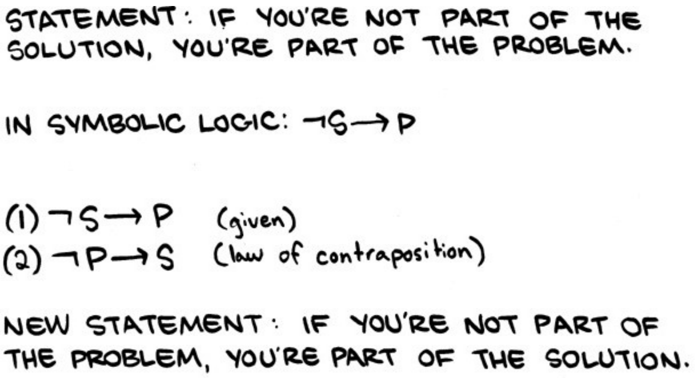
# Discrete Mathematics

## MATH1064, Lecture 5

Jonathan Spreer

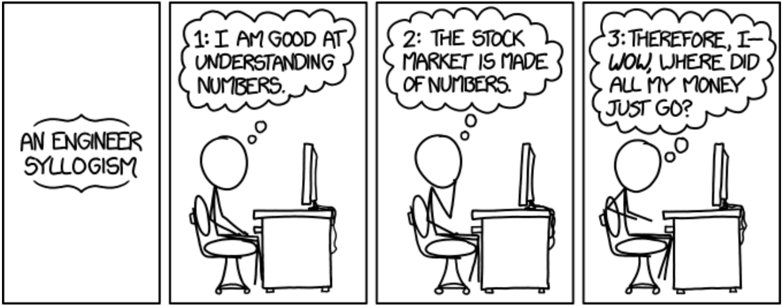


# Extra exercises for Lecture 5

Section 1.4: Problems 5–15

Section 1.5: Problems 1, 2, 31, 32, 38

Section 1.6: Problems 1–7



# Valid and invalid arguments

An argument form is a sequence of compound propositions.

All but the last proposition form are called premises.
The last compound proposition is called the conclusion, and is sometimes written with a "therefore" sign: $\therefore$

Example:

1. $p \rightarrow q$ (premise)
2. $p$ (premise)

c. $\therefore q$ (conclusion)

An argument form is valid if, whenever all of the premises are true, then the conclusion is true also. Otherwise the argument form is invalid.

**Observation**

The argument form with premises $p_1, \ldots, p_k$ and conclusion $c$ is valid if and only if $p_1 \wedge \ldots \wedge p_k \rightarrow c$ is a tautology!

# A more complex deduction

Instead of truth tables, we can prove that an argument is valid using rules of inference and logical equivalences.

1. $p \to \neg r$
2. $r \vee \neg q$
3. $q$
4. $\neg q \vee r$ *(from (2) by commutativity)*
5. $q \to r$ *(from (4) by rewriting $\to$)*
6. $r$ *(from (3,5) by modus ponens)*
7. $\neg(\neg r)$ *(from (6) by double negative)*

c. $\therefore\ \neg p$ *(from (1,7) by modus tollens)*

# Vacuous truth

For all real numbers $r$ such that $r^2 = -1$, we have $r > r$.

There is no real number for which $r^2 = -1$.
This means that $r^2 = -1$ is always false, and so the conditional

$$(r^2 = -1) \rightarrow \text{anything}$$

is always true!

In symbols:

$$\forall r \in \mathbb{R}, \left(r^2 = -1\right) \rightarrow \left(r > r\right)$$

is a true proposition.

There is no real number for which $r^2 = -1$, so the conditional is always true since its hypothesis is always false. Hence the conditional is a tautology. We call this vacuous truth.

# Implicit quantification

Mathematicians often say things like:

*If $x$ is larger than 3, then $x^2$ is larger than 9.*

This is not a statement, since we do not know the value of $x$.
We are just being lazy: there is an implicit $\forall$ in here!

$$\forall x \in \mathbb{R},\ x > 3 \to x^2 > 9.$$

*Every natural number can be expressed as the sum of four squares.*

This time there are implicit $\forall$ and $\exists$ quantifiers:

$$\forall n \in \mathbb{N},\ \exists a, b, c, d \in \mathbb{Z} \text{ such that } n = a^2 + b^2 + c^2 + d^2.$$

# Things you can do with logic

**Theorem**

*If $V$ is a perfect virus checker ... then $V$ is itself a virus!*

Our definitions:

- a virus is a computer program that, when it is run, will modify the operating system of the computer;
- a virus checker is a computer program that, given some other computer program $P$, attempts to determine whether $P$ is a virus;
- a perfect virus checker is a virus checker that *correctly* identifies whether $P$ is a virus for *every* program $P$.

