Math 2001. Introduction to Discrete Mathematics

06.01.2022.

Course Information:

Instructor: Tianyuan Xu (Eddy) Math 202.

Topics: Basic set/logic theory, enumeration techniques, useful/typical proof methods

Website: https://math.colorado.edu/~tixu6187/2001s22.html

— Lecture summaries, notes, hw and other materials will be posted under "LECTURES"

— has the Canvas link too.

Office Hours: By appointment.

Grading: HW 30%, Midterms 20% × 2, Final Exam 30%

HW:
- Posted on the website under "LECTURES".
- due on Fridays and Tuesdays at 11:59 pm
- the deadline is strict.
- to be submitted in pdf form at Canvas/Assignment

Textbook: Book of Proof, by Richard Hammack

(in Canvas/Files and on the course website)

Today:

1. Basic Notions (for sets)

Def:
- (set & element) A <u>set</u> is a collection of objects. The objects are called <u>elements</u> of the set.
- (finiteness) A set is <u>finite</u> if it contains a finite number of (distinct) <u>elements</u>, and is <u>infinite</u> otherwise.

  "elt's"
- (Cardinality) The number of elts in a set A is called the <u>cardinality</u> of the set and denoted by $|A|$.

Notation: To express an object a is an elt in a set A, we write $a \in A$.

e.g. $1 \in \{1, 2\}$; $3 \notin \{1, 2\}$.

Notation: We often write a set in one of two forms:

(1) list all elts and enclose them in a pair of braces $\{ \quad \}$.

e.g. $\{1, 2, 3, 4\}$ is a finite set of cardinality 4.

(2) in the form $\{\text{expression} \underset{=}{:} \text{rules}\}$ or $\{\text{expression} \underset{=}{|} \text{rules}\}$.

the set builder notation

e.g. $\{2n \mid n \text{ is an integer}\}$ is the set of all even integers.

$= \{\ldots, -6, -4, -2, 0, 2, 4, 6, \ldots\}$

E.g. · (The empty set) We allow the empty set $\{ \}$, a set containing no elts.

We denote the empty set by ϕ. (so $|\phi| = 0$.)

· (number systems) We will use $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ to stand for the sets of all integers, rational numbers, real numbers, respectively.

- $\{ \underbrace{n \in \mathbb{Z}}_{\text{expression}} \mid \underbrace{0 < n < 5}_{\text{rule}} \} = \{1, 2, 3, 4\}$

- $\{ x \in \mathbb{R} \mid x^2 = 2 \} = \{ \sqrt{2}, -\sqrt{2} \}$

- $\{ n \in \mathbb{Z} \mid |n| < 3 \} = \{ -2, -1, 0, 1, 2 \}$

- Recall that $\mathbb{Q} = \{ x \in \mathbb{R} \mid x = \frac{m}{n}$ for some $m, n \in \mathbb{Z}$ and $n \neq 0 \}$.

Later: we'll prove that $\sqrt{2} \notin \mathbb{Q}$, i.e., that

we cannot write $\sqrt{2}$ in the form $\frac{m}{n}$ for any $m, n \in \mathbb{Z}$

with $n \neq 2$.

[So $\mathbb{Q}$ is "strictly smaller than" $\mathbb{R}$.)

2. Subsets and equality of sets

Def: A subset of a set A is a set B consisting (only) of objects from A, i.e., a set B s.t. (such that) every elt of B is an elt of A.

Two different notations:

set don't have to be "homogeneous".

- "elt in set": we write "$a \in A$" to mean that a is an elt of A.

  e.g. $1 \in \{1,2,3,4\}$, $\{2\} \in \{1, \{2\}\}$ ✓

- "set contained in a set": we write $B \subseteq A$ to mean that B is a subset of A, e.g. $\{1\} \subseteq \{1,2,3,4\}$, $\{2\} \subseteq \{1,2,3,4\}$, $\{2,3\} \subseteq \{1,2,3,4\}$

  $\{2\} \not\subseteq \{1, \{2\}\}$ because $2 \notin \{1, \{2\}\}$.

E.g. If $A = \{3, 5, \{-2, 3\}\}$, then $|A| = 3$, $\{5\} \notin A$, $\{-2,3\} \in A$, $\{3,5\} \subseteq A$.

