Transition: DS + Algorithms

Proofs +
Sets

Recap

Worksheet - how did it go?

Next 3 readings posted

HW1 - coming!

Last time: Proofs

① If n is div by 6, then n is div by 3.

look up dfn!

direct:

n is div by 6

$\Rightarrow \exists k \in \mathbb{Z}$ s.t. $6k = n$

So: $n = 6k$

$= 2 \cdot 3 \cdot k$

$= 3 \cdot (2k)$

so let $\ell = 2k \in \mathbb{Z}$

then $n = 3 \cdot \ell$, $\ell \in \mathbb{Z}$

$\Rightarrow n$ is div by 3 $\blacksquare$

If n is div by 3, it is div by 6

F: need an n that is div by 3, but <u>not</u> 6.

Let $n = 21$ $\square$

Two way implications

Example: For any $n \in \mathbb{Z}$,

$$n \text{ is odd} \iff n^2 \text{ is odd.}$$

- Here, $\iff$ reads as "if and only if"
- Sometimes written $p \leftrightarrow q$

so $(p \to q) \wedge (q \to p)$

How to prove:

Let's try:

For any $n \in \mathbb{Z}$,
n is odd $\Longleftrightarrow$ n^2 is odd.

Proof:

$\underline{\Longrightarrow}$:

$\underline{\Longleftarrow}$:

Proof by contradiction: (or indirect proof)

Recall that a contradiction is a logical statement which is always false

Ex: $\left.\begin{array}{l} 2=1 \\ x=x+1 \end{array}\right\}$ F

Consider $p \to q$:

p	q	$p \to q$
T	T	T
T	F	F
F	T	T
F	F	T

Bad row: want to exclude.

so: $p \wedge \neg q$ is thing to avoid!

Proof by contradiction:
Assume $p \wedge \neg q$, then show some logical contradiction exists.

Example: $\forall n$, If n^2 is even, then n is even.

Assume $\forall n$, n^2 is even, but n is odd.

$n^2 = 2k$ and $n = 2l+1$, $k, l \in \mathbb{Z}$

$$n^2 = (2l+1)^2 = 4l^2 + 4l + 1 \quad = 2k$$
$$= 2\underbrace{(2l^2+2l)}_{\text{integer}}+1$$

$\Rightarrow n^2$ is odd (by defn)

but: $n^2 = 2k \rightarrow$ even.

contradiction

Another:

Prove that $\overbrace{\sqrt{2} \text{ is irrational.}}^{P}$

Recall: x rational means

$\exists a,b \in \mathbb{Z}$ s.t. $x = a/b$

integers

$1/2$, $5/3$, .. $4/2 = 2/1$ $\frac{6}{9} = \frac{2}{3}$

If $\sqrt{2}$ is irrational:

$\exists a,b \in \mathbb{Z}$ s.t. $\sqrt{2} = \frac{a}{b}$.

$\Leftrightarrow \forall a,b,\ \sqrt{2} \neq a/b$

Reduced form: cancel common divisors

↳ if x is rational, $x = a/b$ and

a & b have no common divisors

Proof: assume $\sqrt{2}$ is rational, + then make a contradiction

$$\Rightarrow \sqrt{2} = a/b, \quad a, b \in \mathbb{Z} \text{ + no common divisors}$$

Math: square both sides,

$$2 = a^2/b^2 \Rightarrow 2(b^2) = a^2 \quad \#1$$

$$\Rightarrow a^2 \text{ is even} \Rightarrow \boxed{a \text{ is even}}$$

$\exists k$, s.t. $2k = a$

$$2b^2 = a^2 = (2k)^2$$

$$\cancel{2}b^2 = \cancel{4}^{2}k^2 \Rightarrow b^2 = 2k^2 \Rightarrow b^2 \text{ is even}$$

$$\Rightarrow \boxed{b \text{ is even}} \quad \#2$$

2 is a divisor of both a + b

$\sqrt{2} = a/b$ $a=2k$, $b=2l$ both even

cancel the 2:

$\sqrt{2} = k/l$ repeat!

k is even & l is even

a & b would need ∞ # of 2 divisors.

