Lecture 6

Hom PB 1 - due TATED

- strategy (for me = player B)
- reason / argument / proof that A cannot prevent B
- reason / arg / proof that B can follow strategy

- how B executes move?

- Sets - intro
- Sets - operations
- Product rule (cartezian prod)
- Sum rule (union)

1	0	0	0	1
2	0	0	1	0
5	0	1	0	1
	0	0	1	1
11	1	0	1	1
11	1	0	1	1

-2

1	0	0	0	1
2	0	0	1	0
3	0	0	1	1
5	0	1	0	1
11	1	0	1	1
	0	1	0	1

-6

Recap: implication

$\boxed{A \Rightarrow B}$

hypothesis conclusion

True except

A=T
B=F

False case

"if A, then B" $\neq$ "A and B"

OR form / equivalent

$\boxed{B \vee \neg A}$

cond = True

hyp = False

contrapositive / contradict proof

$\boxed{\neg B \Rightarrow \neg A}$

if cond False $\Rightarrow$ hyp False

NOT THE SAME

$\boxed{B \Rightarrow A} \equiv \boxed{A \vee \neg B} \equiv \boxed{\neg A \Rightarrow \neg B}$

converse

inverse

reverse

Proofs

PB1 $\boxed{\text{Infinitely many primes}}$ $\mathbb{P} = \{2, 3, 5, 7, 11, 13, 17, 19 \ldots\}$

recap: $\forall n \in \mathbb{N}, n \geq 2$

$n =$ product of prime numbers (UNIQUE)

$n = 12 = 2 \cdot 2 \cdot 3 = 2^2 \cdot 3$

$40 = 2 \cdot 2 \cdot 2 \cdot 5 = 2^3 \cdot 5$

$100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 \cdot 5^2$

$60 = 2 \cdot 2 \cdot 3 \cdot 5 = 2^2 \cdot 3 \cdot 5$

proof by contradiction: assume $\mathbb{P}$ finite

$\mathbb{P} = \{\underset{p_1}{2}, \underset{p_2}{3}, \underset{p_3}{5} \ldots \underset{\text{last prime}}{p_k}\}$

consider

$x = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_k + 1$

does x has proper divisors? NO!

$X = p_1 \cdot p_2 \cdots \quad p_k + 1$

$X \div p_i$ rem $= 1$ $\Rightarrow$ no proper divisors $\Rightarrow$ $\boxed{X \text{ prime}}$

$\boxed{X > p_k}$ contradiction $X \in \mathbb{P}$

$p_k =$ biggest in $\mathbb{P}$.

$\Downarrow$

concl = True ($\mathbb{P}$ infinite)

PB2 $\boxed{n^3+5 \text{ odd}} \Longrightarrow n \text{ even}$ $(a+b)^3 = a^3+3a^2b+3ab^2+b^3$

$n \in \mathbb{N}$

proof by contradiction : $\boxed{\text{assume}}$ $\neg(\text{conclusion}) = \neg(n \text{ even})$

$\equiv (n = \text{odd}) \equiv n = 2k+1$

$n^3+5 = (2k+1)^3+5 = 8k^3+12k^2+6k+1+5$

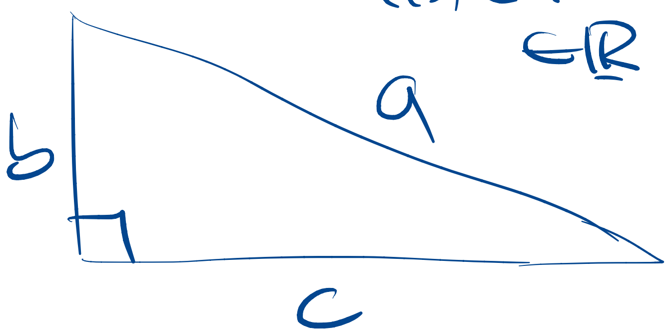
$= 8k^3+12k^2+6k+6 = \boxed{2}(\underbrace{4k^3+6k^2+3k+3}_{\text{anythin}}) = \text{even}$

contradicts $n^3+5 = \text{odd}$

$\Longrightarrow$ cond true (n even)

