Last time

Finish RSA

Today

- Module 3: Counting/Combinatorics
  - Sets & set operations

Next time

- Basic rules for counting

Motivating Example: Password Spaces

4-digit PIN: $10{,}000 = 10^4$

4- lower case chars: $26^4 = 456{,}976$

4- upper or lower case chars: $52^4 = 7{,}311{,}616$

NSF passwords: 7 to 10 chars

upper, lower case letters

digits

≥ 2 letters

≥ 2 digits

Sets:

$S_1 = \{0000, 0001, 0002, \ldots, 9999\}$ 4-digit PINs

$S_2 = \{red, blue, green, yellow\}$

$= \{blue, green, yellow, red\}$

Common sets:

$\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ natural numbers

$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ integers

$\mathbb{Z}^+ = \{1, 2, 3, \ldots\}$ positive integers

$\mathbb{Q} = \{p/q \mid p \in \mathbb{Z}, q \in \mathbb{Z}, q \neq 0\}$ rationals

$\{v \mid \text{conditions on } v\}$

$\mathbb{R} =$ real numbers

$\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ int. mod n

$\emptyset = \{\}$ empty set

Set Builder Notation

$S = \{ v \mid \text{conditions on } v \}$

$3 \in S$

$7 \notin S$

"element of"

"not element of"

e.g. $S = \{ x \mid x \in \mathbb{Z},\ |x| < 5 \}$

what is S? $S = \{-4, -3, -2, -1, 0, 1, 2, 3, 4\}$

Cardinality : size of set

$|S| =$ "size" of set S

$= 9$

cardinalities can be finite – e.g. $|S| = 9$

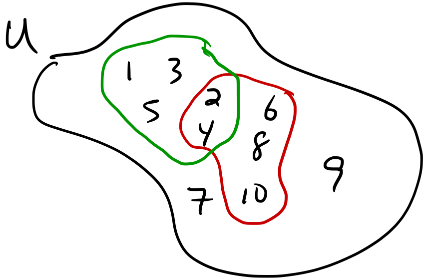
or infinite – e.g. $|\mathbb{N}|, |\mathbb{Z}|, |\mathbb{Q}|, |\mathbb{R}|$

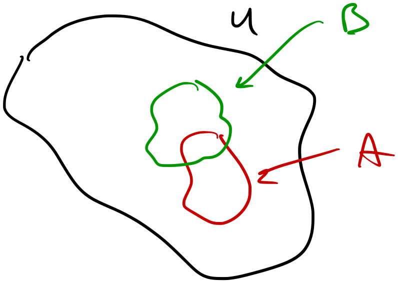
Venn Diagram

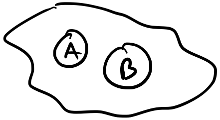
$U = \{1, 2, 3, \ldots, 10\}$

A = "evens" = $\{x \mid x \in U, x \text{ is even}\} = \{2, 4, 6, 8, 10\}$

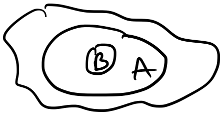
B = "≤ 5" = $\{x \mid x \in U, x \leq 5\} = \{1, 2, 3, 4, 5\}$







<u>Def.</u> A & B are <u>disjoint</u> if A & B share no elements in common, i.e. they have empty intersection.

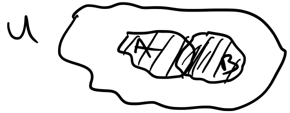


<u>Def.</u> B is a <u>subset</u> of A if every element of B is an element of A. $B \subseteq A$

$A \subseteq A$

<u>Def:</u> Proper subset $B \subset A$: $B \subseteq A$ <u>and</u> A contains other elements

Set opertions



$U = \{1, 2, \ldots, 10\}$

$A = \{2, 4, 6, 8, 10\}$

$B = \{1, 2, 3, 4, 5\}$

① Unions

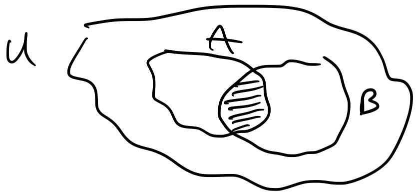
$$A \cup B = \{x \mid x \in A \ \underline{\text{or}}\ x \in B\}$$

$A \cup B = \{1, 2, 3, 4, 5, 6, 8, 10\}$

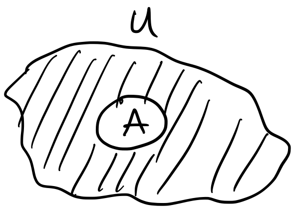
② Intersection

$$A \cap B = \{x \mid x \in A \ \underline{\text{and}}\ x \in B\}$$

$A \cap B = \{2, 4\}$



③ Complement



$$\overline{A} = \{x \mid x \in U \text{ and } x \notin A\}$$

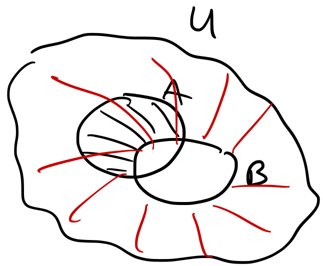
$\overline{A} = \{1, 3, 5, 7, 9\}$

$\overline{B} = \{6, 7, 8, 9, 10\}$

Set Difference

$$A - B = \{ x \mid x \in A \text{ and } x \notin B \}$$

$$= A \cap \overline{B}$$

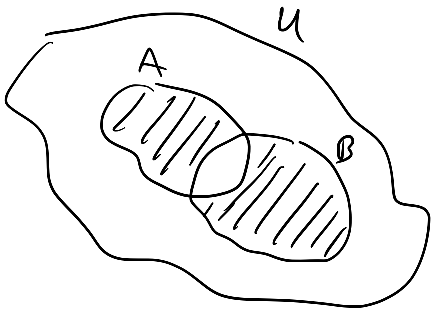


Symmetric Difference

$$A \,\Delta\, B = \{ x \mid (x \in A \text{ and } x \notin B) \text{ or } (x \in B \text{ and } x \notin A) \}$$

$$= (A - B) \cup (B - A)$$

$$= (A \cap \overline{B}) \cup (B \cap \overline{A})$$



also... $= (A \cup B) - (A \cap B)$

$$= (A \cup B) \cap \overline{(A \cap B)}$$

Power Set

$$\mathcal{P}(A) = \text{set of all subsets of } A$$

$$A = \{\overset{1}{a}, \overset{1}{b}, \overset{0}{c}\}$$

$$\mathcal{P}(A) = \{\overset{000}{\emptyset}, \overset{100}{\{a\}}, \overset{010}{\{b\}}, \{c\}, \{a,b\}, \{a,c\}, \{b,c\}, \{a,b,c\}\}$$

$$|\mathcal{P}(A)| = 2^{|A|}$$