II Quantum Information & Computing

Ishan Nath, Lent 2024

Based on Lectures by Prof. Nilanjana Datta

March 11, 2024

Contents

1 Preliminaries 2
1.1 Dirac Notation . . . 2
1.2 Tensor Products of Operators . . . 2
1.3 Projective (von Neumann) Measurements . . . 3
1.4 Extended Born Rule . . . 5
1.5 Fixed Choice of Basis . . . 6
1.6 States as Information . . . 7
1.7 Distinguishing Non-Orthogonal States . . . 10
1.8 Basic Unitary Operators . . . 12

2 Entanglement 14
2.1 Applications of Entanglement . . . 14

3 Quantum Cryptography 17
3.1 Quantum Key Decryption . . . 18

4 Classical Computation and Computational Complexity 21
4.1 Query Complexity and Promise Problems . . . 22
4.2 Circuit Quantum Computation . . . 23
4.3 Deutsch-Jozsa Algorithm . . . 25
4.4 Simon's Algorithm . . . 27

5 Quantum Fourier Transform 29
5.1 Periodicity Determination . . . 29
5.2 Implementation . . . 31

6 Search Problems 33
6.1 Unstructured Search . . . 33

Index 36

1 Preliminaries

1.1 Dirac Notation

Let $\mathcal{H}$ be a finite-dimensional Hilbert space. We denote by $|\psi\rangle$ an element of $\mathcal{H}$, and $\langle\psi|$ is the corresponding element of $\mathcal{H}^*$.

The inner product of $|\psi\rangle, |\phi\rangle \in \mathcal{H}$ is

$$\langle\psi|\phi\rangle \in \mathbb{C}.$$

For the case $\mathcal{H} = \mathbb{C}^2$, we let $|0\rangle, |1\rangle$ be an orthonormal basis.

The outer product $|\psi\rangle\langle\phi|$ is an element of $\mathcal{H}^*$.

If $\mathcal{H} = \mathbb{C}^n$ with orthonormal basis $\{|i\rangle\}$, then $\langle i|j\rangle = \delta_{ij}$ and

$$\sum_i |i\rangle\langle i| = \mathrm{id}\,.$$

If $\mathcal{H}$ is a space with basis $\{|e_i\rangle\}$ for $i = 1, \dots, n$ and $\mathcal{K}$ is a space with basis $\{|f_j\rangle\}$ for $j = 1, \dots, m$, then $\mathcal{H} \otimes \mathcal{K}$ is a Hilbert space with basis $|e_i\rangle|f_j\rangle$.

A vector $|\psi\rangle$ is said to be a product vector if $|\psi\rangle = |u\rangle \otimes |v\rangle$. Otherwise, it is an entangled vector.

We focus on tensor products of $\mathcal{H} = \mathbb{C}^2$ with itself. Then $\mathcal{H}^{\otimes k}$ has basis

$$\{|i_1\rangle \otimes \cdots \otimes |i_n\rangle\} = \{|i_1 \dots i_n\rangle\}.$$

So the basis vectors are labelled by bit strings of length k.

Note that we have the following simple fact:

$$\langle v|w\rangle = \mathrm{Tr}\,|w\rangle\langle v|\,.$$

This can be seen by writing $|v\rangle, |w\rangle$ on orthonormal basis $\{|e_i\rangle\}$. Hence we see that

$$\langle\psi|P|\psi\rangle = \mathrm{Tr}\,P\,|\psi\rangle\langle\psi|\,.$$

1.2 Tensor Products of Operators

Let $\mathcal{H} = \mathbb{C}^n$ and $K = \mathbb{C}^n$. If $A \in M_n(\mathbb{C})$ and $B \in M_n(\mathbb{C})$, then $A \otimes B$ acts on $\mathcal{H} \times \mathcal{K}$, hence is an element of $M_{mn}(\mathbb{C})$.

We can check the following:

- $A \otimes I \neq I \otimes A$.
- $A \otimes B = (A \otimes I)(I \otimes B)$.
- Moreover, if we define

  $$|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle),$$

  then

  $$(A \otimes I)\,|\phi^+\rangle = (I \otimes A^T)\,|\phi^+\rangle\,.$$

The third postulate of quantum mechanics is that time evolution of a closed quantum system is determined by a unitary and deterministic

$$|\psi(t_2)\rangle = U(t_1, t_2)\,|\psi(t_1)\rangle\,.$$

The fourth postulate says that measurement is determined by a Hermitian operator. This means that measurement is not probabilistic, and the state of the system is disturbed.

1.3 Projective (von Neumann) Measurements

Take $\mathcal{H} = \mathbb{C}^n$ and orthonormal basis $\mathcal{B} = \{|e_i\rangle\}$. Suppose that the initial state is $|\psi\rangle = \sum a_i\,|e_i\rangle$. Then the measurement in the basis $\mathcal{B}$ has outcomes $j \in \{1, 2, \dots, n\}$, with

$$\Pr(j) = |a_j|^2 = \langle\psi|P_j|\psi\rangle\,.$$

Here, if the post measurement state is $|e_j\rangle$, then this corresponds to the projection operator $P_j = |e_j\rangle\langle e_j|$. Then

$$|\psi_{\text{after}}\rangle = \frac{P_j\,|\psi\rangle}{\sqrt{\Pr(j)}} = e^{i\omega}\,|e_j\rangle\,.$$

These projection measurements are complete: note $\sum P_j = I$, and $P_j P_k = \delta_{jk} P_j$.

We can also have incomplete projective measurements. If

$$\mathcal{H} = \bigoplus_{i=1}^{d} \mathcal{E}_i,$$

with $\dim \mathcal{E}_i = d_i$ and $\sum d_i = n$, let $\mathcal{E}_j$ have onb $\{|e_k^{(j)}\rangle\}$. Then the projection operator onto $\mathcal{E}_j$ is

$$\Pi_j = \sum_{k=1}^{d_j} |e_k^{(j)}\rangle\,\langle e_k^{(j)}|\,.$$

This is the measurement relative to the orthogonal decomposition. The outcomes will be the labels of the subspaces, $j \in \{1, 2, \dots, d\}$. Then

$$\Pr(j) = \langle \psi | \Pi_j | \psi \rangle ,$$

and if the outcome is j, then

$$|\psi_{\text{after}}\rangle = \frac{\Pi_j |\psi\rangle}{\sqrt{\Pr(j)}}.$$

We can refine an incomplete measurement to a complete measurement. Take the same setup as before, then construct an orthonormal basis of $\mathcal{H}$ which is consistent with $\mathcal{E}_i$.

Example 1.1. (Parity Measurement)

Take $b_1 b_2 \in \{0,1\}^2$. Then $b_1 + b_2$ is the parity of $b_1 b_2$.

Take $\mathcal{H} = (\mathbb{C}^2)^{\otimes 2}$, with onb $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$. We can decompose

$$\mathcal{H} = \mathcal{E}_0 \oplus \mathcal{E}_1,$$

where

$$\mathcal{E}_1 = \operatorname{span}\{|00\rangle, |11\rangle\}, \qquad \mathcal{E}_1 = \operatorname{span} |01\rangle, |10\rangle\}.$$

The outcome is $j \in \{0, 1\}$. If we define

$$\Pi_0 = |00\rangle \langle 00| + |11\rangle \langle 11| , \qquad \Pi_1 = |01\rangle \langle 01| + |10\rangle \langle 10| ,$$

then

$$\Pr(j) = \langle \psi | \Pi_j | \psi \rangle .$$

We can extend to a complete measurement. Let

$$P_{ij} = |ij\rangle \langle ij| ,$$

for $i, j \in \{0, 1\}$. Then once again

$$\Pr(ij) = \langle \psi | \Pi_{ij} | \psi \rangle .$$

In quantum mechanics, we have a quantum observable A, a Hermitian operator. Then the outcome is an eigenvalue of A, say $\{a_k\}$. Let Π_k be the projection onto the eigenspace $\mathcal{E}_k$ of a_k. Then

$$\mathcal{E}_k = \operatorname{span}\{|\phi_i^{(k)}\rangle, i = 1, \dots, d_k\}.$$

Here d_k is the degeneracy. The spectral projection of A is

$$A = \sum_{k=1}^{r} a_k \Pi_k.$$

Let's look at taking a refinement of an incomplete measurement. Take $\mathcal{E}_i$ orthonormal spaces, and $\{|e_k^{(i)}\rangle\}$ an onb for $\mathcal{E}_i$. Then the complete measurement is

$$P_k^{(i)} = |e_k^{(i)}\rangle \langle e_k^{(i)}| \,.$$

The outcomes are (i, k), with

$$\Pr(i, k) = \langle \psi | P_k^{(i)} | \psi \rangle \,.$$

For the incomplete measurement,

$$\Pr(i) = \sum_{k=1}^{d_i} \Pr(i, k).$$

1.4 Extended Born Rule

Consider measuring part of a composite system. Say S_1 has $\mathcal{H} \cong \mathbb{C}^m$, and S_2 has $\mathcal{K} \cong \mathbb{C}^n$. Then if we want to measure S_1 only, let $\{|e_i\rangle\}$ be an onb of $\mathcal{H}$. Then,

$$\mathcal{H} = \bigoplus_{i=1}^{m} \mathcal{E}_i,$$

with

$$\mathcal{E}_i = \operatorname{span}\{|e_i\rangle \otimes |\phi\rangle \quad \forall\, |\phi\rangle \in \mathcal{K}\}.$$

