

Advanced Quantum Information Theory

Toby Cubitt*

Lent term, 2015

*tsc25@cam.ac.uk

Contents

0	Notation and Terminology	7
0.1	Miscellaneous	7
0.2	Hilbert spaces	7
0.3	Computer science	7
0.4	Operators	8
0.5	Hamiltonians	8
1	Complexity Theory	9
1.1	Computational Problems	9
1.2	Computation	11
1.2.1	Classical computation	12
1.2.2	Quantum computation	13
1.3	Complexity Classes	14
1.3.1	Classical complexity classes	14
1.3.2	Quantum complexity classes	16
1.4	Reduction	18
1.5	Complexity Zoo	19

Theorems and Definitions

Problem 1	Factoring	9
Problem 2	Travelling salesman	10
Problem 3	SAT	10
Problem 4	Factoring (decision variant)	10
Definition 5	Decision problem	10
Definition 6	Promise problem	11
Thesis 1	Church-Turing Thesis	12
Definition 7	Logic gate	12
Definition 8	Classical circuit	12
Definition 9	Quantum gate	13
Definition 10	Quantum circuit	14
Definition 11	Polynomial-time (P)	14
Thesis 2	Strong Church-Turing Thesis	15
Definition 12	Non-deterministic polynomial-time (NP)	15
Definition 13	Bounded-error quantum polynomial-time (BQP)	16
Definition 14	Quantum Merlin-Arthur (QMA)	17
Definition 15	Polynomial-time many-one reduction	18
Definition 16	Polynomial-time equivalence	18
Definition 17	NP-hard	18
Definition 18	NP-complete	18
Definition 19	QMA-hard	19
Definition 20	QMA-complete	19

Chapter 0

Notation and Terminology

0.1 Miscellaneous

s.t.	“such that”
w.l.o.g.	“without loss of generality”

0.2 Hilbert spaces

\bar{x}	complex conjugate of x
\mathbb{C}^2	2-dimensional Hilbert space (“qubit”)
\mathbb{C}^d	d -dimensional Hilbert space (“qudit”)
$\mathcal{H}^{\otimes n}$	$\bigotimes_1^n \mathcal{H} = \underbrace{\mathcal{H} \otimes \mathcal{H} \otimes \dots \otimes \mathcal{H}}_{n \text{ copies}}$ (e.g. n qubits: $(\mathbb{C}^2)^{\otimes n}$)
$\text{span}\{ \psi_i\rangle\}$	linear subspace spanned by $ \psi_1\rangle, \psi_2\rangle, \dots$

0.3 Computer science

$f(n) = O(g(n))$	$\exists c > 0, N > 0$ s.t. $\forall n > N : f(n) < c g(n) $
$f(n) = \Omega(g(n))$	$\exists c > 0, N > 0$ s.t. $\forall n > N : f(n) > c g(n) $
$\{0, 1\}^n$	set of all strings of 0’s and 1’s of length n
$\{0, 1\}^*$	set of all strings of 0’s and 1’s of arbitrary finite length

0.4 Operators

$\mathcal{B}(\mathcal{H})$	bounded operators on Hilbert space \mathcal{H} (recall: X bounded $\Leftrightarrow \forall \psi\rangle : \ X \psi\rangle\ < \infty$)
$\mathbb{1}$	identity operator
$\Pi^{(0)}$	projector $\Pi^{(0)} = 0\rangle\langle 0 $
$\Pi^{(1)}$	projector $\Pi^{(1)} = 1\rangle\langle 1 $
$\ker X$	kernel $\ker X := \text{span}\{ \psi\rangle : X \psi\rangle = 0\}$
$\text{supp } X$	support* $\text{supp } X := (X\rangle)^\perp$
X^\dagger	Hermitian conjugate (or adjoint)
$H^\dagger = H$	Hermitian (or self-adjoint) operator
$H > 0$	positive operator (implies Hermitian): $H > 0 \Leftrightarrow \forall \psi\rangle : \langle \psi H \psi\rangle > 0$
$H \geq 0$	positive-semidefinite (or non-negative) operator: replace “ $>$ ” by “ \geq ” in definition of positive operator
$A \geq B$	$A - B \geq 0$ (A, B Hermitian operators)
$A \geq c$	$A - c\mathbb{1} \geq 0$ (A Hermitian operator, $c \in \mathbb{R}$)

0.5 Hamiltonians

*Warning: quantum information terminology! Sometimes called “co-image” elsewhere.