

CS939-15 Quantum Computing

26/27

Department

Computer Science

Level

Taught Postgraduate Level

Module leader

Matthias Caro

Credit value

15

Module duration

10 weeks

Assessment

Multiple

Study location

University of Warwick main campus, Coventry

Description

Introductory description

Quantum computing is an interdisciplinary field that lies at the intersection of computer science, mathematics, and physics. This computational paradigm relies on principles of quantum mechanics, such as superposition and entanglement, to obtain powerful algorithms.

Module aims

This module aims to provide a self-contained, comprehensive introduction to quantum computing, focusing on the design and analysis of quantum algorithms, as well as covering topics in quantum information and quantum cryptography, such as: quantum teleportation, quantum money, and post-quantum cryptography.

Outline syllabus

This is an indicative module outline only to give an indication of the sort of topics that may be covered. Actual sessions held may differ.

Quantum computing — motivation, foundations, and prominent applications.

Review of linear algebra in the context of quantum information, Dirac's bracket notation, limitation of classical algorithms.

The four postulates of quantum mechanics, qubits, quantum gates and circuits.

Basic quantum algorithms I — Deutsch's algorithm, analysing quantum algorithms, and implementing quantum circuits via QISKIT.

Basic quantum algorithms II — Simon's problem and the Bernstein -Vazirani algorithm.

Grover's quantum search algorithm, the BBBV Theorem, and applications of Grover's algorithm. RSA, and Shor's integer factorisation algorithm.

Introduction to quantum cryptography (post-quantum security, quantum key distribution).

Introduction to quantum information (superdense coding, nocloning theorem, quantum teleportation) Applications (quantum money, the Elitzur-Vaidman bomb).

Learning outcomes

By the end of the module, students should be able to:

- Understand the quantum computing paradigm:- Understand how to model quantum computation via quantum circuits.- Understand the role of measurements to read out results of a quantum computation. - Have a grasp of the role of superposition and entanglement in quantum computation.
- Understand the power and limitation of quantum computers:- Understand the underlying power of quantum mechanics for computation.- Identify problems for which a quantum speedup is possible.- Understand the fundamental limitations of quantum algorithms.
- State the four postulates of quantum mechanics and their application to computation:- Design and analyse quantum algorithms.- Grasp the notions of quantum states, unitary evolution, measurements, and composite systems.- Restate the postulates in terms of density matrices.
- Analyse fundamental quantum algorithms:- Shor's algorithm.- Grover's search.- The Bernstein-Vazirani algorithm.- Simon's problem.- The Deutsch-Jozsa paradigm.
- Understand the principles of quantum information and quantum communication:- Understand quantum teleportation and its limits.- Describe the framework of quantum error-correcting codes.
- Understand the implications of quantum computing on cryptography and security:- Understand the foundations of post-quantum cryptography.- Understand how quantum computers can break the RSA cryptosystem.- Use quantum mechanics to obtain a monetary scheme.

Indicative reading list

[Reading lists can be found in Talis](#)

[Specific reading list for the module](#)

Subject specific skills

Designing and analysing quantum algorithms.

Transferable skills

Study

Study time

Type	Required
Lectures	30 sessions of 1 hour (20%)
Seminars	10 sessions of 1 hour (7%)
Private study	110 hours (73%)
Total	150 hours

Private study description

Revising linear algebra, the postulates of quantum mechanics, the principles of superposition, measurement, and entanglement. Analysing the algorithm discussed in class, including: Deutsch's algorithm, the Deutsch-Josza algorithm, the Bernstein-Vazirani algorithm, Grover's algorithm, Simon's algorithm, and Shor's algorithm.

Costs

No further costs have been identified for this module.

Assessment

You do not need to pass all assessment components to pass the module.

Students can register for this module without taking any assessment.

Assessment group D3

	Weighting	Study time	Eligible for self-certification
Problem Set 1	10%		Yes (extension)
Problem Set 1. This assessment is eligible for self-certification (extension).			
Problem Set 2	10%		Yes (extension)
Problem Set 2. This assessment is eligible for self-certification (extension).			
Problem Set 3	10%		Yes (extension)
Problem Set 3. This assessment is eligible for self-certification (extension).			

	Weighting	Study time	Eligible for self-certification
Centrally-timetabled examination (On-campus) CS939 examination	70%		No

- Answerbook Pink (12 page)

Assessment group R3

	Weighting	Study time	Eligible for self-certification
In-person Examination - Resit CS939 MSc resit examination	100%		No

- Answerbook Gold (24 page)

Feedback on assessment

Comments on assignments alongside a mark will be provided, solutions will be discussed in the seminars.

[Past exam papers for CS939](#)

Availability

Courses

This module is Optional for:

- Year 1 of TCSA-G5PD Postgraduate Taught Computer Science
- Year 1 of TMAA-G1PF Postgraduate Taught Mathematics of Systems