Mein Semester-Studium an der Otto-von-Guericke Universität in 2014-2015.

Wie läuft das Studiumprozess?

1 step

- Scoring system in OvGU vs BSU
- Possible forms of examinations
- Advices for successful graduation

2 step

Mathematics

- Combinatorial optimization
- Algebraic Number Theory

3 step

Computer Science

- Swarm intelligence
- Biometrics and security

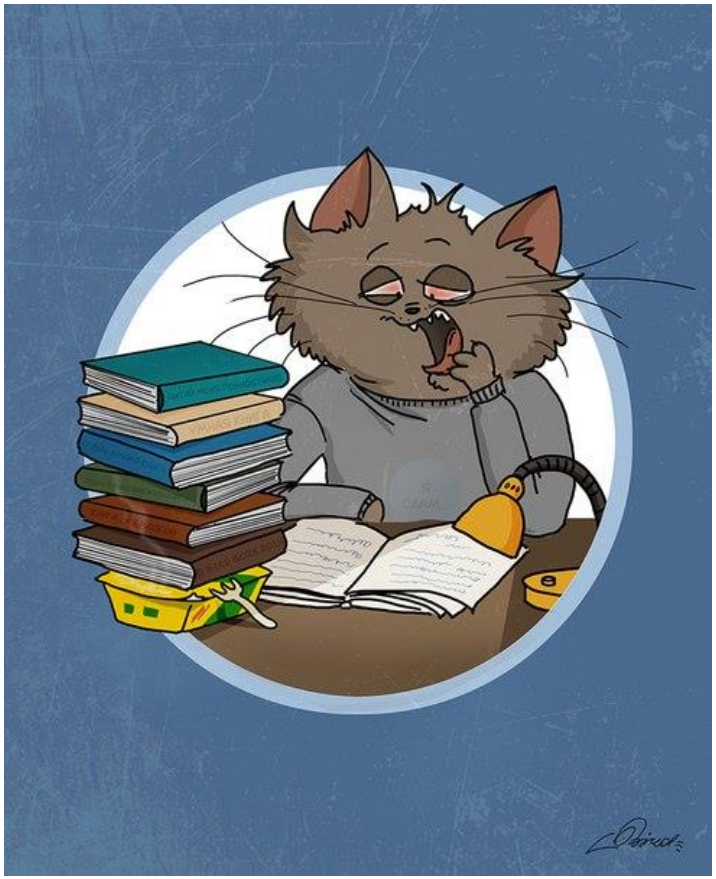
4 step

Your questions?

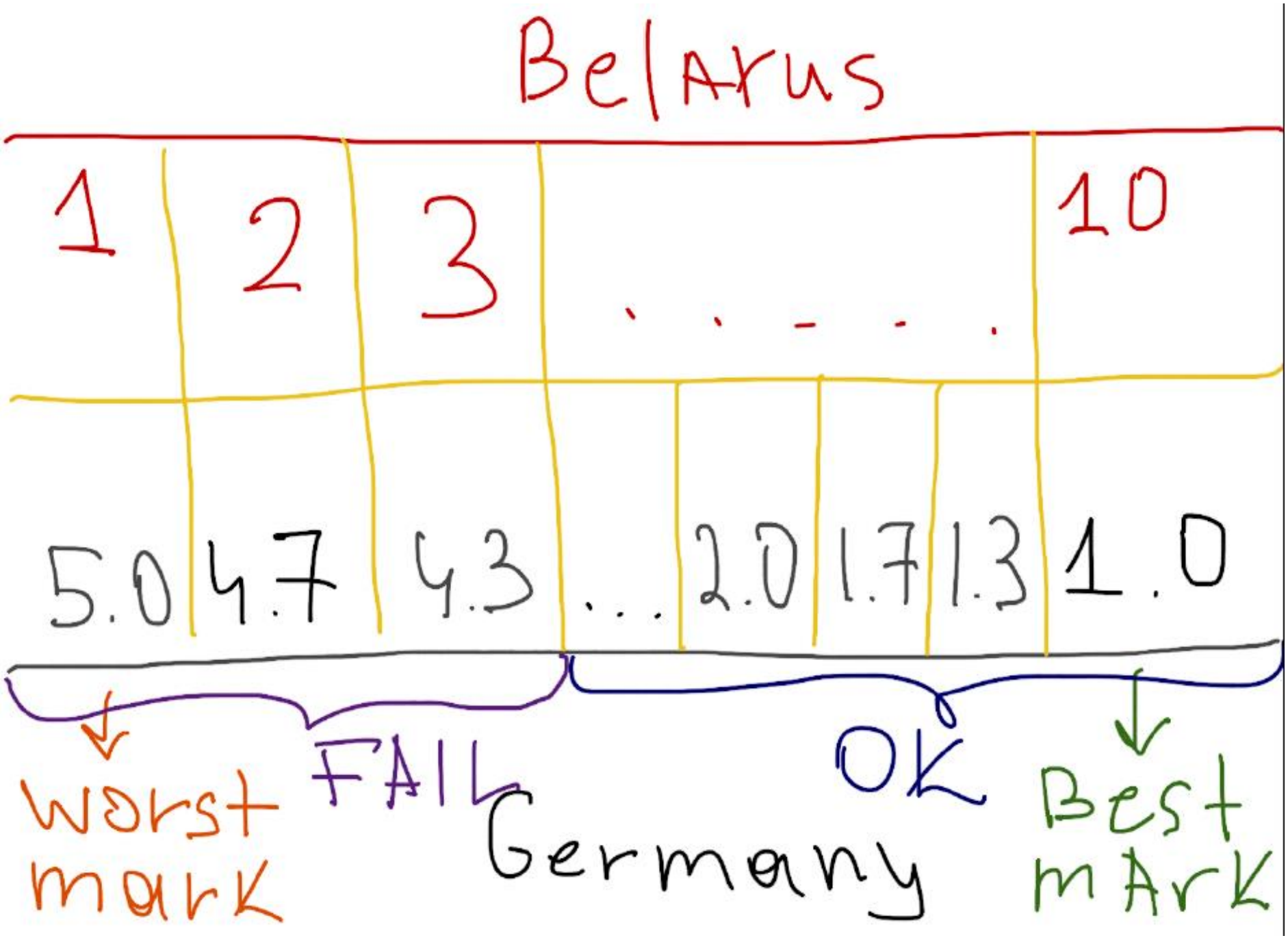
GOAL:

Successful semester graduation!

General info:



- What is the point system?
- What does it mean to pass an exam successufully?
- What does it mean to graduate a semester?