If $\{|f_j\rangle\}$ is an onb of $\mathcal{K}$, then $\mathcal{H} \otimes \mathcal{K}$ has onb $\{|e_i\rangle\, |f_j\rangle\}$. Suppose we have initial state

$$|\psi\rangle = \sum_{i,j} a_{ij}\, |e_i\rangle\, |f_j\rangle \,.$$

Then the outcomes of this measurement is $k \in \{1, 2, \ldots, m\}$, with projection operator $\Pi_k = P_k \otimes I$. Then

$$\Pr(k) = \langle \psi | P_k \otimes I | \psi \rangle \,.$$

Note we can easily find that

$$\Pr(k) = \sum_j |a_{kj}|^2.$$

If the outcome is k, then the wavefunction collapses as

$$|\psi\rangle \mapsto |\psi_{\text{after}}\rangle = \frac{(P_k \otimes I)\, |\psi\rangle}{\sqrt{\Pr(k)}}.$$

1.5 Fixed Choice of Basis

Take $\mathcal{H} \cong \mathbb{C}^n$, $\mathcal{B} = \{|e_i\rangle\}$, and $\mathcal{B}' = \{|e_i'\rangle\}$. Then the complete projective measurement relative to $\mathcal{B}'$ can be obtained by taking a measurement relative to $\mathcal{B}$: it is the action of some unitary operator.

Hence there exists a unitary operator U such that

$$|e_j'\rangle = U\,|e_j\rangle\,.$$

Suppose that

$$|\psi\rangle = \sum a_j\,|e_j'\rangle\,.$$

How can we get the probability of outcomes and $|\psi_{\text{after}}\rangle$ for a measurement in $\mathcal{B}'$ by doing a measurement in $\mathcal{B}$?

First, we act on $|\psi\rangle$ by $U^\dagger$. Then we can do a measurement in $\mathcal{B} = \{|\psi_j\rangle\}$. The outcomes will be $j \in \{1, 2, \ldots, m\}$, with $\Pr(j) = |a_j|^2$, and $|\psi_{\text{after}}\rangle = |e_j\rangle$. Finally, we can act on $|\phi_{\text{after}}\rangle$ by U, to get

$$|\phi_{\text{after}}'\rangle = U\,|e_j\rangle = |e_j'\rangle\,.$$

Example 1.2.

Take $\mathcal{H} = (\mathbb{C}^2)^{\otimes n}$. Then we can look at measuring the first k qubits.

For $n = 3$, $k = 1$, we have a complete projective measurement relative to $\mathcal{B}$ on the first qubit. This has outcomes 0 and 1. If we have

$$|\psi\rangle\,\frac{i}{2}\,|000\rangle + \frac{1}{2}\,|001\rangle - \frac{1}{2}\,|101\rangle + \frac{3}{10}\,|110\rangle - \frac{2i}{5}\,|111\rangle\,,$$

then we have

$$\Pr(1) = \langle\psi|P_1 \otimes I|\psi\rangle = \frac{1}{2}.$$

Then we have

$$|\psi_{\text{after}}\rangle = (P_1 \otimes I)\,|\psi\rangle\,/\sqrt{\Pr(1)} = |1\rangle\,|\alpha\rangle\,.$$

Note that two states $|\psi\rangle\,, |\phi\rangle$ are distinguishable if there exists a measurement which gives two distinct outcomes when done on $|\psi\rangle$ and $|\phi\rangle$. Then only perpendicular states are reliably distinguishable, where reliably meanly with probability 1.

Now suppose $|\psi\rangle \in \mathcal{H}$, and $|\phi\rangle = e^{i\theta}\,|\psi\rangle$. Then these correspond to the same physical states, as there is no measurement that can distinguish between them.

Indeed, if

$$|\psi\rangle = \sum a_j |e_j\rangle ,$$

then

$$|\phi\rangle = \sum e^{i\theta} a_j |e_j\rangle ,$$

with $|e^{i\theta}a_j| = |a_j|$. Moreover, if $|\psi'\rangle = U|\psi\rangle$, then

$$|\phi'\rangle = U|\phi\rangle = e^{i\theta}U|\psi\rangle = e^{-\theta}|\psi'\rangle .$$

1.6 States as Information

Information is encoded in the states of a quantum system, e.g. $|\psi\rangle \in \mathcal{H}$. In classical information, this is a special case where information is encoded in an orthonormal state.

We have a list of general operations allowed on a quantum system A with Hilbert space $\mathcal{H}_A$.

- Add an *ancilla*, which is an auxiliary system B with space $\mathcal{H}_B$, in a fixed state $|\phi_0\rangle_B$. Then we now have system AB in state $|\psi\rangle_A \otimes |\phi_0\rangle_B$.
- We can let a unitary operator U act on AB, or A.
- We can take measurements on AB, or A.

Now we have the important no-cloning theorem. This says that quantum states cannot be copied and cloned. In the classical scenario, this is easily possible. However, let us consider the quantum scenario, with system A, B, M and Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_M$.

Suppose we have some information to be copied, which is $|\psi\rangle = |\psi\rangle_A$. Then B and M are in fixed states $|\phi_0\rangle_B$ and $|M_0\rangle_M$. Initially, our state is

$$|\psi\rangle_A \otimes |\phi_0\rangle_B \otimes |M_0\rangle_M .$$

We will show that states cannot be copied via a unitary operation. Suppose there exists U such that

$$U|\psi\rangle_A |\phi_0\rangle_B |M_0\rangle_M = |\psi\rangle_A |\psi\rangle_B |M_\psi\rangle_M .$$

We might require that cloning works either for all $|\psi\rangle \in \mathcal{H}_A$, or for restricted subset of states in A.

Theorem 1.1. *Let $\mathcal{S}$ be any set of states of A that contains at least one pair of non-orthogonal states. Then there is no unitary cloning device that clones every state in $\mathcal{S}$.*

Proof: Assume cloning is possible for $|\xi\rangle, |\eta\rangle$ which are non-orthogonal distinct states. Then

$$\begin{aligned} U|\xi\rangle_A|\phi_0\rangle_B|M_0\rangle_M &= |\xi\rangle_A|\xi\rangle_B|M_\xi\rangle_M\,, \\ U|\eta\rangle_A|\phi_0\rangle_B|M_0\rangle_M &= |\eta\rangle_A|\eta\rangle_B|M_\eta\rangle_M\,. \end{aligned}$$

Taking the inner products, the left hand side becomes $\langle\xi|\eta\rangle$. But the right hand side is $\langle\xi|\eta\rangle\langle\xi|\eta\rangle\langle M_\xi|M_\eta\rangle$.

Therefore, we get that

$$1 = \langle\xi|\eta\rangle\langle M_\xi|M_\eta\rangle\,,$$

since $\langle\xi|\eta\rangle \neq 0$. Taking the modulus,

$$|\langle M_\xi|M_\eta\rangle| > 1,$$

but this is at most 1 by Cauchy-Schwarz.

So there is no unitary cloning device that can perfectly copy non-orthogonal states.

Assuming quantum cloning is possible, superluminal communication is possible. Indeed, suppose Alice and Bob share

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}[|00\rangle + |11\rangle],$$

where each has one qubit. Then Alice considers the two bases

$$\mathcal{B}_0 = \{|0\rangle, |1\rangle\}, \qquad \mathcal{B}_1 = \{|+\rangle, |-\rangle\},$$

where $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$. If Alice wants to send the message yes, she measures A in basis $\mathcal{B}_0$. This outputs 0 and 1 with probability 1/2 each, and the final state is either $|0\rangle_A|0\rangle_B$ or $|1\rangle_A|1\rangle_B$, respectively. We can check that

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}[|{+}{+}\rangle + |{-}{-}\rangle].$$

Hence, Alice gets + and − with probability 1/2, and the final state is either $|{+}{+}\rangle$ or $|{-}{-}\rangle$. Interestingly, $\mathcal{B}_0$ and $\mathcal{B}_1$ are mutually unbiased states, so measuring any state of $\mathcal{B}_1$ relative to $\mathcal{B}_1$, or vice versa, gives the same probability.

Hence if the message is yes, then Bob's qubit collapse to $|0\rangle$ or $|1\rangle$, otherwise it collapses to $|+\rangle$ or $|-\rangle$. We claim that these yes/no preparations of B cannot be detected b Bob by any local action on B.

Indeed, for any measurement that Bob does, corresponding to a projection Π_i, the outcomes i will be the same for the yes/no preparations, and also for the case in which no measurement was done by Alice.

Indeed, suppose Bob does a measurement with outcome i and projection operator Π_i. Then the probability Bob gets i given Alice sent yes is

$$\begin{aligned}\mathrm{Prob}(i|\mathrm{yes}) &= \frac{1}{2}\langle 0|\Pi_i|0\rangle + \frac{1}{2}\langle 1|\Pi_i|1\rangle = \frac{1}{2}[\mathrm{Tr}\,\Pi_i(|0\rangle\langle 0| + |1\rangle\langle 1|)] \\ &= \frac{1}{2}\mathrm{Tr}(\Pi_i).\end{aligned}$$

Similarly, the probability given Alice sent no is also $\mathrm{Tr}\,\Pi_i/2$. And as well, if no measurement was done,

$$\mathrm{Prob}(i) = \langle \phi^+|I_A \otimes \Pi_i|\phi^+\rangle = \frac{1}{2}\mathrm{Tr}\,\Pi_i.$$

But if quantum cloning was possible, Bob could make $N \gg 1$ copies of B, at some time. If Alice sent yes, then Bob has N $|0\rangle$ or N $|1\rangle$, and if Alice sent no, then Bob has N $|+\rangle$ or N $|-\rangle$.

