Universität Zürich[UZH]

I·Math Institut für Mathematik

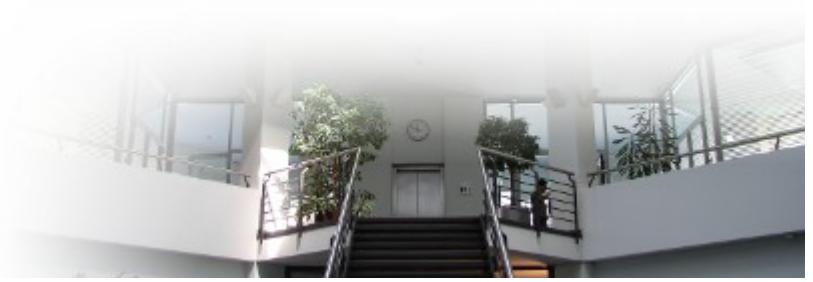
Course Introduction

Mathematics Courses in the Spring semester 2024

Course overview

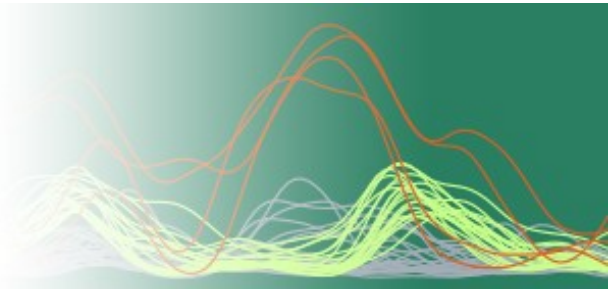
- STA 120 Introduction to Statistics – Furrer
- STA 425 Survival Analysis
- STA 421 Foundations of Bayesian Methodology
- STA 408 Statistical Methods in Epidemiology
- MAT 903 Statistics for Mathematicians – Bovet
- MAT 548 Geometry of Numbers – Gorodnik
- MAT 005 Coding Theory – Rosenthal
- MAT 576 Finite Fields: Theory and Application – Gassner
- MAT 827 Numerical Methods for Hyperbolic PDEs – Liu
- MAT 645 Introduction to Riemannian Geometry – Moshayedi
- MAT 826 Hierarchische Matrizen (H-Matrizen) – Sauter
- MAT 820 Numerisches Praktikum – Sauter
- MAT 017 Introduction to Isogeny-Based Cryptography – Sconza
- MAT 610 Harmonic Analysis – Widmayer

University of Zurich[UZH]



Statistik Module

University of Zurich[UZH]



STA120 Introduction to Statistics

- Der Titel spricht für sich
- Nur als Wahlmodul ganze Universität anrechenbar

https://user.math.uzh.ch/furrer/download/sta120/script_sta120.pdf

Vorkenntnisse: keine

Dr. Zofia Baranczuk

Englisch, Dienstag 10-13 (2+1), 5 ECTS

University of Zurich[UZH]

STA425 Survival Analysis

- General concepts of censoring, summary statistics
- Estimation of survival curves,
- Regression models for censored observations

Vorkenntnisse: STA402

Prof. Dr. Torsten Hothorn

Englisch, halbsemestrig, 1. Hälfte Dienstag 9-12 (2+1), 3 ECTS

University of Zurich[UZH]

STA421 Foundations of Bayesian Methodology

- Contrasting the classical and Bayesian approaches
- Discussing the mechanisms of the Bayesian paradigm
- Performing analyses in R (with JAGS and R-INLA)

Vorkenntnisse: STA402/MAT924

PD Dr. Malgorzata Roos

Englisch, Donnerstags 9-12 (2+1+P), 4 CP

University of Zurich[UZH]

STA408 Statistical Methods in Epidemiology

- risk, odds and rate ratios
- specialized regression methods (propensity score adjustments and conditional logistic regression)
- causal inference, imputation and measurement error

Vorkenntnisse: STA404, STA121 oder STA406

Prof. (ZFH) Dr. Beate Sick

Englisch, Montag 9-12 (2+1), 5 ECTS, HRS

University of Zurich[UZH]

Modules in Open and Reproducible Science (CRS-STS)

5 Steps to Good Data Science Practice in R (10SMOS_2)

Nur als Wahlmodul ganze Universität anrechenbar

Vorkenntnisse: keine, mini STA472

Flipped learning courses with online preparation and on-site practice of the concepts using R for practicals

1 ECTS

Tuesdays 16:15-18:00, biweekly

Portfolio exam: quizzes, homework and in-class work count towards credit

Learning goals: 5 Steps to Good Data Science Practice in R

Participants who successfully passed the module

- know how to use a version control system such as Gitlab and have practiced using it for the duration of the module
- are able to write functions in R and use unit tests as well as other advanced R programming techniques
- understand how to avoid questionable research practices
- know key principles of good statistical practice and are able to apply them
- know how to use some specific tools for meta data handling in R

5 Steps to Good Data Science Practice in R: for whom?

Students of all disciplines

- who work at least in part empirically.
- who have gained first experience with research
- who are active users of the scientific literature
- who had an introduction to statistics
- who have good computer knowledge is expected including experience in R (e.g. be comfortable in manipulating data and objects and know how to use existing functions and packages).