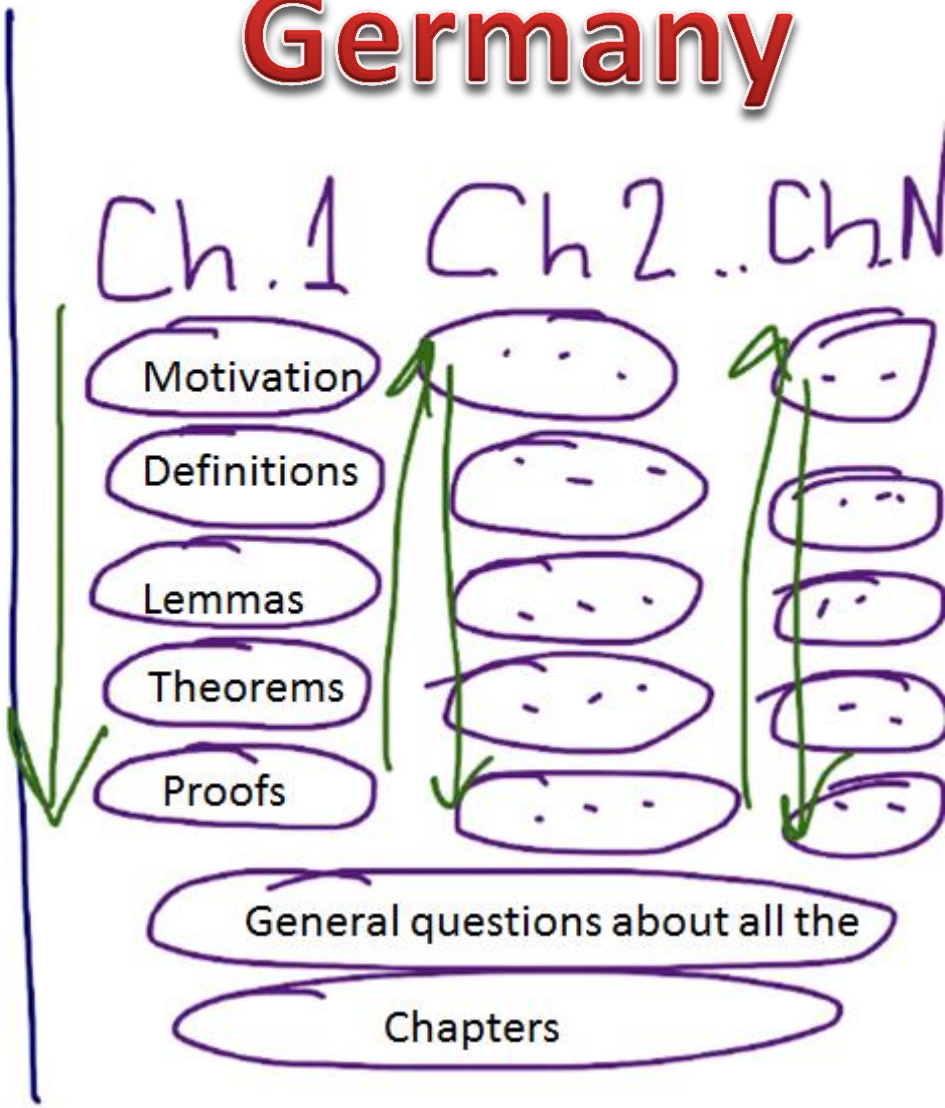

Belarus
1
2
3
10
5.0
4.7
4.3
2.0
1.7
1.3
1.0
worst mark
FAIL
OK
Best mark
Germany

Exam

Belarus

- N randomly taken questions

Germany



Point system

Basically in OvGU you study 2 types of subjects:

- Mathematics
- Informatics

Credit_Points(mark,type):=

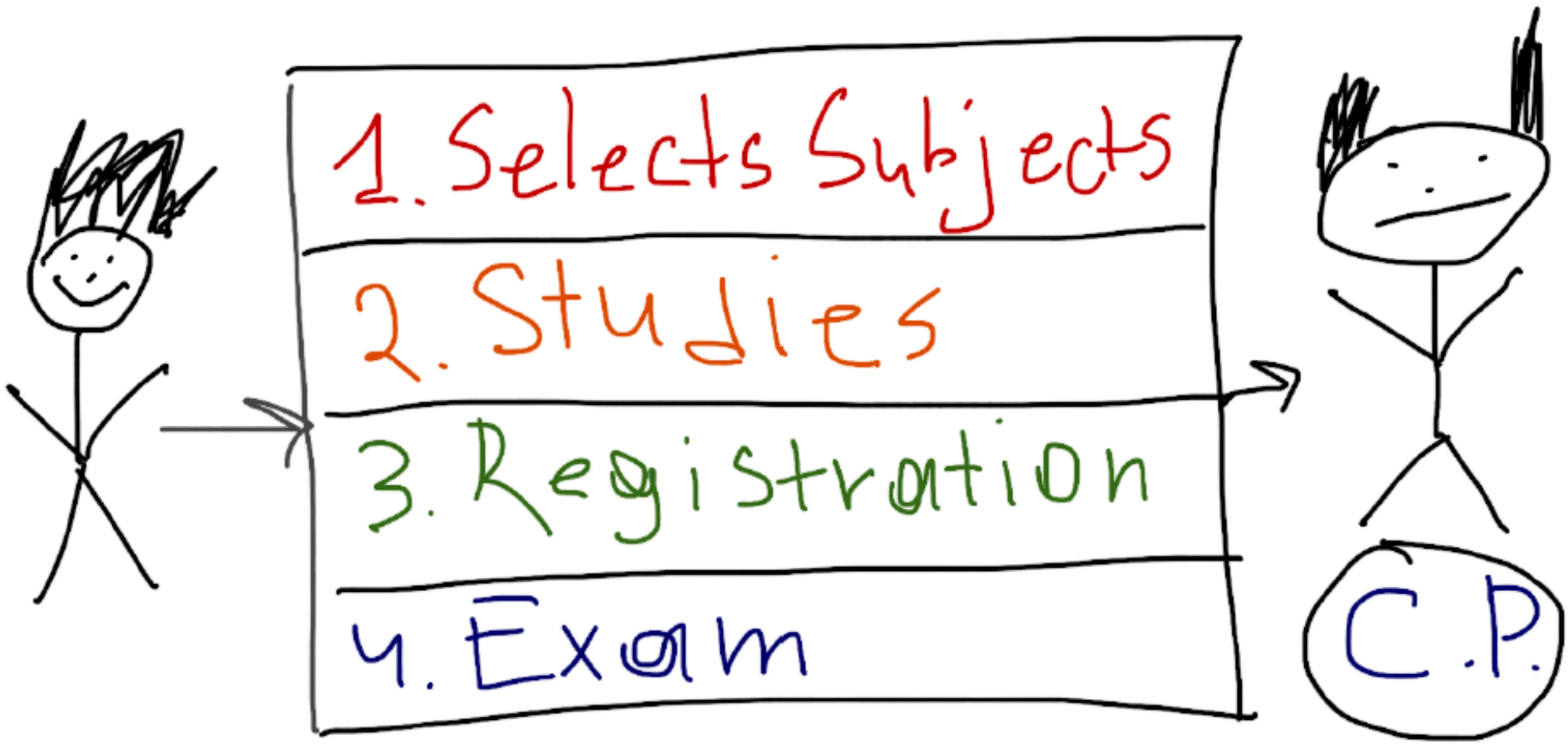
$$\begin{cases} 9.0\ , mark \leq 4.0\ and\ type = Math. \\ 6.0\ , mark \leq 4.0\ and\ type = Inf. \\ 0, mark > 4.0 \end{cases}$$

To pass Examinations successfully:

$$\sum_{marks}\sum_{types} Credit\_Points(marks, types) \geq 30$$

30 is ENOUGH!

Educational process



Subjects' selection

Basically a list of subjects provided by Prof.Girlich

You manually select all the interesting subjects

Advantages

+

- You study only that subjects, which you want => High motivation!

Disadvantages

-

Timetable problem:

- You can't select 2 subjects at one and the same time;
- "Windows" in a timetable (2classes: first 7.00 – 9.00

  second 13.00 – 15.00)

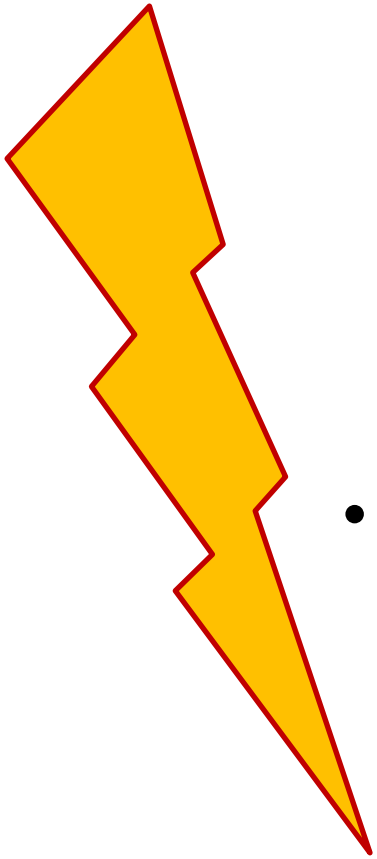
Study

- Attend lectures and exercises
- Do homework (basically without testing the presence)
- Basically no preliminary tests and admissions for exams (but there are some exceptions)

Registration

- Fill (web) form
- Make (web) query

Exam



Mathematics

- Orally in German or English (or mixed)
- Duration of the exam$\approx 30 - 40$ min

Informatics

(computer science)

- Written ($\approx$centralized test)
- Referat ($\approx$ course work)

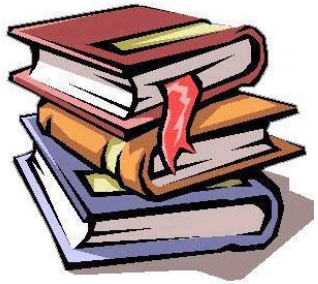
Computer Science

- Swarm Intelligence
- Biometrics and Security


Swarm Intelligence

What is Swarm?

