# Discrete Mathematics, 1st lecture

Peeter Laud

Cybernetica AS

September 6th, 2012

# Discrete Mathematics

MTAT.05.008

Autumn 2012

| | | | |
|---|---|---|---|
| Lectures | Thu 14:15–15:45 | L2-405 | Peeter Laud |
| Practice sessions<br>or | Mon 14:15–15:45<br>Thu 16:15–17:45 | L2-207<br>L2-202 | Margus Niitsoo |
| Behind the scenes | | | Reimo Palm |

http://research.cyber.ee/~peeter/teaching/diskmat12s

peeter.laud@cyber.ee

| | | |
|---|---|---|
| To pass: | three tests during lectures or in January | 15+30+30pt |
| | Homework in practice sessions | 30pt |
| | Checking others' homework | |

This is **not** MTAT.05.109 “Elements of Discrete Mathematics”

# Contents of the course

1. Recap: sets, relations, functions
2. Elements of graph theory
    1. Eulerian and Hamiltonian graphs
    2. Flows, covers, matchings
    3. Edge and vertex coloring
3. Basics of counting
    1. Combinations, permutations, etc.
        - Identities between them
    2. Principle of inclusion and exclusion
    3. Generating functions
    4. Ramsey theory (ordered substructures of random structures)
    5. (if time: Polya theory of counting)

# Actual contents

## Proving mathematical statements

Appreciating proofs

Because you'll need to evaluate arguments in your professional career

### Proving theorems is...

- similar to putting together puzzles
- quite similar to programming, really...
- definitely **non**-magical

Verifying a proof — like checking if a puzzle has been correctly assembled

# What is a proof?

A proof of a statement $S$ is an inference in an axiomatic system that ends with $S$

## Axiomatic system

...consists of

- A language for statements
- A set of statements — axioms
- A set of inference rules

# An example system

## Basic 1st order propositional calculus

### Language

$F, G ::= A \mid \neg F \mid F \Rightarrow G \mid \forall x.F$
$A ::= P(t_1, \ldots, t_k)$, etc.
$P$ — predicate symbols
$t_1, \ldots, t_k$ — terms (incl. variables)

### Inference rules

$$\frac{F \Rightarrow G \quad F}{G}\ \text{(MP)} \qquad \frac{F}{\forall x.F}\ \text{(G)}$$

### Axioms (actually, axiom *schemata*)

(A1) $F \Rightarrow F$
(A2) $F \Rightarrow (G \Rightarrow F)$
(A3) $(F \Rightarrow (G \Rightarrow H)) \Rightarrow ((F \Rightarrow G) \Rightarrow (F \Rightarrow H))$
(A4) $\neg F \Rightarrow (F \Rightarrow G)$
(A5) $\forall x.F \Rightarrow F[x := t]$
(A6) $\forall x.(F \Rightarrow G) \Rightarrow (\forall x.F \Rightarrow \forall x.G)$
(A7) $F \Rightarrow \forall x.F$ if $x$ does not occur *freely* in $F$

# Example proof

Let us prove $\forall x.\forall y.P(x, y) \Rightarrow \forall y.\forall x.P(x, y)$

# Example proof

Let us prove $\forall x.\forall y.P(x,y) \Rightarrow \forall w.\forall z.P(z,w)$

## Axioms

(A2) $F \Rightarrow (G \Rightarrow F)$
(A3) $(F \Rightarrow (G \Rightarrow H)) \Rightarrow ((F \Rightarrow G) \Rightarrow (F \Rightarrow H))$
(A5) $\forall x.F \Rightarrow F[x := t]$
(A6) $\forall x.(F \Rightarrow G) \Rightarrow (\forall x.F \Rightarrow \forall x.G)$
(A7) $F \Rightarrow \forall x.F$ if $x$ does not occur *freely* in $F$

## Inference rules

$$\frac{F \Rightarrow G \quad F}{G} \text{ (MP)}$$

$$\frac{F}{\forall x.F} \text{ (G)}$$

# Example proof

Let us prove $\forall x.\forall y.P(x,y) \Rightarrow \forall w.\forall z.P(z,w)$

**Axioms**

(A2) $F \Rightarrow (G \Rightarrow F)$
(A3) $(F \Rightarrow (G \Rightarrow H)) \Rightarrow ((F \Rightarrow G) \Rightarrow (F \Rightarrow H))$
(A5) $\forall x.F \Rightarrow F[x := t]$
(A6) $\forall x.(F \Rightarrow G) \Rightarrow (\forall x.F \Rightarrow \forall x.G)$
(A7) $F \Rightarrow \forall x.F$ if $x$ does not occur *freely* in $F$

**Inference rules**

$$\frac{F \Rightarrow G \quad F}{G} \text{ (MP)}$$

$$\frac{F}{\forall x.F} \text{ (G)}$$

1. (A5) $\forall x.\forall y.P(x,y) \Rightarrow \forall y.P(z,y)$

# Example proof

Let us prove $\forall x.\forall y.P(x,y) \Rightarrow \forall w.\forall z.P(z,w)$

## Axioms

(A2) $F \Rightarrow (G \Rightarrow F)$
(A3) $(F \Rightarrow (G \Rightarrow H)) \Rightarrow ((F \Rightarrow G) \Rightarrow (F \Rightarrow H))$
(A5) $\forall x.F \Rightarrow F[x := t]$
(A6) $\forall x.(F \Rightarrow G) \Rightarrow (\forall x.F \Rightarrow \forall x.G)$
(A7) $F \Rightarrow \forall x.F$ if $x$ does not occur *freely* in $F$

## Inference rules

$$\frac{F \Rightarrow G \quad F}{G} \text{ (MP)}$$

$$\frac{F}{\forall x.F} \text{ (G)}$$

1. (A5) $\forall x.\forall y.P(x,y) \Rightarrow \forall y.P(z,y)$
2. (A5) $\forall y.P(z,y) \Rightarrow P(z,w)$

# Example proof

Let us prove $\forall x.\forall y.P(x,y) \Rightarrow \forall w.\forall z.P(z,w)$

**Axioms**

(A2) $F \Rightarrow (G \Rightarrow F)$
(A3) $(F \Rightarrow (G \Rightarrow H)) \Rightarrow ((F \Rightarrow G) \Rightarrow (F \Rightarrow H))$
(A5) $\forall x.F \Rightarrow F[x := t]$
(A6) $\forall x.(F \Rightarrow G) \Rightarrow (\forall x.F \Rightarrow \forall x.G)$
(A7) $F \Rightarrow \forall x.F$ if $x$ does not occur *freely* in $F$

**Inference rules**

$$\frac{F \Rightarrow G \quad F}{G} \text{ (MP)}$$

$$\frac{F}{\forall x.F} \text{ (G)}$$

1. (A5) $\forall x.\forall y.P(x,y) \Rightarrow \forall y.P(z,y)$
2. (A5) $\forall y.P(z,y) \Rightarrow P(z,w)$
3. (A2) $(\forall y.P(z,y) \Rightarrow P(z,w)) \Rightarrow (\forall x.\forall y.P(x,y) \Rightarrow (\forall y.P(z,y) \Rightarrow P(z,w)))$

# Example proof

Let us prove $\forall x.\forall y.P(x,y) \Rightarrow \forall w.\forall z.P(z,w)$

**Axioms**

(A2) $F \Rightarrow (G \Rightarrow F)$
(A3) $(F \Rightarrow (G \Rightarrow H)) \Rightarrow ((F \Rightarrow G) \Rightarrow (F \Rightarrow H))$
(A5) $\forall x.F \Rightarrow F[x := t]$
(A6) $\forall x.(F \Rightarrow G) \Rightarrow (\forall x.F \Rightarrow \forall x.G)$
(A7) $F \Rightarrow \forall x.F$ if $x$ does not occur *freely* in $F$

**Inference rules**

$$\frac{F \Rightarrow G \quad F}{G}\ \text{(MP)}$$

$$\frac{F}{\forall x.F}\ \text{(G)}$$

1. (A5) $\forall x.\forall y.P(x,y) \Rightarrow \forall y.P(z,y)$
2. (A5) $\forall y.P(z,y) \Rightarrow P(z,w)$
3. (A2) $(\forall y.P(z,y) \Rightarrow P(z,w)) \Rightarrow (\forall x.\forall y.P(x,y) \Rightarrow (\forall y.P(z,y) \Rightarrow P(z,w)))$
4. ($MP_{3,2}$) $\forall x.\forall y.P(x,y) \Rightarrow (\forall y.P(z,y) \Rightarrow P(z,w))$

# Example proof

Let us prove $\forall x.\forall y.P(x,y) \Rightarrow \forall w.\forall z.P(z,w)$

## Axioms

(A2) $F \Rightarrow (G \Rightarrow F)$
(A3) $(F \Rightarrow (G \Rightarrow H)) \Rightarrow ((F \Rightarrow G) \Rightarrow (F \Rightarrow H))$
(A5) $\forall x.F \Rightarrow F[x := t]$
(A6) $\forall x.(F \Rightarrow G) \Rightarrow (\forall x.F \Rightarrow \forall x.G)$
(A7) $F \Rightarrow \forall x.F$ if $x$ does not occur *freely* in $F$