MAT 903 Statistics for Mathematicians

MAT903 Statistics for Mathematicians

Statistics is the mathematical discipline whose purpose is to make sense of **data generated by a random phenomenon**.

Its goal is to **determine characteristics about the random phenomenon** (the process of statistical inference) and **quantify their uncertainty**.

This course will provide an introduction to the basic notions of Statistics where essentially all results are proved rigorously.

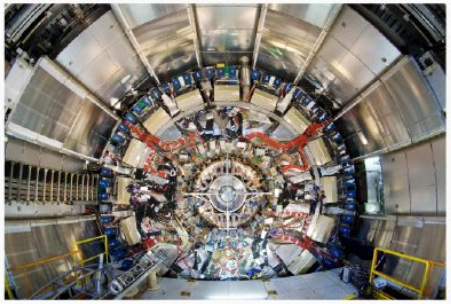
Prior Knowledge: First year analysis and MAT 901 Stochastics

Prof. Dr. Alexandre Bovet

English, Monday 1pm-3pm (course) & Thursday 3pm-5pm (exercises), 6 ECTS

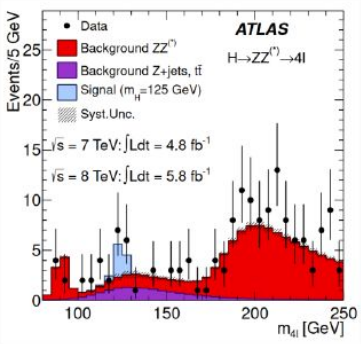
Framework for Parametric Statistical Inference

Random phenomenon
e.g. scientific experiment



Measurement

Data



Observed values

$\{x_1, x_2, ..., x_n\}$

Statistical inference

Mathematical probabilistic model
with parameter θ

$$F(x;\theta) = \mathbb{P}[X \leq x]$$

1. There is a distribution $F(x;\theta)$ depending on an unknown $\theta \in \mathbb{R}^p$.
2. We observe the realisation of n independent identically distributed random variables $X_1, \ldots, X_n$ that follow this distribution.
3. Use the observations to make statements about the true value of θ and quantify the uncertainty associated with those statements.

Objectives

- Presenting the basic ideas of parameter inference in a coherent and rigorous manner.
- Providing a conceptually compact course.
- Not primarily a course on statistical theory, rather a course on entry-level statistical inference for an audience of mathematicians.
- Providing a solid foundation for applying basic statistics approaches and for understanding more advanced concepts (e.g. regression, non-parametric inference and Bayesian inference).

Plan

1. Regular Probability Models (weeks 1 & 2)
    - Discrete & Continuous Models
    - Exponential Families of Distributions
    - Transforming Probability Models
    - Model Selection and Exploratory Data Analysis
2. Sampling from Probability Distributions (weeks 3 & 4)
    - Sampling, Statistics and Sufficiency
    - Sampling from a Normal Distribution & from an Exponential Family
    - Approximate Sampling Distributions
3. Point Estimation of Model Parameters (weeks 5, 6 & 7)
    - Criteria for Comparing Estimators
    - Fundamental Limitations to Estimation Accuracy
    - Methods for Constructing Estimators
    - Estimation Methods vs Estimators vs Estimates
4. Tests of Hypotheses for Model Parameters (weeks 8, 9, 10 & 11)
    - Test Functions and Error Types
    - The Neyman-Pearson Framework
    - Methods for Constructing Test Functions
    - The p-Value
    - Accepting vs Not Rejecting
5. Confidence Intervals for Model Parameters (weeks 12 & 13)
    - Confidence Intervals and Confidence Levels
    - Pivots and Approximate Pivots
    - The Duality with Hypothesis Tests
    - Optimality in Interval Estimation
    - Interpreting Confidence Intervals