Main topics



Part 1: Fundamentals of swarm intelligence

- Swarm stability and stability analysis
- Swarm aggregation
- Swarm in known environments
- Swarm in unknown environments: Particle Swarm Optimization
- Dynamic Optimization
- Multi-Objective Particle Swarm Optimization

Part 2: Swarm and multi-agent systems

- Division of labor and task allocation
- Swarm clustering and sorting
- Ant systems and optimization

Part 3: Applications

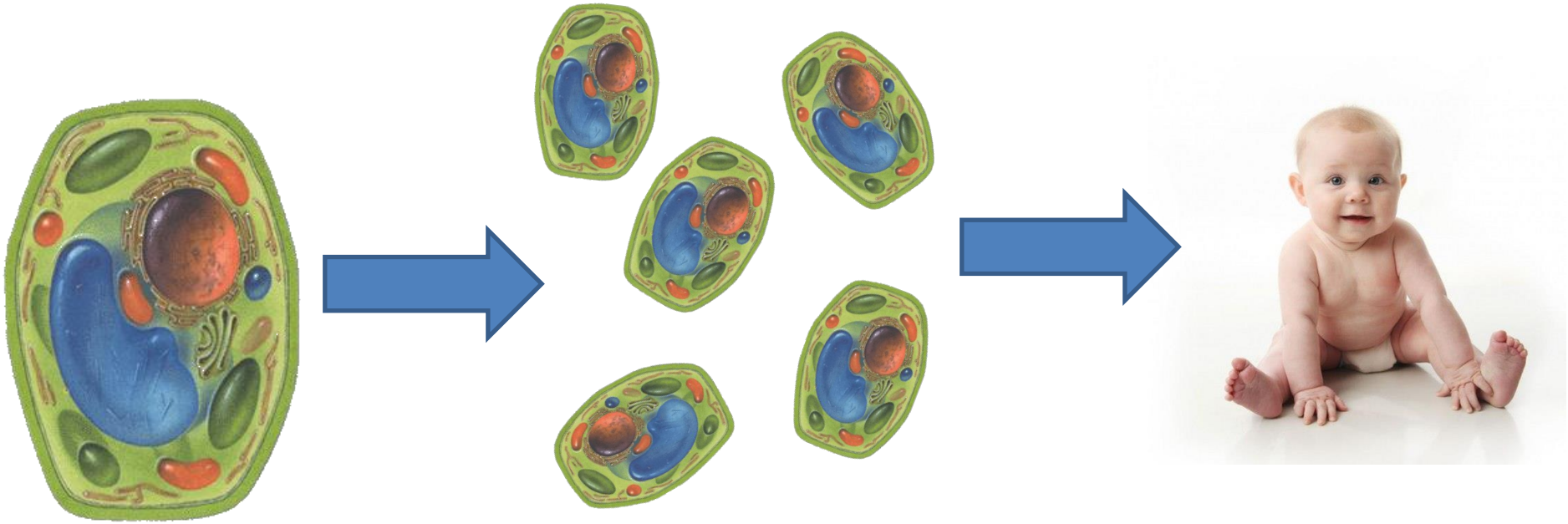
- Swarm localization and display
- Swarm robotics
- (Self-assembly swarm)

What is Swarm Intelligence?

- A **collective behavior** of
- **simple entities**
- having **simple rules** with
- ability of **local interactions**.

”The whole is more than the sum of its parts!”

Emergence effect



Global behavior

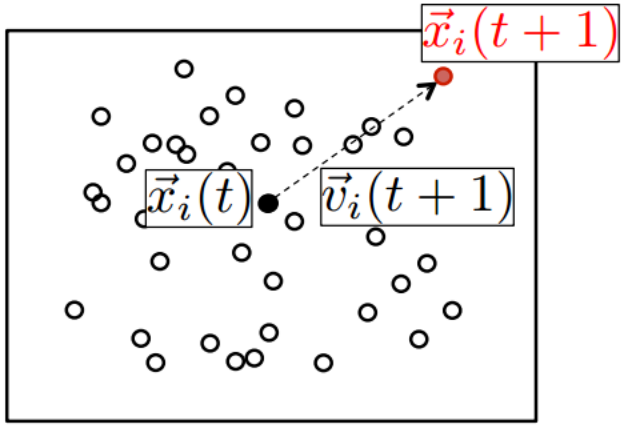
Did you say "Swarm model"?

The swarm model

- Consider a swarm of M individuals in an n-dimensional space.
- We model the individuals as points and ignore their dimensions.
- The position of member i of the swarm at time t is described by $\vec{x}_i(t) \in \mathbb{R}^n$
- Assume synchronous motions, no time delays and a *fully connected network*
- The equations of motion (Kinematics) for individual i:

$$\vec{x}_i(t+1) = \vec{x}_i(t) + \vec{v}_i(t+1)$$

$$\vec{v}_i(t+1) = w\vec{v}_i(t) + \vec{f}_i$$

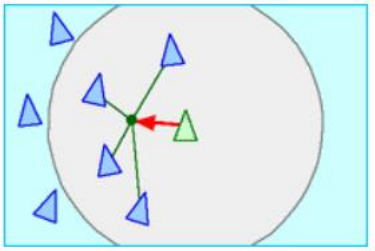


What about rules?

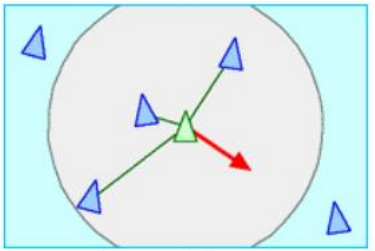
1. Attraction (Cohesion): steer to move towards the average position of local flock-mates

2. Repulsion (Separation): steer to avoid crowding local flock-mates

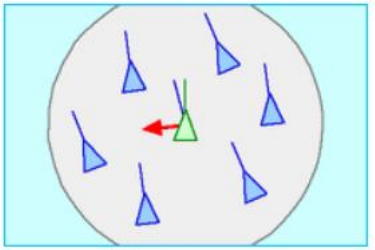
3. Alignment: steer towards the average heading of local flock-mates



Attraction



Repulsion



Alignment

Examples of SO:

Economy:

Stock markets regulate the relative prices of companies without central control.

Traffic:

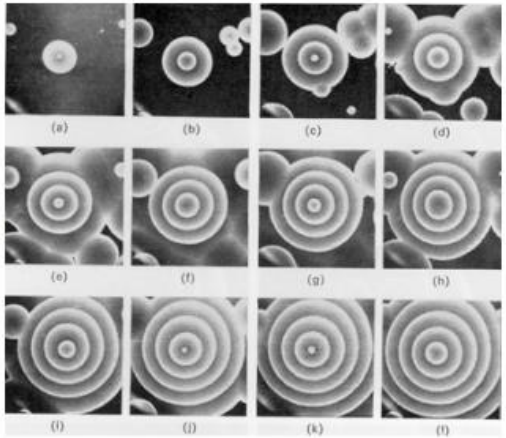
Highway traffic organizes itself, might lead to traffic jams.

Internet:

Traffic control and routing use methods which adapt to properties of local views of the system.

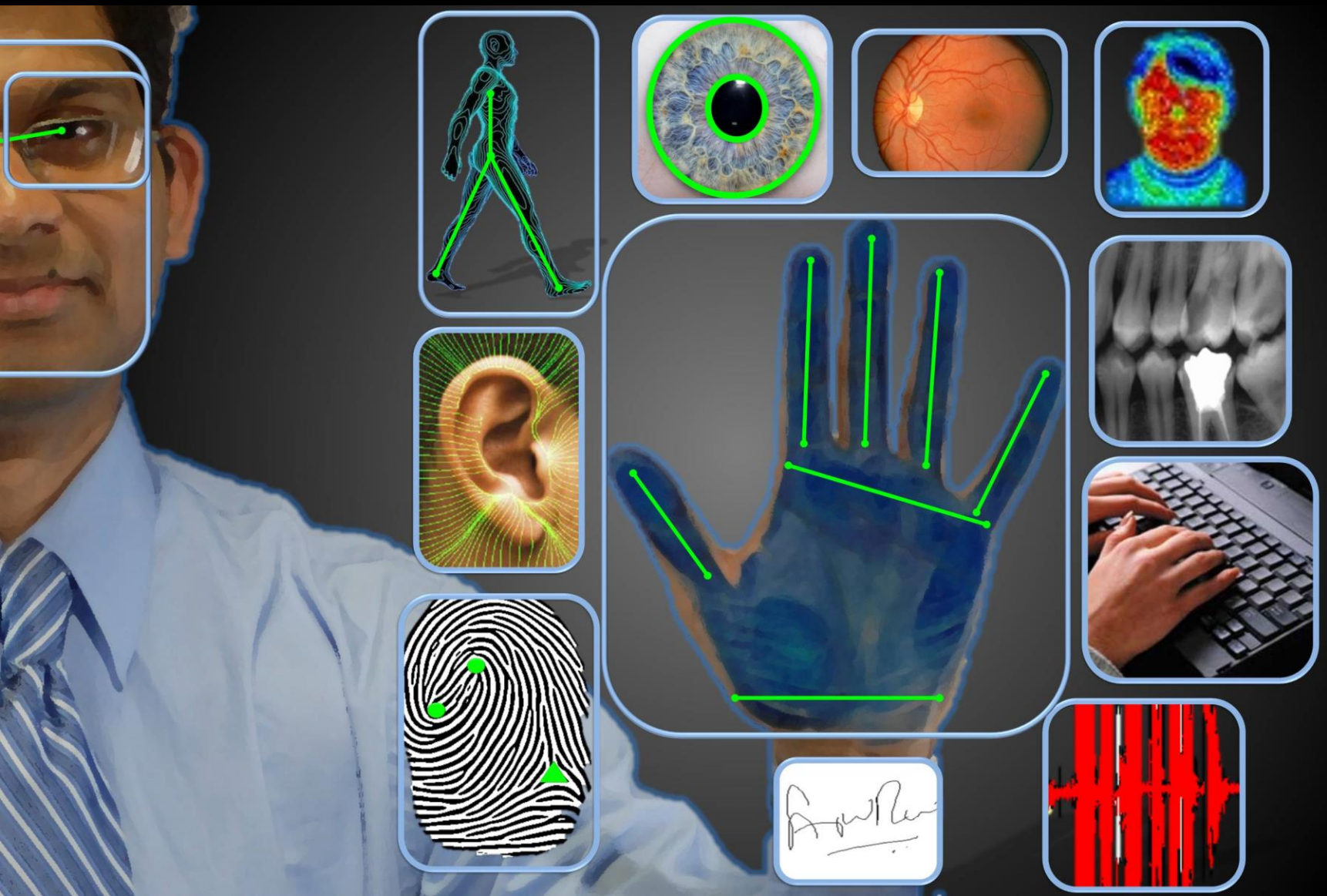
Mathematics, Chemistry, Physics:

- Simple rules lead to complex patterns
- The Belousov-Zhabotinsky reaction is a family of oscillating chemical reactions.




Is it necessary?
BOOK

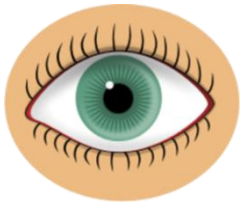
Biometrics and security



Concept

- Lecture
  - Weekly
  - Video Projector (Slides) – Note: Slides should be used as script!
  - Whiteboard, Tablet PC
  - English slide versions: Work in Progress .
  - Students presentation to selected topics and discussion within the course – Referat Presentation
- Exercise for work on individual topic for Referat: https://omen.cs.uni-magdeburg.de/einschreiben/
  - Registration and selection of your topic at first exercise (exercises start on 16.10.14: select your topic and collect your related references)
  - Milestones will be introduced in the first exercise

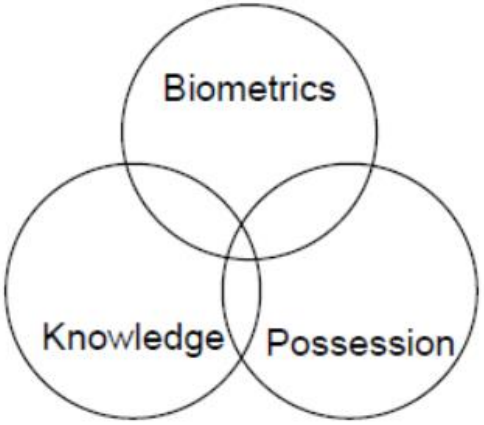
Lecture notes



- Part 1 (Introduction and Fundamentals)
- Part 2 (Speech and Handwriting)
- Part 3 (Gait, Keystroke Dynamics and Lip Movement)
- Part 4 (Fingerprint)
- Part 5 (Iris)
- Part 6 (Face)
- Part 7 (Rest)

Biometrics and Security

- Biometric System:
  - system for the purpose of the automated recognition of individuals based on their behavioural and biological characteristics
- Use Cases: User Authentication
  - Advantage
    - Directly linked with person's body or behavior
    - Misuse by third person not possible in an easy way
    - Authentication by Verification or Identification
  - Problem:
    - Error Rates (false positives and false negatives) and
    - They can only be obtained statistically → Large Test Sets
    - Immitations, fakes, replays, impersonation etc.



See: http://www.3dface.org/media/vocabulary.html or
http://www.christoph-busch.de/standards.html , website request 7.10.2013

Confidentility, Privacy, Anonymity or Pseudonymity, Unobservability, Unlinkability

Confidentility during inter-process communication

Claus Vielhauer, Jana Dittmann, Stefan Katzenbeisser: Design Aspects of Secure Biometric Systems and Biometrics in the Encrypted Domain, In: Patrizio Campisi (Eds.): Security and Privacy in Biometrics, Springer London, ISBN 978-1-4471-5229-3,

Reference Storage

confidentility of stored data

Behavioral / Physiological Trait from Subject

Data Acquisition

Pre-processing

Feature Extraction

Comparison & Classification

Result

confidentility of the acquired data

confidentility of the pre-processed data

confidentility of the feature data

confidentility of the compared and classified data

confidentility of the result

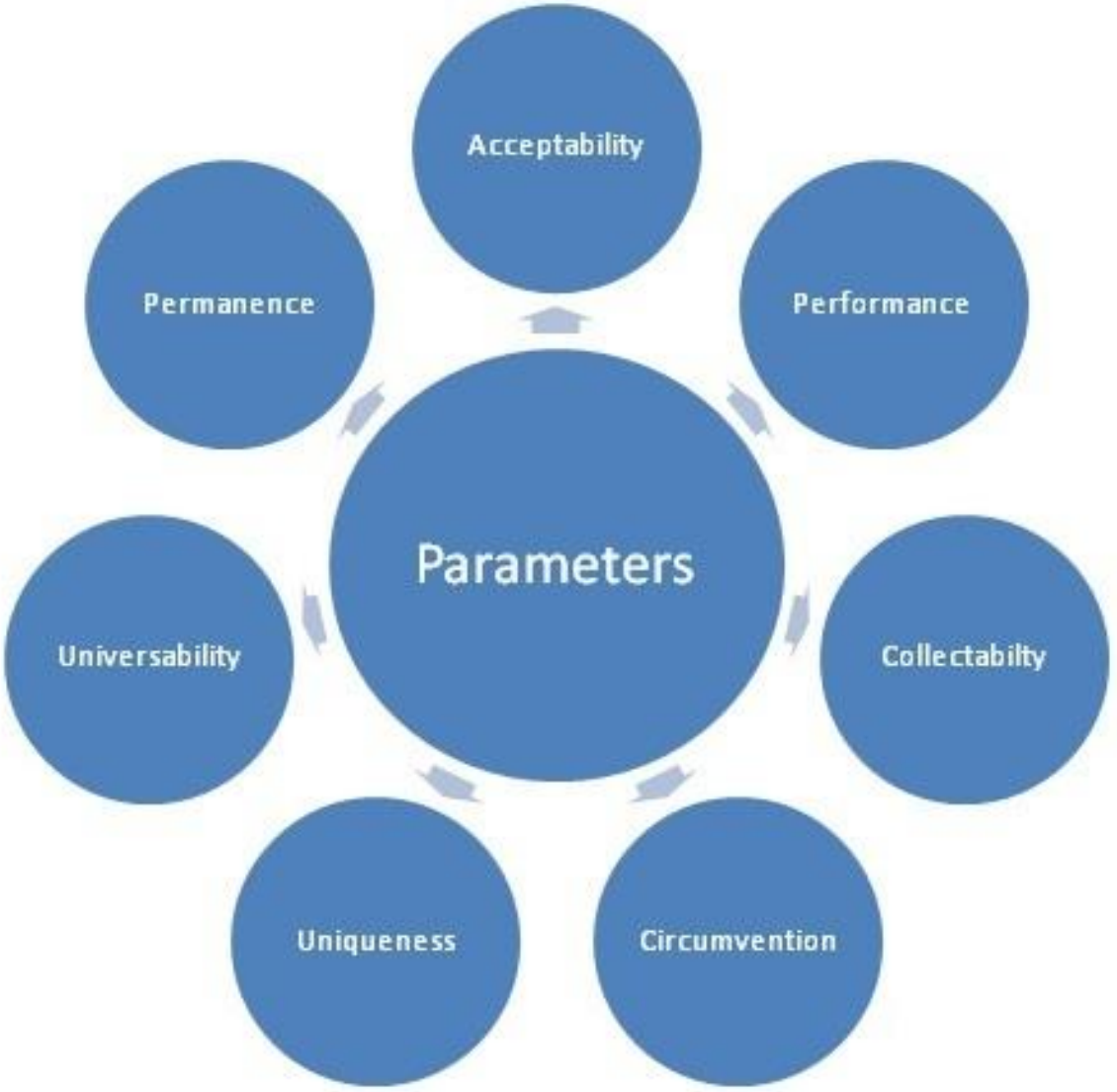
Privacy of the human

Privacy of person related data - the ability of a human to determine and control her- or himself which information about her- or himself is revealed including data collection, usage with storage, changing processes, transfer, locking and deletion - need to be ensured in and through all steps, the storage and during result presentation

