2.111/8.370/18.435 (Quantum Computation) Lecture Notes

Evan Chen

Fall 2015

This is MIT's graduate 18.435, also numbered 2.111 and 8.370, instructed by Seth Lloyd. The formal name for this class is "Quantum Computation".

The permanent URL for this document is `http://web.evanchen.cc/coursework.html`, along with all my other course notes.

I joined this class after the fourth lecture; hence the notes for earlier classes may not be faithful representations of the actual lectures.

Contents

1 Classical Logic Gates **3**

2 Quantum Computation **4**
- 2.1 Qubits and The Vector Space $\mathbb{C}^2$ . . . 4
- 2.2 Operators . . . 4
- 2.3 Difference from Quantum Mechanics . . . 4
- 2.4 Pauli matrices . . . 5

3 September 24, 2015 **6**
- 3.1 Review of Pauli Matrices . . . 6
- 3.2 Higher Dimensions . . . 6
- 3.3 Back to qubits . . . 7
- 3.4 More on Pauli matrices . . . 8

4 September 29, 2015 **9**
- 4.1 Multiple Qubits, and Tensor Products . . . 9
- 4.2 Basis Computation . . . 10
- 4.3 Entanglement . . . 10

5 October 1, 2015 **12**
- 5.1 Triplet States . . . 12
- 5.2 Group Theory Digression . . . 12
- 5.3 Measurement and reduced density matrices . . . 13

6 October 6, 2015 **15**
- 6.1 CNOT Gate . . . 15
- 6.2 No-Cloning Theorem . . . 15
- 6.3 Entropy . . . 16
- 6.4 CNOT Again . . . 16

7 October 8, 2015 **17**

8 October 15, 2015 **20**
8.1 Deustch-Jozsa 20
8.2 Greenberger-Horne-Zeilinger Paradox 22

9 October 20, 2015 **23**
9.1 Superdense Coding 23
9.2 Quiz Warmup 23
9.3 Teleportation 24

10 November 3, 2015 **25**
10.1 Fast Fourier Transformation 25
10.2 Quantum Fourier Transformation 25
10.3 The Circuit 26

11 November 5, 2015 **27**
11.1 Digression on Flipping Bits 27
11.2 Atomic Clocks 28

12 November 10, 2015 **29**
12.1 Synopsis 29
12.2 The Quantum Phase Algorithm 29

13 November 12, 2015 **31**
13.1 Shor's Algorithm 31

14 November 17, 2015 **32**
14.1 Graph Isomorphism Problem 32
14.2 Shor's Algorithm 32

15 November 24, 2015 **33**
15.1 Sparse matrix completion 33
15.2 Homework Problems 33
15.3 Grover's Algorithm 33

16 December 1, 2015 **35**
16.1 Grover's search algorithm, continued 35

17 December 3, 2015 **36**
17.1 Error Correction 36

A December 10, 2015 **37**
A.1 Review topics 37
A.2 Classical and Quantum Logic 37
A.3 Quantum Algorithms 38

B Notes for Exam **38**

§1 Classical Logic Gates

Reversible logic gates: Toffoli, Fredkin, CNOT, NOT, wire. Universal set of gates e.g. AND, OR, NOT, (COPY). Toffoli and Fredkin are universal on their own with suitable additional inputs.

§2 Quantum Computation

§2.1 Qubits and The Vector Space $\mathbb{C}^2$

Let $\mathbb{C}^2$ be a complex vector space, equipped with the usual Hermitian inner form.

In this class, we consider **qubits**, which we can think of as the following two vectors in the normed vector space $\mathbb{C}^2$:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \text{and} \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

The notation $|\bullet\rangle$ will in generally mean such a vector, with the $-$ being a variable name, which (unlike in math or Python) can not only consist of letters, but also numbers, symbols, Unicode characters, ...

Given $|\psi\rangle = \begin{pmatrix} a \\ b \end{pmatrix} \in \mathbb{C}^2$, we then define the transpose

$$\langle\psi| = \begin{pmatrix} \overline{a} \ \overline{b} \end{pmatrix}$$

the column vector in the dual space $(\mathbb{C}^2)^\vee$, identified using the inner form. In other words, if we use † to denote **Hermitian conjugation** (conjugate transpose) then $\langle\psi| \overset{\text{def}}{=} (|\psi\rangle)^\dagger$.

§2.2 Operators

In general, we are going to use vectors $|\psi\rangle$ of norm 1 to denote a **state**.

Then, an **observable** will correspond to a Hermitian operator A (meaning $A = A^\dagger$; i.e. A equals its own conjugate transpose) in the following fashion. The possible outcomes of A are the two *eigenvalues* of A (recall that Hermitian operators can always be diagonalized), possibly the same. In any case, let v_1 and v_2 be eigenvectors of A, with eigenvalues λ_1 and λ_2 and which form an orthonormal basis of $\mathbb{C}^2$ (this is automatically true if $\lambda_1 \neq \lambda_2$). So A can output either λ_1 or λ_2. We should think of this as "measuring the spin along the directions v_1, v_2".

