VE203 Review Class Week 7

Tianyi Ge

Fall 2018

Outline

Pure Set Theory

- The only objects are sets
- Like $\{\emptyset\}$, $\{\{\emptyset\},\emptyset\}$, etc.

Definition

Let V be the set of all sets. L is the set of all sets that have $\emptyset$ as a member.

$$L = \{x \in V | \emptyset \in X\}$$

- $(L, \subseteq)$ is a complete lattice because every subset $A \subseteq L$ has both l.u.b. $(\bigvee A)$ and g.l.b $(\bigwedge A)$.

Successor Operation

Definition

$S : V \to V$,

$$S(x) = x \cup \{x\}, \quad \forall x \in V$$

Definition

$F : L \to L$,

$$F(A) = A \cup S''A, \quad \forall A \in L$$

- Successor operation operates sets (object-level).
- F treats A the set of sets (set-level).
- E.g. $S(\emptyset) = \emptyset \cup \{\emptyset\} = \{\emptyset\}$
- E.g. $F(\{\emptyset\}) = \{\emptyset\} \cup \{S(\emptyset)\} = \{\emptyset, \{\emptyset\}\}$

A flawed definition of $\mathbb{N}$

- Further, F is order-preserving.
- According to *Tarski-Knaster Theorem*, F has at least a fixed point, i.e. $F(X) = X \cup S''X = X$.
- In other words, if you take arbitrary element x in X and do successor operation once, you will find that the result $S(x)$ is still in X.
- We define the $\subseteq -$least fixed point as $\mathbb{N}_{def}$.

$$
\begin{aligned}
0 &:= \emptyset \\
1 &:= S(\emptyset) = \{\emptyset\} \\
2 &:= S(S(\emptyset)) = \{\emptyset, \{\emptyset\}\} \\
&\vdots
\end{aligned}
$$

A flawed definition of $\mathbb{N}$

Example

$$\{0,1,2\} \Leftrightarrow \boldsymbol{\{\emptyset,\{\emptyset\},\{\emptyset,\{\emptyset\}\}\}}$$
$$F(\{0,1,2\}) = \{0,1,2,3\}$$

- To get 3, we treat the current set $\{0,1,2\}$ as the new element and put it into our new set.

$$\begin{array}{rl} 3 \Leftrightarrow & \boldsymbol{\{\emptyset,\{\emptyset\},\{\emptyset,\{\emptyset\}\}\}} \\ & \Downarrow \\ \{0,1,2,\mathbf{3}\} \Leftrightarrow \{\emptyset,\{\emptyset\},\{\emptyset,\{\emptyset\}\}, & \boldsymbol{\{\emptyset,\{\emptyset\},\{\emptyset,\{\emptyset\}\}\}} \quad \} \end{array}$$

- The natural number matches the cardinality of the corresponding set

A flawed definition of $\mathbb{N}$

- Now we know that $F(\mathbb{N}_{def}) = \mathbb{N}_{def}$
- $\mathbb{N}_{def}$ is the $\subseteq$-least fixed point, which means any other fixed point X ($\emptyset \in X$) satisfies that $\mathbb{N}_{def} \subseteq X$.

Theorem

The order $\leq$ is a well ordering of $\mathbb{N}_{def}$.

Theorem

$\mathbb{N}_{def}$ satisfies the principle of induction: If a property $P(x)$ is such that $P(0)$ holds, and for all n N def, if $P(n)$ holds, then $P(n+1)$ holds, then for all $n \in \mathbb{N}_{def}$, $P(n)$ holds

Principle of Induction in $\mathbb{N}_{def}$

- If principle of induction does not hold, then for some $n \in \mathbb{N}_{def}$ $P(n)$ does not hold.

Proof.

Let $A = \{n \in \mathbb{N}_{def} | P(n)\} \subset \mathbb{N}_{def}$, also $\emptyset \in A$. Thus A becomes the least fixed point rather than $\mathbb{N}_{def}$. $\square$

Steps for Induction

Steps

1. Define the property $P(n)$ properly.
2. Show that $P(n_0)$ holds. n_0 is not necessarily 0.
3. Show that $\forall n \in \mathbb{N}$ with $n \geq n_0$, $P(n) \Rightarrow P(n+1)$. Use the result from $P(n)$ to derive $P(n+1)$.
4. Conclusion.

Strong Induction

Steps

1. Define $A(n)$ properly.
2. Show that $A(n_0)$ holds.
3. Show that $\forall n \geq n_0$, if for all $n_0 \leq k \leq n$, $A(k)$ holds, then $A(n+1)$ holds.
4. Conclusion.