Now Bob does a measurement in $\mathcal{B}_0$ If Alice said yes, then he receives a string of N ones or N zeroes. Otherwise, she gets a uniform random bit string of length N. Then the probability of distinguishing the outcome is $2/2^N$.

This is a specific example of the *no-signalling principle*. We assume that we have a state $|\phi\rangle_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$, where Alice knows A and Bob knows B.

Then this principle says that no local action on A by Alice can change the outcome probability distribution of any measurement on B by Bob.

Proof: If Bob does a measurement in basis $\mathcal{B} = \{|b\rangle\}$ of $\mathcal{H}_B$, then Bob's outcomes are in $\{1, 2, \ldots, d_B\}$. Let $\{|a\rangle\}$ for $a \in \{1, \ldots, d_A\}$ be an onb of $\mathcal{H}_A$. Then suppose

$$|\phi\rangle = \sum_{ab} c_{ab}|a\rangle|b\rangle.$$

We then get that the probability of measuring b is

$$\mathrm{Prob}(b) = \langle \phi|I_A \otimes P_B|\phi\rangle = \sum_{a=1}^{d_A}|c_{ab}|^2.$$

After this, the outcome is

$$|\psi_{\mathrm{after}}\rangle = \frac{1}{\sqrt{\mathrm{Prob}(b)}}(I_A \otimes P_B)|\phi\rangle.$$

Now assume that Alice does a measurement on A in basis $\{|a\rangle\}$, then Bob does a measurement in $\{|b\rangle\}$. Then

$$\mathrm{Prob}(a) = \langle\phi|P_a \otimes I_B|\phi\rangle = \sum_{b=1}^{d_B} |c_{ab}|^2.$$

If the outcome is a, then

$$|\phi''\rangle = \frac{1}{\sqrt{\mathrm{Prob}(a)}}(P_a \otimes I)\,|\phi\rangle\,.$$

Now after Bob measures, we start with initial state $|\phi''\rangle_{AB}$, then

$$\begin{aligned}\mathrm{Prob}(b|a) = \langle\phi''|I_A \otimes P_B|\phi''\rangle &= \frac{1}{\mathrm{Prob}(a)}\,\langle\phi|(P_a \otimes I_B)(I_A \otimes P_b)(P_a \otimes I_B)|\phi\rangle \\ &= \frac{1}{\mathrm{Prob}(a)}\,\langle\phi|P_a \otimes P_b|\phi\rangle\,.\end{aligned}$$

Hence we see that

$$\mathrm{Prob}(a,b) = \mathrm{Prob}(b|a)\,\mathrm{Prob}(a) = \langle\phi|P_a \otimes P_b|\phi\rangle = |c_{ab}|^2.$$

Hence we see that

$$\mathrm{Prob}(b) = \sum_a p(a,b) = \sum_{a=1}^{d_A} |c_{ab}|^2.$$

1.7 Distinguishing Non-Orthogonal States

Suppose we are given $|\psi\rangle \in \mathcal{H}$. We are told that either $|\psi\rangle = |\alpha_0\rangle$ or $|\alpha_1\rangle$, with probability 1/2. We are told that $\langle\alpha_0|\alpha_1\rangle \neq 0$, so the states are not perpendicular. Say that $|\,\langle\alpha_0|\alpha_1\rangle\,| = \cos\theta$.

We are interested in trying to best identify the state of $|\psi\rangle$. One strategy is to just guess, with probability 1/2. But we can do better by doing measurements on $|\psi\rangle$. Suppose we have projection operators Π_0, Π_1, with $\Pi_0 + \Pi_1 = I$. Then the average success probability will be

$$p_{\text{success}} = \frac{1}{2}\,\mathrm{Prob}(\text{outcome is } 0|\,|\psi\rangle = |\alpha_0\rangle) + \frac{1}{2}\,\mathrm{Prob}(\text{outcome is } 1|\,|\psi\rangle = |\alpha_1\rangle).$$

Then the probabilities are, respectively,

$$\langle\alpha_0|\Pi_0|\alpha_0\rangle \qquad \text{and} \qquad \langle\alpha_1|\Pi_1|\alpha_1\rangle\,.$$

Hence we can calculate

$$p_{\text{success}} = \frac{1}{2}\operatorname{Tr}[\Pi_0(|\alpha_0\rangle\langle\alpha_0| - |\alpha_1\rangle\langle\alpha_1|)] + \frac{1}{2}.$$

The optimal choice of measurement maximizes p_{success}. Note that

$$p_{\text{success}}(\Pi_0) = \frac{1}{2} + \frac{1}{2}\operatorname{Tr}(\Pi_0\Delta),$$

where

$$\Delta = |\alpha_0\rangle\langle\alpha_0| - |\alpha_1\rangle\langle\alpha_1|\,.$$

Δ is a Hermitian operator, satisfying that for all $|\beta\rangle \in \mathcal{H}$ perpendicular to $|\alpha_0\rangle$ and $|\alpha_1\rangle$, that $\Delta|\beta\rangle = 0$. Hence

$$\ker\Delta \supseteq \operatorname{span}\{|\beta\rangle \in \mathcal{H} \mid \langle\alpha_i|\beta\rangle = 0, i = 0, 1\}.$$

Thus Δ acts non-trivially only on a two-dimensional subspace, $\mathcal{V} = \operatorname{span}\{|\alpha_0\rangle, |\alpha_1\rangle\}$. So Δ has at most two non-zero eigenvalues, and since $\operatorname{Tr}\Delta = 0$, we get it has two eigenvalues $\pm\delta$, with eigenvectors $|\pm p\rangle$.

Hence we know that

$$\Delta = \delta P_\delta - \delta P_{-\delta}.$$

Therefore, in the basis $\{|\pm p\rangle\}$, we have

$$\Delta = \begin{pmatrix} \delta & 0 \\ 0 & -\delta \end{pmatrix}.$$

Now we want to find the optimal success portfolio. We begin by finding δ in terms of $|\alpha_0\rangle$ and $|\alpha_1\rangle$. Let $|\alpha_0^\perp\rangle \in \mathcal{V}$ such that $|\alpha_0\rangle, |\alpha_0^\perp\rangle$ is an orthonormal basis of $\mathcal{V}$. Now say that

$$|\alpha_1\rangle = c_0|\alpha_0\rangle + c_1|\alpha_0^\perp\rangle\,.$$

As our state is normalised, $|c_0|^2 + |c_1|^2 = 1$. Then in this orthonormal basis,

$$\Delta = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} - \begin{pmatrix} |c_0|^2 & c_0c_1^* \\ c_0^*c_1 & |c_1|^2 \end{pmatrix} = \begin{pmatrix} |c_1|^2 & -c_0c_1^* \\ c_0^*c_1 & -|c_1|^2 \end{pmatrix}.$$

We can find the eigenvalues of this as $\pm\delta = \pm|c_1| = \pm\sin\theta$, the angle between the vectors. Then,

$$\begin{aligned} p_{\text{success}}(\Pi_0) &= \frac{1}{2} + \frac{1}{2}\operatorname{Tr}[\Pi_0(\delta|p\rangle\langle p| - \delta|-p\rangle\langle -p|)] \\ &= \frac{1}{2} + \frac{1}{2}\sin\theta[\langle p|\Pi_0|p\rangle - \langle -p|\Pi_0| - p\rangle]. \end{aligned}$$

We choose Π_0 such that it projects onto a subspace containing $|p\rangle$. Then we have

$$p^*_{\text{success}} = \frac{1}{2} + \frac{1}{2}\sin\theta.$$

This is the *Holevo-Holstrom theorem*: given any one of two equally likely states $|\alpha_0\rangle$ and $|\alpha_1\rangle$, with $|\langle\alpha_0|\alpha_1\rangle| = \cos\theta \neq 0$, then the probability of successfully identifying the state by any measurement satisfies

$$p^*_{\text{success}} \leq \frac{1}{2} + \frac{\sin\theta}{2},$$

and as we have shown, this bound is tight.

We can generalise this to unambiguous state discrimination, where we have three outcomes in our measurement: 1 if the state is $|\alpha_0\rangle$, 0 if the state is $|\alpha_1\rangle$, and a third fail state if the process has failed.

1.8 Basic Unitary Operators

Here we will look at some unitary operators, corresponding to quantum gates. First, we look at one-qubit gates.

The first is the *Hadamard gate*

$$H = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

This satisfies $H|0\rangle = |+\rangle$, $H|1\rangle = |-\rangle$, and it is indeed a unitary matrix. We can show that

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}[|00\rangle + |11\rangle] = \frac{1}{\sqrt{2}}[|{+}{+}\rangle + |{-}{-}\rangle],$$

by using the fact that

$$(A \otimes B) = (I \times B)(A \times I), \qquad (A \times I)|\phi^+\rangle = (I \times A^T)|\phi^+\rangle.$$

We also have a reflection matrix

$$H = \text{Ref}(\theta) = \begin{pmatrix} \cos 2\theta & \sin 2\theta \\ \sin 2\theta & -\cos 2\theta \end{pmatrix}.$$

This corresponds to reflection in the real Euclidean space.

