IDMA LOGIC

Our language for making precise mathematical statements and arguments

STATEMENT / PROPOSITION Declarative sentence that is either true or false

(The world isn't black-or-white, but mathematics is)

PROPOSITIONAL VARIABLES or **BOOLEAN VARIABLES**

p, q, r take values True T, 1
or False F, 1, 0

Combine into **COMPOUND STATEMENTS** (or **PROPOSITIONAL FORMULAS**) using **CONNECTIVES**

Advantages compared to natural language
- More concise
- More precise - avoids ambiguity
- Reveals high-level logic structure of statements and arguments

But this is just a tool to make precise our common sense logical reasoning - this is no "new" reasoning

PROPOSITIONAL LOGIC Basic structure of logic sentences

PREDICATE LOGIC: When we want to discuss more in detail properties of objects (integers, graphs) and how they are related

(There are also other types of logic which we won't discuss in this course)

Start with PROPOSITIONAL LOGIC - how truth value of compound statement depends on components

AND

p	q	$p \wedge q$
F	F	F
F	T	F
T	F	F
T	T	T

$p \wedge q$
True precisely when
p & q both true

OR

p	q	$p \vee q$
F	F	F
F	T	T
T	F	T
T	T	T

$p \vee q$
Two meanings in natural language
- inclusive
- exclusive (not both true)

We define $\vee$ to have inclusive meaning

NOT

p	q	$\sim p$
F	F	T
F	T	T
T	F	F
T	T	F

$\sim p$ true precisely when p false

Also denoted $\neg p$ $\quad \overline{p}$

IMPLICATION or CONDITIONAL

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

$p \Rightarrow q$ or $p \to q$
"p implies q"
"if p then q"
Many theorems have this structure:
if (some assumptions hold) then (conclusion)
p: ANTECEDENT / HYPOTHESIS
q: CONSEQUENT / CONCLUSION

Implication only claims "if p then q" – not necessarily causal
False if p true but q false. But otherwise? True (by definition)
(p SUFFICIENT for q to hold, not necessary)

Implication $p \to q$

CONVERSE $q \to p$

CONTRAPOSITIVE $\sim q \to \sim p$

p: "It's raining" q: "the asphalt is wet"

$p \to q$ "if it's raining, then the asphalt is wet"

$q \to p$ "if the asphalt is wet, then it's raining"

$\sim q \to \sim p$ "if the asphalt is not wet, then it's not raining"

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

So truth value of implication an converse not related in general.

But implication and contrapositive always have same truth value EQUIVALENT $\equiv$

Means that if we want to prove $p \to q$, can equally well prove $\sim q \to \sim p$

IMPORTANT

EQUIVALENCE or BICONDITIONAL

p	q	$p \Leftrightarrow q$
F	F	T
F	T	F
T	F	F
T	T	T

"p is equivalent to q"

"p if and only if q" iff

$p \Leftrightarrow q$ or $p \leftrightarrow q$

p is a NECESSARY and SUFFICIENT condition for q

Sentences built from $P, Q, R, \wedge, \vee, \sim, \rightarrow, \leftrightarrow$ are syntactic objects

If S_1, S_2 sentences, then

$S_1 \leftrightarrow S_2$ is a sentence; true when S_1 & S_2 take same truth value

$S_1 \equiv S_2$ is a claim that the two sentences are logically equivalent

TAUTOLOGY Propositional formula that is always true

If $S_1 \equiv S_2$, then $S_1 \leftrightarrow S_2$ is a tautology

Ex $(p \rightarrow q) \leftrightarrow (\sim q \rightarrow \sim p)$

BTW parantheses — add to disambiguate
But NOT $(\sim)$ assumed to bind harder than other connectives, so we don't need to write, e.g.,
$((\sim q) \rightarrow (\sim p))$ (though this is not wrong either)

ABSURDITY or CONTRADICTION Propositional formula that is always false

Ex $p \wedge \sim p$

SATISFIABLE propositional formula evaluates to true for some truth value assignment

BASIC PROPERTIES OF AND, OR, NOT

(1)	$p \vee q$	$\equiv$	$q \vee p$	} COMMUTATIVITY
(2)	$p \wedge q$	$\equiv$	$q \wedge p$	
(3)	$p \vee (q \vee r)$	$\equiv$	$(p \vee q) \vee r$	} ASSOCIATIVITY
(4)	$p \wedge (q \wedge r)$	$\equiv$	$(p \wedge q) \wedge r$	
(5)	$p \vee (q \wedge r)$	$\equiv$	$(p \vee q) \wedge (p \vee r)$	} DISTRIBUTIVITY
(6)	$p \wedge (q \vee r)$	$\equiv$	$(p \wedge q) \vee (p \wedge r)$	
(7)	$\sim(\sim p)$	$\equiv$	p	LAW OF THE EXCLUDED MIDDLE
(8)	$\sim(p \vee q)$	$\equiv$	$\sim p \wedge \sim q$	} DE MORGAN'S LAWS
(9)	$\sim(p \wedge q)$	$\equiv$	$\sim p \vee \sim q$	