PB3

$a, b, c > 0 \in \mathbb{R}$



Task: $a < b+c$

Δabc

$\widehat{bac} = 90^\circ$ (right angle)

by contradiction

$\boxed{\text{assume}} \neg(a < b+c) \equiv$

$\equiv (a \geq b+c)$

Pythagora: $a^2 = b^2 + c^2$

$$a \geq b+c \Rightarrow a^2 \geq (b+c)^2 \Rightarrow \cancel{b^2} + \cancel{c^2} \geq \cancel{b^2} + \cancel{c^2} + 2bc$$

$$\Rightarrow \boxed{0 \geq 2bc}$$ contradiction $\Rightarrow a < b+c$

PB4 $\sqrt{3} \notin \mathbb{Q}$

$\mathbb{Q} = \{\text{rational numbers}\}$

$= \{x = \frac{a}{b} \mid a, b \in \mathbb{Z},\ b \neq 0\}$

$= \{\frac{a}{b} \mid a, b \in \mathbb{Z},\ b > 0\}$

Proof by contradiction

assume $\sqrt{3} \in \mathbb{Q}$

$\exists a, b \in \mathbb{Z}$ s.t. $\boxed{\sqrt{3} = \frac{a}{b}}$

$\Rightarrow 3 = \frac{a^2}{b^2} \Rightarrow 3 \cdot b^2 = a^2$

prime decomp.

$a = 3^x \cdot (\text{other primes})$

$b = 3^y \cdot (\text{other primes})$

$$3 \cdot \underbrace{(3^y)^2 (\text{other primes})^2}_{b^2} = \underbrace{(3^x)^2 (\text{other primes})^2}_{\text{even } a^2}$$

$$3 \cdot 3^{2y} (\text{other primes}) = 3^{2x} (\text{other primes})$$

$$3^{2y+1} = 3^{2x}$$

odd

odd $2y+1 = 2x$ even

(*) $\forall n \in \mathbb{N} \quad \sqrt{n} \notin \mathbb{N} \Rightarrow \sqrt{n} \notin \mathbb{Q}$

exercise

proof direct by cases

(PBS) k bits two's complement $N = b_{k-1} b_{k-2} \ldots b_1 b_0$

I want to write on k+1 bits (extend by bit representation). Prove that the new bit $b_k = b_{k-1}$

$b_k b_{k-1} b_{k-2} \ldots b_0$

by cases

I $b_{k-1} = 0$ $N = \boxed{0}\, b_{k-2} b_{k-3} \ldots b_1 b_0$

k+1 bits $0\ 0\ b_{k-2} b_{k-3} \ldots b_1 b_0$

(unsigned representation).

II $b_{k-1} = 1$ $(N<0)$ $N = 1\ b_{k-2}\ b_{k-3} \ldots b_1 b_0$

$= -2^{k-1} + \text{complement}$

new N on k+1 bits

$1\ 1\ b_{k-2} b_{k-3} \ldots b_0 = -2^k + 2^{k-1} + \text{complement}$

$$-2^k + 2^{k-1} \stackrel{?}{=} -2^{k-1}$$

$$2^{k-1} + 2^{k-1} \stackrel{?}{=} 2^k$$

$$2 \cdot 2^{k-1} \stackrel{?}{=} 2^k \quad \checkmark$$

(PB6) $n \in \mathbb{N}$ $n \geq 1$ then $10^n = a^2 + b^2$ (sum of two squres)

proof by cases.

I $n = \text{odd} = 2k+1$ $\quad 10^n = 10^{2k+1} = 10^{2k} \cdot 10 =$

$= (10^k)^2 (9+1) = (10^k)^2 \cdot (3^2 + 1^2) =$

$= \underbrace{(10^k \cdot 3)}_{a}^2 + \underbrace{(10^k \cdot 1)}_{b}^2$

II $n = \text{even} = 2k+2$ $\quad 10^n = 10^{2k+2} = 10^{2k} \cdot \underbrace{10^2}_{100}$

$= (10^k)^2 (8^2 + 6^2) = \underbrace{(10^k \cdot 8)}_{a}^2 + \underbrace{(10^k \cdot 6)}_{b}^2$