Some other one-qubit gates are

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \sigma_x, \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \sigma_z, \qquad Y = ZX = -XZ = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Here X is the quantum not gate, so $X\left|k\right\rangle = \left|k \oplus 1\right\rangle$, and $Z\left|k\right\rangle = (-1)^k \left|k\right\rangle$.

We can generalise Z to a phase gate

$$P_\theta = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}.$$

Let's move on to two qubit gates. The first is a controlled-X gate, which is

$$CX = \begin{pmatrix} (I) & (0) \\ (0) & (X) \end{pmatrix}.$$

This gives $CX\left|i\right\rangle\left|j\right\rangle = \left|i\right\rangle\left|j \oplus i\right\rangle$. We can generalise to make different qubits the control and the target, e.g.

$$CX_{12}\left|0\right\rangle\left|1\right\rangle = \left|0\right\rangle\left|1\right\rangle, \qquad CX_{21}\left|0\right\rangle\left|1\right\rangle = \left|1\right\rangle\left|1\right\rangle.$$

Similarly, we have the controlled Z gate,

$$CZ = \begin{pmatrix} (I) & (0) \\ (0) & (Z) \end{pmatrix}.$$

We can check that CZ_{12} has the same action as CZ_{21}. More importantly, we can find that

$$CX_{21} = (H \otimes H)(CX_{12})(H \otimes H).$$

2 Entanglement

Suppose A and B have two qubits, so $\mathcal{H} = \mathbb{C}^2 \otimes \mathbb{C}^2$. We consider a basis for $\mathcal{H}$ as

$$\begin{aligned} |\phi^\pm\rangle &= \frac{1}{\sqrt{2}}[|00\rangle \pm |11\rangle], \\ |\psi^\pm\rangle &= \frac{1}{\sqrt{2}}[|01\rangle \pm |10\rangle]. \end{aligned}$$

Then $\{|\phi^+\rangle, |\phi^-\rangle, |\psi^+\rangle, |\psi^-\rangle\}$ is known as the *Bell basis*.

Bell states are maximally entangled states. We know the state of AB exactly, but we have no information about the states of A or B individually.

The bell states satisfy the following:

$$\begin{aligned} |\phi^+\rangle &= (I \otimes I)\,|\phi^+\rangle \\ |\phi^-\rangle &= (Z \otimes I)\,|\phi^+\rangle = (I \otimes Z)\,|\phi^+\rangle \\ |\psi^+\rangle &= (I \otimes X)\,|\phi^+\rangle \\ |\psi^-\rangle &= (Y \otimes Z)\,|\phi^+\rangle, \end{aligned}$$

where we recall that $Y = ZX$. We can also check that

$$|\phi^+\rangle = CX(H \otimes I)\,|00\rangle.$$

The Bell states can be characterized by two classical bits:

- The parity bit.
- The phase bit.

This information can be recovered by doing a measurement on the two qubits in the Bell basis $\mathcal{B}$. Such a measurement is called a *Bell measurement*.

Note that this measurement needs to be done on both qubits, i.e. they need to be in the same location.

The projection operators are P_{ij} with outcomes ij, where, for example

$$P_{00} = |\phi^+\rangle\langle\phi^+|.$$

2.1 Applications of Entanglement

First we look at superdense coding.

Suppose Alice wants to send a classical message to Bob, using a qubit channel. Alice has a message of bit size 2, and she wishes to send a single qubit to represent her message.

This is possible, provided Alice and Bob share a Bell state $|\phi^+\rangle_{AB}$. They use a protocol called superdense coding, which involves Alice interacting with her qubit, then sending her qubit to Bob, and Bob then has both qubits.

- If Alice wishes to send 00. Alice does nothing, so the interaction is $I \otimes I$, and Bob receives $|\phi^+\rangle$.
- If she wishes to send 01, Alice interacts with Z, and Bob receives $|\phi^-\rangle$.
- If she wishes to send 10, Alice interacts with X, and Bob receives $|\psi^+\rangle$.
- If she wishes to send 11, Alice interacts with Y, and Bob receives $|\psi^-\rangle$.

The Bob does a Bell measurement, and is able to decode Alice's message.

Now let's look at teleportation. Again Alice and Bob share a Bell state $|\phi^+\rangle_{AB}$. Alice has another qubit C in some state $|\psi\rangle$, and she want to send $|\psi\rangle$ to Bob.

However, she has no means to physically send C to Bob. There is no qubit channel, hence only classical communication is possible.

Amazingly, she can indeed send this information, through a protocol known as *quantum teleportation*. The state transfer is unaffected by any process in the intervening space. Note that the qubit C is not physically transferable.

The overview of the protocol is as follows. First Alice does a local operation on C, A. Then Alice communicates classically to Bob, after which Bob does a local operation on his qubit.

First, say that

$$|\psi\rangle_C = a\,|0\rangle + b\,|1\rangle\,,$$

with $|a|^2 + |b|^2 = 1$. Hence the initial state of the overall space is $|\psi\rangle_C \otimes |\phi^+\rangle_{AB}$, which we can see is

$$|\psi\rangle = \frac{1}{\sqrt{2}}[a\,|000\rangle + a\,|011\rangle + b\,|100\rangle + b\,|111\rangle].$$

Then she sends CA through a CX gate, with C the control and A the target. This sends $|\psi\rangle \to |\phi_1\rangle$, where

$$|\phi_1\rangle = \frac{1}{\sqrt{2}}[a\,|000\rangle + a\,|111\rangle + b\,|110\rangle + b\,|101\rangle].$$

Then she sends C through a Hadamard gate, to get

$$|\phi_2\rangle = \frac{1}{\sqrt{2}}[a\,|{+}00\rangle + a\,|{+}11\rangle + b\,|{-}10\rangle + b\,|{-}01\rangle].$$

We can check that this is equal to

$$\begin{aligned}|\phi_2\rangle &= \frac{1}{2}[|00\rangle_{CA}\,(a\,|0\rangle_B + b\,|1\rangle_B) + |01\rangle_{CA}\,(a\,|1\rangle_B + b\,|0\rangle_B) + \cdots]\\ &= \frac{1}{2}[|00\rangle_{CA}\,|\psi\rangle_B + |01\rangle_{CA}\,X\,|\psi\rangle_B + |10\rangle_{CA}\,Z\,|\psi\rangle_B + |11\rangle_{CA}\,(-Y\,|\psi\rangle_B)].\end{aligned}$$

Afterwards Alice does a measurement on the standard basis, on CA. By the extended born rule, depending on the outcome (each with probability 1/4), the post-measurement state of CAB is a product state. If Alice's outcome is ij, then the post-measurement state of B is $X^j Z^i\,|\psi\rangle$.

Then Alice classically communicates her measurement to Bob. In order for Bob to get the qubit $|\psi\rangle$, he transforms by $Z^i X^j$, so his state is

$$Z^i X^j (X^j Z^i)\,|\psi\rangle = |\psi\rangle_B\,.$$

We can draw a diagram of this. It looks cool I guess?

One takeaway of this is that $H \cdot CX$ corresponds to the rotation of Bell states to computational basis states.

3 Quantum Cryptography

How do we communicate securely? Many people have tried to develop schemes to communicate securely, e.g. Caesar ciphers, involving a permutation of the alphabet. Obviously this is not secure.

In fact, the only provably secure means of communication is via a one-time pad, which required a secret key.

In a public key cryptosystem, there are a paired public and private key. Say Alice and Bob want to communicate. Alice encrypts her message using a public key, and Bob receives and decodes the message using a private key.

The benefit of this system is that no shared private key is needed, however this is also not provably secure. Security relies on the assumptions of computational hardness, i.e. that there exists tasks that are computable in principle but not computable in practice, i.e. there are no polynomial time algorithms for the task.

One such example is prime factorisation. Suppose $p, q \in \mathbb{N}$ are of $n = 100$ binary digits. Then multiplying p and q is possible in $\mathcal{O}(n^2)$ times, however given $N \in \mathbb{N}$ we cannot find the factors of N in any polynomial time algorithm. The fastest algorithm known is of order $\mathcal{O}(2^{n^{1/2}})$.

The advantage of this is that no shared key is required. But it can be readily broken by a quantum computer, for example Shor's factoring algorithm.

The drawback of encoding information in a quantum state is:

- Received information cannot be reliable identified.
- Any attempt to read the message results in the information being destroyed.

This is advantageous for quantum cryptography.

Let's look at classical secure communication. Here Alice and Bob are communicating over a channel with an eavesdropper, Eve. Eve is able to intercept the message and read it, then send it to Bob.

The aim is for Alice to send Bob a secure message, such that Eve learns nothing, while Eve wants to learn as much as possible.

We assume that the classical channel is authenticated, and Eve cannot block or modify the message.

For a one time pad, Alice and Bob share a private key K, a binary string not known to Eve. K is shared before the message, and is also independent of the message M that Alice wants to send to Bob. We assume $|K| = |M|$, and so $K, M \in \{0, 1\}^m$.

