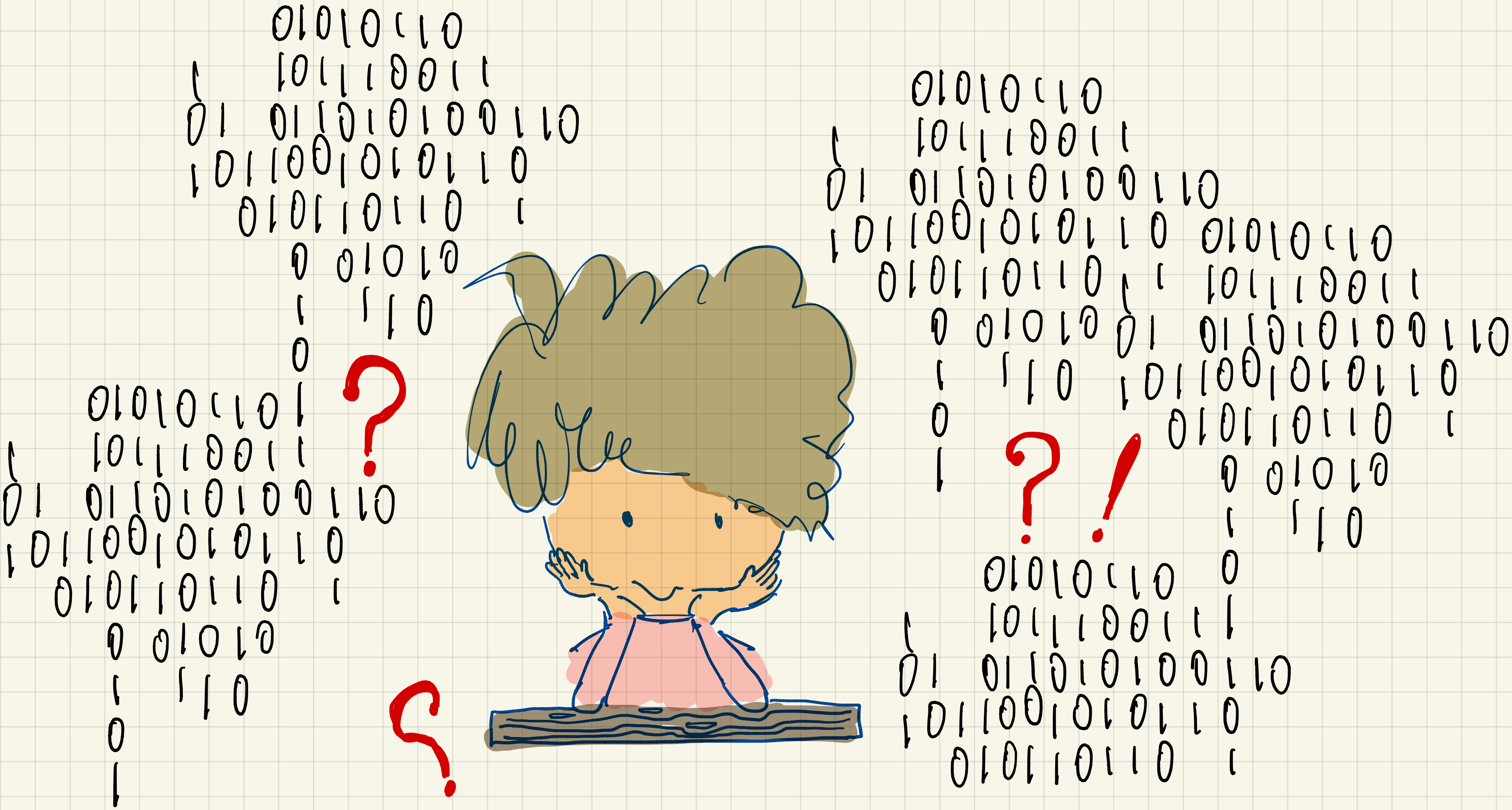

Lecture 1001

Proofs :

In general, given a "statement", we want to establish whether it's true or false. A statement that is either true or false is called "PROPOSITION"

Examples:
- For every non-negative integer n, n^2+n+41 is prime

  $\forall n \in \mathbb{N} \cup \{0\}.\ n^2+n+41$ is prime

- There exists an integer greater than zero that is not the product of primes.