## Inference rules

$$\frac{F \Rightarrow G \quad F}{G} \text{ (MP)}$$

$$\frac{F}{\forall x.F} \text{ (G)}$$

1. (A5) $\forall x.\forall y.P(x,y) \Rightarrow \forall y.P(z,y)$
4. (MP$_{3,2}$) $\forall x.\forall y.P(x,y) \Rightarrow (\forall y.P(z,y) \Rightarrow P(z,w))$
5. (A3) $(\forall x.\forall y.P(x,y) \Rightarrow (\forall y.P(z,y) \Rightarrow P(z,w))) \Rightarrow ((\forall x.\forall y.P(x,y) \Rightarrow \forall y.P(z,y)) \Rightarrow (\forall x.\forall y.P(x,y) \Rightarrow P(z,w)))$

# Example proof

Let us prove $\forall x.\forall y.P(x,y) \Rightarrow \forall w.\forall z.P(z,w)$

## Axioms

(A2) $F \Rightarrow (G \Rightarrow F)$
(A3) $(F \Rightarrow (G \Rightarrow H)) \Rightarrow ((F \Rightarrow G) \Rightarrow (F \Rightarrow H))$
(A5) $\forall x.F \Rightarrow F[x := t]$
(A6) $\forall x.(F \Rightarrow G) \Rightarrow (\forall x.F \Rightarrow \forall x.G)$
(A7) $F \Rightarrow \forall x.F$ if $x$ does not occur *freely* in $F$

## Inference rules

$$\frac{F \Rightarrow G \quad F}{G}\ (\mathrm{MP})$$

$$\frac{F}{\forall x.F}\ (\mathrm{G})$$

1. (A5) $\forall x.\forall y.P(x,y) \Rightarrow \forall y.P(z,y)$
4. (MP$_{3,2}$) $\forall x.\forall y.P(x,y) \Rightarrow (\forall y.P(z,y) \Rightarrow P(z,w))$
5. (A3) $(\forall x.\forall y.P(x,y) \Rightarrow (\forall y.P(z,y) \Rightarrow P(z,w))) \Rightarrow ((\forall x.\forall y.P(x,y) \Rightarrow \forall y.P(z,y)) \Rightarrow (\forall x.\forall y.P(x,y) \Rightarrow P(z,w)))$
6. (MP$_{5,4}$) $(\forall x.\forall y.P(x,y) \Rightarrow \forall y.P(z,y)) \Rightarrow (\forall x.\forall y.P(x,y) \Rightarrow P(z,w))$

# Example proof

Let us prove $\forall x.\forall y.P(x,y) \Rightarrow \forall w.\forall z.P(z,w)$

**Axioms**

(A2) $F \Rightarrow (G \Rightarrow F)$
(A3) $(F \Rightarrow (G \Rightarrow H)) \Rightarrow ((F \Rightarrow G) \Rightarrow (F \Rightarrow H))$
(A5) $\forall x.F \Rightarrow F[x := t]$
(A6) $\forall x.(F \Rightarrow G) \Rightarrow (\forall x.F \Rightarrow \forall x.G)$
(A7) $F \Rightarrow \forall x.F$ if $x$ does not occur *freely* in $F$

**Inference rules**

$$\frac{F \Rightarrow G \quad F}{G} \text{ (MP)}$$

$$\frac{F}{\forall x.F} \text{ (G)}$$

1. (A5) $\forall x.\forall y.P(x,y) \Rightarrow \forall y.P(z,y)$
6. ($\mathrm{MP}_{5,4}$) $(\forall x.\forall y.P(x,y) \Rightarrow \forall y.P(z,y)) \Rightarrow (\forall x.\forall y.P(x,y) \Rightarrow P(z,w))$
7. ($\mathrm{MP}_{6,1}$) $\forall x.\forall y.P(x,y) \Rightarrow P(z,w)$

# Example proof

Let us prove $\forall x.\forall y.P(x,y) \Rightarrow \forall w.\forall z.P(z,w)$

**Axioms**

(A2) $F \Rightarrow (G \Rightarrow F)$
(A3) $(F \Rightarrow (G \Rightarrow H)) \Rightarrow ((F \Rightarrow G) \Rightarrow (F \Rightarrow H))$
(A5) $\forall x.F \Rightarrow F[x := t]$
(A6) $\forall x.(F \Rightarrow G) \Rightarrow (\forall x.F \Rightarrow \forall x.G)$
(A7) $F \Rightarrow \forall x.F$ if $x$ does not occur *freely* in $F$

**Inference rules**

$$\frac{F \Rightarrow G \quad F}{G} \text{ (MP)}$$

$$\frac{F}{\forall x.F} \text{ (G)}$$

7. $(\mathrm{MP}_{6,1})$ $\forall x.\forall y.P(x,y) \Rightarrow P(z,w)$
8. $(\mathrm{G}_7)$ $\forall z.(\forall x.\forall y.P(x,y) \Rightarrow P(z,w))$

# Example proof

Let us prove $\forall x.\forall y.P(x,y) \Rightarrow \forall w.\forall z.P(z,w)$

**Axioms**

(A2) $F \Rightarrow (G \Rightarrow F)$
(A3) $(F \Rightarrow (G \Rightarrow H)) \Rightarrow ((F \Rightarrow G) \Rightarrow (F \Rightarrow H))$
(A5) $\forall x.F \Rightarrow F[x := t]$
(A6) $\forall x.(F \Rightarrow G) \Rightarrow (\forall x.F \Rightarrow \forall x.G)$
(A7) $F \Rightarrow \forall x.F$ if $x$ does not occur *freely* in $F$

**Inference rules**

$$\frac{F \Rightarrow G \quad F}{G} \text{ (MP)}$$

$$\frac{F}{\forall x.F} \text{ (G)}$$

8. ($G_7$) $\forall z.(\forall x.\forall y.P(x,y) \Rightarrow P(z,w))$
9. (A6) $\forall z.(\forall x.\forall y.P(x,y) \Rightarrow P(z,w)) \Rightarrow (\forall z.\forall x.\forall y.P(x,y) \Rightarrow \forall z.P(z,w))$

# Example proof

Let us prove $\forall x.\forall y.P(x,y) \Rightarrow \forall w.\forall z.P(z,w)$

**Axioms**

(A2) $F \Rightarrow (G \Rightarrow F)$
(A3) $(F \Rightarrow (G \Rightarrow H)) \Rightarrow ((F \Rightarrow G) \Rightarrow (F \Rightarrow H))$
(A5) $\forall x.F \Rightarrow F[x := t]$
(A6) $\forall x.(F \Rightarrow G) \Rightarrow (\forall x.F \Rightarrow \forall x.G)$
(A7) $F \Rightarrow \forall x.F$ if $x$ does not occur *freely* in $F$

**Inference rules**

$$\frac{F \Rightarrow G \quad F}{G} \text{ (MP)}$$

$$\frac{F}{\forall x.F} \text{ (G)}$$

8. (G$_7$) $\forall z.(\forall x.\forall y.P(x,y) \Rightarrow P(z,w))$
9. (A6) $\forall z.(\forall x.\forall y.P(x,y) \Rightarrow P(z,w)) \Rightarrow (\forall z.\forall x.\forall y.P(x,y) \Rightarrow \forall z.P(z,w))$
10. (MP$_{9,8}$) $\forall z.\forall x.\forall y.P(x,y) \Rightarrow \forall z.P(z,w)$

# Example proof

Let us prove $\forall x.\forall y.P(x,y) \Rightarrow \forall w.\forall z.P(z,w)$

## Axioms

(A2) $F \Rightarrow (G \Rightarrow F)$
(A3) $(F \Rightarrow (G \Rightarrow H)) \Rightarrow ((F \Rightarrow G) \Rightarrow (F \Rightarrow H))$
(A5) $\forall x.F \Rightarrow F[x := t]$
(A6) $\forall x.(F \Rightarrow G) \Rightarrow (\forall x.F \Rightarrow \forall x.G)$
(A7) $F \Rightarrow \forall x.F$ if $x$ does not occur *freely* in $F$

## Inference rules

$$\frac{F \Rightarrow G \quad F}{G} \text{ (MP)}$$

$$\frac{F}{\forall x.F} \text{ (G)}$$

10. (MP$_{9,8}$) $\forall z.\forall x.\forall y.P(x,y) \Rightarrow \forall z.P(z,w)$
11. (A7) $\forall x.\forall y.P(x,y) \Rightarrow \forall z.\forall x.\forall y.P(x,y)$

# Example proof

Let us prove $\forall x.\forall y.P(x,y) \Rightarrow \forall w.\forall z.P(z,w)$

## Axioms

(A2) $F \Rightarrow (G \Rightarrow F)$
(A3) $(F \Rightarrow (G \Rightarrow H)) \Rightarrow ((F \Rightarrow G) \Rightarrow (F \Rightarrow H))$
(A5) $\forall x.F \Rightarrow F[x := t]$
(A6) $\forall x.(F \Rightarrow G) \Rightarrow (\forall x.F \Rightarrow \forall x.G)$
(A7) $F \Rightarrow \forall x.F$ if $x$ does not occur *freely* in $F$