The process is simple. First Alice computes $C = M \oplus K$, which she then sends to Bob. Bob is then able to compute $C \oplus K = M \oplus K \oplus K = M$.

Here Eve can only learn $|M|$, the length of the message. She cannot learn any more, as the distribution of any K will be $1/2^m$, given that K is chosen uniformly at random.

Hence the one time pad is secure, but of course it is only a one-time thing, as if Alice sends $C_1 = M_1 \oplus K$ and $C_2 = M_2 \oplus K$, then Eve can learn $C_1 \oplus C_2 = M_1 \oplus M_2$.

The drawback of a one-time pad is that it is very inefficient. Alice and Bob must generate K before every communication attempt, which may be impossible if they need to send signals very regularly.

3.1 Quantum Key Decryption

This is where we can use QIC, namely QKD. It allows Alice and Bob to generate a private key, then use this for secure communication via a one-time pad (note QKD does not encrypt the message, only provides the key).

We will look at the BB84 protocol for QKD. Here Alice and Bob communicate with both a classical channel and a qubit channel. Eve now has access to both channels.

We claim that Eve cannot gain any information about the key without being detected by Alice and Bob. Indeed, this is the measurement postulate. Eve's actions can be detected by discussion over the classical channel.

To communicate, first Alice generates two m-bit strings $\mathbf{x}$ and $\mathbf{y}$, uniformly at random, and prepares and m-qubit state $|\psi_{\mathbf{xy}}\rangle = |\psi_{x_1 y_1}\rangle \otimes \cdots \otimes |\psi_{x_m y_m}\rangle$, where

$$|\psi_{00}\rangle = |0\rangle\,, \quad |\psi_{10}\rangle = |1\rangle\,, \quad |\psi_{01}\rangle = |+\rangle\,, \quad |\psi_{11}\rangle = |-\rangle\,.$$

So Alice is using two bases, $\mathcal{B}_0 = \{|0\rangle\,, |1\rangle\}$ and $\mathcal{B}_1 = \{|+\rangle\,, |-\rangle\}$. If $y_i = 0$, then $|\psi_{x_i y_i}\rangle \in \mathcal{B}_0$, else it is in $\mathcal{B}_1$.

Now $\mathcal{B}_0$ and $\mathcal{B}_1$ are mutually unbiased bases, meaning measuring any state of one basis in the other gives equally likely outcomes.

Then Alice sends these m qubits to B, one-by-one, through the qubit channel, and Bob gets m qubits. These might not be in the state $|\psi_{\mathbf{xy}}\rangle$ due to tampering by Eve or noise in the qubit channel.

Suppose Bob did receive $|\psi_{\mathbf{xy}}\rangle$. Then Bob generates $\mathbf{y}' = y'_1 \dots y'_m \in \{0,1\}^m$ uniformly at random. If $y'_i = 0$, then he does a measurement on the i'th qubit in basis $\mathcal{B}_0$. Otherwise, he acts on $|\psi_{x_i y_i}\rangle$ by H, and then measures it in $\mathcal{B}_0$.

The outcomes of these measurements are $\mathbf{x}' = x'_1 \dots x'_m$. Now note that if $y'_i = y_i$, then $x'_i = x_i$ almost surely. This is because Alice and Bob encoded and decoded in the same basis.

After this, Alice and Bob publicly compare $\mathbf{y}$ and $\mathbf{y}'$, and discard all x_i's and x'_i's for which $y'_i \neq y_i$. These give shorter strings $\tilde{\mathbf{x}}$ and $\tilde{\mathbf{x}}'$, which give a shared private key. Note if $y'_i \neq y_i$, then x'_i and x_i are totally uncorrelated.

If we include the possibility of observation and noise, then we need two more steps. First, Alice and Bob perform information reconciliation (IR). They are given strings $\tilde{\mathbf{x}}$ and $\tilde{\mathbf{x}}'$, which may not be equal. Therefore they wish to find the bit error rate (proportion of non-equal bits). They do this by comparing a random sample of their bit values.

The remaining unrevealed bits form shorter strings $\bar{\mathbf{x}}$, $\bar{\mathbf{x}}'$. Then they want to correct these errors. This can be done with high probability via IR, at the cost of sacrificing some more bits. This gets strings x^* and $x^{*\prime}$.

Now we need a further step, in order to ensure Eve has no information about the two bit strings. This is privacy amplification (PA). From the estimated bit error rate, Alice and Bob can estimate the maximum amount of information that Eve can have about x^* and $x^{*\prime}$. Then we replace these two strings with shorter strings on which Eve has (essentially) no information.

The bit error rate is dependent on Eve's information. So Alice and Bob will assume that all error arose from Eve's actions.

Eve can intercept the message in two ways:

(i) Intercept and resend attack.

(ii) General coherent attack. This involves taking a collection of qubits, putting them through a system, and resending.

We will assume that the chat is noiseless.

We will only look at the intercept and resend attack, when Eve measures in the Breidbart basis:

$$|\alpha_0\rangle = \cos\frac{\pi}{8}|0\rangle + \sin\frac{\pi}{8}|1\rangle, \qquad |\alpha_1\rangle = \sin\frac{\pi}{8}|0\rangle - \cos\frac{\pi}{8}|1\rangle.$$

Then Eve's measurement outcomes and post measurement states are $(0, |\alpha_0\rangle)$ and $(1, |\alpha_1\rangle)$. The bit error rate in $\tilde{x}$ and $\tilde{x}'$ arising from Eve's attack can be calculated as follows. Note that

$$\begin{aligned}\mathrm{Prob}(x' = 1 \mid A \text{ sent } |0\rangle) &= \mathrm{Prob}(x' = 1 \mid |\alpha_0\rangle)\,\mathrm{Prob}(|\alpha_0\rangle \mid |0\rangle) \\ &\quad + \mathrm{Prob}(x' = 1 \mid |\alpha_1\rangle)\,\mathrm{Prob}(|\alpha_1\rangle \mid |0\rangle) \\ &= |\langle 1|\alpha_0\rangle|^2 |\langle \alpha_0|0\rangle|^2 + |\langle 1|\alpha_1\rangle|^2 |\langle 0|\alpha_1\rangle|^2 \\ &= \frac{1}{4}.\end{aligned}$$

This is true for any signal that Alice sent. Hence the bit error rate is 25%. Alice and Bob can estimate the bit error rate by taking a random sample in $\tilde{x}$ and $\tilde{x}'$. This gives shorter strings $\bar{x}$ and $\bar{x}'$. This can be corrected with information reconciliation, which gives x^* and $x^{*\prime}$. Then we can perform privacy amplification to get x_*, x'_* on which Eve knows almost nothing.

Let's look at an example of information reconciliation. Suppose $\bar{x} = \mathbf{a} = a_1 \cdots a_7$, and $\bar{x}' = \mathbf{b} = b_1 \cdots b_7$, and they are confidence the bit error rate is 1/7. They publicly agree to use the check matrix

$$H = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}.$$

This is the Hamming code $[7, 4]$. Alice computes $\mathbf{s}^A = H\mathbf{a}^T$, and Bob computes $\mathbf{s}^B = H\mathbf{b}^T$. Alice tells Bob what $\mathbf{s}^A$ is, publicly, and Bob computes

$$\mathbf{s} = \mathbf{s}^B - \mathbf{s}^A = H(\mathbf{a}^T - \mathbf{b}^T) = H\mathbf{e}^T.$$

Now $\mathbf{e}^T$ has at most one 1 in it, assuming our bit error rate is correct. From classical cryptography, this Hamming code can correct at most one error. Hence there exists a unique bit string $\mathbf{v} \in \{0, 1\}^7$ with $\omega(\mathbf{v}) \leq 1$, where ω is the weight, such that $H\mathbf{v}^T = \mathbf{s}$. Therefore $\mathbf{e} = \mathbf{v}$.

So since Bob knows H and $\mathbf{s}$, Bob can find $\mathbf{e}$, and so can convert $\mathbf{b}$ to $\mathbf{b} + \mathbf{e} = \mathbf{a}$.

Now let's look at an example of privacy amplification. Here we take 3 bit example, in which Eve knows at most one bit.

Then Alice and bob compute

$$\mathbf{c} = (a_1 \oplus a_3, a_2 \oplus a_3) \in \{0, 1\}^2.$$

We claim that Eve knows nothing about $\mathbf{c}$. This is just a case bash, over all possible bit strings $\mathbf{a}$ and their result $\mathbf{c}$. Note Alice and Bob publicly agree on how to form $\mathbf{c}$.

4 Classical Computation and Computational Complexity

We first define what we mean by a *computational task*. Here, our input is a bit string, and the input size is the length of the bit string.

For example, the question ‘is 10111 prime?’, is not a computational task. Instead, ‘given an n-bit string A, determine whether A is prime’, is a computational task.

The output is a bit string. If it is a single bit output, then it is called a *decision problem*.

We denote $B = B_1 = \{0, 1\}$, $B_n = \{0, 1\}^n$, and $B^* = \bigcup_n B_n$.

Definition 4.1. A *language* is a subset $L \subset B^*$.

A decision problem corresponds to recognizing the language for which the answer is 1.

Example 4.1. (Primality Testing)

This is the decision problem of recognizing the language $L \subset B^*$, which comprises of all bit strings that represent prime numbers in binary.