Assume $\exists\, a, b \in \mathbb{Z}$ s.t.

$$2a + 4b = 7$$

need to derive a contradiction

$$2(a + 2b) = 7$$

7 is even $\lightning$

$7 = 2 \cdot 3 + 1 \longrightarrow$ odd

$$\neg(\exists\, a, b \;\; 2a + 4b = 7)$$

$$\underset{\text{negation}}{\equiv} \forall\, a, b \;\; 2a + 4b \neq 7$$

$\forall a, b \quad P(a,b) \to Q(a,b)$

Contrapositive: $\forall a, b \quad \neg Q(a,b) \to \neg P(a,b)$

$p \to q$

$\neg q \to \neg p$

Sets

<u>Unordered</u> collections.

Vs ordered sets (or tuples) $(1,2) \neq (2,1)$

<u>Ex</u>: $\{1,3,5,7\} = \{1,3,1,5,5,7\}$

$\phi = \{\}$ empty set

$\{1,2,3,\ldots,100\}$ pattern $\{1,2,\ldots 8\}$

$\{n^2 \mid n \in \mathbb{N}\} = \{n^2 : n \in \mathbb{N}\} = \{1,4,9,16,\ldots\}$

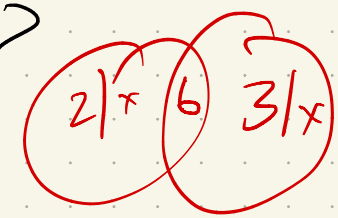
$\{x^2+y^2 \mid x,y \in \mathbb{Z}\}$

$\{\phi, \{1,2\}, \{1\}, \{2\}\}$

Cardinality & repetition:

For any set, we don't count with multiplicity.

So: $\{x : 2|x \ \underline{\text{or}}\ 3|x\}$



$= \{2, 3, 4, 6, 8, 9, 10, 12, \dots\}$

The size of a set S = # of <u>distinct</u> elements.

So $|\{1, 2, 3, \cancel{2}, 5, \cancel{1}\}| = 4$

Subsets

$$X \subseteq Y \overset{\text{dfn}}{\iff} \forall x,\ x \in X \to x \in Y.$$

Examples:

- $\{1, 3, 5\} \subseteq \{1, 2, 3, \dots, 100\}$

- $\emptyset \subseteq \{1, 2, 3\}$

Why? $\forall x \in \emptyset,$ need it in $\{1,2,3\}$

also

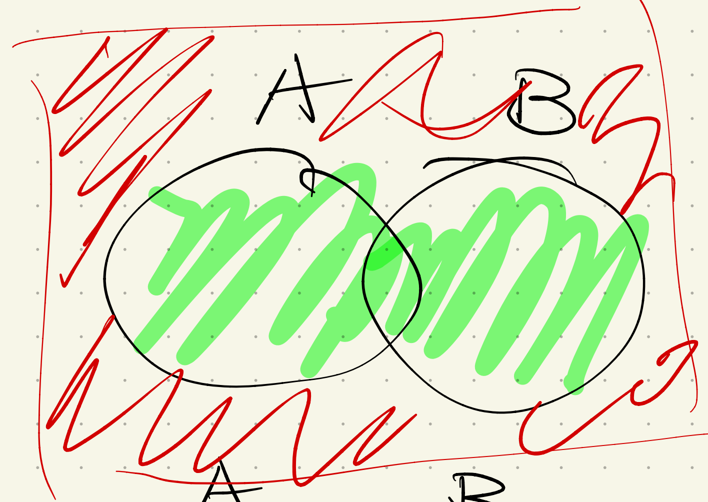
$$A \cup \emptyset = A$$

Union:

$$A \cup B = \{x \mid x \in A \lor x \in B\}$$

or

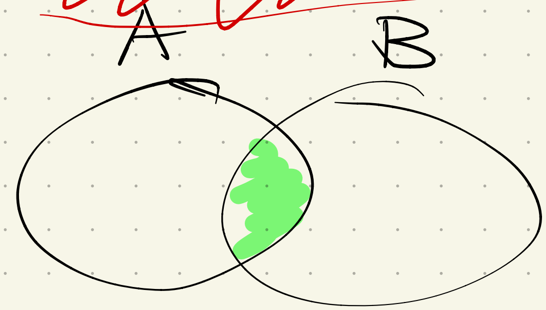
$\overline{A \cup B}$



Intersection

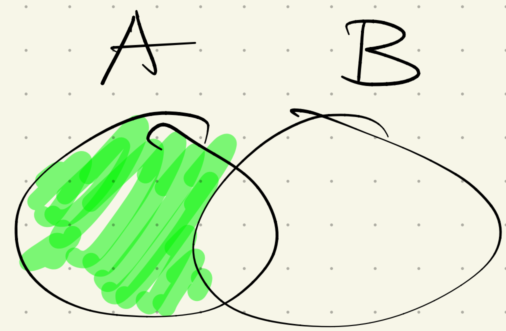
$$A \cap B = \{x \mid x \in A \land x \in B\}$$