## Inference rules

$$\frac{F \Rightarrow G \quad F}{G} \text{ (MP)}$$

$$\frac{F}{\forall x.F} \text{ (G)}$$

10. (MP$_{9,8}$) $\forall z.\forall x.\forall y.P(x,y) \Rightarrow \forall z.P(z,w)$
11. (A7) $\forall x.\forall y.P(x,y) \Rightarrow \forall z.\forall x.\forall y.P(x,y)$
12. (A2) $(\forall z.\forall x.\forall y.P(x,y) \Rightarrow \forall z.P(z,w)) \Rightarrow (\forall x.\forall y.P(x,y) \Rightarrow (\forall z.\forall x.\forall y.P(x,y) \Rightarrow \forall z.P(z,w)))$

# Example proof

Let us prove $\forall x.\forall y.P(x,y) \Rightarrow \forall w.\forall z.P(z,w)$

## Axioms

(A2) $F \Rightarrow (G \Rightarrow F)$
(A3) $(F \Rightarrow (G \Rightarrow H)) \Rightarrow ((F \Rightarrow G) \Rightarrow (F \Rightarrow H))$
(A5) $\forall x.F \Rightarrow F[x := t]$
(A6) $\forall x.(F \Rightarrow G) \Rightarrow (\forall x.F \Rightarrow \forall x.G)$
(A7) $F \Rightarrow \forall x.F$ if $x$ does not occur *freely* in $F$

## Inference rules

$$\frac{F \Rightarrow G \quad F}{G} \text{ (MP)}$$

$$\frac{F}{\forall x.F} \text{ (G)}$$

10. (MP$_{9,8}$) $\forall z.\forall x.\forall y.P(x,y) \Rightarrow \forall z.P(z,w)$
11. (A7) $\forall x.\forall y.P(x,y) \Rightarrow \forall z.\forall x.\forall y.P(x,y)$
12. (A2) $(\forall z.\forall x.\forall y.P(x,y) \Rightarrow \forall z.P(z,w)) \Rightarrow (\forall x.\forall y.P(x,y) \Rightarrow (\forall z.\forall x.\forall y.P(x,y) \Rightarrow \forall z.P(z,w)))$
13. (MP$_{12,10}$) $\forall x.\forall y.P(x,y) \Rightarrow (\forall z.\forall x.\forall y.P(x,y) \Rightarrow \forall z.P(z,w))$

# Example proof

Let us prove $\forall x.\forall y.P(x,y) \Rightarrow \forall w.\forall z.P(z,w)$

**Axioms**

(A2) $F \Rightarrow (G \Rightarrow F)$
(A3) $(F \Rightarrow (G \Rightarrow H)) \Rightarrow ((F \Rightarrow G) \Rightarrow (F \Rightarrow H))$
(A5) $\forall x.F \Rightarrow F[x := t]$
(A6) $\forall x.(F \Rightarrow G) \Rightarrow (\forall x.F \Rightarrow \forall x.G)$
(A7) $F \Rightarrow \forall x.F$ if $x$ does not occur *freely* in $F$

**Inference rules**

$$\frac{F \Rightarrow G \quad F}{G} \text{ (MP)}$$

$$\frac{F}{\forall x.F} \text{ (G)}$$

11. (A7) $\forall x.\forall y.P(x,y) \Rightarrow \forall z.\forall x.\forall y.P(x,y)$
13. (MP$_{12,10}$) $\forall x.\forall y.P(x,y) \Rightarrow (\forall z.\forall x.\forall y.P(x,y) \Rightarrow \forall z.P(z,w))$
14. (A3) $(\forall x.\forall y.P(x,y) \Rightarrow (\forall z.\forall x.\forall y.P(x,y) \Rightarrow \forall z.P(z,w))) \Rightarrow ((\forall x.\forall y.P(x,y) \Rightarrow \forall z.\forall x.\forall y.P(x,y)) \Rightarrow (\forall x.\forall y.P(x,y) \Rightarrow \forall z.P(z,w)))$

# Example proof

Let us prove $\forall x.\forall y.P(x,y) \Rightarrow \forall w.\forall z.P(z,w)$

## Axioms

(A2) $F \Rightarrow (G \Rightarrow F)$
(A3) $(F \Rightarrow (G \Rightarrow H)) \Rightarrow ((F \Rightarrow G) \Rightarrow (F \Rightarrow H))$
(A5) $\forall x.F \Rightarrow F[x := t]$
(A6) $\forall x.(F \Rightarrow G) \Rightarrow (\forall x.F \Rightarrow \forall x.G)$
(A7) $F \Rightarrow \forall x.F$ if $x$ does not occur *freely* in $F$

## Inference rules

$$\frac{F \Rightarrow G \quad F}{G} \text{ (MP)}$$

$$\frac{F}{\forall x.F} \text{ (G)}$$

11. (A7) $\forall x.\forall y.P(x,y) \Rightarrow \forall z.\forall x.\forall y.P(x,y)$
13. (MP$_{12,10}$) $\forall x.\forall y.P(x,y) \Rightarrow (\forall z.\forall x.\forall y.P(x,y) \Rightarrow \forall z.P(z,w))$
14. (A3) $(\forall x.\forall y.P(x,y) \Rightarrow (\forall z.\forall x.\forall y.P(x,y) \Rightarrow \forall z.P(z,w))) \Rightarrow ((\forall x.\forall y.P(x,y) \Rightarrow \forall z.\forall x.\forall y.P(x,y)) \Rightarrow (\forall x.\forall y.P(x,y) \Rightarrow \forall z.P(z,w)))$
15. (MP$_{14,13}$) $(\forall x.\forall y.P(x,y) \Rightarrow \forall z.\forall x.\forall y.P(x,y)) \Rightarrow (\forall x.\forall y.P(x,y) \Rightarrow \forall z.P(z,w))$

# Example proof

Let us prove $\forall x.\forall y.P(x,y) \Rightarrow \forall w.\forall z.P(z,w)$

## Axioms

(A2) $F \Rightarrow (G \Rightarrow F)$
(A3) $(F \Rightarrow (G \Rightarrow H)) \Rightarrow ((F \Rightarrow G) \Rightarrow (F \Rightarrow H))$
(A5) $\forall x.F \Rightarrow F[x := t]$
(A6) $\forall x.(F \Rightarrow G) \Rightarrow (\forall x.F \Rightarrow \forall x.G)$
(A7) $F \Rightarrow \forall x.F$ if $x$ does not occur *freely* in $F$

## Inference rules

$$\frac{F \Rightarrow G \quad F}{G} \text{ (MP)}$$

$$\frac{F}{\forall x.F} \text{ (G)}$$

11. (A7) $\forall x.\forall y.P(x,y) \Rightarrow \forall z.\forall x.\forall y.P(x,y)$
15. $(\mathrm{MP}_{14,13})$
 $(\forall x.\forall y.P(x,y) \Rightarrow \forall z.\forall x.\forall y.P(x,y)) \Rightarrow (\forall x.\forall y.P(x,y) \Rightarrow \forall z.P(z,w))$
16. $(\mathrm{MP}_{15,11})$ $\forall x.\forall y.P(x,y) \Rightarrow \forall z.P(z,w)$

# Example proof

Let us prove $\forall x.\forall y.P(x,y) \Rightarrow \forall w.\forall z.P(z,w)$

**Axioms**

(A2) $F \Rightarrow (G \Rightarrow F)$
(A3) $(F \Rightarrow (G \Rightarrow H)) \Rightarrow ((F \Rightarrow G) \Rightarrow (F \Rightarrow H))$
(A5) $\forall x.F \Rightarrow F[x := t]$
(A6) $\forall x.(F \Rightarrow G) \Rightarrow (\forall x.F \Rightarrow \forall x.G)$
(A7) $F \Rightarrow \forall x.F$ if $x$ does not occur *freely* in $F$

**Inference rules**

$$\frac{F \Rightarrow G \quad F}{G} \text{ (MP)}$$

$$\frac{F}{\forall x.F} \text{ (G)}$$

16. (MP$_{15,11}$) $\forall x.\forall y.P(x,y) \Rightarrow \forall z.P(z,w)$
17. (G$_{16}$) $\forall w.(\forall x.\forall y.P(x,y) \Rightarrow \forall z.P(z,w))$

# Example proof

Let us prove $\forall x.\forall y.P(x,y) \Rightarrow \forall w.\forall z.P(z,w)$

## Axioms

(A2) $F \Rightarrow (G \Rightarrow F)$
(A3) $(F \Rightarrow (G \Rightarrow H)) \Rightarrow ((F \Rightarrow G) \Rightarrow (F \Rightarrow H))$
(A5) $\forall x.F \Rightarrow F[x := t]$
(A6) $\forall x.(F \Rightarrow G) \Rightarrow (\forall x.F \Rightarrow \forall x.G)$
(A7) $F \Rightarrow \forall x.F$ if $x$ does not occur *freely* in $F$