  $\exists n \in \mathbb{N}.\quad \neg(n \text{ is a product of primes})$

Note: a product can also be empty or consist of just one number

- For every number x, if $x \geq 2$, then $x^2 \geq 4$.

$$\forall x \in \mathbb{R}.\ x \geq 2 \Longrightarrow x^2 \geq 4.$$

- If $a.b$ is irrational, then a is irrational or b is irrational

$$ab \notin \mathbb{Q} \Longrightarrow (a \notin \mathbb{Q} \vee b \notin \mathbb{Q})$$

While all the above are propositions, each consists of smaller propositions combined in some operators.

$P \Longrightarrow Q$: If P is true, then Q is true (implication)

$P \vee Q$: P or Q

$P \wedge Q$: P and Q

$\neg P$: Not P

$\left.\right\}$ Boolean Ops

$\forall x.\ P(x)$: Universal Quantifier (true if $P(x)$ true for all x)

$\exists x.\ P(x)$: Existential quantifier (true if $P(x)$ true for some x)

Let's explore n^2+n+41.

$n=0: \quad 0+0+41 = 41$ prime

$n=1: \quad 1+1+41 = 43$ prime

$n=2: \quad 4+2+41 = 47$ prime

$n=3: \quad 9+3+41 = 53$ prime

$\vdots$

$n=39: \quad 39^2+39+41 = 1601$ prime

$n=40: \quad 40^2+40+41 = 1681 \quad (41 \times 41)$ ✗ (Counter example)

disproves the claim

No proof by examples!!!

Let's define the operators $\neg$, $\wedge$, $\vee$, $\Rightarrow$

Assume P and Q are propositions

True $\equiv 1$

False $\equiv 0$

P	$\neg P$
0	1
1	0

Not

P	Q	$P \wedge Q$
0	0	0
0	1	0
1	0	0
1	1	1

And

P	Q	$P \vee Q$
0	0	0
0	1	1
1	0	1
1	1	1

Or

P	Q	$P \Rightarrow Q$
0	0	1
0	1	1
1	0	0
1	1	1

Implies

In particular $P \Rightarrow Q$ may be not so intuitive.

$P \Rightarrow Q$ means "whenever P is true, Q is also true"

The only row that violates this condition is the third row.

Remember: $P \Rightarrow Q$ is itself a proposition (can be either true or false)

In English we often say "P implies Q". What we usually mean is $(P \Rightarrow Q)$ is true.

Why $0 \Rightarrow 0$ is True ?

and $0 \Rightarrow 1$ is True ?

Consider: $\forall x \in \mathbb{R}.\ (x > 5) \Rightarrow (x^2 > 16)$ ✓

This statement is true because $(x>5) \Rightarrow (x^2 > 16)$ is true for every x.

✓ $x = 4$: $0 \Rightarrow 0$

✓ $x = 5$: $0 \Rightarrow 1$

✓ $x = 6$: $1 \Rightarrow 1$

$\vdots$

Can't find a value for x that will produce $1 \Rightarrow 0$.

Important observation:

When $(P \Rightarrow Q)$ is true, this does not tell us much about the truth value of P or that of Q.

P	Q	$P \Rightarrow Q$
0	0	1
0	1	1
1	0	0
1	1	1

Both P and Q can be either 0 or 1

(we could be in any of the 3 rows)

Other ways of Saying $P \Rightarrow Q$

P	Q	$P \Rightarrow Q$	$\neg P$	$\neg Q$	$\neg P \vee Q$	$\neg Q \Rightarrow \neg P$	$P \wedge \neg Q$
0	0	1	1	1	1	1	0
0	1	1	1	0	1	1	0
1	0	0	0	1	0	0	1
1	1	1	0	0	1	1	0