and



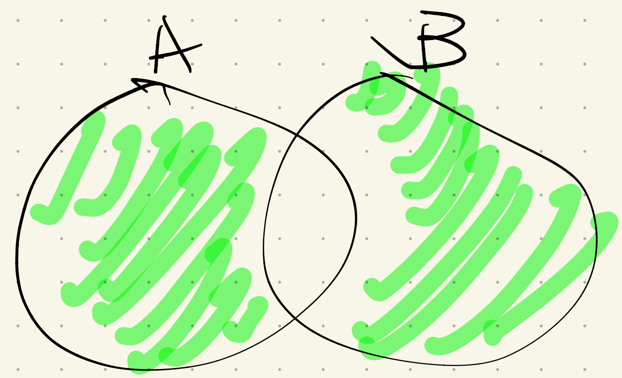
Set difference

$$A - B \text{ (or } A / B) = \{x \mid x \in A \land x \notin B\}$$



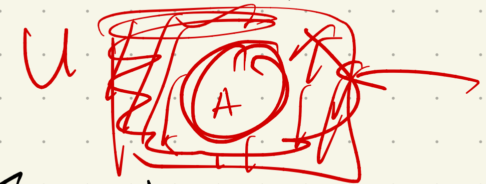
Symmetric difference

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



DeMorgan (+ operations) $\forall A, B \subseteq U$,

$\overline{A \cup B} = \bar{A} \cap \bar{B}$ + $\overline{A \cap B} = \bar{A} \cup \bar{B}$



How to prove?

First, complement $\bar{A} = \{x \mid x \notin A\}$

Prove $X = Y$: show $X \subseteq Y$ and $Y \subseteq X$

1. Show $\overline{A \cup B} \subseteq \bar{A} \cap \bar{B}$

Take $x \in \overline{A \cup B}$, show in $\bar{A} \cap \bar{B}$

$x \notin A \cup B \Rightarrow x \notin A$ and $x \notin B$

rewrite: $x \in \bar{A}$ and $x \in \bar{B} \Rightarrow x \in \bar{A} \cap \bar{B}$

② Take $x \in \overline{A} \cap \overline{B}$

$$x \in \overline{A} \text{ and } x \in \overline{B}$$

$$\iff \neg(x \in A) \text{ and } \neg(x \in B)$$

$$\iff \neg\,(x \in A \text{ or } x \in B)$$

$$x \notin (A \cup B)$$

$$\Rightarrow x \in \overline{A \cup B}$$

Those Laws!

Name	Identities	
Idempotent laws	$A \cup A = A$	$A \cap A = A$
Associative laws	$(A \cup B) \cup C = A \cup (B \cup C)$	$(A \cap B) \cap C = A \cap (B \cap C)$
Commutative laws	$A \cup B = B \cup A$	$A \cap B = B \cap A$
Distributive laws	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
Identity laws	$A \cup \emptyset = A$	$A \cap U = A$
Domination laws	$A \cap \emptyset = \emptyset$	$A \cup U = U$
Double complement law	$\overline{\overline{A}} = A$	
Complement laws	$A \cap \overline{A} = \emptyset$ $\overline{U} = \emptyset$	$A \cup \overline{A} = U$ $\overline{\emptyset} = U$
De Morgan's laws	$\overline{A \cup B} = \overline{A} \cap \overline{B}$	$\overline{A \cap B} = \overline{A} \cup \overline{B}$
Absorption laws	$A \cup (A \cap B) = A$	$A \cap (A \cup B) = A$

Cartesian Products

Sometimes, order does matter!

Tuples or strings!

Formalize: Given 2 sets A and B, the product of A and B, written $A \times B$, is the set of ordered pairs where the first element is from A and the second from B

$$A \times B = \{ (a,b) : \qquad \}$$

Examples:

Bit strings:

Strings:

$\mathbb{R}^2$ or $\mathbb{R}^3$:

Caution

$$(A \times B) \times C \neq A \times B \times C$$

Element of $(A \times B) \times C$:

element of $A \times B \times C$:

Another

What is $\emptyset \times \{a, b\}$?