CS419-15 Quantum Computing

24/25

Department
Computer Science
Level
Undergraduate Level 4
Module leader
Sergii Strelchuk
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 -V-azirani 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 implications of quantum computing on cryptography and security:- Understand the foundations of post-quantum cryptography.- Hack the RSA cryptosystem via a quantum computer.- Use quantum mechanics to obtain a monetary scheme.
- Understand the quantum computing paradigm:- Have an overview of a range of project management techniques- Understand how failure to correctly manage a project can lead to failure.- Understand how project management techniques provide quantifiable metrics for project progress
- 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, andcomposite systems.- Restate the postulates in terms of density matrices.
- Understand the principles of quantum information andquantum communication:- Understand quantum teleportation and its limits.- Describe the framework of quantum error-correcting codes.- Discuss Everett's many worlds interpretation.
- Analyse fundamental quantum algorithms:- Shor's algorithm.- Grover's search.- The Berstein-Vazirani algorithm.- Simon's problem.- The Deutsch-Jozsa paradigm.

Indicative reading list

Please see Talis Aspire link for most up to date list.

View reading list on Talis Aspire

Subject specific skills

Designing and analysing quantum algorithms.

Transferable skills

Understanding quantum mechanics and the power of quantum computing.

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 Berstein-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 D6

	Weighting	Study time
Problem Set 1	10%	
Problem Set. This assessment is eligible for self-certification (extension).		
Problem Set 2	10%	
Problem Set 2. This assessment is eligible for self-certification (extension).		
Problem Set 3	10%	
Problem Set 3. This assessment is eligible for self-certification (extension).		
In-person Examination	70%	
CS419 examination		

	Weighting	Study time

- Answerbook Pink (12 page)

Assessment group R2

	Weighting	Study time
In-person Examination - Resit	100%	
CS419 MEng resit examination		

- 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 CS419

Availability

Pre-requisites

Student must have studied the material in:
CS130 + CS131: Mathematics for Computer Scientists 1 + 2, or

CS136 + CS137 Discrete Mathematics and its Applications 1 + 2, or

MA106 Linear Algebra + ST111 Probability A

Courses

Course availability information is based on the current academic year, so it may change.
This module is Optional for:

- Year 5 of UCSA-G504 MEng Computer Science (with intercalated year)
- UCSA-G503 Undergraduate Computer Science MEng
  - Year 4 of G503 Computer Science MEng
  - Year 4 of G503 Computer Science MEng

This module is Option list A for:

- Year 4 of UCSA-G4G3 Undergraduate Discrete Mathematics

- Year 5 of UCSA-G4G4 Undergraduate Discrete Mathematics (with Intercalated Year)

This module is Option list B for:

- Year 4 of UCSA-G408 Undergraduate Computer Systems Engineering
- Year 5 of UCSA-G409 Undergraduate Computer Systems Engineering (with Intercalated Year)