Anonymity or pseudonymity of the human, Unobservability and Unlinkability of all actions preformed by the human

Anonymity or Pseudonymity of the subject, Unobservability and Unlinkability of all actions preformed need to be granted in and through all steps, the storage and during result presentation

General Criteria for Evaluation of Biometric Methods



Application cases

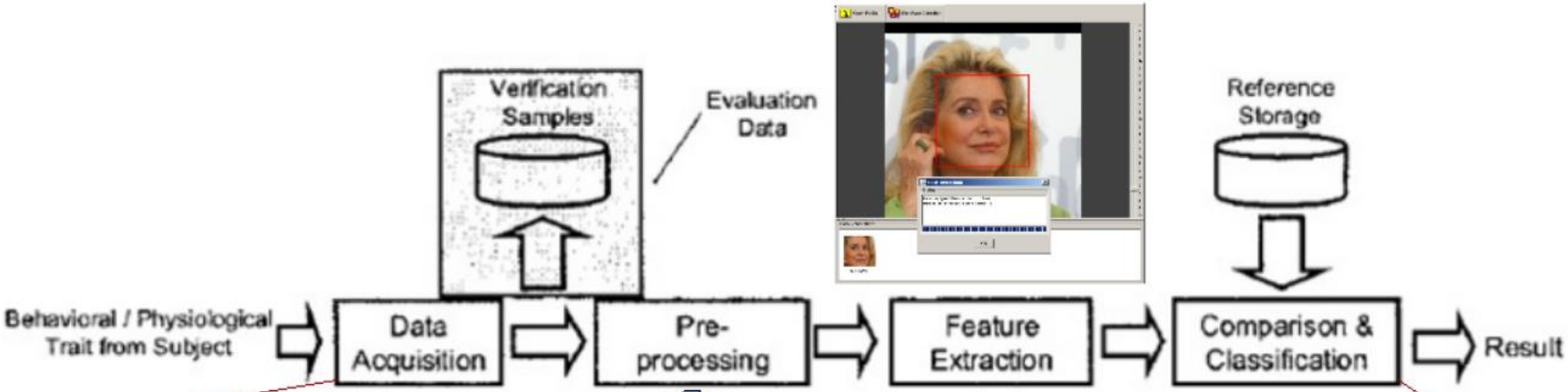
- Security
  - Border Controll
  - Surveillance
  - Crime Scene Traces
  - Access Protection
  - ...
- Convenience
  - Recognition = Understanding
  - Personalization of services or devices
  - Situation awarness
  - Management issues such as time and attendance management
  - ...

Face Biometrics: Tasks description

- to use the face detection and face recognition tool - *«Faint»* (the Face Annotation Interface) - to perform person identification on the the collection of face images - *the "Labeled faces in the wild" database* - from publicly available source;
- to analyse the efficiency of the system before and after the attack attempt using StirTrace on face images (FP/FN errors);
- to discuss the influence of different parameterizations (here 'Maximum numbers of Eigenfaces used') on the classification performance;
- to project the samples in the database to the characters of 'Doddingtons Zoo' and – if possible – to apply the 'Doddingtons rules of thumb' for the evaluation of the authentication performance.

Summarized and presented by
Bartashevich Palina and
Polujan Alexandr

Face Biometrics: Biometric processing pipeline



"Labeled faces in the wild"
vs
Utrecht ECVP face database

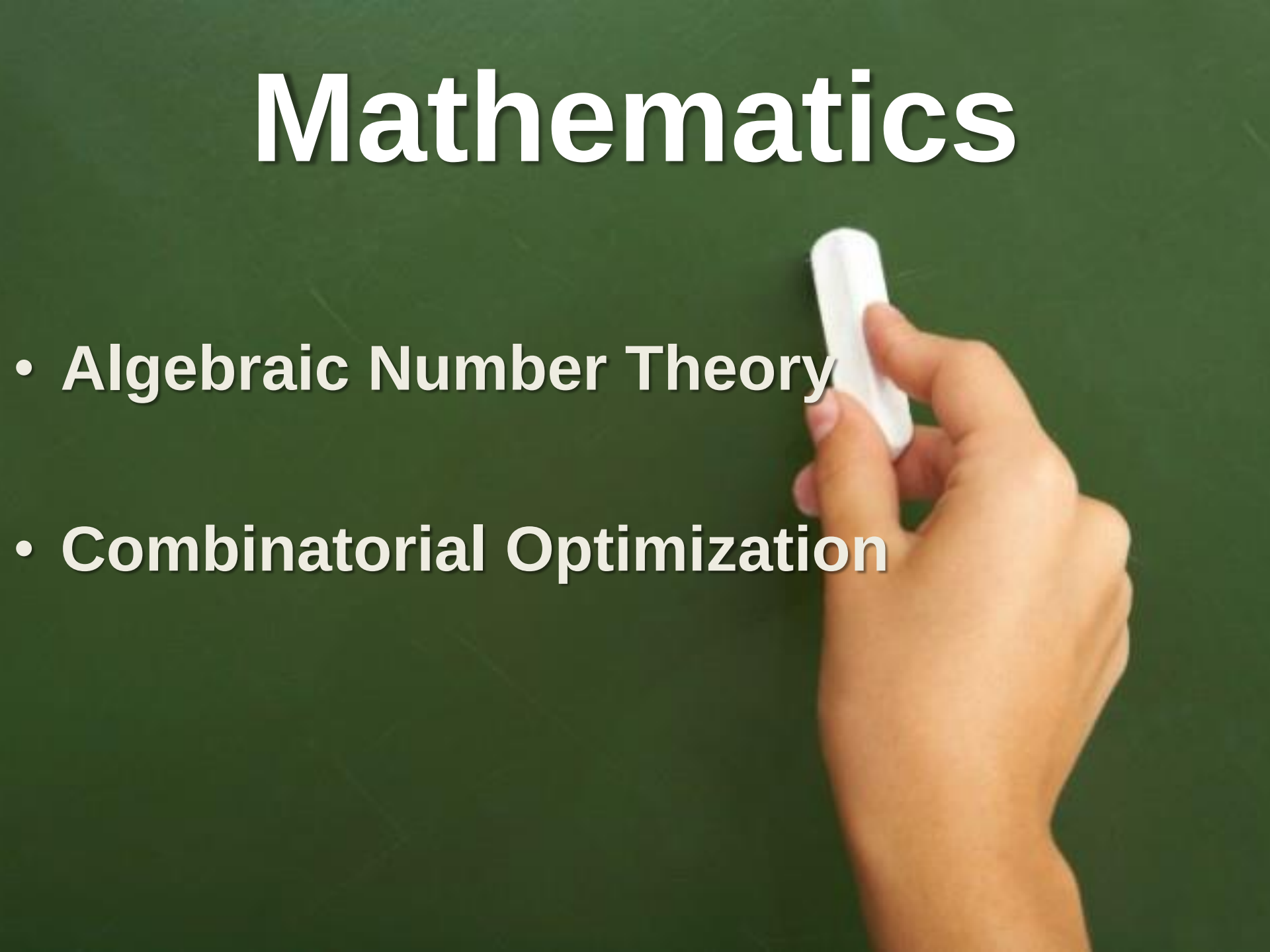
Testing and Training sets

Summarized and presented by
Bartashevich Palina and
Polujan Alexandr
Biometrics and Security – BioSec WS14/15
WS14/15 Topic01b: Face Biometrcs

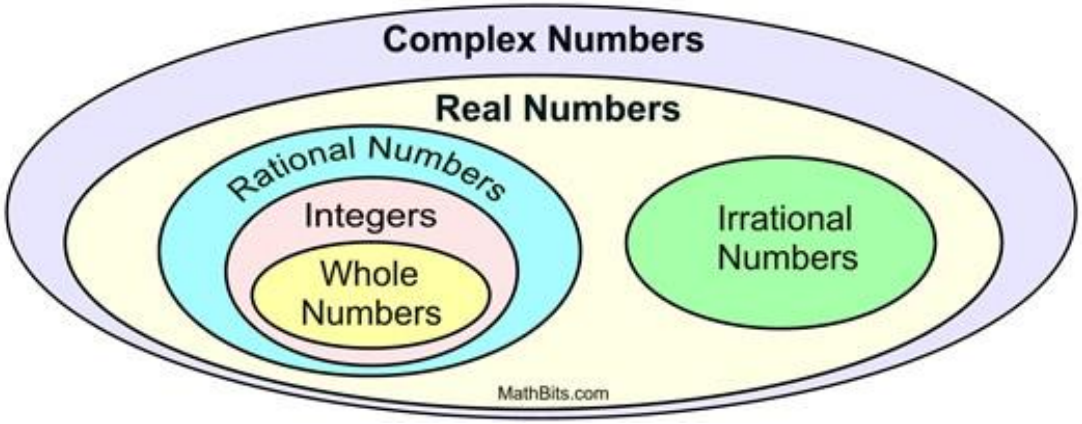
Is it necessary?