A more general computational task has output size greater than one. For example, FACTOR($\mathbf{x}$) is a problem that takes an input $\mathbf{x} \in B_n$, and output either $\mathbf{u}$, a factor of $\mathbf{x}$, or 1 if $\mathbf{x}$ is prime.

The circuit model of classical computation is as follows. We are given an input $x = b_1 \cdots b_n$, extended (padded) with 0’s to form

$$b_1 b_2 \cdots b_n 00 \cdots 0.$$

These extra bits serve as extra workspace.

A *computational step* is an application of a designated boolean function $f : B_m \to B_n$ on some designated bits. This updates the input string. Moreover these elementary steps should be fixed operations, and should not become more complicated as n increases.

It can be shown that we can restrict the boolean gates to AND, OR and NOT, and that these operations are universal, i.e. any boolean function of any dimension can be constructed by applying these functions sequentially. The output is the value of some subset of bits.

For each input size n, we have a *circuit* C_n, which is a prescribed sequence of steps (C_n is a function only of n). We also have a *circuit family* $(C_1, C_2, \ldots)$.

We also want to extend our model to incorporate probabilistic choices. In the circuit model, we can do this by extending $b_1 \cdots b_n 0 \cdots 0$ to $b_1 \cdots b_n r_1 \cdots r_k 0 \cdots 0$, where $r_1, \ldots, r_k$ are 0 and 1 uniformly at random. The output is now a sample from a probability distribution.

In computational complexity theory (CCP) a fundamental problem is determining the worst-case run time complexity of an algorithm. In the circuit model this is just the size of circuit C_n, say $T(n)$. Often we are interested if $T(n) = \mathcal{O}(n^k)$ for some k, i.e. T is bounded by a polynomial. In this case we write $T(n) = \mathcal{O}(\mathrm{poly}(n))$. If $T(n)$ is not polynomially bounded, the computation is regarded as intractable. We have the following terminology:

- **P**: polynomial time. The class of all languages for which the problem has a classical algorithm which runs in polynomial time, and gives the correct answer w.p. 1.
- **BPP**: bounded error probabilistic poly time. The class of languages whose problem has a randomised poly algorithm with correct answer at least 2/3 for every input.

Example 4.2.

The problem FACTOR(N, M) is as follows: given an integer N of n digits and $M < N$, decide if N has non-trivial factor less than M. The fastest known classical algorithm runs in time $\exp(\mathcal{O}(n^{1/3}(\log n)^{2/3}))$.

This is not known to be in **BPP**.

In fact 2/3 for **BPP** is not required, as we may take our algorithm for 2/3 and repeat it many times and take the most likely outcome.

Replacing the resource of time with space gives class **PSPACE**. In fact we can see **P** $\subseteq$ **BPP** $\subseteq$ **PSPACE**, as poly many operations can act on only poly many bits. It is not known if these inclusions are strict!

4.1 Query Complexity and Promise Problems

In computation, there is another scenario that is often considered. In this scenario, we are given as an input a *black box* or *oracle* that computes some function $f : B_m \to B_n$. We can query the black box by giving it inputs, and this is the only way to gain information about the box.

At the start, it is unknown what f is, but there is some *promise*, which is some restriction f must satisfy. We want to find some property about f, by querying the box the least number of times. The *query complexity* is the number of times the oracle is used, but we may also be interested in the total time complexity.

Example 4.3. (Black Box Problems)

Here are some examples of black box problems.

1. The "balanced vs constant" problem: we have $f : B_n \to B$, which is promised to be either constant, or balanced in the sense that $f(x) = 0$ for exactly half of the inputs.

   We then want to determine whether f is balanced, either correct with certainty or with some large probability.

2. Boolean satisfiability: we have $f : B_n \to B$ with no restriction, and we want to determine whether there is x with $f(x) = 1$.
3. Search; we have $f : B_n \to B$ with exactly on x satisfying $f(x) = 1$, and we wish to find this x.
4. Periodicity: we have $f : \mathbb{Z}_n \to \mathbb{Z}_n$, where f is periodic with some period r. We are asked to find r.

4.2 Circuit Quantum Computation

The circuit model for classical computation can be generalized to the quantum world easily. Our starting string is replaced with a sequence of qubits in the basis state $|b_1\rangle \cdots |b_n\rangle |0\rangle \cdots |0\rangle$. A set is the application of a quantum gate, which is a prescribed unitary operation to a choice of qubits. Note we do not need randomize qubits, as a random choice can be generated by a measurement on $H|0\rangle$.

Again for each input size n we have quantum circuit C_n. A quantum algorithm is then defined by a (uniform) family of quantum circuits $(C_1, C_2, \ldots)$. Circuits often have nice drawings.

We saw in classical computation there is a universal set consisting of {NOT, AND, OR}. In fact we may delete OR from this set. We can show there is no set of 2-bit reversible gates that are universal, but universal 3-bit reversible gates exist, e.g. the Fredkin gate

$$F(0b_2b_3) = 0b_2b_3, \qquad F(1b_2b_3) = 1b_3b_2.$$

The Toffoli gate is another example:

$$\text{Toff}(0b_2b_3) = 0b_2b_3, \qquad \text{Toff}(1b_2b_3) = 1CX(b_2b_3).$$

In the quantum case all gates are reversible as they are unitary, but the situation is more complicated, as gates are parametrised by continuous parameters. Hence no finite set can generate them all exactly by finite circuits. However there are *approximately universal* gates which generate any unitary gate with arbitrary accuracy $\varepsilon > 0$ (with respect to the operator norm). If we have $\varepsilon = 0$ the set is *exactly universal*.

For approximately universal sets, the size of the circuit C that acts as W will generally be exponential in the number of qubits n. Moreover, for fixed U, the size of C can be taken to be bounded by $\text{poly}(\log(1/\varepsilon))$: this is Solovay-Kitaev.

Example 4.4.

Some examples of approximately universal sets:

- $\{CX,\ \text{all 1-qubit gates}\}$.
- $\{CX, H, T\}$, where $T = \text{diag}(1, e^{i\pi/4})$.
- $\{\text{Toffoli 3-qubit gate}, H\}$.

The latter is universal for all gates with real entries. The first example is exactly universal.

Now we define the complexity class **BQP**, standing for bounded error quantum poly time. This is the direct generalisation of **BPP**, and is the class of langauges in which there is a poly time quantum algorithm whose output answer is correct with probability at least 2/3.

We can show $\mathbf{BPP} \subseteq \mathbf{BQP}$, as any poly sized classical circuit can be converted to a reversible quantum circuit. The natural question is are these classes equal? This is unsolved, although it is believed they are unequal. We know that $\text{FACTOR}(M, N)$ is in **BQP**, but not if it is in **BPP**. More generally we are interested in tasks that show resource benefit for a quantum solution vs. a classical one.

We will now show how to get a reversible version of any function. Given $f : B_m \to B_n$, we can express it in reversible form $\tilde{f} : B_{m+n} \to B_{m+n}$ as follows: we introduce $\oplus$, bitwise addition. Now define

$$\tilde{f}(b, c) = (b, c \oplus f(b)).$$

Then $\tilde{f}$ is easily computable and given $\tilde{f}$ we can recover f by choosing $\tilde{f}(b, 0 \cdots 0) = (b, f(b))$. Moreover $\tilde{f}$ is reversible, since it is self-inverse. Hence when quantifying problems, we use $\tilde{f}$ for any oracle problem involving f. Specifically the *quantum oracle* for $f : B_m \to B_n$ is the quantum gate

$$U_f \left|x\right\rangle \left|y\right\rangle = \left|x\right\rangle \left|y \oplus f(x)\right\rangle.$$

Now this U_f is unitary, as any $g : B_k \to B_k$ reversible is a permutation on the k-bit strings, so the linear map is a permutation matrix. Hence U_f is unitary.

Since U_f is a quantum operation, it can act on superimposed inputs. Indeed if we input an equal superposition of all 2^m possible m-bit strings, we get

$$U_f : \frac{1}{2^{m/2}} \sum_x |x\rangle |0\rangle \to |\psi_f\rangle = \frac{1}{2^{m/2}} \sum_x |x\rangle |f(x)\rangle .$$

Such a computation is called computation by *quantum parallelism*. By quantum processing we are able to obtain global information about the nature of the function f. Note we can get a uniform superposition over all x values by doing

$$H \otimes \cdots \otimes H |0\rangle \cdots |0\rangle = \frac{1}{2^{m/2}} \sum_{x \in B_n} |x\rangle .$$

An important feature is that we have created a superposition of exponentially many terms, with only a linear number of elementary operations by applying H m times.

4.3 Deutsch-Jozsa Algorithm

The first such example of an exponential benefit of quantum computation is a quantum algorithm for the balanced vs constant black-box promise problem.

Recall here, we are given a Boolean function $f : B_n \to B$, which is either constant or 'balanced', i.e. it is 0 for exactly half of the 2^n inputs.

A little thought shows that classically $2^n/2 + 1$ queries (i.e. exponentially many) are necessary and sufficient in the worst case. Sufficiency is clear. For necessity, suppose we have a deterministic algorithm which works on $K \leq 2^{n-1}$ queries.

An adversary can force the algorithm to fail as follows: when applied, he has not chosen his function f, but continues to answer 0. At the end, his function is fixed on K inputs, and he may fix the other $2^n - K$ to either be constant or balanced, and contradict the algorithms conclusion.

