

Índice

Agradecimientos	I
1. El sorprendente mundo cuántico.	1
1.1. Axiomática.	1
1.2. La paradoja EPR en Teoría de la Información.	1
2. Computación Cuántica: Una introducción.	1
2.1. Bits cuánticos	1
2.2. Cambio de base.	1
2.3. Operadores.	1
2.4. Puertas y circuitos cuánticos.	1
2.5. Computación probabilista vs computación cuántica.	2
2.6. Principio de no clonación	2
3. Factorización prima.	2
3.1. Transformada de Fourier cuántica en \mathbb{Z}_m	2
3.2. Algoritmo de Shor	3
3.2.1. Búsqueda del orden.	3
3.2.2. Relacionando factorización con búsqueda del orden.	5
3.2.3. Aproximación racional de números reales.	6
3.3. ¿El fin de RSA?	6
4. Complejidad clásica.	6
4.1. Las clases de la computación probabilista	8
4.2. La clase PSPACE	9
4.3. Oráculos	9
4.4. La jerarquía polinómica.	9
4.5. La clase AC de complejidad circuital.	10
4.6. La clase AM	10
5. Complejidad cuántica.	10
5.1. Máquinas de Turing cuánticas.	10
5.2. La clase BQP	10
5.3. Relación entre NP y BQP	11
5.4. Relación entre PSPACE y BQP	12
5.5. Separación de BQP y PH mediante oráculos.	12
5.6. BQP en Hipercomputación Relativista	17
Referencias	17
Índice alfabético	20
Índice de figuras	21
Apéndices	22
Apéndice A. Notación	22
A.1. Notación asintótica	22
Apéndice B. Álgebra Tensorial	22
Apéndice C. Elementos de Probabilidad	22

Apéndice D. Teoría de Grupos y Anillos	25
Apéndice E. Resultados auxiliares	25
E.1. Demostración de los lemas de la sección 5.5	26
Apéndice F. Implementación del algoritmo de Shor	26