MAT 548 Geometry of Numbers

MAT 548 — Geometry of Numbers

Lecturer: *Prof. Alexander Gorodnik*

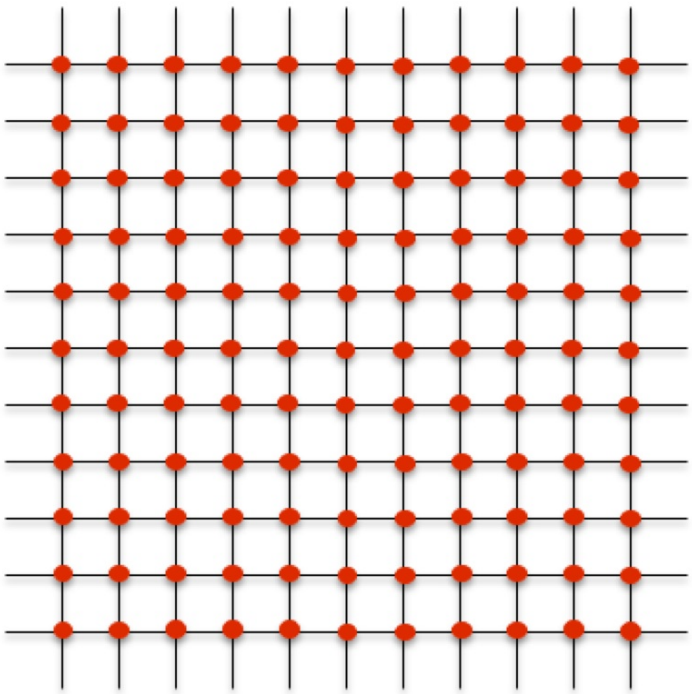
Email: alexander.gorodnik@math.uzh.ch

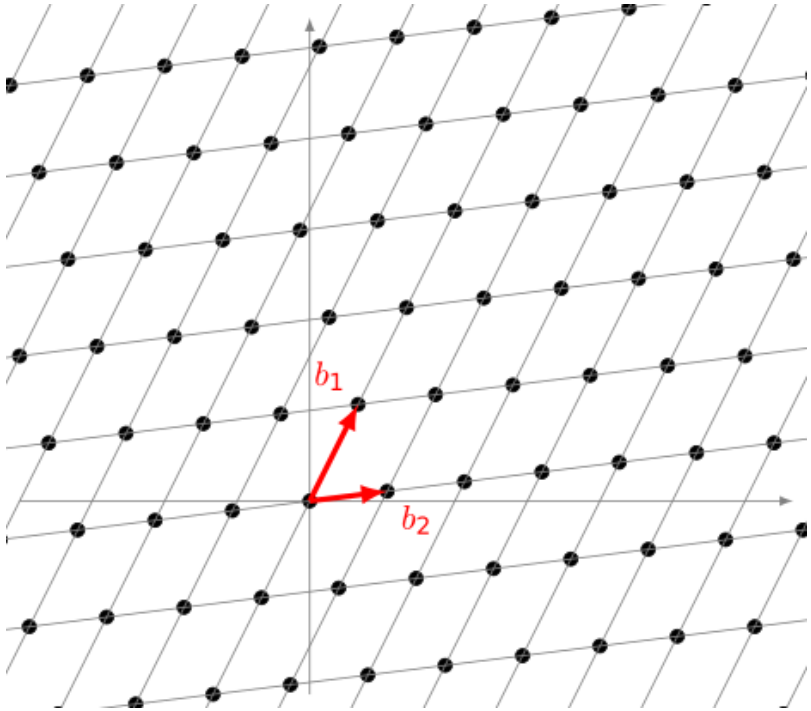
Office: K22

In this course, we study lattices in $\mathbb{R}^d$ and related problems.

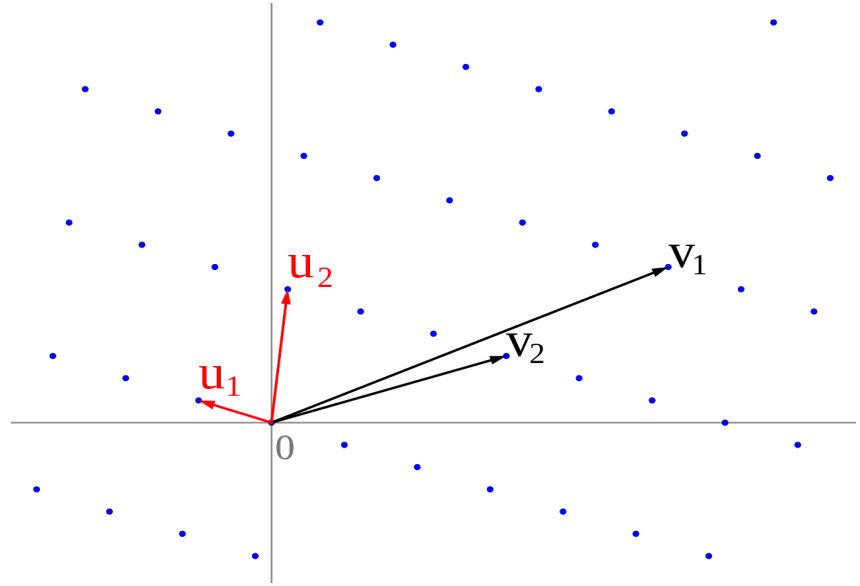
A lattice is a subgroup spanned by a basis of $\mathbb{R}^d$:

$$\Lambda = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_d.$$

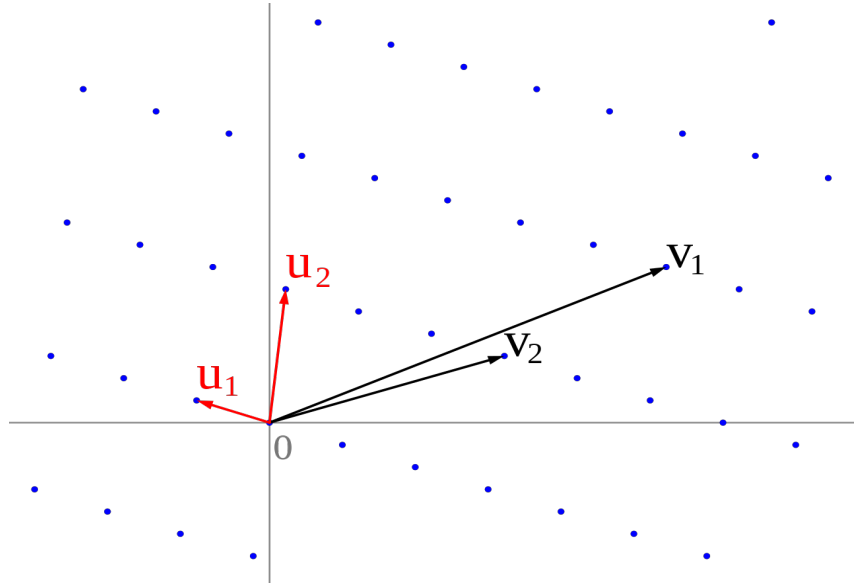




How to parametrise
the set of lattices $\mathcal{L}$ in $\mathbb{R}^d$?



How to parametrise
the set of lattices $\mathcal{L}$ in $\mathbb{R}^d$?

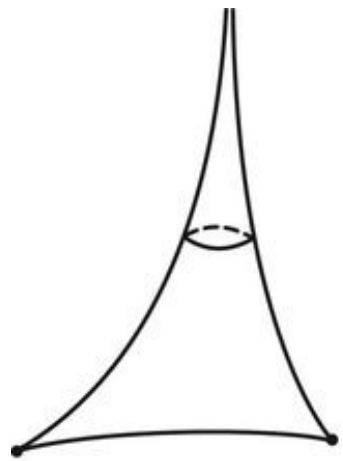


Answer:

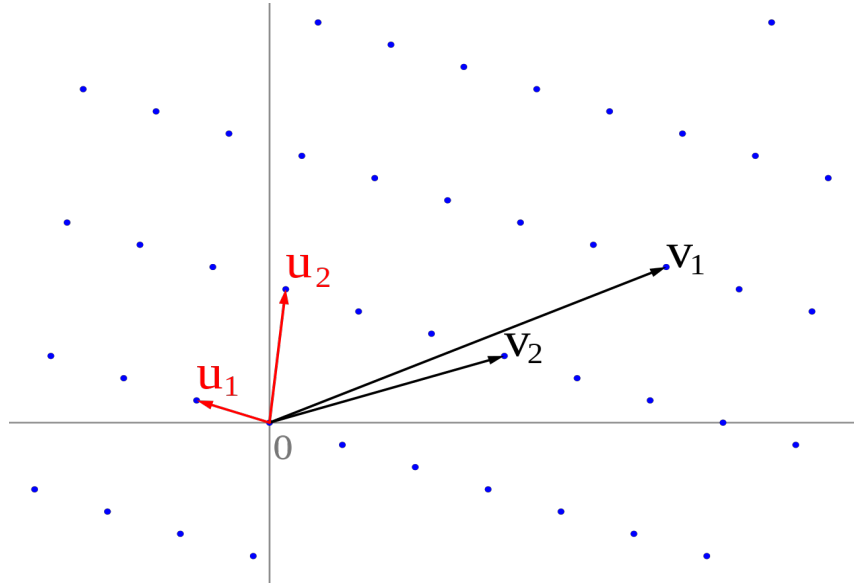
$$\mathcal{L} \simeq G/\Gamma$$

where

$$G = \{g \in \mathrm{M}_d(\mathbb{R}) : \det(g) \neq 0\},$$
$$\Gamma = \{g \in \mathrm{M}_d(\mathbb{Z}) : \det(g) = \pm 1\}.$$



How to parametrise
the set of lattices $\mathcal{L}$ in $\mathbb{R}^d$?

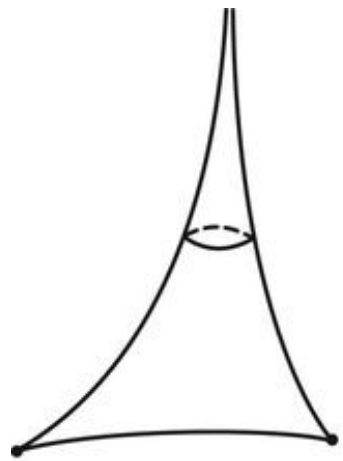


Answer:

$$\mathcal{L} \simeq G/\Gamma$$

where

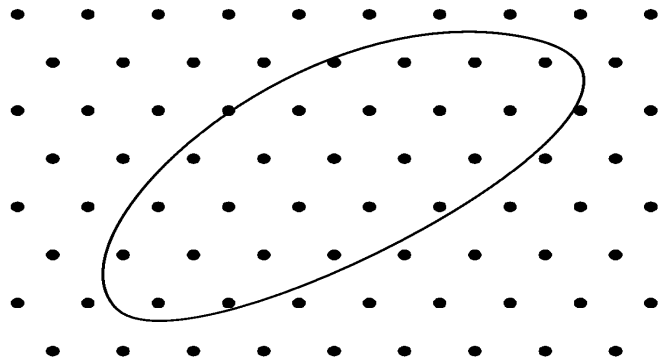
$$G = \{g \in \mathrm{M}_d(\mathbb{R}) : \det(g) \neq 0\},$$
$$\Gamma = \{g \in \mathrm{M}_d(\mathbb{Z}) : \det(g) = \pm 1\}.$$



Understanding properties of the space $\mathcal{L}$ has many applications in
Number Theory, Combinatorics, Coding Theory, ...