Mathematics

- Algebraic Number Theory
- Combinatorial Optimization



Algebraic Number Theory



- Lectures (In German) - 2 times a week
- Exercises – once a week
- Lecturer Dr. Kai-Uwe Schmidt
- Official web-page

http://www-e.uni-magdeburg.de/kai-usch/lectures/AZT/

Motivation

Problem 1: Solve the equation or prove, that it has no solutions:

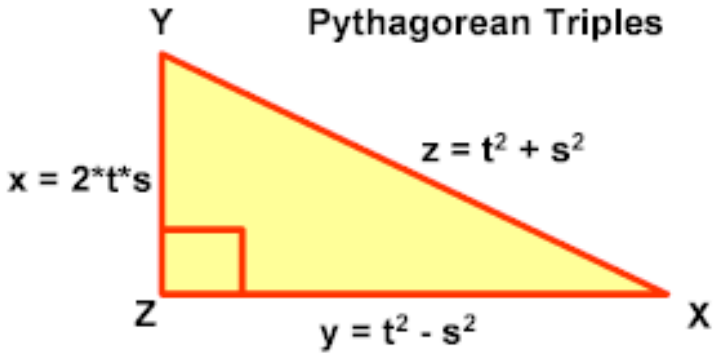
$$x^n + y^n = z^n, n \in \mathbb{N}; x, y, z \in \mathbb{Z}; xyz \neq 0$$

Problem 2: Solve the equation:

$$x^2 - n_0 y^2 = z, for\ fixed\ n_0 \in \mathbb{Z}; x, y, z \in \mathbb{Z}$$

Problem 1

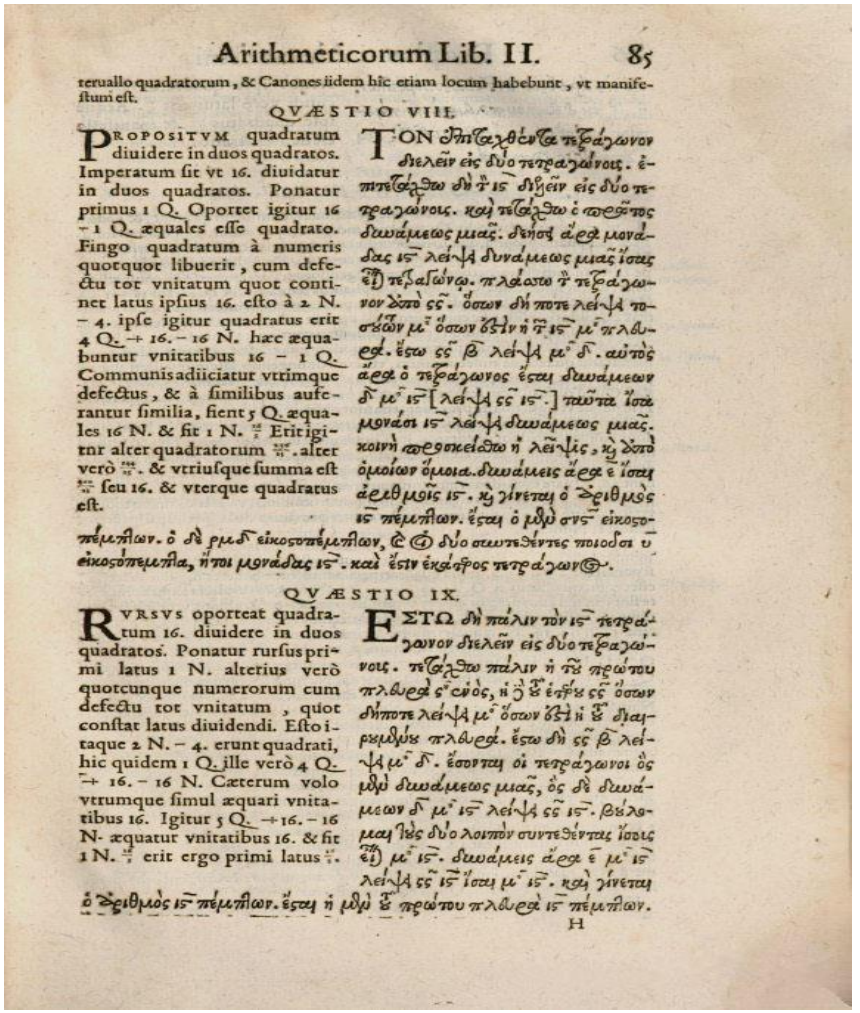
- So called Fermat's Last Theorem
- Firstly was stated in Ancient times as Pythagorean Triple problem (motivated by Pythagorean Theorem)



- Around 1637 was generalized by Fermat in the margin of his copy of the *Arithmetica* next to Diophantus' sum-of-squares problem

Problem 1

"It is impossible to separate a cube into two cubes, or a fourth power into two fourth powers, or in general, any power higher than the second, into two like powers. I have discovered a truly marvelous proof of this, which this margin is too narrow to contain."



Arithmeticorum Lib. II. 85

teruallo quadratorum, & Canones iidem hîc etiam locum habebunt, vt manifestum est.

QVÆSTIO VIII.

PROPOSITVM quadratum diuidere in duos quadratos. Imperatum sit vt 16. diuidatur in duos quadratos. Ponatur primus 1 Q. Oportet igitur 16 − 1 Q. æquales esse quadrato. Fingo quadratum à numeris quotquot libuerit, cum defectu tot vnitatum quot continet latus ipsius 16. esto à 2 N. − 4. ipse igitur quadratus erit 4 Q. + 16. − 16 N. hæc æquabuntur vnitatibus 16 − 1 Q. Communis adiiciatur vtrimque defectus, & à similibus auferantur similia, fient 5 Q. æquales 16 N. & fit 1 N. $\frac{4}{5}$. Erit igitur alter quadratorum $\frac{16}{25}$. alter verò $\frac{9}{25}$. & vtriusque summa est $\frac{25}{25}$ seu 16. & vterque quadratus est.

Τὸν δὴ τεθὲν τὸν τετράγωνον διελεῖν εἰς δύο τετραγώνους. ἐπιτεθέτω δὴ ὁ ις διῃρεῖν εἰς δύο τετραγώνους. καὶ τεθέτω ὁ πρῶτος δυνάμεως μιᾶς. δεήσει ἄρα μονάδας ις λείψει δυνάμεως μιᾶς ἴσους ἔσται τετραγώνῳ. πλάσσω τὸ τετράγωνον ἀπὸ ς. ὅσων ἄρα ποτὲ λείψει τοσῶν μ ὅσων ἐστὶν ἡ ις μ πλευρά. ἔσω ς β λείψει μ δ. αὐτὸς ἄρα ὁ τετράγωνος ἔσται δυνάμεων δ μ ις [λείψει ς ις.] πάντα ἴσα μονάσι ις λείψει δυνάμεως μιᾶς. κοινὴ προσκείσθω ἡ λεῖψις, καὶ ἀπὸ ὁμοίων ὅμοια. δυνάμεις ἄρα ε ἴσαι ἀριθμοῖς ις. καὶ γίνεται ὁ ἀριθμὸς ις πέμπτων. ἔσται ὁ μὲν σις εἰκοσιπέμπτων. ὁ δὲ ρμδ εἰκοσιπέμπτων, ἃ ἐστὶ δύο στερεόντες ποιοῦσι τὰ εἰκοσιπέμπτα, ἤτοι μονάδας ις. καὶ ἔστιν ἑκάτερος τετράγωνος.