We are using a **truth table** to show

$$(P \Rightarrow Q) = (\neg P \vee Q) = (\neg Q \Rightarrow \neg P)$$

Contrapositive

$$\neg(P \Rightarrow Q) = P \wedge \neg Q$$

Boolean function

$$f : \{0,1\}^n \longrightarrow \{0,1\} \quad \left(\{0,1\}^n = \underbrace{\{0,1\} \times \{0,1\} \times \dots \times \{0,1\}}_{n \text{ times}} \right)$$

Example: $f : \{0,1\} \times \{0,1\} \times \{0,1\} \longrightarrow \{0,1\}$

is a function of 3 Boolean variables.

$x\ y\ z$	$f(x,y,z)$
0 0 0	0
0 0 1	1
0 1 0	1
0 1 1	0
1 0 0	1
1 0 1	0
1 1 0	0
1 1 1	1

What's the logic? What is f really saying?

Any Boolean function can be constructed using $\{\neg, \wedge, \vee\}$ operators.

We say $\{\neg, \wedge, \vee\}$ is UNIVERSAL.

$$f(x,y,z) = (\neg x \wedge \neg y \wedge z) \vee (\neg x \wedge y \wedge \neg z) \vee (x \wedge \neg y \wedge \neg z) \vee (x \wedge y \wedge z)$$

Worksheet:

$x\ y\ z$	$f(x,y,z)$
0 0 0	0
0 0 1	1
0 1 0	1
0 1 1	0
1 0 0	1
1 0 1	0
1 1 0	0
1 1 1	1

$$\frac{0 \quad 0 \quad 1}{\neg x \wedge \neg y \wedge z}$$

$$\frac{0 \quad 1 \quad 0}{\neg x \wedge y \wedge \neg z}$$

$$\frac{1 \quad 0 \quad 0}{x \wedge \neg y \wedge \neg z}$$

$$\frac{1 \quad 1 \quad 1}{x \wedge y \wedge z}$$

$\Longrightarrow$

$$(\neg x \wedge \neg y \wedge z) \vee (\neg x \wedge y \wedge \neg z) \vee \ \dots \ \vee (x \wedge y \wedge z)$$

Other facts:

$\{\neg, \wedge\}$ is universal

$\{\neg, \vee\}$ is universal

Why? De Morgan's Law

$$\neg(A \wedge B) = \neg A \vee \neg B$$

$$\neg(A \vee B) = \neg A \wedge \neg B$$

so $A \wedge B = \neg(\neg A \vee \neg B)$ Replace $\wedge$ by $\neg$ and $\vee$

$A \vee B = \neg(\neg A \wedge \neg B)$ Replace $\vee$ by $\neg$ and $\wedge$

How do we prove De Morgan's Law?

Truth table!

Example of contrapositive:

$P: \ a \cdot b \notin \mathbb{Q}$

$Q: \ a \notin \mathbb{Q} \vee b \notin \mathbb{Q}$

$\neg P: \ a \cdot b \in \mathbb{Q}$

$\neg Q: \ a \in \mathbb{Q} \wedge b \in \mathbb{Q}$ (De Morgan's Law)

$$(P \Rightarrow Q) \equiv (\neg Q \Rightarrow \neg P)$$

$$a \cdot b \notin \mathbb{Q} \Rightarrow (a \notin \mathbb{Q} \vee b \notin \mathbb{Q})$$

Equivalent to

$$(a \in \mathbb{Q} \wedge b \in \mathbb{Q}) \Rightarrow a \cdot b \in \mathbb{Q}$$

Commutativity:

$$A \wedge B = B \wedge A$$

$$A \vee B = B \vee A$$

All can be verified by truth tables.

Associativity:

$$A \wedge (B \wedge C) = (A \wedge B) \wedge C = A \wedge B \wedge C$$

$$A \vee (B \vee C) = (A \vee B) \vee C = A \vee B \vee C$$

Distributivity:

$$A \wedge (B \vee C) = (A \wedge B) \vee (A \wedge C)$$

$$A \vee (B \wedge C) = (A \vee B) \wedge (A \vee C)$$