- Strong induction allows using all the proved previous conclusions to derive the next, rather than only the previous one.

Recursive Defined Functions

1. $f(0) = n_0$ (initial condition).
2. $G(n, f(n)) = (n+1, f(n+1))$ (rule).
3. $X = \{R \in \mathcal{P}(\mathbb{N} \times \mathbb{N}) | (0, n_0) \in R\}$
4. X is a complete lattice because arbitrary set $A \subseteq X$ satisfies that $\bigwedge A = \bigcap A$ and $\bigvee A = \bigcup A$ ($(0, n_0) \in \bigcap A$).
5. $F : X \to X$ with $F(R) = R \cup G" R$ is order preserving ($R \subseteq T \Rightarrow F(R) \subseteq F(T)$).
6. There exists a least f in X s.t. $F(f) = f \cup G" f = f$ (why least?).
7. Thus f represents $\{(0, f(0)), (1, f(1)), \ldots\}$.

Structural Induction

Definition

- A is $\subseteq$-least, $B \subseteq A$, A is closed under $C_1, \cdots, C_n$.
- For all $b \in B$, P(b) holds
- For all $a_1, \cdots, a_m$ and c and $1 \leq i \leq n$, if $P(a_1), \cdots, P(a_m)$ all hold and c is obtained from $a_1, \cdots, a_m$ by a single application of C_i, then $P(c)$ holds

- Use part of the proved conclusions to derive the next one. The index of next conclusion is determined by some defined principle C_i.

Outline

Subsets of size k

Definition

Let A be a finite set and $0 \leq k \leq |A|$, then

$$\mathscr{P}_k(A) = \{x \in \mathscr{P}(A) | |x| = k\}$$

Definition

$$\binom{n}{k} = |\mathscr{P}_k([n])|, \quad 0 \leq k \leq n$$

- The notation $\binom{n}{m}$ is more powerful than C_n^m.
- Please notice the order of n and m.

Pascal's Triangle

Lemma

For all $n \in \mathbb{N}$ *and for all* $0 \leq k \leq n$, $\binom{n}{k} = \binom{n}{n-k}$

Theorem

For all $n \in \mathbb{N}$ *and for all* $0 \leq k \leq n$,

$$\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$$

- To understand the proof, imagine that you pick a special item and split the items to two parts.

Binomial Theorem

Theorem

For $n \in \mathbb{N}$ with $n \geq 1$,

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$$

- You can prove by induction.

Corollary

$$(1+y)^n = \sum_{k=0}^{n} \binom{n}{k} y^k$$

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n$$

Other finite sets

Theorem

$$|\mathscr{P}_n([2n])| = \sum_{k=0}^{n} \binom{n}{k}^2$$

- To understand the proof, remind *Cauchy Product*.

Theorem

$$|\mathscr{P}([n])| = 2^n$$

Counting

Theorem

The number of solutions to the equation $x_1 + \cdots + x_n = r$ *with* $x_1, \cdots, x_n \in \mathbb{N}$ *is*

$$\binom{n+r-1}{r}$$

Proof.

Construct a bijection between the set of solutions and $\mathscr{P}_{n-1}([n+r-1])$

$$F(x_1, \cdots, x_n) = \{x_1, x_1 + x_2 + 1, \cdots, n - 2 + \sum_{i=1}^{n-1} x_i\}$$

Only consider the subsets of size $n-1$ because x_n is automatically determined after the first $n-1$ variables are determined. $\square$

Counting

- Of course many other methods to prove this are available.
- What if $x_1, \cdots, x_n \in \mathbb{N} \backslash \{0\}$?

Example

Prove that if $x_i > 0$, the number of solutions to

$$x_1 + \cdots + x_n = r$$

is equal to

$$\binom{2n + r - 1}{r + n}$$

- Hint: denote $y_i = x_i - 1$

Counting

- The problem of $x_1 + \cdots + x_n = r$ is equivalent to deliver r items into n different parts.

Theorem

Let $n \in \mathbb{N}$ and $0 \leq k \leq n$. The number of of ordered k-tuples of distinct elements of $[n]$ is

$$\binom{n}{k} k!$$

- An advanced tool called Generating functions ($\hookleftarrow$*Hyperlink*) will greatly enhance your counting abilities. Maybe it will help you with assignments.
- *Hyperlink*$\hookrightarrow$ Ordinary generating functions
- *Hyperlink*$\hookrightarrow$ Exponential generating functions

Generating Functions (Extra Part)

- You are not required to understand this page. Only for interests.