## Inference rules

$$\frac{F \Rightarrow G \quad F}{G} \text{ (MP)}$$

$$\frac{F}{\forall x.F} \text{ (G)}$$

17. ($G_{16}$) $\forall w.(\forall x.\forall y.P(x,y) \Rightarrow \forall z.P(z,w))$
18. (A6)
$\forall w.(\forall x.\forall y.P(x,y) \Rightarrow \forall z.P(z,w)) \Rightarrow (\forall w.\forall x.\forall y.P(x,y) \Rightarrow \forall w.\forall z.P(z,w))$

# Example proof

Let us prove $\forall x.\forall y.P(x,y) \Rightarrow \forall w.\forall z.P(z,w)$

## Axioms

(A2) $F \Rightarrow (G \Rightarrow F)$
(A3) $(F \Rightarrow (G \Rightarrow H)) \Rightarrow ((F \Rightarrow G) \Rightarrow (F \Rightarrow H))$
(A5) $\forall x.F \Rightarrow F[x := t]$
(A6) $\forall x.(F \Rightarrow G) \Rightarrow (\forall x.F \Rightarrow \forall x.G)$
(A7) $F \Rightarrow \forall x.F$ if $x$ does not occur *freely* in $F$

## Inference rules

$$\frac{F \Rightarrow G \quad F}{G} \text{ (MP)}$$

$$\frac{F}{\forall x.F} \text{ (G)}$$

17. $(\mathrm{G}_{16})$ $\forall w.(\forall x.\forall y.P(x,y) \Rightarrow \forall z.P(z,w))$
18. (A6)
$\forall w.(\forall x.\forall y.P(x,y) \Rightarrow \forall z.P(z,w)) \Rightarrow (\forall w.\forall x.\forall y.P(x,y) \Rightarrow \forall w.\forall z.P(z,w))$
19. $(\mathrm{MP}_{18,17})$ $\forall w.\forall x.\forall y.P(x,y) \Rightarrow \forall w.\forall z.P(z,w)$

# Example proof

Let us prove $\forall x.\forall y.P(x,y) \Rightarrow \forall w.\forall z.P(z,w)$

**Axioms**

(A2) $F \Rightarrow (G \Rightarrow F)$
(A3) $(F \Rightarrow (G \Rightarrow H)) \Rightarrow ((F \Rightarrow G) \Rightarrow (F \Rightarrow H))$
(A5) $\forall x.F \Rightarrow F[x := t]$
(A6) $\forall x.(F \Rightarrow G) \Rightarrow (\forall x.F \Rightarrow \forall x.G)$
(A7) $F \Rightarrow \forall x.F$ if $x$ does not occur *freely* in $F$

**Inference rules**

$$\frac{F \Rightarrow G \quad F}{G} \text{ (MP)}$$

$$\frac{F}{\forall x.F} \text{ (G)}$$

19. (MP$_{18,17}$) $\forall w.\forall x.\forall y.P(x,y) \Rightarrow \forall w.\forall z.P(z,w)$
20. (A7) $\forall x.\forall y.P(x,y) \Rightarrow \forall w.\forall x.\forall y.P(x,y)$

# Example proof

Let us prove $\forall x.\forall y.P(x,y) \Rightarrow \forall w.\forall z.P(z,w)$

**Axioms**

(A2) $F \Rightarrow (G \Rightarrow F)$
(A3) $(F \Rightarrow (G \Rightarrow H)) \Rightarrow ((F \Rightarrow G) \Rightarrow (F \Rightarrow H))$
(A5) $\forall x.F \Rightarrow F[x := t]$
(A6) $\forall x.(F \Rightarrow G) \Rightarrow (\forall x.F \Rightarrow \forall x.G)$
(A7) $F \Rightarrow \forall x.F$ if $x$ does not occur *freely* in $F$

**Inference rules**

$$\frac{F \Rightarrow G \quad F}{G} \text{ (MP)}$$

$$\frac{F}{\forall x.F} \text{ (G)}$$

19. (MP$_{18,17}$) $\forall w.\forall x.\forall y.P(x,y) \Rightarrow \forall w.\forall z.P(z,w)$
20. (A7) $\forall x.\forall y.P(x,y) \Rightarrow \forall w.\forall x.\forall y.P(x,y)$
21. (A2) $(\forall w.\forall x.\forall y.P(x,y) \Rightarrow \forall w.\forall z.P(z,w)) \Rightarrow (\forall x.\forall y.P(x,y) \Rightarrow$ $(\forall w.\forall x.\forall y.P(x,y) \Rightarrow \forall w.\forall z.P(z,w)))$

# Example proof

Let us prove $\forall x.\forall y.P(x,y) \Rightarrow \forall w.\forall z.P(z,w)$

## Axioms

(A2) $F \Rightarrow (G \Rightarrow F)$
(A3) $(F \Rightarrow (G \Rightarrow H)) \Rightarrow ((F \Rightarrow G) \Rightarrow (F \Rightarrow H))$
(A5) $\forall x.F \Rightarrow F[x := t]$
(A6) $\forall x.(F \Rightarrow G) \Rightarrow (\forall x.F \Rightarrow \forall x.G)$
(A7) $F \Rightarrow \forall x.F$ if $x$ does not occur *freely* in $F$

## Inference rules

$$\frac{F \Rightarrow G \quad F}{G} \text{ (MP)}$$

$$\frac{F}{\forall x.F} \text{ (G)}$$

19. $(\mathrm{MP}_{18,17})$ $\forall w.\forall x.\forall y.P(x,y) \Rightarrow \forall w.\forall z.P(z,w)$
20. (A7) $\forall x.\forall y.P(x,y) \Rightarrow \forall w.\forall x.\forall y.P(x,y)$
21. (A2) $(\forall w.\forall x.\forall y.P(x,y) \Rightarrow \forall w.\forall z.P(z,w)) \Rightarrow (\forall x.\forall y.P(x,y) \Rightarrow (\forall w.\forall x.\forall y.P(x,y) \Rightarrow \forall w.\forall z.P(z,w)))$
22. $(\mathrm{MP}_{21,19})$ $\forall x.\forall y.P(x,y) \Rightarrow (\forall w.\forall x.\forall y.P(x,y) \Rightarrow \forall w.\forall z.P(z,w))$

# Example proof

Let us prove $\forall x.\forall y.P(x,y) \Rightarrow \forall w.\forall z.P(z,w)$

**Axioms**

(A2) $F \Rightarrow (G \Rightarrow F)$
(A3) $(F \Rightarrow (G \Rightarrow H)) \Rightarrow ((F \Rightarrow G) \Rightarrow (F \Rightarrow H))$
(A5) $\forall x.F \Rightarrow F[x := t]$
(A6) $\forall x.(F \Rightarrow G) \Rightarrow (\forall x.F \Rightarrow \forall x.G)$
(A7) $F \Rightarrow \forall x.F$ if $x$ does not occur *freely* in $F$

**Inference rules**

$$\frac{F \Rightarrow G \quad F}{G} \text{ (MP)}$$

$$\frac{F}{\forall x.F} \text{ (G)}$$

20. (A7) $\forall x.\forall y.P(x,y) \Rightarrow \forall w.\forall x.\forall y.P(x,y)$
22. (MP$_{21,19}$) $\forall x.\forall y.P(x,y) \Rightarrow (\forall w.\forall x.\forall y.P(x,y) \Rightarrow \forall w.\forall z.P(z,w))$
23. (A3) $(\forall x.\forall y.P(x,y) \Rightarrow (\forall w.\forall x.\forall y.P(x,y) \Rightarrow \forall w.\forall z.P(z,w))) \Rightarrow ((\forall x.\forall y.P(x,y) \Rightarrow \forall w.\forall x.\forall y.P(x,y)) \Rightarrow (\forall x.\forall y.P(x,y) \Rightarrow \forall w.\forall z.P(z,w)))$

# Example proof

Let us prove $\forall x.\forall y.P(x,y) \Rightarrow \forall w.\forall z.P(z,w)$

## Axioms

(A2) $F \Rightarrow (G \Rightarrow F)$
(A3) $(F \Rightarrow (G \Rightarrow H)) \Rightarrow ((F \Rightarrow G) \Rightarrow (F \Rightarrow H))$
(A5) $\forall x.F \Rightarrow F[x := t]$
(A6) $\forall x.(F \Rightarrow G) \Rightarrow (\forall x.F \Rightarrow \forall x.G)$
(A7) $F \Rightarrow \forall x.F$ if $x$ does not occur *freely* in $F$