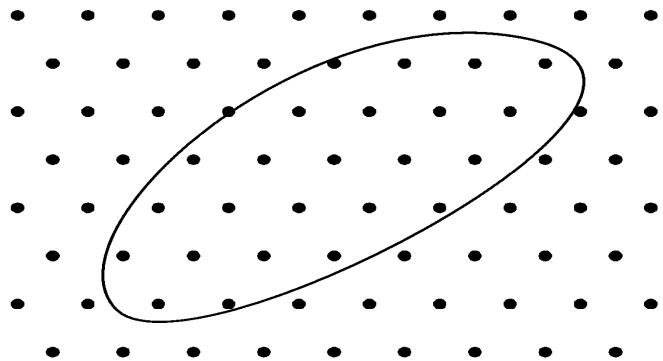
A Sample Problem

Is there a lattice point $x \in \Lambda$ contained in a given domaim Ω in $\mathbb{R}^d$?



A Sample Problem

Is there a lattice point $x \in \Lambda$ contained in a given domaim Ω in $\mathbb{R}^d$?

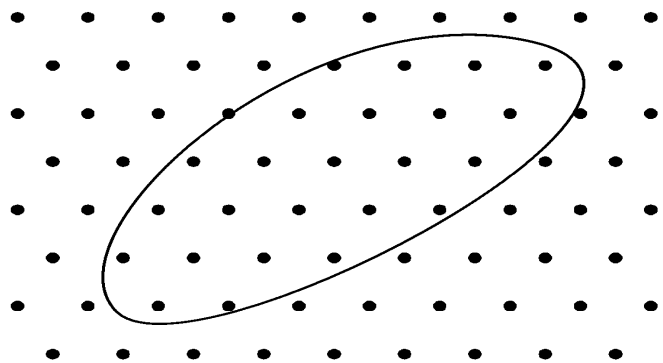


Known: (Minkowski Thm) For a convex centrally symmetric Ω,

$$\text{vol}(\mathbb{R}^d/\Lambda) \leq \text{vol}(\Omega)/2^d \implies \exists \text{ non-zero } x \in \Lambda \cap \Omega.$$

A Sample Problem

Is there a lattice point $x \in \Lambda$ contained in a given domaim Ω in $\mathbb{R}^d$?



Known: (Minkowski Thm) For a convex centrally symmetric Ω,

$$\text{vol}(\mathbb{R}^d/\Lambda) \leq \text{vol}(\Omega)/2^d \implies \exists \text{ non-zero } x \in \Lambda \cap \Omega.$$

Unknown: (Minkowski Conjecture) Let $a_1, \ldots, a_d \in \mathbb{R}$.
For $\Omega = \{x \in \mathbb{R}^d : |x_1 + a_1| \times \cdots \times |x_d + a_d| \leq 1\}$,

$$\text{vol}(\mathbb{R}^d/\Lambda) \leq 2^d \implies \exists x \in \Lambda \cap \Omega.$$

A Sample Application: Rational Approximations

Given $(x_1, \cdots, x_d) \in \mathbb{R}^d$, find good approximations $(\frac{p_1}{q}, \cdots, \frac{p_d}{q}) \in \mathbb{Q}^d$.

A Sample Application: Rational Approximations

Given $(x_1, \cdots, x_d) \in \mathbb{R}^d$, find good approximations $(\frac{p_1}{q}, \cdots, \frac{p_d}{q}) \in \mathbb{Q}^d$.

When $d = 1$, this involves the Theory of Continued Fractions:

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4 + \ddots}}}},$$

A Sample Application: Rational Approximations

Given $(x_1, \cdots, x_d) \in \mathbb{R}^d$, find good approximations $(\frac{p_1}{q}, \cdots, \frac{p_d}{q}) \in \mathbb{Q}^d$.

When $d = 1$, this involves the Theory of Continued Fractions:

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4 + \ddots}}}},$$

Known: Given any $(x_1, \cdots, x_d) \in \mathbb{R}^d$, there exist approximations

$$|x_1 - \tfrac{p_1}{q}| \leq q^{-(1+1/d)}, \ldots, |x_d - \tfrac{p_d}{q}| \leq q^{-(1+1/d)} \quad \text{with } q \to \infty.$$

A Sample Application: Rational Approximations

Given $(x_1, \cdots, x_d) \in \mathbb{R}^d$, find good approximations $(\frac{p_1}{q}, \cdots, \frac{p_d}{q}) \in \mathbb{Q}^d$.

When $d = 1$, this involves the Theory of Continued Fractions:

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4 + \ddots}}}},$$

Known: Given any $(x_1, \cdots, x_d) \in \mathbb{R}^d$, there exist approximations

$$|x_1 - \tfrac{p_1}{q}| \leq q^{-(1+1/d)}, \ldots, |x_d - \tfrac{p_d}{q}| \leq q^{-(1+1/d)} \quad \text{with } q \to \infty.$$

Unknown: For any $\varepsilon > 0$, there exist approximations

$$|\sqrt[3]{2} - \tfrac{p}{q}| \leq \varepsilon\, q^{-2} \quad \text{with } q \to \infty.$$

Prerequisites

Analysis I-II, Linear Algebra I-II, Algebra I.