BASIC PROPERTIES OF IMPLICATION AND EQUIVALENCE

(a)	$p \to q$	$\equiv$	$\sim p \vee q$
(b)	$p \to q$	$\equiv$	$\sim q \to \sim p$
(c)	$p \leftrightarrow q$	$\equiv$	$(p \to q) \wedge (q \to p)$
(d)	$\sim(p \to q)$	$\equiv$	$p \wedge \sim q$
(e)	$\sim(p \leftrightarrow q)$	$\equiv$	$(p \wedge \sim q) \vee (\sim p \wedge q)$

Proof Compare truth tables of LHS and RHS

E.g. (c)

p	q	$p \to q$	$q \to p$	$(p \to q) \wedge (q \to p)$	$p \leftrightarrow q$
F	F	T	T	T	T
F	T	T	F	F	F
T	F	F	T	F	F
T	T	T	T	T	T

Can also prove logical equivalence by using the rewriting rules above (once they have been proven)

THREE COMPUTATIONAL PROBLEMS

Given as input propositional logic formula F, is F:

(a) a **TAUTOLOGY**?
(i.e., evaluates to true for all assignments)

(b) a **CONTRADICTION**?
(i.e., evaluates to false for all assignments)

(c) **SATISFIABLE**?
(i.e., there exists some assignment for which F evaluates to true)

Closely related problems

F tautology $\Leftrightarrow$ $\neg F$ contradiction

F contradiction $\Leftrightarrow$ F not satisfiable

Are there any good algorithms for these problems?

Important applications in
- hardware verification
- software testing
- automated reasoning
- explainable AI
- bioinformatics
- cryptography
- ...

Brute-force algorithm:
If F has n variables, check all 2^n possible assignments

Time complexity? Scales exponentially
$\sim 2^{k \cdot n}$ for some $k > 0$
Often written $\exp(O(n))$, abusing notation a bit
This is terrible!

Is it possible to do better?

IN THEORY
Question of whether polynomial-time algorithm exists (with worst-case guarantees) is one of MILLENNIUM PRIZE PROBLEMS
Answer worth 1 million USD
Most theoreticians believe that answer is "no"
P vs. NP question

IN PRACTICE
Since the late 1990s, so-called SAT solvers have been developed based on CONFLICT-DRIVEN CLAUSE LEARNING that can deal with industrial instances with millions of variables (but sometimes fail on small instances with just ≈ 100 variables)

Explaining this rigorously is a big open research problem!

ANOTHER INTERESTING OBSERVATION

Suppose I know somehow that F is satisfiable. Can I somehow convince you, so that you can check easily?

YES! I can provide satisfying assignment. This you can verify easily and quickly: Plug in the assignment, and check that the formula evaluates to true.

Suppose I know somehow that F is tautological. Can I somehow convince you, so that you can check easily

NOT CLEAR — what would be a short certificate?

Question of NP vs. co-NP

All of this is related to the research done in my research group

Warm-up

Which of the following are true propositions?

(1) Every $n \in \mathbb{Z}^+$ can be written uniquely as a product of primes and $n \log n = O(n^2)$

(2) If $2+2=4$ then 4 is a prime

(3) If $2+2=5$ then 5 is a prime

(4) If someone in this class has their birthday today, then $LCM(12, 8) = 24$

(2) false, all other true

Propositional logic only analyzes general structure of sentences

But sometimes want to speak about objects (integers, matrices, graphs)

Will abstractly as PREDICATES $P(x), Q(x), R(x,y)$

Examples

$P(x) \triangleq$ x is a positive real number $x \in \mathbb{R}^+$

$Q(x,y) \triangleq$ $x^2 + y^2 = 4$, $x, y \in \mathbb{R}$

$R(x,y)$: $x \leq y$

As can be seen above, sometimes we have convenient special notation for predicates

We can define sets using predicates

S' = subset of S containing elements x for which $P(x)$ holds

$$S' = \{ x \in S \mid P(x) \}$$

Ex $\{ x \in \mathbb{Z} \mid x > 0 \} = \mathbb{Z}^+$

What is $\{ (x,y) \in \mathbb{R}^2 \mid Q(x,y) \}$ for Q as defined above? Circle of radius 2

QUANTIFIERS

For-all quantifier or universal quantifier

$$\forall x \in S \quad P(x)$$

"for all elements x in S it holds that $P(x)$ is true"

Existential quantifier

$$\exists x \in S \quad P(x)$$

"there exists an element x in S such that $P(x)$ holds"

We sometimes drop specification "$\in S$" when the set S is clear from context.