Similarly a probabilistic classical algorithm must also have at least $2^{n-1} + 1$ queries.

However, in the quantum scenario, just one query suffices. The black box is

$$U_f : |x\rangle |y\rangle = |x\rangle |y + \oplus f(x)\rangle ,$$

where $|x\rangle$ comprises n qubits and the output $|y\rangle$ is one qubit. To apply the algorithm, first suppose all qubits are in the standard state $|0\rangle$. We construct an equal superposition of all n-bit strings (in n steps), and set the output register to $|-\rangle$, by applying X and then H to $|0\rangle$. Thus we have

$$\left(\frac{1}{\sqrt{2^n}}\sum_{x\in B_n}|x\rangle\right)|-\rangle\,.$$

Next we run U_f on this state. On a single state, we get (without $\sqrt{2}$ term):

$$\begin{aligned}U_f : |x\rangle\,(|0\rangle - |1\rangle) &\to |x\rangle\,(|f(x)\rangle - |f(x)\oplus 1\rangle)\\ &= (-1)^{f(x)}\,|x\rangle\,(|0\rangle - |1\rangle).\end{aligned}$$

I.e. we flip if $f(x) = 1$, otherwise stay the same. This is sometimes called a *phase kickback*. On the full superposition, we get

$$\left(\frac{1}{\sqrt{2^n}}\sum_{x\in B_n}|x\rangle\right)|-\rangle \mapsto \left(\frac{1}{\sqrt{2^n}}\sum_{x\in B_n}(-1)^{f(x)}\,|x\rangle\right)|-\rangle\,.$$

This just gives us the n-qubit state

$$|f\rangle = \frac{1}{\sqrt{2^n}}\sum_{x\in B_n}(-1)^{f(x)}\,|x\rangle\,.$$

- If f is constant, then
$$|f\rangle = \pm\frac{1}{\sqrt{2^n}}\sum_{x\in B_n}|x\rangle\,.$$
Applying $H_n = H\otimes\cdots\otimes H$, we get $\pm\,|0\cdots 0\rangle$, as H is self-inverse.
- If f is balanced, then $|f\rangle$ will be orthogonal to $|\phi_n\rangle$, which is the sum of all states. But since H_n is unitary, $H_n\,|f\rangle$ will be orthogonal to $H_n\,|\phi_n\rangle = |0\cdots 0\rangle$. So $H_n\,|f\rangle$ will have the form $\sum_x a_x\,|x\rangle$, with the all-zero term absent.

From the above discussion, we can construct $|f\rangle$, apply H_n and measure the n qubits in the computational basis. If the result is $0\cdots 0$, then f was constant, and if the result is a non-zero string, then f was certainly balanced.

Hence we have solved the problem with one query to f, and $(3n+2)$ operators: $(n+1)$ H's, one X to make our input, n H's to perform H_n on $|f\rangle$ and n single qubit measurements to get the output string.

Now we consider the bounded error case. Suppose we tolerate some error. Then the above quantum algorithm still works, but there is a classical randomised algorithm that solves the problem with only a constant number of queries, depending on ϵ as $\mathcal{O}(1/\log\epsilon)$ for any n, and for any fixed $\epsilon > 0$.

Thus we lose the exponential gap between classical and quantum queries. The classical algorithm is picking K values independently at random. If they are the same, say f is constant, otherwise say f is balanced. The second output is always correct, but the first may be erroneous, if f is balanced and we with probability $1/2$ pick the same output as the first, which happens with $1/2^{K=1}$ probability.

Hence the error is bounded by $1/2^{K-1} < \epsilon$, i.e. $K > \log 1/\epsilon$ is sufficient.

Does the above algorithm mean quantum superiority? Probably not.

- The first thing to consider is that if we allow any level of error, we lose the exponential separation. But realistically, exactly-zero error is unrealistic, and we should accept some level of error (e.g. computers are not perfect and do not have infinite precision). This can be addressed: there are black box problems with exponential separation between the classical and quantum algorithms even with error (e.g. Simon's quantum algorithm).
- The second is that the Deutsch-Jozsa problem is a black-box problem. To convert it to a standard task, we want a class of functions that the balanced/-constant decision is hard classically. But no such class is known.

Are there any standard tasks for which we can prove the existence of an exponential speed-up for quantum versus classical computation? No such proofs are known, but the difficulty is in the classical theory, i.e. we know exponential classical algorithms, but we cannot prove there are better ones.

4.4 Simon's Algorithm

Consider the following problem:

We are given a black box boolean function $f : B_n \to B_n$, which is either one-to-one, or two-to-one of the following form: there is an n-bix string $\xi \neq 00\cdots 0$ such that

$$f(x) = f(y) \iff y = x \oplus \xi.$$

Then we wish to determine which type of function f is.

Furthermore, we can ask for a determination of ξ if f is of the second type.

Simon's quantum algorithm solves this problem with only $\mathcal{O}(n)$ queries to f, but on the other hand we can argue that the problem is classically hard, requiring an exponential number of queries for bounded error computation.

Intuitively, if f is two-to-one, we need to query f an exponential number of times to have a reasonable probability of noticing that f is not one-to-one. Indeed, we obtain no information unless we are lucky to choose two queries x and y with

$f(x) = f(y)$, i.e. $x \oplus y = \xi$. Suppose we choose $2^{n/4}$ queries. Then the number of pairs of queries is less than $(2^{n/4})^2$, and for each pair the probability that $x \oplus y = \xi$ is 2^{-n}, so the probability of seeing ξ is less than $2^{-n}2^{n/2} = 2^{-n/2}$.

This argument can be made more rigorous, but we omit the technicalities.

5 Quantum Fourier Transform

The *quantum Fourier transform* can be viewed as a generalisation of the Hadamard operation to higher dimensions, and we are especially interested in $N = 2^n$, i.e n-qubit space. This is the same as the discrete Fourier transform: a unitary matrix.

Let $\mathcal{H}_N$ denote a state space with o.n.b. $\{|0\rangle, \dots, |N-1\rangle\}$, labelled by $\mathbb{Z}_N$. The quantum Fourier transform modulo N, denote QFT_N is a the unitary transform on $\mathcal{H}_N$ defined by

$$\mathrm{QFT}_N : |x\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} \exp\left(2\pi i \frac{xy}{N}\right) |y\rangle .$$

As a matrix, the jk'th entry is

$$[\mathrm{QFT}]_{jk} = \frac{1}{\sqrt{N}} \exp\left(2\pi i \frac{jk}{N}\right) .$$

We 0-label the rows and columns. If $\omega = e^{2\pi i/N}$ is the primitive N'th root of unity, all matrix elements are normalised power of ω, such that:

- The initial row and column contains 1's.
- Each row and column is a geometric sequence; the k'th row/column is a sequence of powers of ω^k.

The fact QFT is unitary is basic algebra. Recall

$$1 + \omega^K + \dots + \omega^{(N-1)K} = \begin{cases} N & N \mid K, \\ 0 & N \nmid K. \end{cases}$$

5.1 Periodicity Determination

A fundamental application of the Fourier transform is the determination of periodicity. Some important mathematical problems can be reduced to such a problem.

Suppose we are give a function $f : \mathbb{Z}_N \to Y$, which is promised periodic with period r, under the assumption f is one-to-one in each period. We want a method of determining r with some constant level of probability, independent of increasing the size of N.

It can be shown $\mathcal{O}(N^{1/2})$ queries to f are necessary and sufficient to achieve this in classical computation. In some cases further information may be available, but periodicity determination still hard. However in the quantum scenario we see that

r can be determined with probability $1-\epsilon$ with only $\mathcal{O}(\log\log N)$ queries, and poly($\log N$) processing steps.

First, we construct a uniform superposition $\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle$, and using on query obtain the state

$$|f\rangle = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle\,|f(x)\rangle\,.$$

Since f is periodic, r divides N exactly, so let $A = N/r$, the number of periods. If we measure the second register, we see $y = f(x_0)$, where x_0 is the least x having $f(x) = y$. Then the first register will be projected into an equal superposition of $x = x_0, x_0 + r, \ldots, x_0 + (A-1)r$, so

$$|\mathrm{per}\rangle = \frac{1}{\sqrt{A}}\sum_{j=0}^{A-1}|x_0 + jr\rangle\,.$$

Here $0 \leq x_0 \leq r-1$ is chosen uniformly at random. Measuring the register of $|\mathrm{per}\rangle$ gives a random element j_0, i.e. a random number altogether. However $|\mathrm{per}\rangle$ seems to contain information about r. The resolution is to use the Fourier transform to pick up periodicities. Applying QFT, we get

$$\mathrm{QFT}\,|\mathrm{per}\rangle = \frac{1}{\sqrt{NA}}\sum_{j=0}^{A-1}\left(\sum_{y=0}^{N-1}\omega^{(x_0+jr)y}\,|y\rangle\right) = \frac{1}{\sqrt{NA}}\sum_{y=0}^{N-1}\omega^{x_0 y}\left[\sum_{j=0}^{A-1}\omega^{jry}\right]|y\rangle\,.$$