Set = collection of items
objects
elements

OUT OF ORDER

$\{1,2,4,3,6,5,10,9,8,7\}$ //

enumeration $U = \{1,2,3,4,5,6,7,8,9,10\}$ $|U| = 10$

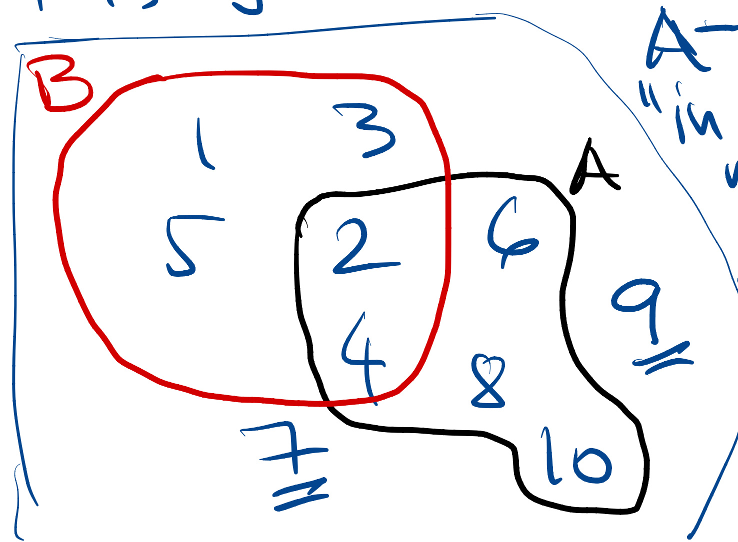
set notation
builder
property

$U = \{x \mid x \in \mathbb{Z},\ x > 0,\ x \le 10\}$
$= \{x \in \mathbb{Z} \mid 0 < x \le 10\}$

$|A| = 5$
$|B| = 5$

$A =$ "evens in U" $= \{2,4,6,8,10\}$ $A \subset U$ subset
$B =$ "≤ 5 in U" $= \{1,2,3,4,5\}$ $B \subset U$ subset

Venn Diagram



$A \cap B =$ "common elem to A and B"
$= \{2,4\}$

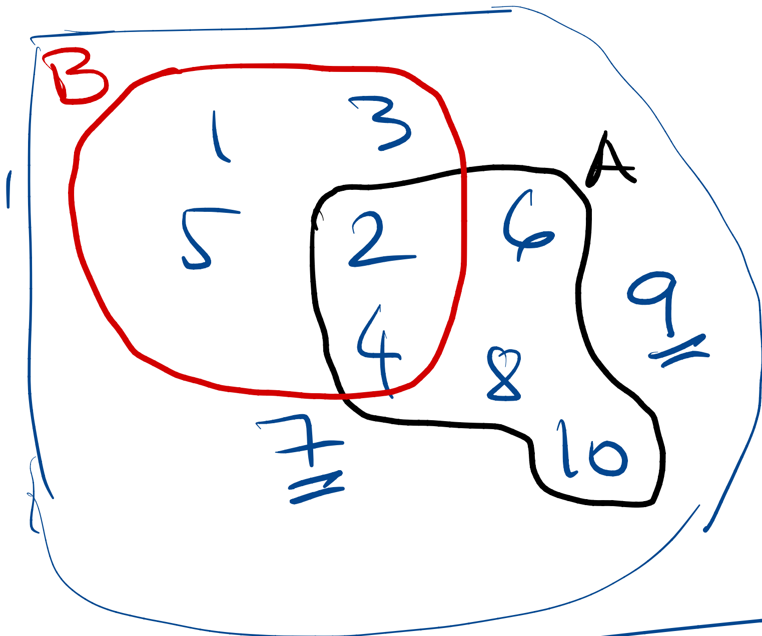
$A \cup B =$ "elements in A or B",
$\{1,2,3,4,5,6,8,10\}$