$\forall n \in \mathbb{Z}^+ \quad n^2 = 25$ false

$\exists n \in \mathbb{Z}^+ \quad n^2 = 25$ true

$\forall n \in \mathbb{Z}^+ \quad \exists m \in \mathbb{Z}^+ \quad n^2 = m$ true

$\forall n \in \mathbb{Z}^+ \quad \exists m \in \mathbb{Z}^+ \quad n = m^2$ false

$\exists m \in \mathbb{Z}^+ \quad \forall n \in \mathbb{Z}^+ \quad n^2 = m$ false

Quantifier order matters

NEGATIONS OF STATEMENTS WITH QUANTIFIERS

$\sim \forall x\, P(x)$

"it is not the case that for all x $P(x)$ holds"

$\Leftrightarrow$ "there is some x for which $P(x)$ is false"

$\sim P(x)$ is true

$$\sim(\forall x \in S \;\; P(x)) \equiv \exists x \in S \;\; \sim P(x)$$

$$\sim(\exists x \in S \;\; P(x)) \equiv \forall x \in S \;\; \sim P(x)$$

Convention

When we write $P(x) \rightarrow Q(x)$

forall-quantifier implicitly assumed

Ex $x > 1 \rightarrow x^2 > 1$

METHODS OF PROOF

Many theorems are of the form
$(p_1 \wedge p_2 \wedge \cdots \wedge p_k) \rightarrow q$

To establish such a theorem, need to prove that if p_i all true, then q also true

DIRECT PROOF

Assume all p_i's true; use this info to prove q true. (Note: cannot assume anything about q — need to prove q true)

Ex If $x, y \in \mathbb{Z}$ are both odd, then $x+y$ even

By definition

$x \in \mathbb{Z}$ odd if $\exists n \in \mathbb{Z}$ s.t. $x = 2n+1$
" even " " $x = 2n$

By assumption, can find m, n s.t.

$$x = 2m+1$$
$$y = 2n+1$$

Then $x+y = (2m+1) + (2n+1)$
$= 2 \cdot (m+n+1)$

so $x+y$ is even. Potentially finish by "QED", "Quod erat demonstrandum", "the claim/theorem follows", or □ (box) To signal that proof is over.

PROOF BY CONTRAPOSITIVE / CONTRAPOSITION

Since $p \to q \equiv \sim q \to \sim p$

can also prove implication by assuming $\sim q$ and showing that $\sim p$ follows

Ex Let $a, b, n \in \mathbb{Z}^+$. Prove that if $\underbrace{n \nmid ab}_{p}$ then $\underbrace{n \nmid a}_{q_1}$ and $\underbrace{n \nmid b}_{q_2}$

$p \to (q_1 \wedge q_2)$

Def $d \mid k$ if $\exists\, c \in \mathbb{Z}$ s.t. $k = c \cdot d$

Assume $\sim(q_1 \wedge q_2) \equiv \sim q_1 \vee \sim q_2$

$\sim q_1$: $n \mid a$ $\quad a = c \cdot n$

Then $a \cdot b = (c \cdot b)\, n$

so $n \mid ab$, which is $\sim p$

$\sim q_2$: $n \mid b$ exactly the same

PROVING AN EQUIVALENCE

$p \leftrightarrow q \equiv (p \to q) \wedge (q \to p)$

So just need to show two implications

Proof template: "We prove that p implies q and vice versa."

"First we show that p implies q" or just "$(\Rightarrow)$"

"Now let us show that q implies p" or just "$(\Leftarrow)$"

Either implication can be proven directly or by contraposition.

Example For any $a \in \mathbb{Z}$ it holds that
a is even if and only if a^2 is even

Proof

($\Rightarrow$) If a is even, then $\exists n$ s.t. $a = 2n$

$a^2 = (2n)^2 = 2 \cdot 2n^2$

so a^2 even

($\Leftarrow$) Proof by contraposition. Suppose
a not even, i.e., odd
then $a = (2n+1)$ for some $n \in \mathbb{Z}$

$a^2 = (2n+1)^2 = 4n^2 + 4n + 1$

$= 2(2n^2 + 2n) + 1$

so not even

PROOF BY CONTRADICTION

Assume the negation of what should be proven.
Derive a contradiction. (Something known to be false)

Want to prove p. Know q

Prove $\neg p \rightarrow \neg q$

$$\left((\neg p \rightarrow \not\Rightarrow \neg q) \wedge q \right) \equiv p \wedge q$$

Check using truth tables!