## Inference rules

$$\frac{F \Rightarrow G \quad F}{G} \text{ (MP)}$$

$$\frac{F}{\forall x.F} \text{ (G)}$$

20. (A7) $\forall x.\forall y.P(x,y) \Rightarrow \forall w.\forall x.\forall y.P(x,y)$
22. (MP$_{21,19}$) $\forall x.\forall y.P(x,y) \Rightarrow (\forall w.\forall x.\forall y.P(x,y) \Rightarrow \forall w.\forall z.P(z,w))$
23. (A3) $(\forall x.\forall y.P(x,y) \Rightarrow (\forall w.\forall x.\forall y.P(x,y) \Rightarrow \forall w.\forall z.P(z,w))) \Rightarrow ((\forall x.\forall y.P(x,y) \Rightarrow \forall w.\forall x.\forall y.P(x,y)) \Rightarrow (\forall x.\forall y.P(x,y) \Rightarrow \forall w.\forall z.P(z,w)))$
24. (MP$_{23,22}$) $(\forall x.\forall y.P(x,y) \Rightarrow \forall w.\forall x.\forall y.P(x,y)) \Rightarrow (\forall x.\forall y.P(x,y) \Rightarrow \forall w.\forall z.P(z,w))$

# Example proof

Let us prove $\forall x.\forall y.P(x,y) \Rightarrow \forall w.\forall z.P(z,w)$

**Axioms**

(A2) $F \Rightarrow (G \Rightarrow F)$
(A3) $(F \Rightarrow (G \Rightarrow H)) \Rightarrow ((F \Rightarrow G) \Rightarrow (F \Rightarrow H))$
(A5) $\forall x.F \Rightarrow F[x := t]$
(A6) $\forall x.(F \Rightarrow G) \Rightarrow (\forall x.F \Rightarrow \forall x.G)$
(A7) $F \Rightarrow \forall x.F$ if $x$ does not occur *freely* in $F$

**Inference rules**

$$\frac{F \Rightarrow G \quad F}{G}\ \text{(MP)}$$

$$\frac{F}{\forall x.F}\ \text{(G)}$$

20. (A7) $\forall x.\forall y.P(x,y) \Rightarrow \forall w.\forall x.\forall y.P(x,y)$
24. ($\mathrm{MP}_{23,22}$)
$(\forall x.\forall y.P(x,y) \Rightarrow \forall w.\forall x.\forall y.P(x,y)) \Rightarrow (\forall x.\forall y.P(x,y) \Rightarrow \forall w.\forall z.P(z,w))$
25. ($\mathrm{MP}_{24,20}$) $\forall x.\forall y.P(x,y) \Rightarrow \forall w.\forall z.P(z,w)$

# Comments on that proof

## Some intermediate statements made sense

1. $\forall x.\forall y.P(x,y) \Rightarrow \forall y.P(z,y)$
7. $\forall x.\forall y.P(x,y) \Rightarrow P(z,w)$
16. $\forall x.\forall y.P(x,y) \Rightarrow \forall z.P(z,w)$
25. $\forall x.\forall y.P(x,y) \Rightarrow \forall w.\forall z.P(z,w)$

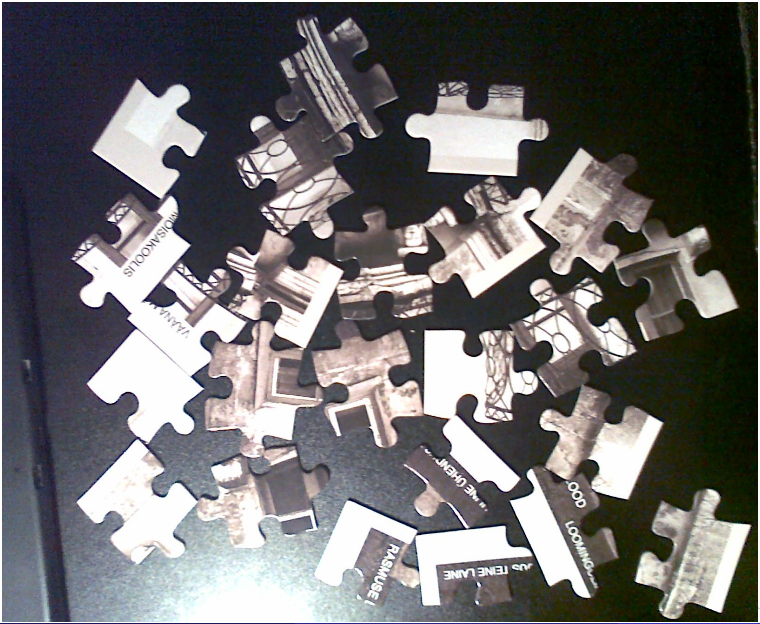
## Some others…

- …were rather less intuitive
  - Especially the instances of (A3)
- …were necessary for the pieces to fit

## Some common patterns emerged

E.g. the derivation $\dfrac{F \Rightarrow G \quad G \Rightarrow H}{F \Rightarrow H}$ took 5 steps and was used thrice

# Assemblying a zig-zag puzzle



# Assemblying a zig-zag puzzle

# Verifying a proof

- Formally, this is purely syntactic
- Each line has to follow from the previous ones
- It is not necessary to understand the subject matter to do the verification

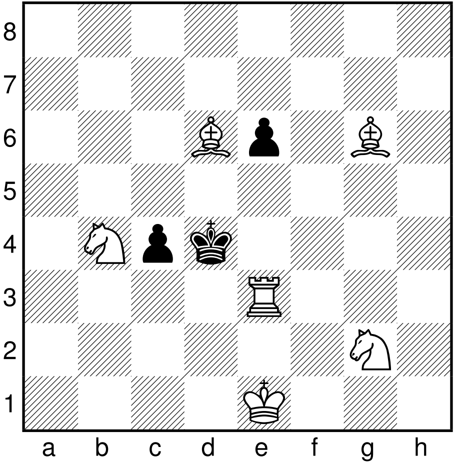
# Verifying the assembly of a zig-zag puzzle

Do the pieces fit together?

# Details omitted. . .

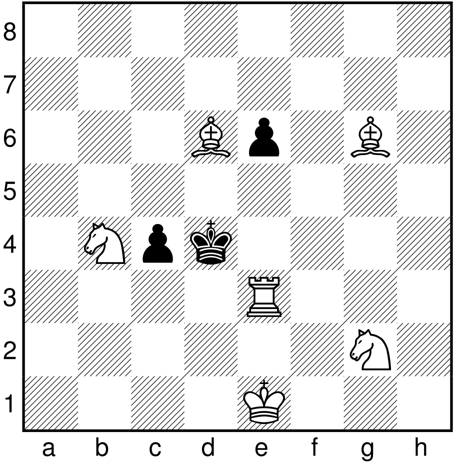
- The “proofs” you’ve seen in previous lectures and textbooks look rather different
- Such list of formulas was not given
- There was much more “semantic” reasoning

# Chess etudes




White to start and checkmate in two moves.

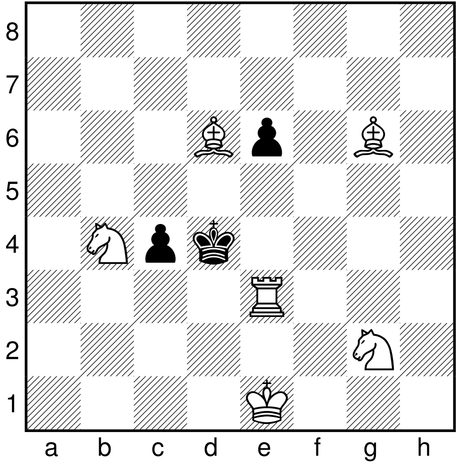
# Chess etudes




White to start and checkmate in two moves.

**Solution**

| | | |
|---|---|---|
| **1** | ♘**h4** | ♚×**e3** |
| **2** | ♘**c2#** | |




White to start and checkmate in two moves.

**Solution**

| | | |
|---|---|---|
| **1** | **♘h4** | **♚×e3** |
| **2** | **♘c2#** | |

- What if black moves 1...c3 or 1...e5 instead?

# Bridge exercises

♠ 8 7 5 4 3
♥ —
♦ Q 9 8 7 6 4 3
♣ 2

N
W E
S

♠ A K Q J 10 9 6
♥ —
♦ 2
♣ Q 9 8 7 5

West leads ♥K.
South to make 6♠.

♠ 8 7 5 4 3
♥ —
♦ Q 9 8 7 6 4 3
♣ 2

N
W E
S

♠ A K Q J 10 9 6
♥ —
♦ 2
♣ Q 9 8 7 5

West leads ♥K.
South to make 6♠.

**Solution**

Although this one is not difficult, it is easy to go wrong at trick one. The winning play is to discard dummy's club, ruff high, then lead the ♦2. On a trump return, dummy's eight-spot provides an entry necessary to set up and enjoy a diamond trick, in case that suit should split **5-0**; any other return permits a high crossruff.

# Bridge exercises

♠ 8 7 5 4 3
♥ —
♦ Q 9 8 7 6 4 3
♣ 2

N
W E
S

♠ A K Q J 10 9 6
♥ —
♦ 2
♣ Q 9 8 7 5

West leads ♥K.
South to make 6♠.

## Solution

Although this one is not difficult, it is easy to go wrong at trick one. The winning play is to discard dummy's club, ruff high, then lead the ♦2. On a trump return, dummy's eight-spot provides an entry necessary to set up and enjoy a diamond trick, in case that suit should split **5-0**; any other return permits a high crossruff.