$A - B = A \setminus B$
"in A and not B"
$\{6,8,10\}$

$B - A =$
$\{1,3,5\}$

$A - B =$ "elem in A" and not in B

$= A \cap \text{not } B = A \cap \overline{B}$



symmetric difference $\simeq$ XOR

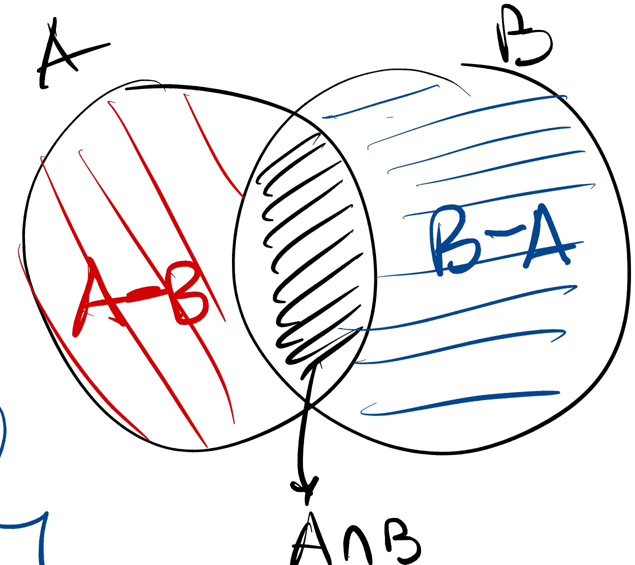
$A \Delta B = (A - B) \cup (B \setminus A)$ } proof?

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

$= \{1, 3, 5, 6, 8, 10\}$

not B = complement of $B = \overline{B}$

$= \text{universe} \setminus B = \{6, 7, 8, 9, 10\}$

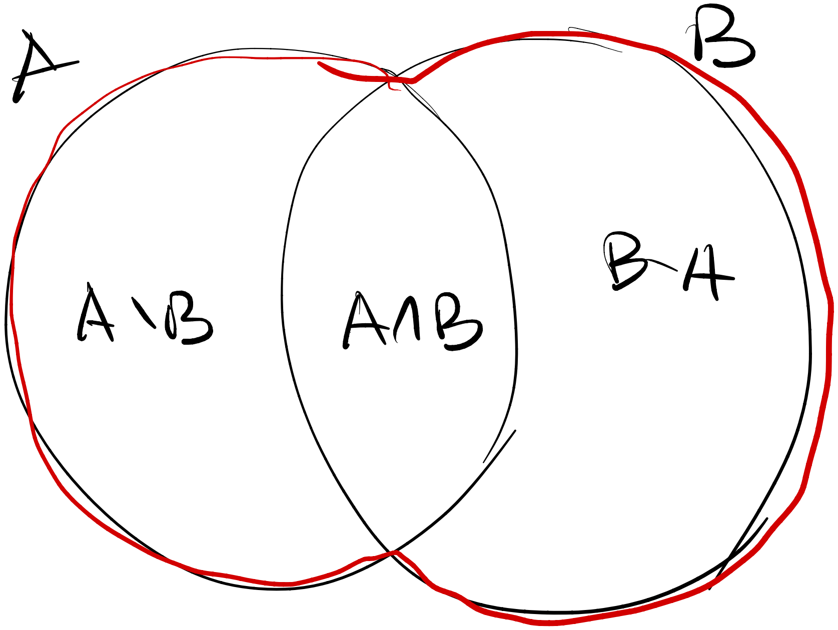


power set = set of subsets

$\mathcal{P}(B) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{4\}, \{5\}, \{1,2\}, \{1,3\}, \{1,4\}, \ldots, \{1,2,3\}, \{1,2,4\}, \{1,2,5\}, \ldots\}$

$|\mathcal{P}(B)| = 2^5 = 2^{|B|}$

Sum Rule: size of union.

