Quantum Computing & Cryptography

Revision notes

Steve Vickers

Past papers

2010 Quantum computing & cryptography
2009 Introduction to quantum and molecular computation

Summary of module

<table>
<thead>
<tr>
<th>Week</th>
<th>Topic</th>
<th>Chapters in Mermin</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Vectors, matrices for qubits</td>
<td>1.1 - 1.4</td>
</tr>
<tr>
<td>2</td>
<td>General vectors</td>
<td>{1.5 - 1.12}</td>
</tr>
<tr>
<td>3</td>
<td>Qubits &amp; their states</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Cryptographic protocols</td>
<td>6.1 - 6.3</td>
</tr>
<tr>
<td>5</td>
<td>Cryptographic issues</td>
<td>[Nielsen/chuang 12.6]</td>
</tr>
<tr>
<td>6</td>
<td>More applications of entanglement</td>
<td>6.4 - 6.5</td>
</tr>
<tr>
<td>7</td>
<td>Quantum algorithms - introduction</td>
<td>2.1 - 2.5</td>
</tr>
<tr>
<td>8</td>
<td>Special gates for quantum algorithms</td>
<td>2.6, 4</td>
</tr>
<tr>
<td>9</td>
<td>Quantum Fourier Transform, period finding</td>
<td>3.4 - 3.9</td>
</tr>
<tr>
<td>10</td>
<td>Breaking RSA</td>
<td>3.1 - 3.10</td>
</tr>
<tr>
<td>11</td>
<td>Quantum error correction</td>
<td>5</td>
</tr>
</tbody>
</table>

Practical focus

- Module most about protocols and algorithms
- What are they trying to achieve?
- How do you run them?
- How do they compare with classical computing?
- How do they work? < circuit diagrams, vector manipulation, some statistics
**Vectors, matrices for Qubits**

- World's worst notation for numbers
- Operations as matrices
  - **Reversible**
  - **permuation**
  - NOT ($\bar{x}$), CNOT, SWAP
  - Skill: write operation in matrix form

**Orbits & their states**

- state = ray of vector
- Bloch sphere for states of 1 qubit
- Entanglement
- Born rule - for measurements
- Important skill: calculate resulting state after a partial measurement

**General vectors**

- Complex numbers
- Basis & ket, (\(|\psi\rangle\& column vectors)
- Tensor products, \(\langle\psi|\phi\rangle\)
- Inner product, \(\langle\psi|\phi\rangle\)
- Applications, e.g., \(\langle n|A|y\rangle\) for matrix entries
- Operators & \(X, Y, Z, H, T\)
- Equations, e.g., \(X^2 = -Z\)
- Skills: normalize vector, use notation with confidence

**Cryptographic protocols**

Current technology: polarized photons

General issues

- What are Alice & Bob trying to achieve?
- What do they actually do? **specification**
  **algorithm**
Cryptography protocols

Quantum 1-time pad (BB 84)

- What are Alice & Bob trying to achieve?
- What do they actually do? (specification)
- Algorithm
- Key distribution
- Quantum & classical messages exchanged

- What effect does Eve have?
- How do Alice & Bob detect Eve?
- Statistical
- Advantage of using quantum?

Cryptography issues

- Quantum "no passive eavesdropping"
- Information reconciliation
- Privacy amplification
- Other attacks

More applications of entanglement

Quantum dense coding

Teleportation

- How does Alice use entanglement to cheat?
- Need to understand vector calculations for entangled states.

Vector, matrix, for Chib
- Unitary vectors
- Bell & other states
- Cryptographic protocols
- Cryptography issues
- Physical applications of entanglement
- Quantum algorithms - introduction
- Special applications of quantum algorithms
- Quantum Fourier transform, phase finding
- Breaking, RSA
- Quantum error correction

Note: No-Cloning Theorem

Similar story, different ending

- What are Alice & Bob trying to achieve?
- What do they actually do? (specification)
- Algorithm
- Bit commitment
- Quantum & classical messages exchanged

- How does Alice use entanglement to cheat?
- Need to understand vector calculations for entangled states.
Quantum algorithms

- Toy problems
  - Deutsch's problem
  - Bernstein-Vazirani
  - Simon

- diagrams easier than algebra

- be sure to understand algorithm & how you execute it

Special gates

Building the gates is quite intricate - I don't expect you to remember all the details

- Grover
  - Geometric using $V$ and $W$

- Toffoli gates - can be built from 2-qubit gates

Breaking RSA

QFT - building gate

- Period finding
  - How to execute algorithm?
  - Continued fractions

RSA - background

- How to execute RSA
- How to use period finding

Quantum error correction

Basic principles rather than details