This looks very different from a game tree. . .

# Recap

- A proof of $S$ is a sequence (ending with $S$) of statements, that
  - are axioms, or
  - are derivable from previous statements using the inference rules.
- Verification means performing certain syntactic checks for each statement in the sequence.
  - Any semantic knowledge we have only helps in assemblying the proof.
- In actual presentations, most details of the sequence of statements are omitted.
  - But anyone *sufficiently skilled in the art* should be able to fill them in.

# Other axiomatic systems

Obtained by adding to the 1st order logic

- specific constants, function and predicate symbols in the language;
- specific axioms and inference rules.

## Peano's axioms for arithmetic

- Constant "0", unary function "$s$", binary predicate "$=$".
- Axioms and axiom schemata:
  - $\forall x.(x = x)$
  - $\forall x, y.\big((x = y) \Rightarrow (F(x) \Rightarrow F(y))\big)$
  - $\forall x.\neg(s(x) = 0)$
  - $\forall x.\forall y.\big((s(x) = s(y)) \Rightarrow (x = y)\big)$
  - $F(0) \wedge \forall x.(F(x) \Rightarrow F(s(x))) \Rightarrow \forall x.F(x)$
- No new inference rules

**Exercise.** Show that "$=$" is symmetric.

# Sets

## Non-definition

A set is an unordered collection of elements (without counts)

“Object x is an element of set X” is denoted by $x \in X$

Two sets are equal if the have the same elements

$$X = Y :\Leftrightarrow \forall z.(z \in X \Leftrightarrow z \in Y)$$

## Definition

A set $X$ is a subset of a set $Y$ if all elements of $X$ are also elements of $Y$. Denoted $X \subseteq Y$.

$$X \subseteq Y :\Leftrightarrow \forall z.(z \in X \Rightarrow z \in Y)$$

## Theorem

*Two sets are equal iff both are subsets of each other.*

$$X = Y \Leftrightarrow (X \subseteq Y \wedge Y \subseteq X)$$

# Operations with sets

- The union $X \cup Y$ of two sets $X$ and $Y$ contains exactly those elements that belong to $X$ or $Y$ (or both).

$$\forall z.(z \in X \cup Y \Leftrightarrow (z \in X \vee z \in Y))$$

- The intersection: $\forall z.(z \in X \cap Y \Leftrightarrow (z \in X \wedge z \in Y))$
- The difference: $\forall z.(z \in X \backslash Y \Leftrightarrow (z \in X \wedge z \notin Y))$
- The complement: Let $U$ be some universal set.
  - All sets in our current application will be subsets of $U$.

  The complement of the set $X \subseteq U$ is $\overline{X} = U \backslash X$.
  - Also denoted $X'$

# Properties of these operations

## A large number of theorems

- $X \subseteq X \cup Y$
- $X \cap Y \subseteq X$
- $X \cup Y = Y \cup X$
- $X \cap Y = Y \cap X$
- $\overline{X \cap Y} = \overline{X} \cup \overline{Y}$
- $\overline{X \cup Y} = \overline{X} \cap \overline{Y}$
- $X \cup (Y \cup Z) = (X \cup Y) \cup Z$
- $X \cap (Y \cap Z) = (X \cap Y) \cap Z$
- $X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$
- $X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$
- $X \subseteq Y \Leftrightarrow X \cup Y = Y$
- $X \subseteq Y \Leftrightarrow X \cap Y = X$

Let us prove some (on blackboard)

# Omitting some proofs

- Why aren't we doing some proofs here?
  - Because the lecture time is limited.
  - Not because some proofs are less important than the others.
- How will you learn those proofs?
  - Some may be done in the practice session.
  - The rest, you should attempt at home.
    - And eventually succeed with all of them.
  - Doing proofs yourself (or in small groups) is an excellent way to study.

# Cartesian products. Relations

## Non-definition

One can form the ordered pair $(x, y)$ of any two objects $x$ and $y$.
$(x, y) = (z, w) :\Leftrightarrow (x = z \wedge y = w)$

Kuratowski's definition: $(x, y) = \{\{x\}, \{x, y\}\}$. **Exercise.** what is $(x, x)$?

## Definition

The Cartesian product $X \times Y$ of sets $X$ and $Y$ is the set of all ordered pairs with first component in $X$ and second component in $Y$.

$$X \times Y = \{(x, y) \mid x \in X, y \in Y\}$$

## Definition

A relation between the sets $X$ and $Y$ (or: "from $X$ to $Y$") is any subset $\rho \subseteq X \times Y$. We denote $(x, y) \in \rho$ also with $x \,\rho\, y$.
A relation on the set $X$ is a relation from $X$ to $X$.

# Partial and total functions (a.k.a. mappings)

## Definition

A relation $\rho \subseteq X \times Y$ is a partial function from $X$ to $Y$ if for all $x \in X$ there exists *at most one* $y \in Y$, such that $(x, y) \in \rho$.

This $y$, if it exists, is usually denoted as $\rho(x)$.

## Definition

A partial function $\rho \subseteq X \times Y$ is a (total) function, if $\rho(x)$ exists for all $x \in X$. Denote $\rho : X \to Y$.

## Definition

A function $f : X \to Y$ is

- injective if $\forall x, x' \in X : (f(x) = f(x') \Rightarrow x = x')$;
- surjective if $\forall y \in Y \exists x \in X : f(x) = y$;
- bijective if it is both injective and surjective.

# Directed graphs

## Definition

A directed graph is a triple $G = (V, E, \mathcal{E})$, where

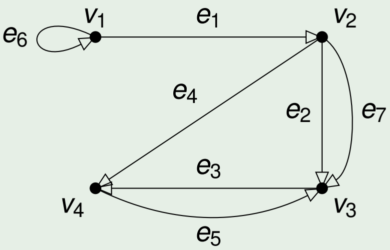
- $V$ is the set of vertices;
- $E$ is the set of edges;
- $\mathcal{E} : E \to V \times V$ is the incidence mapping.

## Example

$$V = \{v_1, v_2, v_3, v_4\}$$

$$E = \{e_1, e_2, e_3, e_4, e_5, e_6, e_7\}$$

$$\begin{aligned}\mathcal{E} = \; & \{(e_1, (v_1, v_2)), (e_2, (v_2, v_3)), \\ & (e_3, (v_3, v_4)), (e_4, (v_2, v_4)), \\ & (e_5, v_4, v_3)), (e_6, (v_1, v_1)), \\ & (e_7, (v_2, v_3))\}\end{aligned}$$



Let $G = (V, E, \mathcal{E})$.

- If $\mathcal{E}$ is injective then $E$ can be seen as a subset of $V \times V$.
- Then we denote the graph as $G = (V, E)$, where $E \subseteq V \times V$.

**Definition**

The graph of a relation $\rho$ on the set $X$ is the directed graph $(X, \rho)$.

**Definition**

Let $\rho \subseteq X \times Y$ and $X \cap Y = \emptyset$. The graph of the relation $\rho$ is the directed graph $(X \cup Y, \rho)$.

# Operations with relations

- Relations are sets. Set operations can be applied to them.
  - If $\rho, \sigma \subseteq X \times Y$ then $\rho \cup \sigma$, $\rho \cap \sigma$, $\rho \backslash \sigma$ and $\overline{\rho} = (X \times Y) \backslash \rho$ are again relations between $X$ and $Y$.
- The inverse of $\rho \subseteq X \times Y$ is $\rho^{-1} := \{(y, x) \,|\, (x, y) \in \rho\} \in Y \times X$.
- The composition of $\rho \subseteq X \times Y$ and $\sigma \subseteq Y \times Z$ is

$$\sigma \circ \rho = \{(x, z) \,|\, \exists y \in Y : \big((x, y) \in \rho \wedge (y, z) \in \sigma\big)\} \enspace .$$

Interpret the operations in terms of graphs.

# Properties of operations

- $(\sigma \cup \tau) \circ \rho = (\sigma \circ \rho) \cup (\tau \circ \rho)$
- $(\sigma \cap \tau) \circ \rho \subseteq (\sigma \circ \rho) \cap (\tau \circ \rho)$
- $\rho \circ (\sigma \circ \tau) = (\rho \circ \sigma) \circ \tau$
- $(\rho \circ \sigma)^{-1} = \sigma^{-1} \circ \rho^{-1}$
- Let $\rho$ a relation from $X$ to $Y$ and let $=_X$, $=_Y$ be the equality relations on $X$ and $Y$. Then $(\rho \circ =_X) = \rho = (=_Y \circ \rho)$.

## Exercise

Prove these properties. Use the graphs of the relations for hints.

# Equivalence relations

## Definition

Let $\rho$ be a relation on $X$. It is

- reflexive, if $\forall x \in X : (x, x) \in \rho$;
- symmetric, if $\forall x, y \in X : \big((x, y) \in \rho \Rightarrow (y, x) \in \rho\big)$;
- transitive, if $\forall x, y, z \in X : \big((x, y) \in \rho \wedge (y, z) \in \rho \Rightarrow (x, z) \in \rho\big)$;
- an equivalence relation, if it is reflexive, symmetric and transitive.

