{a, b, a\} = ...$

Ordered pair $(a, b) \neq (b, a) \neq (a, b, a)$

Similarly, **ordered triple** (a, b, c) and

ordered n-tuple $(a_1, ..., a_n)$, etc.

Cartesian Product

$$S_1 \times S_2 = \{(x, y) \mid x \in S_1 \wedge y \in S_2\}$$

$$S_1 \times ... \times S_n = \{(x_1, ..., x_n) \mid x_i \in S_i \quad \textbf{for } i = 1, ..., n\}$$

Power set of $S = \mathcal{P}(S) = \{A \mid A \subseteq S\}$

$Q.$ What is the size of $\mathcal{P}(S)$?

Example:

If $|S| = 1$, then $|\mathcal{P}(S)| = \underline{2}$

If $|S| = 2$, then $|\mathcal{P}(S)| = \underline{4}$

If $|S| = 3$, then $|\mathcal{P}(S)| = \underline{8}$

$\boldsymbol{Theorem}$: If S is finite, then $|\mathcal{P}(S)| = \underline{2^{|S|}}$

$\boldsymbol{Proof}$: Prove statement $\boldsymbol{P(n)}$:

$$\forall S : |S| = n \;\Rightarrow\; |\mathcal{P}(S)| \;=\; \underline{2^n}$$

by **induction on n**.

<u>Induction on $\mathbb{N}$ or Mathematical Induction</u>

Definition: A predicate P on a set S is a function

$$P : S \rightarrow \mathbb{B} = \{\mathsf{T}, \mathsf{F}\}$$

For $\boldsymbol{x} \in S$: we write $\boldsymbol{P}$ is **true at $\boldsymbol{x}$** or $\boldsymbol{P}$ **holds at $\boldsymbol{x}$** to mean: $\boldsymbol{P(x) = T}$.

Notation: We let $\boldsymbol{k, m, n}$, ... range over **natural numbers** i.e. elements of $\mathbb{N}$.

Mathematical Induction concerns **predicates on $\mathbb{N}$**.

There are **3 versions**.

I Simple Induction (SI)

For any predicate P on $\mathbb{N}$:

If **(Base case)** $P(0)$

and **(Induction step)** $\forall n[P(n) \rightarrow P(n+1)]$

then $\forall n P(n)$

i.e. $\forall n \in \mathbb{N} P(n)$

Notes:

(i) Induction step can be written as:

$$\forall n > 0[P(n-1) \rightarrow P(n)]$$

(ii) In the induction step, $P(n)$ is the **induction hypothesis**.

II Course of Values Induction (CVI)

(Rosen calls this "**Strong Induction**")

Version (a): For any predicate P on $\mathbb{N}$:

If **(Base case)** $P(0)$

and **(Induction step)**

$$\forall n[P(0) \wedge P(1) \wedge \ldots \wedge P(n) \rightarrow P(n+1)]$$

then $\forall n P(n)$

Version (b): For any predicate P on $\mathbb{N}$:

If $\forall n[\forall\, k < n,\ P(k) \rightarrow P(n)]$

then $\forall n P(n)$

III Least number Principle (LNP)

For any predicate P on $\mathbb{N}$:

If $$\exists n P(n)$$

then $$\exists \textbf{ least } n P(n)$$

i.e. $$\exists n[P(n) \wedge \forall\, k < n,\ \neg P(k)]$$

$Q.$ What is the connection between (III) and the others?

Hint: Consider II (b)

Variations of Proof by Induction

For example SI:

(a) Can take 1, or any $b \in \mathbb{N}$, as the base case.

Then SI becomes:

For any predicate P on $\mathbb{N}$:

If (Base case) $P(b)$

and (Induction Step)

$$\forall n \geq b\, [P(n) \to P(n+1)]$$

then $\forall n \geq b,\ P(n)$

Example: [Linz, p.16, Ex. 28]

Prove: $\forall n \geq 4,\ 2^n < n!$

(b) There may be more than one base case, e.g.:

If (Base case) $P(0), P(1), ..., P(k)$

and (Induction Step)

$$\forall n \geq k[P(n) \rightarrow P(n+1)]$$

then $\forall n P(n)$

Definition by Recursion

A function $f : \mathbb{N} \rightarrow A$ (for some set A) can be defined by recursion:

$f(0)$ is defined **explicitly** [Base case]

and $\forall n$, $f(n+1)$ is defined from $f(n)$ [Recursive case]

Alternately, one can have > 1 base cases, (e.g. $0, 1, ..., k$) and for $n \geq k,\ f(n+1)$ can be defined from $f(0), f(1), ..., f(n)$.

Example:

Define, by **recursion** on n:

(1) $f(m,n) = m+n$

(2) $f(m,n) = m \times n$

(3) $f(m,n) = m^n$

(4) $f(n) = n!$

Note:

For (1) - (3), assume you only have 0 and the **successor** operation, $S(n) = n+1$