The bit in the bracket is a geometric series with powers of $\alpha = e^{2\pi i r y/N} = (e^{2\pi i/A})^y$, which is non-zero whenever $A \mid y$. Hence

$$\mathrm{QFT}\,|\mathrm{per}\rangle = \sqrt{\frac{A}{N}}\sum_{k=0}^{r-1}\omega^{x_0(kN/r)}\,|kN/r\rangle\,.$$

The random shift has been eliminated, and only occurs in a pure phase. If we measure the label, we obtain a value $c = k_0 N/r$, so

$$\frac{k_0}{r} = \frac{c}{N}.$$

If k_0 was coprime to r, we can cancel c/N down and read off r as the denominator. If they are not coprime, we get a small denominator r', so we chan check r works by evaluating $f(0)$ and $f(r)$. If k_0 is chosen at random what is the probability of coprimality? We use the following:

Theorem 5.1. *The number of integers less than r, coprime to r grows as $\mathcal{O}(r/\log\log r)$. If $k_0 < r$ is chosen at random, the probability k_0 is coprime to r is*

$$\mathcal{O}(1/\log\log r).$$

Repeating this $\mathcal{O}(\log\log r) < \mathcal{O}(\log\log N)$ times, we obtain a coprime k_0 with constant level of probability. We used the following fact:

Lemma 5.1. *If a single trial has success probability p and we repeat it M itmes independently, for any constant $0 < 1-\epsilon < 1$,*

$$\mathbb{P}(\textit{one success in } M \textit{ trials}) > 1-\epsilon \qquad \textit{if } M = \frac{-\log\epsilon}{p}.$$

Proof: We have probability of one succes in M runs is $1-(1-p)^M$, so $1-(1-p)^M = 1-\epsilon$ if

$$M = \frac{-\log\epsilon}{-\log(1-p)}.$$

Hence any M above this works. Now we want a simple estimate of this. Using the fact $p < -\log(1-p)$, we get

$$M = \frac{-\log\epsilon}{-\log(1-p)} < \frac{-\log\epsilon}{p}.$$

So $M = \mathcal{O}(1/p)$ repetitions suffice.

In each round we query f three times, so $\mathcal{O}(\log\log N)$ in total. We also use the large gate QFT_N, which we can implement in $\mathcal{O}((\log N)^2)$ steps. Everything else is arithmetic on $\mathcal{O}(N)$ integers, which are $\mathrm{poly}(\log N)$. This gives the bound.

The quantum algorithm for periodicity determination will be the basis of Shor's algorith,, and may be generalised to an arbitrary group G as the hidden subgroup problem.

5.2 Implementation

Non-examinable. For N not a power of 2, we do not have an efficient implementation, but approximate by QFT mod 2^k, where 2^k is near enough.

The implementation is really just FFT in the quantum scenario. We begin by showing

$$\mathrm{QFT}\,|x\rangle = \frac{1}{\sqrt{2^n}}\sum_y \exp\left(2\pi i\frac{xy}{2^n}\right)|y\rangle$$

is a product of n one-qubit state. Write $0 \le x, y < 2^{n-1}$ in binary. Discarding whole numbers,

$$\frac{xy}{2^n} \equiv y_{n-1}(.x_0) + y_{n-2}(.x_1x_0) + \cdots + y_0(.x_{n-1}x_{n-2}\ldots x_0),$$

where factors in parentheses are binary expansions. Hence

$$\begin{aligned}\sum_y \exp\left(2\pi i \frac{xy}{2^n}\right) |y\rangle &= \sum_y \exp\left(2\pi i \frac{xy}{2^n}\right) |y_{n-1}\rangle \cdots |y_0\rangle \\ &= (|0\rangle + 2^{\pi i(.x_0)} |1\rangle)(|0\rangle + e^{2\pi i(.x_1 x_0)} |1\rangle) \cdots (|0\rangle + e^{2\pi i(.x_{n-1} \ldots x_0)} |1\rangle).\end{aligned}$$

This factorisation is the key: it should map each basis $|x_{n-1}\rangle \cdots |x_0\rangle$ into the corresponding product state. Note the Hadamard operation is

$$H |x\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i(.x)} |1\rangle).$$

In the i'th stage, in the y_{i-1} register we do $H |x_{n-i}\rangle$, followed by phase shifts of $e^{2\pi i 0.0\ldots01}$ controlled by x_j for $j < n - i$. Accumulating these in the x_{n-i} line, as we do not need it after this stage. Then by swap operations we reverse the order of the qubits.

6 Search Problems

Searching is a fundamentally important task. Many problems can be put in this framework; factoring N is a search of integers less than N which can divide N.

6.1 Unstructured Search

Suppose we are given a database with N items, and want to locate a particular item. We assume it is entirely unstructured, but we can check whether a given item is the one we seek. Our algorithm should locate the item with constant probability independent of N.

For classical computation, $\mathcal{O}(N)$ is necessary and sufficient. Not finding the item gives no further information. For quantum, $\mathcal{O}(\sqrt{N})$ are sufficient (and in fact necessary), so we get quadratic speedup. This is not exponential, but still significant.

If the database is structured, i.e. ordered we can classically locate k with only $\mathcal{O}(\log N)$ queries, with a binary search.

We will discuss Grover's quantum searching algorithm, which achieves $\mathcal{O}(\sqrt{N})$ searching time in the unstructured search. In the structured search, quantum is still only $\mathcal{O}(\log N)$, but with $k \log N$ queries for some $k < 1$.

Recall the projection operator

$$\Pi_{|\alpha\rangle} = |\alpha\rangle \langle\alpha| \, ,$$

and the *reflection in the orthogonal subspace* is

$$I_{|\alpha\rangle} = I - 2 \, |\alpha\rangle \langle\alpha| \, .$$

For any unitary operator U, we can check

$$U \Pi_{|\alpha\rangle} U^\dagger = \Pi_{U(|\alpha\rangle)}, \qquad U I_{|\alpha\rangle} U^\dagger = I_{U|\alpha\rangle}.$$

Example 6.1.

Let $|\alpha^\perp\rangle$ be orthogonal to $|\alpha\rangle$, then if $|v\rangle = x\,|\alpha\rangle + y\,|\alpha^\perp\rangle$,

$$\Pi_{|\alpha\rangle} \, |v\rangle = x \, |\alpha\rangle \, , \qquad I_{|\alpha\rangle} \, |v\rangle = -x \, |\alpha\rangle + y \, |\alpha^\perp\rangle \, ,$$

so $I_{|\alpha\rangle}$ is reflection in the line defined by $|\alpha^\perp\rangle$.

We provide a geometric overview for Grover's rather than the algebraic approach he originally intended. It will be convenient to take $N = 2^n$, and replace the database by black-box $f : B_n \to B$, with $f(x) = 0$ for all strings except one, x_0, which we must determine.

Recall the unitary operator U_f. Instead of using this, we will use the related operation

$$I_{x_0} |x\rangle = \begin{cases} |x\rangle & x \neq x_0, \\ -|x_0\rangle & x = x_0. \end{cases}$$

So I_{x_0} inverts the amplitude of the $|x_0\rangle$ component, i.e. the reflection operator defined above. A black box which performs I_{x_0} may be constructed by setting the output register to $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

We work in $\mathcal{B}_n$, and let $H_n = \bigotimes_n H$. Grover's algorithm operators as follows: Having no information about x_0, we begin with

$$|\psi_0\rangle = H_n |0 \cdots 0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \mathcal{B}_n} |x\rangle .$$

Consider the *Grover iteration operator* Q, defined by

$$Q = -H_n I_0 H_n I_{x_0}.$$

Q has a simple geometric operation:

- In the plane $\mathcal{P}(x_0)$ spanned by $|x_0\rangle$ and $|\psi_0\rangle$, Q is rotation through angle 2α where $\sin\alpha = N^{-1/2}$.
- In the orthogonal subspace to $\mathcal{P}(x_0)$, $Q = -I$, i.e. a reflection.

Thus by applying Q to $|\psi_0\rangle$, we may rotate it around near to $|x_0\rangle$, and determine it with high probability. For large N, $|x_0\rangle$ and $|\psi_0\rangle$ are almost orthogonal, so $2\alpha \approx 2N^{-1/2}$. Hence about $\frac{\pi}{4}N^{1/2}$ iterations will be needed. Each application requires one use of I_{x_0}, so $\mathcal{O}(\sqrt{N})$ are required.

More precisely, $\langle x_0 | \psi_0 \rangle = N^{-1/2}$, so we will need around

$$\frac{\arccos \frac{1}{\sqrt{N}}}{2 \arcsin \frac{1}{\sqrt{N}}}.$$

Example 6.2.

A simple example is the case $N = 4$, so $\sin\alpha = \frac{1}{2}$, and Q is a rotation through $\pi/3$.

The initial state is $|\psi_0\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$, and the angle between $|x_0\rangle$ and $|\psi_0\rangle$ if $\pi/3$ for any x_0, hence after one application of Q, we learn the position of any single marked item with certainty.

Index

ancilla, 7
approximately universal, 24

Bell basis, 14
Bell measurement, 14
black box, 22

circuit, 22
circuit family, 22
computational task, 21

decision problem, 21

exactly universal, 24

Grover iteration operator, 34

Hadamard gate, 12

language, 21

no-signalling principle, 9

phase kickback, 26
promise problem, 23

quantum Fourier transform, 29
quantum oracle, 24
quantum parallelism, 25
quantum teleportation, 15
query complexity, 23

reflection operator, 33