MATH 489 Mathematical Introduction to Quantum Algorithms and Postquantum Cryptography

This syllabus may be subject to update and change.

Course Information

Instructor: Ferruh Özbudak

Level: Undergraduate

Credits: SU Credits: 3 | ECTS: 6

Language: English

Prerequisites:

Linear Algebra (MATH 201 or equivalent)

Textbooks:

Johannes A. Buchmann, Introduction to Quantum Algorithms, AMS, 2024.

Daniel J. Bernstein, Johannes Buchmann, Erik Dahmen, Post-Quantum Cryptography, Springer.

Course Description

This course provides a rigorous mathematical introduction to quantum algorithms and post-quantum cryptography, focusing on theoretical foundations rather than physical realizations. It emphasizes mathematical structures, computational complexity, and cryptographic applications rather than experimental quantum mechanics.

The course will introduce key mathematical aspects of quantum computing and cryptography.

The first 10 weeks focus on quantum algorithms, and the last 4 weeks introduce post-quantum cryptography, which ensures security in a quantum computing era.

Weekly Schedule

Week	Topics	Reference Material
1	Introduction to Quantum Computing from a Mathematical Perspective	Buchmann (Ch. 1)
2	Classical Computation Models and Complexity Theory	Buchmann (Ch. 2)

3 Mathematical Foundations: Hilbert Spaces, Linear Algebra for Quantum Computing Buchmann (Ch. 3)

4 Quantum Gates, Unitary Transformations, and Quantum Circuits Buchmann (Ch. 4)

5 Quantum Fourier Transform: Algebraic and Computational Aspects Buchmann (Ch. 5)

6 Deutsch's and Deutsch-Jozsa Algorithms: Mathematical Analysis Buchmann (Ch. 6)

7 Simon's Algorithm: Algebraic Perspective Buchmann (Ch. 7)

8 Grover's Algorithm: Probabilistic and Complexity-Theoretic View Buchmann (Ch. 8)

9 Shor's Algorithm: Number Theoretic and Algebraic Viewpoint Buchmann (Ch. 9)

10 Cryptographic Implications of Quantum Computing Buchmann (Ch. 10)

11 Mathematical Introduction to Post-Quantum Cryptography Bernstein et al. (Ch. 1)

12 Code-Based Cryptography: McEliece & Niederreiter Cryptosystems (Algebraic and Decoding Approaches) Bernstein et al. (Ch. 2)

13 Lattice-Based Cryptography: Hard Lattice Problems, LWE, NTRU, and Ring-LWE Cryptosystems Bernstein et al. (Ch. 3)

14 Final Discussions and Course Summary from a Mathematical Perspective -

Grading Policy

Project Assignment – 20%

Midterm Exam – 30%

Final Exam – 40%

Participation & Discussions – 10%