References

- Cassels, *An introduction to Diophantine Approximation.*
- Cassels, *An introduction to the Geometry of Numbers.*
- Schmidt, *Diophantine approximation.*
- Siegel, *Lectures on the Geometry of Numbers.*

MAT 005 Coding Theory

University of Zurich[UZH]

I·Math Institute of Mathematics

MAT005: Coding Theory

FS 2023

Prof. Dr. Joachim Rosenthal

Assistants: Michael Schaller, Beatrice Toesca

21.12.2023

Coding Theory: Requirements

Introductory course on algebraic coding theory.
The main topic covered will be Linear Block Codes and their properties.

Requirements:

- MAT211 Algebra (in particular the part on Finite Fields);
- very basic knowledge of algebraic geometry may be useful, but is not required.

Coding Theory: Overview

Modern coding theory started in 1948 with the work of Shannon.
In the algebraic sense, a block code can be viewed as an algebraic subset of an affine space over a finite field, hence techniques of algebraic geometry can be fruitfully applied to the study of codes.

We plan to treat the following topics:

- Linear Block Codes
  - Hamming Codes
  - Cyclic Codes
  - MDS Codes
  - Golay Codes
  - Reed-Solomon Codes
  - BCH-Codes
  - AG-Codes and Goppa Codes
  - Decoding via Berlekamp-Massey algorithm
- Convolutional Codes
- Codes on Graphs

Coding Theory: Assessment

- Homework will be assigned every week and discussed during the exercise class on the following week.
- It is required that the students correctly solve 50% of the homework by the end of the semester and at least 8 exercise sheets.

Coding Theory: Course Material

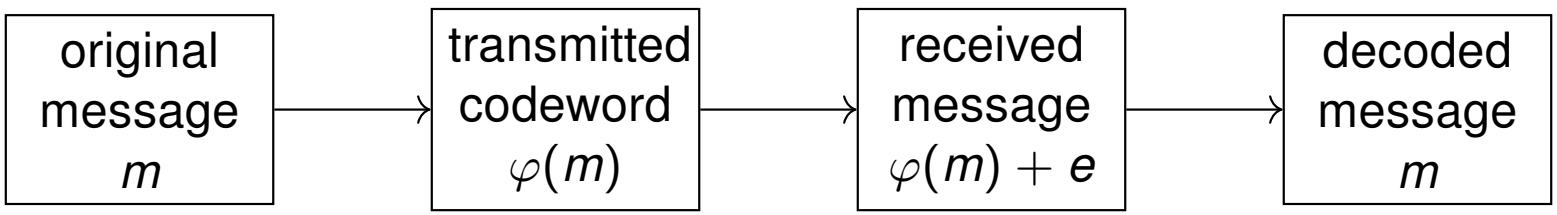
- MacWilliams/Sloane, “The Theory of Error-Correcting Codes", Elsevier;
- Huffman/Pless, “Fundamentals of Error-Correcting Codes", Cambridge University Press;
- Lint, “Introduction to Coding Theory", Springer;
- Roman, “Coding and Information Theory", Springer;
- Script of a previous edition of the course.

What is Coding Theory?

Codes

Devices designed to detect and correct errors that occur during the transmission of a message.

If one symbol arrives wrong, can we recover the original word?
Core $\mapsto$ Cone, More, Care, Code, ... (?)
Communiration $\mapsto$ Communication (!)
Introduce an encoding function φ that adds redundancy!



Claude Shannon: *A mathematical theory of communication* (1948)

First Examples of Codes

Set of messages $\mathcal{M} = \{\text{yes}, \text{no}\}$, alphabet $\mathcal{A} = \{0, 1\}$.

Example 1

φ : yes $\mapsto$ 1, no $\mapsto$ 0. $\mathcal{C} = \mathrm{Im}(\varphi) = \{0, 1\}$.
What if an error occurs? **very BAD!**

Example 2 (Double Repetition Code)

φ : yes $\mapsto$ 11, no $\mapsto$ 00. $\mathcal{C} = \mathrm{Im}(\varphi) = \{00, 11\}$.
What if an error occurs? $\varphi(m) + e = 01$? **still BAD!**

Example 3 (Triple Repetition Code)

φ : yes $\mapsto$ 111, no $\mapsto$ 000. $\mathcal{C} = \mathrm{Im}(\varphi) = \{000, 111\}$.
What if an error occurs? $\varphi(m) + e = 101 \mapsto 111 \mapsto$ yes. **BETTER**

Distance between two codewords $\sim$ number of errors

MAT 576 Finite Fields: Theory and Application

MAT827 Numerical Methods for Hyperbolic PDEs

Numerical Methods for Hyperbolic PDEs

Yongle Liu

Institute of Mathematics, University of Zurich

Exercise tutor: Jianfang Lin

Main focus

In this course, we will focus on the following Hyperbolic conservation laws (PDEs):

$$\boldsymbol{u}_t + \boldsymbol{f}(\boldsymbol{u})_x = 0.$$

- Hyperbolic conservation laws arise in many models in the sciences, ranging from the design of aircraft (Euler equations) to the study of supernovas in astrophysics (MHD equations).
- Since interesting conservation laws like the Euler equations are nonlinear, it is not possible to obtain explicit solution formulas. Hence, numerical methods need to be developed for approximating or simulating the solutions of conservation laws.
- The design and implementation of efficient numerical methods is the main focus of this course.

