Part IIC **Lent term 2019-2020**

QUANTUM INFORMATION & COMPUTATION

Lecture notes[1]

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

CONTENTS

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

   (b) Grovers 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. Leopp 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