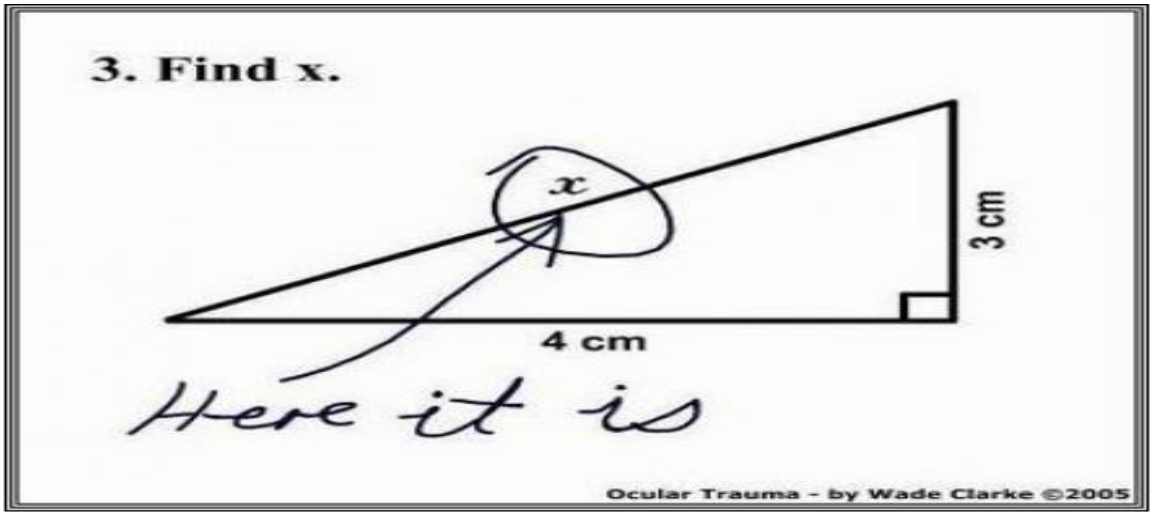
QVÆSTIO IX.

RVRSVS oporteat quadratum 16. diuidere in duos quadratos. Ponatur rursus primi latus 1 N. alterius verò quotcunque numerorum cum defectu tot vnitatum, quot constat latus diuidendi. Esto itaque 2 N. − 4. erunt quadrati, hic quidem 1 Q. ille verò 4 Q. + 16. − 16 N. Cæterum volo vtrumque simul æquari vnitatibus 16. Igitur 5 Q. + 16. − 16 N. æquatur vnitatibus 16. & fit 1 N. $\frac{4}{5}$. erit ergo primi latus $\frac{16}{25}$.

ἔστω δὴ πάλιν τὸν ις τετράγωνον διελεῖν εἰς δύο τετραγώνους. τεθέτω πάλιν ἡ τοῦ πρώτου πλευρὰ ς ε᾽ νός, ἡ δὲ ἑτέρου ς ὅσων δήποτε λείψει μ ὅσων ἐστὶν ἡ δι᾽ ἁμφοῖν πλευρά. ἔστω δὴ ς ε᾽ νς β λείψει μ δ. ἔσονται οἱ τετράγωνοι ὁ μὲν δυνάμεως μιᾶς, ὁ δὲ δυνάμεων δ μ ις λείψει ς ις. βούλομαι δὲ δύο λοιπὸν συντεθέντας ἴσους εἶναι μ ις. δυνάμεις ἄρα ε μ ις λείψει ς ις ἴσαι μ ις. καὶ γίνεται ὁ ἀριθμὸς ις πέμπτων. ἔσται ἡ μὲν τοῦ πρώτου πλευρὰ ις πέμπτων.

H

Problem 1



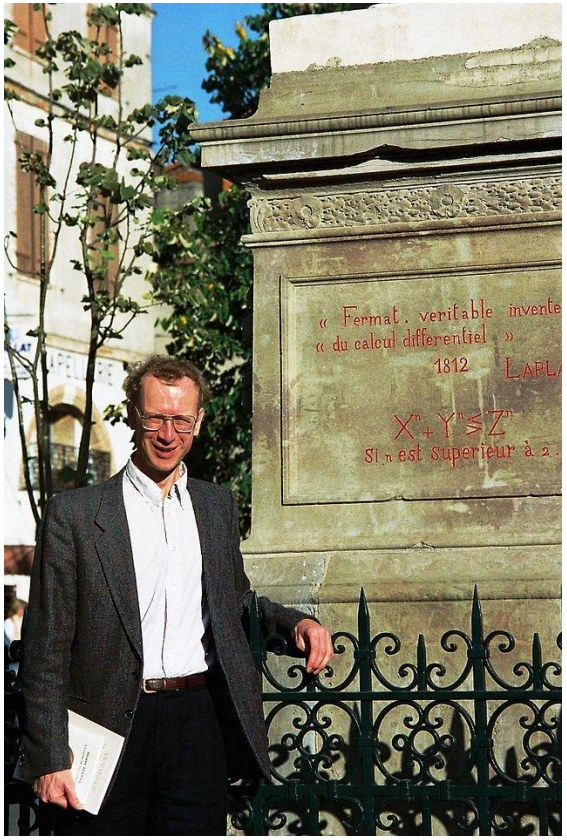
- Nobody knows, was it a Fermat's joke or did he really prove it
- Mathematicians need approximately 350 years to prove this fact
- Thereto they've constructed such branches of Algebra as Finite Fields and Galois Theory

Problem 1

- Finally the general case of this problem was solved in 1996 by British mathematician Andrew John Wiles
- He proved, that equation

$x^n + y^n = z^n, n \in \mathbb{N}; x, y, z \in \mathbb{Z}; xyz \neq 0$

Has no solutions for $n \in \mathbb{N}, n > 2$



Problem 2

- Problem 2: Solve the equation:

$$x^2 - n_0 y^2 = z, for\ fixed\ n_0 \in \mathbb{Z}; x, y, z \in \mathbb{Z}$$

Problem 2

Example 1

- Solve the following equation in $\mathbb{Z}$:

$$x^2 - y^2 = 5$$

$\Rightarrow (x-y)(x+y) = 5$|*Both part factorization* (in $\mathbb{Z}$)

$\Rightarrow \big((x-y),(x+y)\big) \in \alpha\{(1,5),(5,1)\}$| α *is invertible* (in $\mathbb{Z}$)

$\Rightarrow$ Since invertible elements (units) in $\mathbb{Z}$ are ± 1, we obtain

$\Rightarrow \big((x-y),(x+y)\big) \in \pm\{(1,5),(5,1)\}$

$\Rightarrow (x,y) \in \{(3,2),(-3,2),(3,-2),(-3,-2)\}$

- We are able to solve this equation, since we have a unique prime factorization in $\mathbb{Z}$ and we know all the units in $\mathbb{Z}$.

Problem 2

Example 2

- And what about following equation in $\mathbb{Z}$:

$$x^2 + 5y^2 = 6$$

$$\Rightarrow \left(x - \sqrt{-5}y\right)\left(x + \sqrt{-5}y\right) = 6 = 2 \cdot 3 = \left(1 - \sqrt{-5}\right)\left(1 + \sqrt{-5}\right)$$

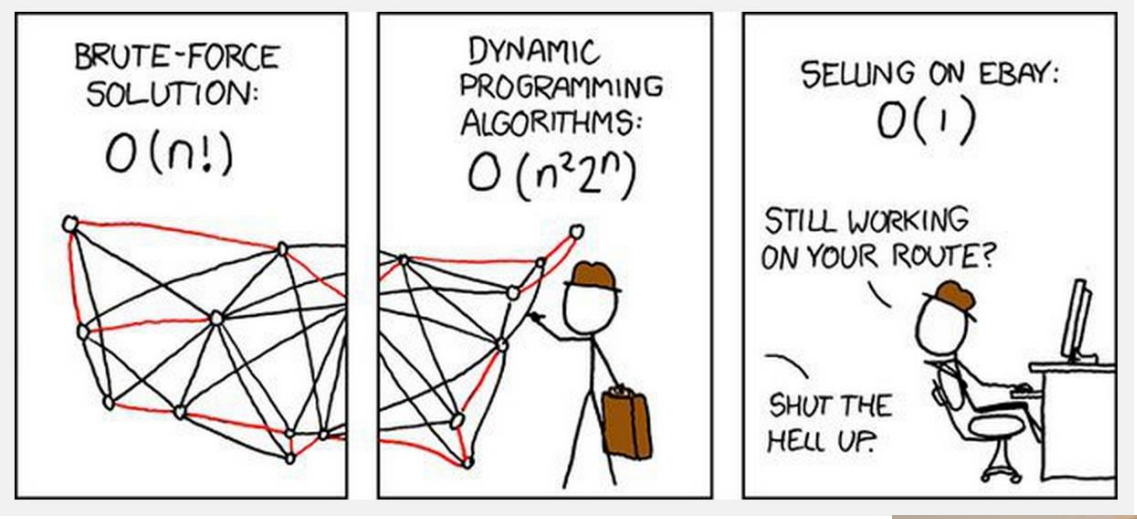
- Factorization is not Unique! How can we repair it?
- How can we find units in $\mathbb{Z}\left[\sqrt{-5}\right]$?