Content

- understand the analytical structure of the solutions of conservation laws (method of characteristics, stability analysis, $\cdots$)
- discuss theoretical properties of the solutions (weak solution, entropy condition, $\cdots$)
- both linear and nonlinear equations in one-dimensional case are considered
- efficient numerical finite volume schemes are described and tested

notes:

- coding in python
- written examination

MAT 645 Introduction to Riemannian Geometry

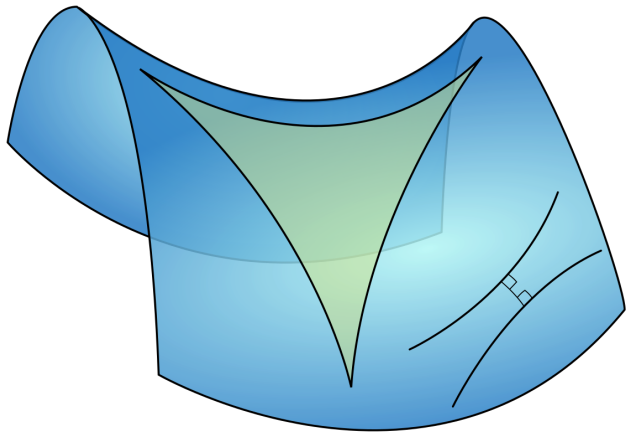
Introduction to Riemannian Geometry

Course Presentation for MAT645

Nima Moshayedi

University of Zurich

21.12.2023



Organizational

Reference

- M. P. do Carmo, *Riemannian Geometry*, Birkhäuser (1992).

Setting

- 2 hours lecture and 2 hours exercise class per week.
- BSc students in the fourth semester and higher & MSc students (suitable also for physics students)
- 6 ECTS
- Oral Exam

Motivation

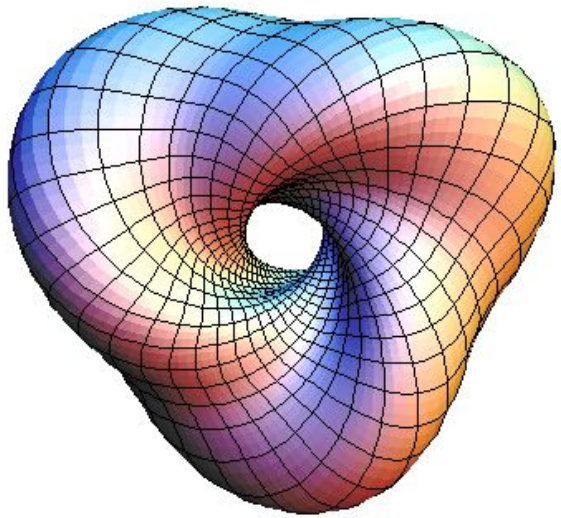
- How can can we extend differential calculus to spaces more general than $\mathbb{R}^n$?
- What are the mathematical concepts behind Einstein's theory of gravity?

$$R_{ij} - \frac{1}{2} g_{ij} R = \frac{8\pi G}{c^4} T_{ij}.$$

- How can we describe physical systems on a curved spacetime?

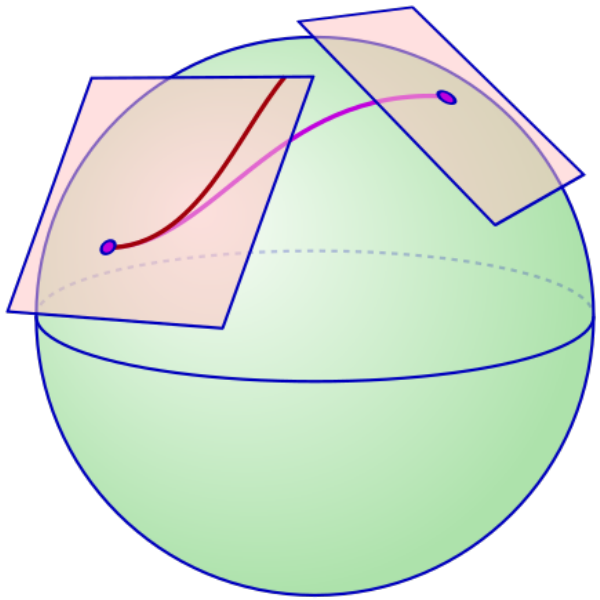
Differentiable Manifolds

- **Chapter 0: Differentiable Manifolds**
  - Tangent Spaces
  - Immersions and Embeddings
  - Examples of Manifolds, Orientation
  - Vector fields, Brackets, Topology of Manifolds



