

Contents

1	Introduction	3
2	Preliminary Notions	9
2.1	Complexity theoretic notions	9
2.2	Quantum states, channels, and measurements	11
2.3	Quantum circuits	21
3	Non-Interactive Quantum Proofs	27
3.1	Definitions of quantum verification procedures and QMA .	28
3.2	Error reduction	37
3.3	Complete promise problems	47
3.4	Variations on QMA	53
3.5	Chapter notes	65
4	Single-Prover Quantum Interactive Proofs	69
4.1	Definitions of quantum interactive proof systems	70
4.2	Perfect completeness and parallelization	78
4.3	SDPs for interactive games and parallel repetition	89
4.4	$\text{QIP} = \text{PSPACE}$	97
4.5	Chapter notes	110
5	Quantum Zero-Knowledge	113

5.1	Definitions of zero-knowledge	116
5.2	Quantum rewinding	125
5.3	Quantum statistical zero knowledge	133
5.4	Chapter notes	141
6	Multi-Prover Quantum Interactive Proofs	143
6.1	Definitions of multi-prover interactive proof systems	145
6.2	The importance of entanglement	151
6.3	Using entanglement in multi-prover games	165
6.4	Containment of NEXP in QMIP*	177
6.5	Further topics	194
6.6	Chapter notes	200
	Acknowledgements	205
	References	207