Problem 2

- To answer these and some more general questions we have to study following chapters:

1. Finite Fields’ Theory and Galois Theory
2. Number Fields’ and Number Rings’ Theory
3. Special chapters of Commutative Algebra
4. Embedding's’ Theory
5. Units in Number Rings

Combinatorial Optimization



- Lectures (In German) - 2 times a week
- Exercises – once a week
- Lecturer Prof. Dr. Volker Kaibel
- Official web-page

https://www.math.uni-magdeburg.de/institute/imo/teaching/wise14/kombopt/

Motivation

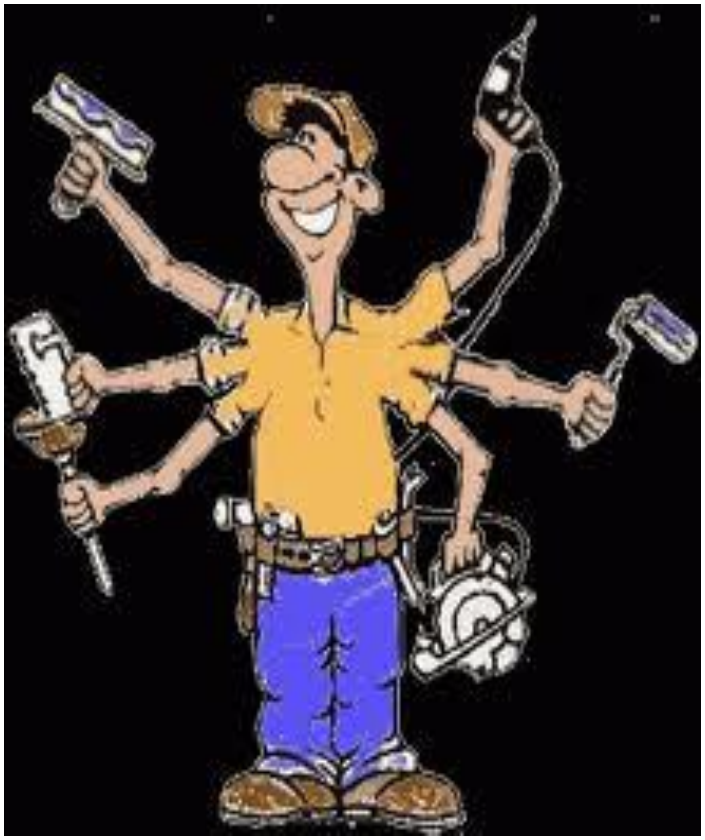
- Shortest Path Problem

Find the shortest path between two cities on a road map.

Motivation

- Solve Assignment Problem

There are a number of *agents* and a number of *tasks*. Any agent can be assigned to perform any task, incurring some *time* that may vary depending on the agent-task assignment. It is required to perform all tasks by assigning exactly one agent to each task and exactly one task to each agent in a given time.



General Approach

- Construct mathematical models of each problem, using combinatorial structures
- Run some “clever” (polynomial) algorithm on the constructed combinatorial structure

Shortest Path Problem

Problem 1.11 (Kürzeste-Wege Problem)

Instanz: *Digraph* $D = (V, A)$, $c \in \mathbb{Q}^A$, $s, t \in V$

Aufgabe: *Finde einen s-t-Weg kürzester c-Länge oder stelle fest, dass es keinen s-t-Weg in D gibt.*

Algorithmus 1.36 (Kürzeste Wege in azyklischen Digraphen)

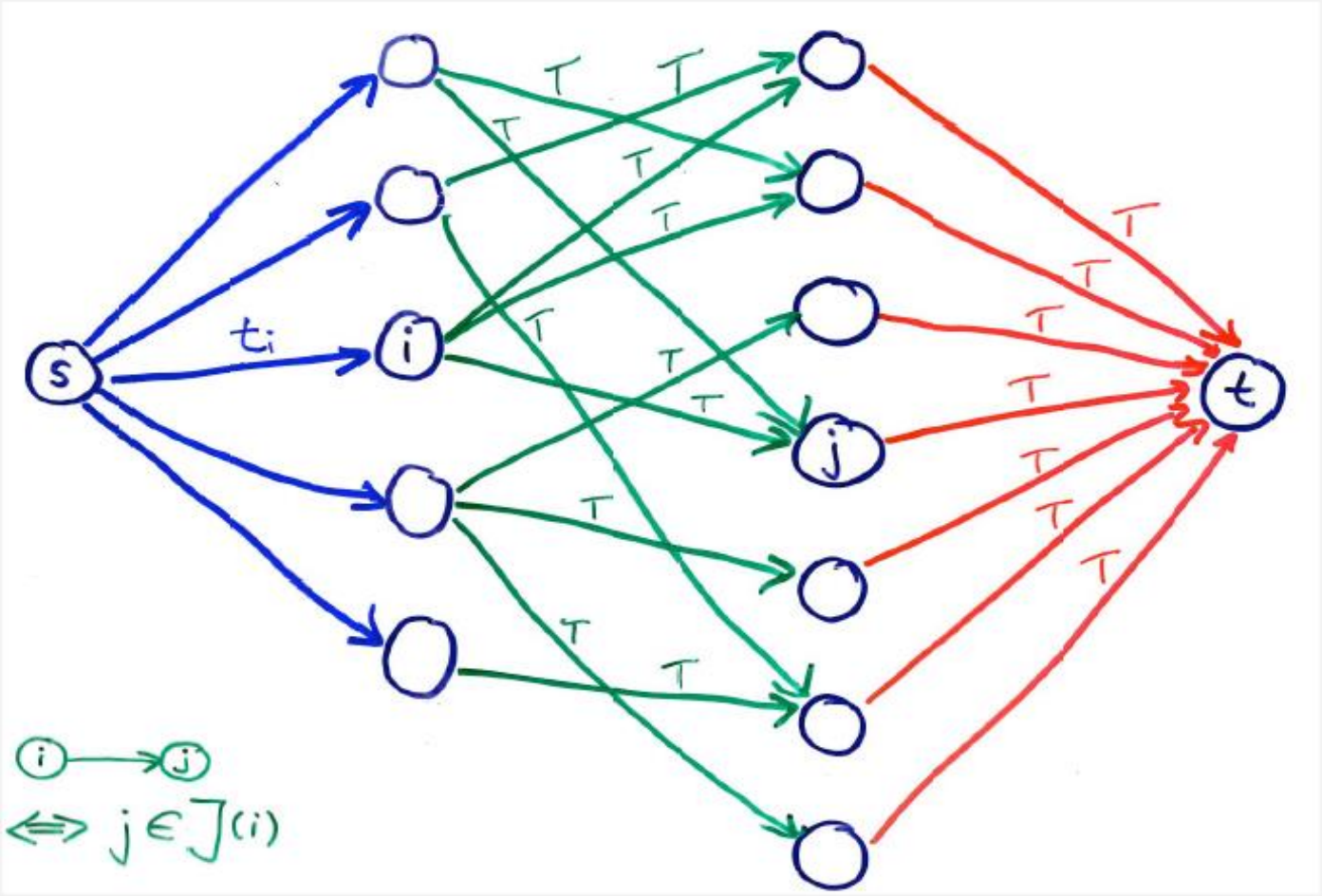
Algorithmus 1.38 (Dijkstra-Algorithmus)

Der Bellman-Ford Digraph

0/1-Knapsack

Assignment Problem

Job-Assignment als Flussproblem



Assignment Problem

FORD & FULKERSON (1954):
(Beschreiben das Problem, das T. E. Harris formuliert hatte.)

> Consider a rail network connecting two cities by way of a number of intermediate cities, where each link of the network has a number assigned to it representing its capacity. Assuming a steady state condition, find a maximal flow from one given city to the other.

FORD & FULKERSON (1962):
(Über das Max-Flow Problem.)

> It was posed to the authors in the spring of 1955 by T.E. Harris, who, in conjunction with General F.S. Ross (Ret.), had formulated a simplified model of railway traffic flow, and pinpointed this particular problem as the central one suggested by the model [11].

Combinatorial Optimization

- To answer these and some more general questions we have to study following chapters:

1. Dynamic Programming
2. Flows and Circulations
3. Matchings
4. Matroids

JUST DO IT.