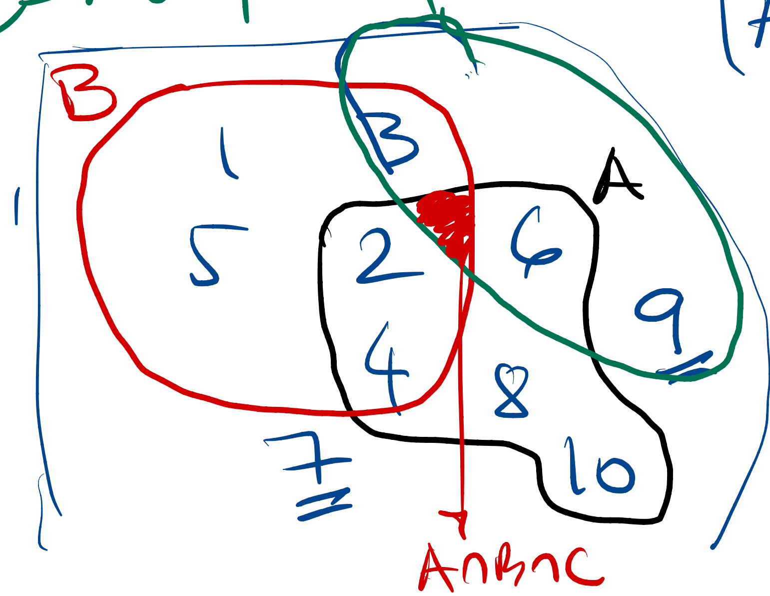


$|A\cup B| = |A\setminus B| + |A\cap B| + |B\setminus A|$

- partition into 3 sets
  - → disjoint sets
  - → union = total

$|A\cup B| = |A| + |B| - |A\cap B|$ ← was double counted.

C = multiples of 3 $= \{x \in U \mid x = 3k,\ k\in\mathbb{Z}\}$



$|A\cup B| = |A| + |B| - |A\cap B|$

$= 5 + 5 - 2 = 8$

$|A\cup B\cup C| = |A| + |B| + |C|$

$- |A\cap B| - |B\cap C| - |C\cap A|$

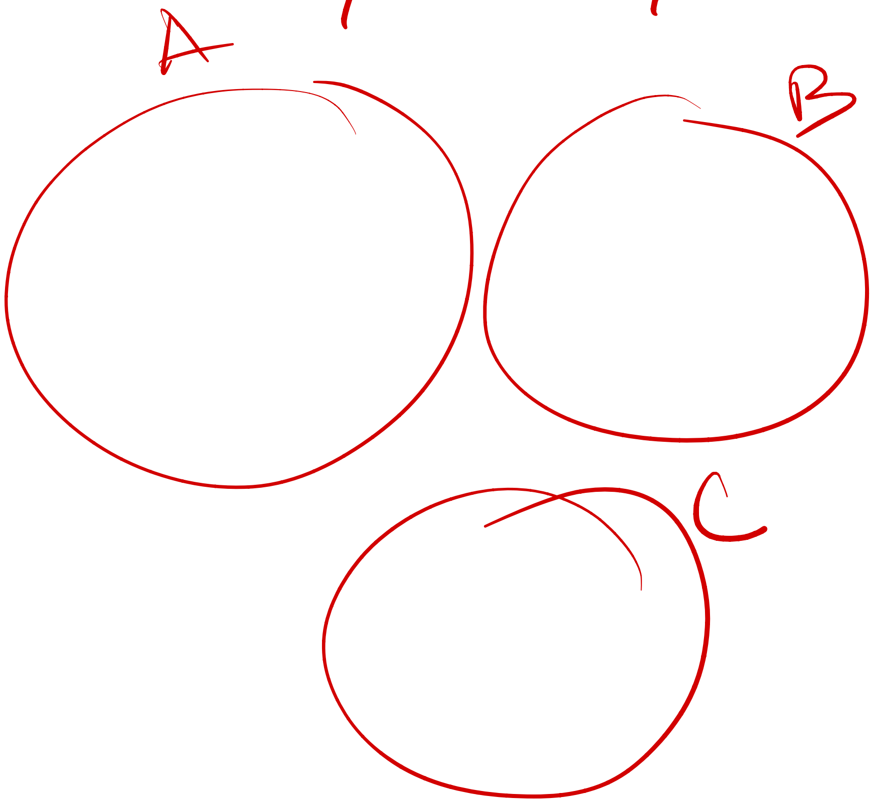
$+ \boxed{|A\cap B\cap C|}$

Principle of Inclusion-Exclusion

Sum Rule for Partition (Partition Rule) (no intersection)

$A \cap B$, $B \cap C$, $C \cap A$

$= \emptyset$ $\quad \emptyset \quad \emptyset$



$|A \cup B \cup C| =$

$|A| + |B| + |C|$