

QUANTUM INFORMATION & COMPUTATION

Lecture notes¹

Nilanjana Datta, DAMTP Cambridge
n.datta@cam.ac.uk

CONTENTS

1. **Introduction: why *quantum* computation and information?**
2. **Principles of quantum mechanics and the Dirac bra-ket notation**
 - (a) Quantum states and operations
 - (b) Quantum measurements
3. **Quantum states as information carriers**
 - (a) The no-cloning theorem
 - (b) Distinguishing non-orthogonal states
 - (c) The no-signalling principle
 - (d) Superdense coding
4. **Quantum gates and Quantum teleportation**
5. **Quantum cryptography – BB84 quantum key distribution**
6. **Basics of classical computation and complexity**
 - (a) Query complexity and promise problems
7. **Circuit model of quantum computation**
8. **The Deutsch-Jozsa algorithm**

Simon's algorithm
9. **Quantum Fourier transform and periodicities**
 - (a) QFT mod N
 - (b) Periodicity determination
 - (c) Efficient implementation of QFT
10. **Quantum algorithms for search problems**
 - (a) The class NP and search problems

¹Based on the lecture notes of Richard Jozsa (DAMTP, Cambridge) from Lent 2018-2019.

(b) Grover's quantum searching algorithm

11. Shor's quantum factoring algorithm

(a) Factoring as a periodicity problem

(b) Computing the period r of $f(k) = a^k \bmod N$

(c) Getting r from a good c value

(d) Assessing the complexity of Shor's algorithm

Some useful references:

M. Nielsen and I. Chuang "Quantum computation and information". CUP.

M. M. Wilde "From Classical to Quantum Shannon Theory", CUP.

B. Schumacher and M. Westmoreland, "Quantum processes, systems and information". CUP 2010.

S. Lepp and W. Wootters, "Protecting information: from classical error correction to quantum cryptography". Academic press 2006.

John Preskill's notes for Caltech course on quantum computation.

Available at <http://www.theory.caltech.edu/people/preskill/ph229/notes/book.ps>