Example

If we have many coins. 5 of \$1, 3 of \$2, 2 of \$5. How many compositions do we have to get \$15?

Solution

We define the *Ordinary Generating Function* for each type of coins:

$$G_1(x) = 1 + x + x^2 + x^3 + x^4 + x^5$$
$$G_2(x) = 1 + x^2 + x^4 + x^6$$
$$G_5(x) = 1 + x^5 + x^{10}$$

The answer is the **coefficient** in front of the term x^{15} in the expansion of $G_1(x)G_2(x)G_5(x)$

Generating Functions (Extra Part)

Solution (continued.)

$$
\begin{aligned}
&G_1(x)G_2(x)G_5(x)\\
=&(1+x+x^2+x^3+x^4+x^5)(1+x^2+x^4+x^6)(1+x^5+x^{10})\\
=&1+x+2x^2+2x^3+3x^4+4x^5+4x^6+\cdots+4x^{15}+\cdots+x^{21}
\end{aligned}
$$

Thus there are 4 compositions in total.

- Although it seems tedious, it's extremely useful when you have infinite coins:

$$G_1(x)=1+x+x^2+x^3+\cdots=\frac{1}{1-x}$$

- *Exponential Generating Function* is even more interesting.

Outline

Groups

Figure: The Big Bang Theory Season 11

Groups

Definition

A group is a pair $(G, \cdot)$ where G is a set and $\cdot : G \times G \to G$, called the group operation and pronounced as the product", that satisfies:

- $x \cdot (y \cdot z) = (x \cdot y) \cdot z$
- There exists an **identity** $e \in G$ such that for all $x \in G$

$$x \cdot e = e \cdot x = x$$

  and for all $x \in G$, there exists the inverse of x: $y \in G$ such that

$$x \cdot y = y \cdot x = e$$

- $\cdot$ is essentially a function and closed on G.
- Is it possible to have two identities? Two inverses?

Abelian Groups

Definition

Let $(G, \cdot)$ be a group, then $(G, \cdot)$ is Abelian if for all $x, y \in G$,

$$x \cdot y = y \cdot x$$

Example

- $(\mathbb{Q} \backslash \{0\}, \cdot)$ is an abelian group.
- Let $X = \{x \in \mathbb{C} \mid |x| = 1\}$. $(X, \cdot)$ is an abelian group.
- Let $X = \{f : \mathbb{R} \to \mathbb{R} \mid f(x) = ax, a \neq 0\}$. $(X, \circ)$ is an abelian group.
- Let $X = \{M$ is a matrix $\mid M$ is a square matrix with size $n \times n\}$. Is $(X, \cdot)$ a group? What if only inversible $M_{n \times n}$?

Algebra in Groups

Lemma

Let $(G, \cdot)$ be a group. If $a, b, c \in G$ and $a \cdot b = a \cdot c$, then $b = c$.

- Cancellation Law

Corollary

Let $(G, \cdot)$ be a group and $a \in G$. If $a \cdot a = a$, then $a = e$

Symmetric Groups

Definition

Let $X = \{f : [n] \to [n] | f \text{ is a bijection}\}$. $(X, \circ)$ is called the symmetric group on n elements and is written as S_n.

- *Cycle Notation* is used to clearly indicate a bijection.
- The Composition of bijections is still a bijection. Using cycle, we see $(k_1 \cdots k_m)(p_1 \cdots p_q)$ ($\circ$ is usually omitted).
- Thus, the multiplication between cycles is essentially the compositions of functions.

Cycles

Example

If $f \in S_6$ is defined as

$$
\begin{aligned}
0 &\to 4 \\
1 &\to 5 \\
2 &\to 0 \\
3 &\to 3 \\
4 &\to 2 \\
5 &\to 1
\end{aligned}
$$

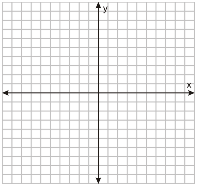
Then f is written as $(15)(042)$. However, it's not the only expression.

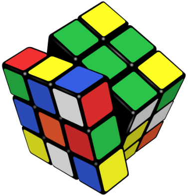
- E.g. $(15)(02)(04)$, $(15)(042)(34)(34)$, $(15)(024)(024)$, $\cdots$

Other Groups in Our Life

Example

- If you have a horse on an infinite $x - y$ map and encode all the eight directions that the horse can go...
- If you are interested in rubik's cube, you will find that each formula is a cycle, which is a bijection of several cubes from one position to another. The identity is the initial status.





The End

Thank You!