# Every perfect virus checker is itself a virus

Proof:

- Let $V$ be a perfect virus checker.
- Write a new program $X$ that does the following:
  1. Use $V$ to examine $X$ itself, and (correctly) determine whether $X$ is a virus.
  2. If the answer is yes, terminate.
  3. If the answer is no, modify the operating system of the computer.

What happens when you run $X$?

- If $X$ is *not* a virus: $X$ will modify the operating system. Therefore $X$ is a virus. Contradiction!
- Therefore $X$ *is* a virus. $X$ just runs $V$ and terminates...
  so it must be $V$ that modifies the operating system!

Therefore $V$ is a virus also. □

# Methods of proof

We just used two methods of proof:

- The overall proof was a direct proof.

  To show that $P(x) \rightarrow Q(x)$,
  choose an arbitrary $x$ from the domain for which $P(x)$ is true
  *($x$ is a perfect virus checker)*
  and use logical inference to show that $Q(x)$ is true also.
  *($x$ is a virus)*

- One of the smaller steps was a proof by contradiction.

  To show that $p$ is true, *(our new program is a virus)*
  assume that $p$ is false *(our new program is not a virus)*
  and use logical inference to prove a contradiction.

We will see these again (and again, and again...)!

# Prime and composite

**Prime numbers**

The natural number $n$ is prime if and only if $n > 1$ and,
for all $r, s \in \mathbb{N}$, if $n = r \cdot s$ then $r = 1$ or $s = 1$.

Examples: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, ...

The second line is:
$\forall r, s \in \mathbb{N},\ (n = r \cdot s) \rightarrow (r = 1 \vee s = 1)$

**Composite numbers**

The natural number $n$ is composite if and only if $n > 1$ and
$n = r \cdot s$ for some $r, s \in \mathbb{N}$ with $r \neq 1$ and $s \neq 1$.

Examples: $4 = 2 \cdot 2, \quad 30 = 5 \cdot 6, \quad 91 = 7 \cdot 13$

The second line is:
$\exists r, s \in \mathbb{N}$ such that $n = r \cdot s \wedge r \neq 1 \wedge s \neq 1$

# Prime and composite

**Observation**

*If $n > 1$, then $n$ is either prime or composite, but not both.*

Why? The conditions

$$\forall r, s \in \mathbb{N}, (n = r \cdot s) \to (r = 1 \vee s = 1)$$

$$\exists r, s \in \mathbb{N} \text{ such that } (n = r \cdot s) \wedge r \neq 1 \wedge s \neq 1$$

are negations of each other!

# The equivalence

For any natural number $n > 1$:

Prime: $\forall r, s \in \mathbb{N}, (n = r \cdot s) \to (r = 1 \lor s = 1)$
Composite: $\exists r, s \in \mathbb{N}$ such that $(n = r \cdot s) \land r \neq 1 \land s \neq 1$

# Prime factorisation

**Theorem**

*Every natural number $n > 1$ can be written as a product of primes.*

$$\begin{aligned} 2 &= 2 \\ 6 &= 2 \cdot 3 \\ 17 &= 17 \\ 120 &= 2 \cdot 2 \cdot 2 \cdot 3 \cdot 5 \\ 2015 &= 5 \cdot 13 \cdot 31 \end{aligned}$$

We will use a proof by contradiction.

# Prime factorisation

**Proof.** Suppose the theorem is false. Then there exists a natural number $n > 1$ that is not a product of primes.

Choose the smallest such number $n$. From the previous lemma, either $n$ is prime or $n$ is composite. We take cases:

- If $n$ is prime, then $n$ is trivially a product of primes ($n = n$).
- If $n$ is composite, then $n = r \cdot s$ for natural numbers $r \neq 1$ and $s \neq 1$. This implies that $1 < r < n$ and $1 < s < n$.

  Because we chose $n$ to be the smallest natural number that is not a product of primes, both $r$ and $s$ (which are smaller) must be products of primes. Therefore $n = r \cdot s$ is a product of primes also.

So, regardless of whether $n$ is prime or composite, we find that $n$ is a product of primes. This contradicts our choice of $n$.

Therefore every natural number $n > 1$ is a product of primes. $\square$