# Equivalence classes

## Definition

Let $\rho$ be an equivalence relation on $X$. Let $x \in X$. The equivalence class of $x$ (*modulo* $\rho$) is the set $x/\rho := \{y \in X \,|\, x \;\rho\; y\}$.

## Theorem

*Let $\rho$ be an equivalence relation on $X$. Let $x, y \in X$. Then either $x/\rho = y/\rho$ or $x/\rho \cap y/\rho = \emptyset$.*

Hence an equivalence relation may be interpreted as some “fuzzy equality”.

## Exercise

How does the graph $(X, \rho)$ of an equivalence relation $\rho$ on $X$ look like?

## Definition

The factor set of $X$ (by $\rho$) is the set $X/\rho := \{x/\rho \,|\, x \in X\}$.

# Kernels of mappings

## Definition

Let $f : X \to Y$ be a (total) mapping. The kernel of $f$ is the following relation on $X$:

$$\mathrm{Ker}\, f := \{(x, x') \,|\, x, x' \in X, f(x) = f(x')\}$$

Show that $\mathrm{Ker}\, f$ is an equivalence relation.

## Theorem

*Let $f : X \to Y$. There exists a set $Z$ and a surjective function $g : X \to Z$ and an injective function $h : Z \to Y$, such that $f = h \circ g$.*

Hint: the set $Z$ is $X/(\mathrm{Ker}\, f)$.

# Discrete Mathematics, 2nd lecture

Peeter Laud

Cybernetica AS

September 13th, 2012

# Partial orders

## Definition

Let $\rho$ be a relation on the set $X$. It is

- reflexive, if $\forall x \in X : x \mathrel{\rho} x$;
- antisymmetric, if $\forall x, y \in X : \big((x \mathrel{\rho} y \wedge y \mathrel{\rho} x) \Leftrightarrow x = y\big)$;
- transitive, if $\forall x, y, z \in X : \big(x \mathrel{\rho} y \wedge y \mathrel{\rho} z \Rightarrow x \mathrel{\rho} z\big)$;
- a partial order on $X$, if it is reflexive, antisymmetric and transitive.

## Example

- "$\leqslant$" on numbers
- subset inclusion
- divisibility (on $\mathbb{N}$)

# Closure operations

## Definition

Let $\rho$ be a relation on $X$. A **P**-closure of $\rho$ is a relation $\sigma$, such that

1. $\sigma$ has the property **P**;
2. $\rho \subseteq \sigma$;
3. $\sigma$ is the smallest relation (wrt. subset inclusion) satisfying 1 and 2.

**P** might be "transitive", "reflexive [and] transitive", ...
If $\rho$ has the property **P**, then what is the **P**-closure of $\rho$?

## Notation

Let $\rho^0 = (=_X)$ and $\rho^i = \rho^{i-1} \circ \rho$ for $i \in \mathbb{N}$.

## Theorem

*Let $\rho$ be a relation on $X$. The transitive closure of $\rho$ equals $\rho^+ = \bigcup_{i=1}^{\infty} \rho^i$.*
*The reflexive transitive closure of $\rho$ equals $\rho^* = \bigcup_{i=0}^{\infty} \rho^i$.*

# Existence of closures

**Theorem**

*Let* **P** *be a property of relations (on the set $X$).* **P***-closures exist iff*

- *the full relation $X \times X$ has the property* **P***;*
- *if $\rho_1, \rho_2, \ldots$ have the property* **P***, then $\rho_1 \cap \rho_2 \cap \cdots$ also has the property* **P***.*

# Existence of closures

## Theorem

*Let* **P** *be a property of relations (on the set $X$).* **P***-closures exist iff*

- *the full relation $X \times X$ has the property* **P***;*
- *if $\rho_1, \rho_2, \ldots$ have the property* **P***, then $\rho_1 \cap \rho_2 \cap \cdots$ also has the property* **P***.*

Actually, closures are a more general notation. Let us have

- a set $Y$;
- a partial order $\sqsubseteq$ over $Y$;
- a a subset $P \subseteq Y$ of elements $y \in Y$ with property **P**.

Then we can define the **P**-closure of $y \in Y$ as the smallest $y' \in P$ larger than $y$.

# Undirected graphs

## Definition

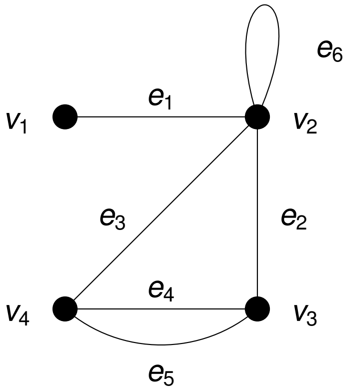
(Undirected) graph is a triple $G = (V, E, \mathcal{E})$, where

- $V$ is the set of vertices (also denote $V(G)$);
- $E$ is the set of edges (also denote $E(G)$).
- $\mathcal{E} : E \longrightarrow \mathcal{P}(V)$ is the incidency mapping. For all $e \in E$, $\mathcal{E}(e)$ must have 1 or 2 elements.

# Example

Let $V = \{v_1, v_2, v_3, v_4\}$, $E = \{e_1, e_2, e_3, e_4, e_5, e_6\}$ and

| $e$ | $\mathcal{E}(e)$ |
|---|---|
| $e_1$ | $\{v_1, v_2\}$ |
| $e_2$ | $\{v_2, v_3\}$ |
| $e_3$ | $\{v_2, v_4\}$ |
| $e_4$ | $\{v_3, v_4\}$ |
| $e_5$ | $\{v_3, v_4\}$ |
| $e_6$ | $\{v_2\}$ |




A drawing may illustrate a graph.
But a graph itself is still the triple $(V, E, \mathcal{E})$.

# Notations, definitions...

Let $G = (V, E, \mathcal{E})$ be a graph.

- If $v \in \mathcal{E}(e)$, then $v$ and $e$ are incident.
- If there exists $e$, such that $\mathcal{E}(e) = \{v_1, v_2\}$, then $v_1$ and $v_2$ are adjacent (naabertipud).
- If $\mathcal{E}(e) = \{v_1, v_2\}$, then $v_1$ and $v_2$ are the endpoints of $e$. Denote also $v_1 \overset{e}{—} v_2$.

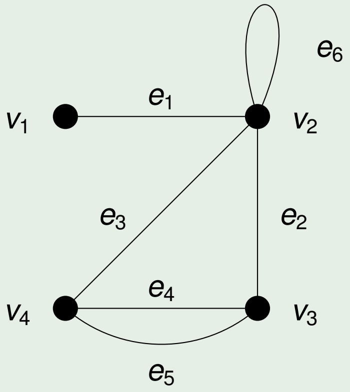
Let $G = (V, E, \mathcal{E})$ be a directed graph. Notations:

- If $\mathcal{E}(e) = (v_1, v_2)$, then $v_1$ is the start vertex and $v_2$ the end vertex of $e$.

# Notations, definitions... (cont.)

$e \in E$ is a multiple edge, if there exists $e' \in E \setminus \{e\}$, such that $\mathcal{E}(e) = \mathcal{E}(e')$.
$e \in E$ is a loop, if $|\mathcal{E}(e)| = 1$.

**Example**



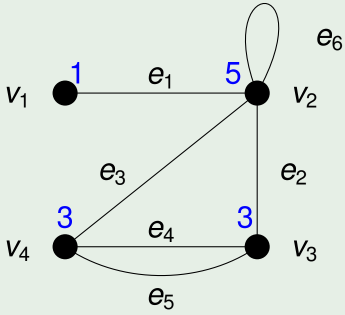

A simple graph is a graph without loops and multiple edges.

# Notations, definitions... (cont.)

The degree of a vertex $v$ in the graph $(V, E, \mathcal{E})$ is the number of edges incident to it (the loops count twice). Denote $\deg(v)$.

$$\deg(v) = |\{e \in E \mid v \in \mathcal{E}(e)\}| + |\{e \in E \mid \mathcal{E}(e) = \{v\}\}|$$

## Example



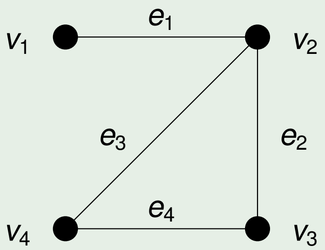
## Definition

Let $G = (V, E)$ be undirected simple graph. Let $V = \{v_1, \ldots, v_n\}$. The adjacency matrix (naabrusmaatriks) of $G$ is a $n \times n$ matrix $\mathbf{A} = [a_{ij}]$, where

- If $(v_i, v_j) \in E$, then $a_{ij} = 1$.
- If $(v_i, v_j) \notin E$, then $a_{ij} = 0$.

The adjacency matrix is symmetric and its main diagonal contains zeroes.