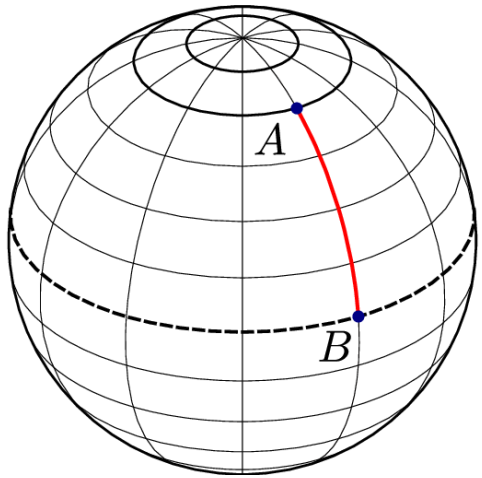
Riemannian Metrics & Connections

- **Chapter 1: Riemannian Metrics**
- **Chapter 2: Affine and Riemannian Connections**
  - Affine Connections
  - Riemannian Connections
  - The Levi-Civita Connection
  - Covariant Derivatives



Geodesics & Curvature

- **Chapter 3: Geodesics**
  - Geodesic Flow
  - Exponential Map
  - Minimizing Properties of Geodesics
- **Chapter 4: Curvature**
  - Riemannian Curvature
  - Sectional Curvature
  - Ricci Curvature and Scalar Curvature
  - Tensors on Riemannian Manifolds



End of Presentation

If you have further questions, contact the Lecturer:

Nima Moshayedi
Office: Y27 J32
Email: nima.moshayedi@math.uzh.ch

MAT 826 Hierarchische Matrizen (H-Matrizen)

I·Math Institut für Mathematik

MAT 820 Numerisches Praktikum

MAT 017 Introduction to Isogeny-Based Cryptography

Introduction to Isogeny-based Cryptography

Instructor: Silvia Sconza
Type of Module: Seminar

General information

Target groups:

- BSc students from 3rd semester;
- MSc students.

General information

Target groups:

- BSc students from 3rd semester;
- MSc students.

Requirements:

- MAT211 Algebra;
- MAT512 Elliptic Curves.

General information

Target groups:

- BSc students from 3rd semester;
- MSc students.

Requirements:

- MAT211 Algebra;
- MAT512 Elliptic Curves.
- Basic knowledge of Algebraic Number Theory and/or Cryptography will be helpful, but *not required*.

Overview:

The seminar will focus on the following topics:

Overview:

The seminar will focus on the following topics:

- Algebraic structure of $\mathrm{End}(E)$;

Overview:

The seminar will focus on the following topics:

- Algebraic structure of $\mathrm{End}(E)$;
- Group action present in the *ordinary* case;

Overview:

The seminar will focus on the following topics:

- Algebraic structure of $\mathrm{End}(E)$;
- Group action present in the *ordinary* case;
- Isogeny graphs;

Overview:

The seminar will focus on the following topics:

- Algebraic structure of $\mathrm{End}(E)$;
- Group action present in the *ordinary* case;
- Isogeny graphs;
- Couveignes-Rostovtsev-Stolbunov protocol (*ordinary* case);

Overview:

The seminar will focus on the following topics:

- Algebraic structure of $\mathrm{End}(E)$;
- Group action present in the *ordinary* case;
- Isogeny graphs;
- Couveignes-Rostovtsev-Stolbunov protocol (*ordinary* case);
- SIDH protocol (*supersingular* case);

Overview:

The seminar will focus on the following topics:

- Algebraic structure of $\mathrm{End}(E)$;
- Group action present in the *ordinary* case;
- Isogeny graphs;
- Couveignes-Rostovtsev-Stolbunov protocol (*ordinary* case);
- SIDH protocol (*supersingular* case);
- CSIDH protocol (*supersingular* case).

MAT 610 Harmonic Analysis

Harmonic Analysis

Origin: representation of functions as superposition of basic "waves".

Key topics (real-variable theory)

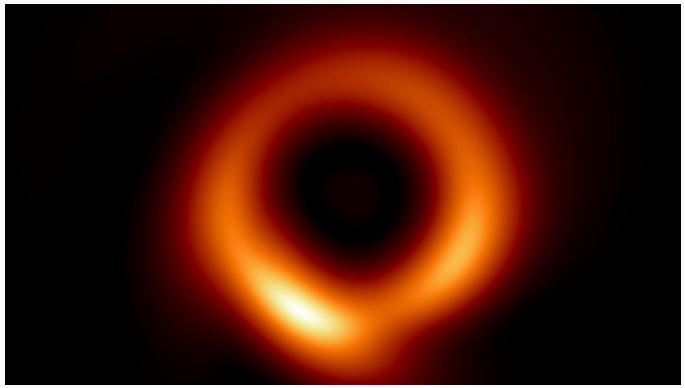
Fourier series and transforms, singular integrals ...

Fundamental mathematics connections to

Functional Analysis, Differential Equations, Complex Analysis, Quantum Mechanics, Representation Theory, Number Theory, Geometry, Orthogonal Polynomials ...

Wide-ranging applications

signal processing, audio or image compression, medical imaging, data analysis ...



Prerequisites

Analysis I–III (including measure theory, functional analysis of Lebesgue spaces)