THEOREM $\sqrt{2}$ is an irrational number.

Proof. By contradiction

Suppose $\sqrt{2}$ is not an irrational number. We will show that this leads to absurdity.

If $\sqrt{2}$ is not irrational, then it is rational. That is, there are $p, q \in \mathbb{Z}$ such that

$$\sqrt{2} = \frac{p}{q} \tag{1}$$

$\sqrt{2}$ is positive, so p and q can be chosen positive

Furthermore, we can divide away all common factors so that

$$GCD(p, q) = 1 \tag{2}$$

If we square (1) we get

$$2 = \frac{p^2}{q^2}$$

and multiplying by q^2 yields

$$2q^2 = p^2 \tag{3}$$

Hence, the square p^2 is even. We just proved that this implies that p is even. That is there is some $n \in \mathbb{Z}^+$ such that

$$p = 2n \tag{4}$$

If we substitute (4) in (3) we get

$$2q^2 = (2n)^2 = 4n^2 \qquad (5)$$

or, after dividing by 2,

$$q^2 = 2n^2 \qquad (6)$$

From this we see that q is also even, i.e., there is some $m \in \mathbb{Z}^+$ such that

$$\boxed{q = 2m} \qquad (7)$$

We have now shown that p and q have a common factor 2, so

$$\boxed{GCD(p,q) \geq 2} \qquad (8)$$

But this contradicts how we chose p and q in (2) ⊗

After carefully checking, we see that all steps after (1) are perfectly sound. Hence, the source of the contradiction must be (1). This shows that $\sqrt{2}$ cannot be rational, and the theorem follows. ▨

THEOREM There is an infinite number of primes.

Proof By contradiction.

Suppose that there is a finite number of primes $p_1, p_2, \dots, p_n$

Every number can be written as a product of primes. (We don't need the Fundamental Theorem of Arithmetic for this — we just claim that it can be done in *some* way)

Consider the number

$$N = p_1 p_2 \cdots p_n + 1 = \prod_{i=1}^{n} p_i + 1$$

How can we factor N as product of primes?

For all i we have $p_i \nmid N$, since division yields remainder 1

But then either N is prime, or it contains a prime factor other than $p_1, p_2, \dots, p_n$

This contradicts that $p_1, p_2, \dots, p_n$ is a list of all prime numbers. ∎

For which values of $n \in \mathbb{Z}^+$ does it hold that $n! > 2^n$?

n	$n!$	2^n
1	1	2
2	2	4
3	6	8
4	24	16
5	120	32
6	720	64

For all $n \geq 4$, probably ?

How to prove this?

THEOREM For all $n \geq 4$ it holds that $n! > 2^n$

Proof By induction

Base case ($n = 4$) $4! = 24 > 16 = 2^4$.

Induction step Suppose that

$$n! > 2^n \qquad (1\#)$$

for some arbitrary $n \geq 4$

Then we have that

$$\begin{aligned} (n+1)! &= (n+1)\, n! && [\text{by } 1\#] \\ &> (n+1)\, 2^n && [n \geq 4] \\ &> 2 \cdot 2^n \\ &= 2^{n+1} \end{aligned}$$

which concludes the induction step.

The theorem follows by the induction principle. ▨

Prove that

$$1 + 2 + 4 + 8 + \dots + 2^{n-1} + 2^n = \sum_{i=0}^{n} 2^i = 2^{n+1} - 1$$

We show this by mathematical induction

Base case ($n = 0$):

$$1 = 2^{0+1} - 1 = 2 - 1$$

Induction step: Suppose that

$$\sum_{i=0}^{n} 2^i = 2^{n+1} - 1 \qquad (IH)$$

holds. We need to show that

$$\sum_{i=0}^{n+1} 2^i = 2^{n+2} - 1. \qquad (*)$$

By calculating and using the induction hypothesis, we get that

$$\sum_{i=0}^{n+1} 2^i = \sum_{i=0}^{n} 2^i + 2^{n+1} \qquad [IH]$$

$$= 2^{n+1} - 1 + 2^{n+1}$$

$$= 2 \cdot 2^{n+1} - 1$$

$$= 2^{n+2} - 1$$

which establishes the induction step. The equality follows by the principle of mathematical induction.