## Example




| | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| 1 | 0 | 1 | 0 | 0 |
| 2 | 1 | 0 | 1 | 1 |
| 3 | 0 | 1 | 0 | 1 |
| 4 | 0 | 1 | 1 | 0 |

# Number of vertices with odd degree

## Theorem

*An undirected simple graph contains an even number of vertices of odd degree.*

## Proof.

Count the ones in the adjacency matrix of $G = (V, E)$.

- Their number is $2 \cdot |E|$.
- Their number is $\sum_{v \in V} \deg(v)$.

These two quantities are equal.

$\Rightarrow$ The sum of degrees of all vertices is even.

$\Rightarrow$ An even number of summands are odd.

$\square$

Similarly, any undirected graph contains an even number of vertices of odd degree.

# In- and outdegrees in directed graphs

In a directed graph $(V, E, \mathcal{E})$ we define for a vertex $v$

- its indegree $\overrightarrow{\deg}(v)$ — the number of edges ending in $v$;
- outdegree $\overleftarrow{\deg}(v)$ — the number of edges starting in $v$.

## Theorem

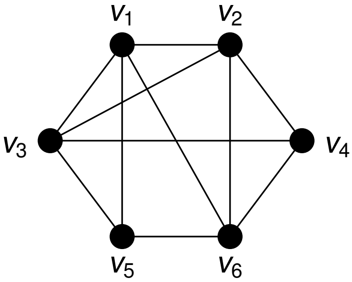
$$\sum_{v \in V} \overrightarrow{\deg}(v) = \sum_{v \in V} \overleftarrow{\deg}(v).$$

(Similar to previous one)

# Notations, definitions...

- A walk in the graph $G = (V, E)$ (from vertex $x$ to vertex $y$) is a sequence
$$P : x = v_0 \xrightarrow{e_1} v_1 \xrightarrow{e_2} v_2 \xrightarrow{e_3} v_3 \xrightarrow{e_4} \ldots v_{k-1} \xrightarrow{e_k} v_k = y \ .$$
- The number $k$ is the length of the walk $P$. Denote $|P|$.
- Let $x \overset{P}{\rightsquigarrow} y$ denote that $P$ is a walk from $x$ to $y$.
- A path is a walk where all vertices are distinct (only $v_0$ and $v_k$ may coincide).
- A walk is closed if $v_0 = v_k$.
- A closed path is a cycle.
- A graph is connected if there is a walk between each two of its vertices.
- The distance $d(u, v)$ between vertices $u, v \in V$ is the length of the shortest walk connecting them.

# Examples




Walk: $v_1 — v_2 — v_4 — v_6 — v_2 — v_3$
Path: $v_1 — v_2 — v_3 — v_4$
Closed walk: $v_1 — v_2 — v_3 — v_1 — v_5 — v_6 — v_1$
Cycle: $v_1 — v_2 — v_6 — v_5 — v_1$
$d(v_1, v_4) = 2$, $d(v_1, v_2) = 1$, $d(v_1, v_1) = 0$.

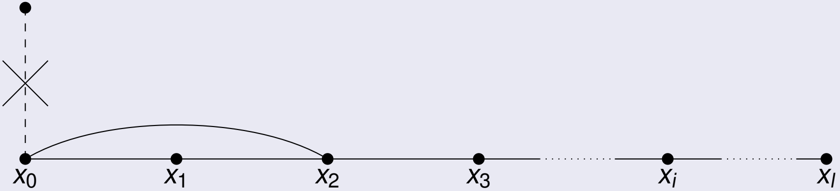
# Existence of cycles

## Theorem

*A simple graph, where the degree of each vertex is at least $k \geqslant 2$, has a cycle of length at least $k+1$.*

## Proof.

Let $x_0 - x_1 - \cdots - x_l$ be an open path of maximal length in this graph.




All neighbours of $x_0$ are located in this path.

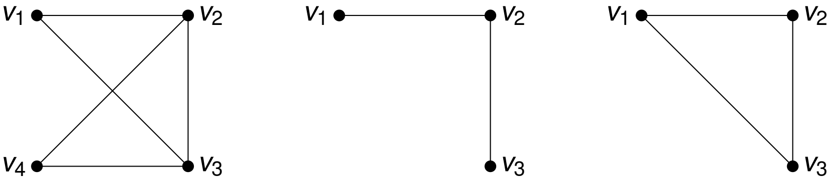
Let $x_i$ be the neighbour of $x_0$ with maximal index. Then $i \geqslant k$.

$x_0 - x_1 - \cdots - x_i - x_0$ is a cycle of length $i+1 \geqslant k+1$. □

# Subgraphs

A subgraph of a graph $G = (V, E)$ is a graph $G' = (V', E')$, where $V' \subseteq V$, $E' \subseteq E$ and for all $e \in E'$ holds $\mathcal{E}(e) \subseteq V'$. Denote $G' \leqslant G$.

A subgraph $(V', E')$ is induced (by the set $V'$), if the set $E'$ is as large as possible, i.e. $\mathcal{E}(e) \subseteq V' \Rightarrow e \in E'$ holds for all $e \in E$.




The connected components of a graph $G$ are its maximal connected subgraphs.

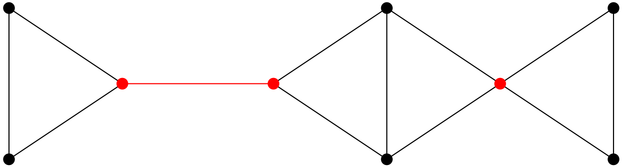
# Bridges and cut-vertices

**Definition**

An edge of a graph is bridge if its removal increases the number of connected components.

**Definition**

A vertex of a graph is cut vertex if its removal (together with its incident edges) increases the number of connected components.

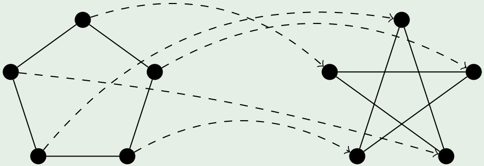


# Graph isomorphisms

## Definition

An isomorphism from $G_1 = (V_1, E_1)$ to $G_2 = (V_2, E_2)$ is a bijective mapping $f : V_1 \longrightarrow V_2$, such that $x, y \in V_1$ are adjacent iff $f(x), f(y) \in V_2$ are adjacent.

## Example



## Definition

Graphs $G_1$ and $G_2$ are isomorphic (denote $G_1 \cong G_2$), if there exists an isomorphism between them.

# Names for certain graphs

- A null graph is a graph without edges. A null graph of $n$ vertices is denoted by $O_n$.
- A complete graph is a simple graph with an edge between each pair of vertices. A complete graph of $n$ vertices is denoted by $K_n$.

## Proposition

Graph $K_n$ has $\frac{n(n-1)}{2}$ edges.

Graph $G = (V, E)$ is bipartite, if $V$ can be partitioned to two sets $V_1$ and $V_2$ (i.e. $V_1 \cup V_2 = V$ and $V_1 \cap V_2 = \emptyset$), such that the endpoints of any edge belong in different parts.

(More generally: a graph is $k$-partite if its vertices can be partitioned into $k$ parts such that all edges are between different parts.)

A bipartite simple graph with parts of vertices $V_1$ and $V_2$ is complete bipartite if there is an edge between each $v_1 \in V_1$ and $v_2 \in V_2$. Let $K_{m,n}$ denote the complete bipartite graph with $|V_1| = m$ and $|V_2| = n$.

**Proposition**

$K_{m,n}$ has $mn$ edges.

# Necessary and sufficient condition for bipartiteness

**Theorem**

*A graph is bipartite $\Leftrightarrow$ all its cycles are of even length.*

**Proof $\Rightarrow$.**

A cycle goes a number of times from the first part to the second and the same number of times from the second part to the first.

**Proof $\Leftarrow$.**

Assume $G = (V, E)$ is connected. Otherwise consider each connected component separately.

...

# Fixing these two parts

### Start coloring vertices black and white.

Pick a vertex $v_0 \in V$ and colour it white.

### Repeat...

Let $u$ be a coloured vertex that has uncoloured neighbours. Let $v$ be one of such neighbours. Colour it with the opposite colour to $u$. Remember that the colour of $u$ was used to choose the colour of $v$. Denote it $v \xrightarrow{c} u$.

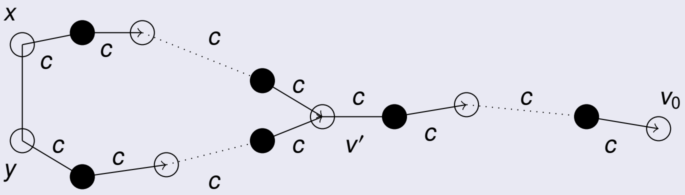
### Stop when

- there appear adjacent vertices $x$ and $y$ of the same colour;
- we run out of vertices to colour.

# After stopping...

## If problems occur

If such vertices $x$ and $y$ appear then




we have a cycle of odd length $x$ — $\cdots$ — $v'$ — $\cdots$ — $y$ — $x$.

## If we can color everything

If we run out of vertices, then the black vertices form one part and white vertices the other part of vertices of the bipartite graph. □