Upshot about $\in$ vs. $\subseteq$: · To check $a \in A$, either inspect if a appears in A if A is listed or check that a satisfies the defining rule for A if A is given in the set-builder notation (e.g. $6 \in \{2n \mid n \in \mathbb{Z}\}$ because $4 = 2 \cdot 3$ and $3 \in \mathbb{Z}$).

· To check $B \subseteq A$, check that for every elt $b \in B$, we have $b \in A$.

Def: We say two sets A, B are <u>equal</u> if they contain the same elts.

Equivalently, A and B are equal if every elt of A is in B and every elt of B is in A.

Equivalently, A and B are equal if $A \subseteq B$ and $B \subseteq A$.

$\downarrow$

Point: We'll often need to prove two sets A, B are equal. To do so, we'll often prove $A \subseteq B$ and $B \subseteq A$.

Example: (A nontrivial set equality)

Let $A = \{2a+5b \mid a, b \in \mathbb{Z}\}$

e.g. $a=1, b=1,\ 2a+5b = 2\cdot 1+5\cdot 1 = 7$

$a=1, b=2,\ 2a+5b = 2\cdot 1+5\cdot 2 = 12$

$a=-1, b=1,\ 2a+5b = 2\cdot(-1)+5\cdot 1 = 3 \ldots$

"every number of the form $2a+5b$ where a, b are integers is an integer"

easier

Proposition: $A = \mathbb{Z}$.

Analysis: We'll prove the proposition by proving $A \subseteq \mathbb{Z}$ and $\mathbb{Z} \subseteq A$.

"every integer is of the form $2a+5b$ for some integers a, b".

harder.

0? $\quad 0 = 2\cdot\underset{a}{\underline{5}} + 5\cdot(\underset{b}{\underline{-2}})$ ✓

1? $\quad 1 = 2\cdot 3 + 5\cdot(-1)$ ✓

$k = 2\cdot(3k) + 5\cdot(-1\cdot k)$

Pf: We show $A \subseteq \mathbb{Z}$ and $\mathbb{Z} \subseteq A$.

(i) ($A \subseteq \mathbb{Z}$) Let x be an arbitrary elt in A. Then by def of A, we have $x = 2 \cdot a + 5 \cdot b$ for some integers a, b. Since the product of two int. is always another int., $2 \cdot a$ and $5 \cdot b$ are int.

Since the sum of two int. is always an int, it further follows that $2 \cdot a + 5 \cdot b \in \mathbb{Z}$. i.e., $x \in \mathbb{Z}$.

It follows that $A \subseteq \mathbb{Z}$.

(2) ($\mathbb{Z} \subseteq A$). Let k be any elt of $\mathbb{Z}$. ie., suppose $k \in \mathbb{Z}$.

(Using the trick we observed:) Then $3k \in \mathbb{Z}$, $-k \in \mathbb{Z}$, and $k = 2\cdot(3k) + 5\cdot(-k)$,

so k is of the form $2a+5b$, namely for int. $a = 3k$, $b = -k$. so $k \in A$.

It follows that $\mathbb{Z} \subseteq A$.

By (1) and (2), we conclude that $A = \mathbb{Z}$. $\square$

3. Cartesian products of sets

Def: The Cartesian product of two sets A and B is the set

$$A \times B \underset{\text{def.}}{:=} \{ (a,b) \mid a \in A,\ b \in B \}$$

More generally, the Cartesian product of a sequence of sets $A_1, A_2, \ldots, A_k$ is the set

$$A_1 \times A_2 \times \cdots \times A_k := \{ (a_1, a_2, \ldots, a_k) \mid a_i \in A_i \text{ for every } 1 \le i \le k \}.$$

Eg. (Menu example) Let $A = \{\text{burger}, \text{pizza}, \text{hotdog}\}$. $B = \{\text{Coke}, \text{Sprite}\}$.

Then

$$A \times B = \left\{ \begin{matrix} (\text{burger}, \text{Coke}), (\text{pizza}, \text{Coke}), (\text{hotdog}, \text{Coke}) \\ (\text{burger}, \text{Sprite}), (\text{pizza}, \text{Sprite}), (\text{hotdog}, \text{Sprite}) \end{matrix} \right\}$$

In particular, if A and B describe the food and drink options at a restaurant, then $A \times B$ describe the food-drink combo options.

E.g. (Dice Example) Think of the set $S = \{1, 2, 3, 4, 5, 6\}$ as the set of possible outcomes when you throw and read a dice. Then

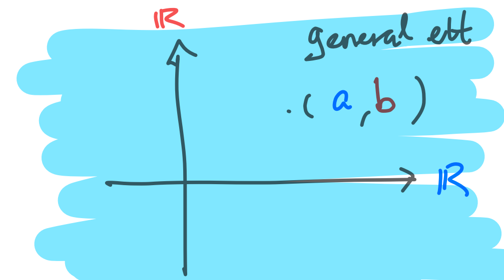
$$S \times S = \{ (s_1, s_2) \mid s_1 \in S,\ s_2 \in S \} = \left\{ \begin{matrix} (1,1), & (1,2) & \cdots & (1,6) \\ (2,1) & \cdots & & \cdots \\ \cdots & \cdots & & (6,6) \end{matrix} \right\}$$

encodes the possible outcomes of throwing and reading a dice twice in a row.

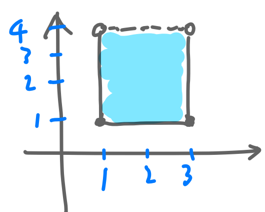
$$A \times B = \{ (a,b) \mid 1 \le a \le 3,\ 1 \le b < 4 \}$$

E.g. $\mathbb{R}^2$ and $[1,3] \times [1,4) \subseteq \mathbb{R}^2$.

Def: $\mathbb{R}^2$ stands for $\mathbb{R} \times \mathbb{R}$, visualized as



$A \times B$:



Note: From the menu and dice examples, we note the following

Prop: For any sets A, B, we have $|A \times B| = |A| \cdot |B|$.

More generally, for any sets $|A_1 \times A_2 \times \cdots \times A_k| = |A_1| \cdot |A_2| \cdot \cdots \cdot |A_k|$.

In particular, the product $A_1 \times A_2 \times \cdots \times A_k$ is finite if and only if (precisely when) $A_1, A_2, \ldots, A_k$ are all finite.

Rmk: Taking the Cartesian product of a set A with itself gives Cartesian powers

$$A^k := \underbrace{A \times A \times \cdots \times A}_{k \text{ times}} \quad \text{for any positive int. } k.$$

4. Power set of sets

Def: The <u>power set</u> of a set A is the set of all subsets of A.

We denote the power set of A by $\mathcal{P}(A)$.

E.g. $A = \{1, 2\} \Rightarrow \mathcal{P}(A) = \{\phi, \{1\}, \{2\}, \{1, 2\}\} \Rightarrow |\mathcal{P}(A)| = 4.$

Note: We have $\phi \subseteq A$ for every set A.

Q: What is $|\mathcal{P}(A)|$ in general?

Is it related to / determined by $|A|$?

Meta Q: How do we approach this question?

$\rightarrow$ start with "small" (baby) examples!

Baby cases:

- $|A| = 0$, i.e. $A = \phi$. $\Rightarrow P(A) = \{\phi\}$. $\Rightarrow |P(A)| = 1$
- $|A| = 1$, say $A = \{a\}$ $\Rightarrow P(A) = \{\phi, \{a\}\}$ $\Rightarrow |P(A)| = 2$
- $|A| = 2$, say $A = \{a, b\}$ $\Rightarrow P(A) = \{\phi, \{a\}, \{b\}, \{a, b\}\}$ $\Rightarrow |P(A)| = 4$
- $|A| = 3$, say $A = \{a, b, c\}$ $\Rightarrow P(A) = \left\{ \begin{array}{c} \phi, \{a\}, \{b\}, \{c\} \\ \{a,b\}, \{a,c\} \{b,c\} \\ \{a, b, c\}. \end{array} \right\}$ $\Rightarrow |P(A)| = 8$.
- $|A| = 4$ $\xrightarrow{\text{Ex.}}$ $\Rightarrow |P(A)| = 16$.

Conjecture: $|P(A)| = 2^{|A|}$. Q: Can you prove the conjecture?