Now any state $|\psi\rangle$ can be written in the form

$$|\psi\rangle = \alpha_1 v_1 + \alpha_2 v_2$$

for $|\alpha_1|^2 + |\alpha_2|^2 = 1$. In that case, **the observation of the state $|\psi\rangle$ measured along A is supposed to give λ_1 with probability α_1 and to λ_2 with probability α_2.**

Note that the expected value of measuring $|\psi\rangle$ along A is $\langle\psi| A |\psi\rangle$. Also, if $\lambda_1 = \lambda_2$ then A doesn't measure anything at all – the eigenvalues returned are always the same!

We'll write this all again for general dimensions.

§2.3 Difference from Quantum Mechanics

Note that already we notice two differences from classical mechanics:

- States are not discrete; they are *linear*, and have probabilities.
- The state space is *complex*; $\mathbb{C}$ is intimately tied to quantum mechanics, unlike classical mechanics when we mostly only see $\mathbb{R}$.

§2.4 Pauli matrices

We will now consider a basis of the Hermitian 2×2 matrices The **Pauli matrices** are defined as

$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}.$$

Their normalized eigenvectors are

$$\left|\uparrow\right\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad \left|\downarrow\right\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$
$$\left|\rightarrow\right\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} \qquad \left|\leftarrow\right\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix}$$
$$\left|\otimes\right\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ i \end{pmatrix} \qquad \left|\odot\right\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -i \end{pmatrix}.$$

We call them "up" and "down" respectively (i.e. the first two are z-up and z-down). So, measuring a state $\left|\psi\right\rangle$ by σ_z should be thought of as "measuring along the z-axis".

We care about the Pauli matrices because

Theorem 2.1

id, σ_x, σ_y, σ_z form an orthonormal basis of the 2×2 Hermitian matrices.

Further properties:

Problem 2.2 (Homework 2.1)**.** Show that

- These are conjugate transposes ($\sigma_x^\dagger = \sigma_x$, et cetera).
- They are involutions (squares are id).
- $\sigma_x \sigma_y = i\sigma_z$ and cyclically.
- $[\sigma_x, \sigma_y] = 2i\sigma_z$.
- $\left|\uparrow\right\rangle$, $\left|\downarrow\right\rangle$ are eigenvectors of σ_z with eigenvalues $+1$ and -1 respectively.
- $\left|\rightarrow\right\rangle$, $\left|\leftarrow\right\rangle$ are eigenvectors of σ_x with eigenvalues ± 1.
- $\left|\otimes\right\rangle$, $\left|\odot\right\rangle$ are eigenvectors of σ_y with eigenvalues ± 1.

§3 September 24, 2015

§3.1 Review of Pauli Matrices

Observe that

$$\sigma_x \left|\uparrow\right\rangle = \left|\downarrow\right\rangle \quad \text{and} \quad \sigma_x \left|\downarrow\right\rangle = \left|\uparrow\right\rangle .$$

Problem 3.1 (Homework 2.2)**.** Show that

$$\begin{aligned}
\sigma_z \left|\otimes\right\rangle &= \left|\odot\right\rangle \\
\sigma_z \left|\odot\right\rangle &= \left|\otimes\right\rangle \\
\sigma_y \left|\rightarrow\right\rangle &= \bullet \left|\leftarrow\right\rangle \\
\sigma_y \left|\leftarrow\right\rangle &= \bullet \left|\rightarrow\right\rangle \\
\sigma_x \left|\otimes\right\rangle &= \bullet \left|\odot\right\rangle \\
\sigma_x \left|\odot\right\rangle &= \bullet \left|\otimes\right\rangle .
\end{aligned}$$

Fill in the values of $\bullet$.

To review from last time:

$$\begin{aligned}
\left|\psi\right\rangle &= \alpha \left|\uparrow\right\rangle + \beta \left|\downarrow\right\rangle \\
&= \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \\
\left\langle\psi\right| = \left|\psi\right\rangle^\dagger &= (\overline{\alpha} \, \overline{\beta})
\end{aligned}$$

Then

$$\begin{aligned}
\left\langle\psi\right| \sigma_z \left|\psi\right\rangle = (\overline{\alpha} \, \overline{\beta})\sigma_z \begin{pmatrix} \alpha \\ \beta \end{pmatrix} &= |\alpha|^2 - |\beta|^2 \\
&= p(\uparrow)(+1) + p(\downarrow)(-1).
\end{aligned}$$

Thus this equals the expected value of the spin (viewed as ±1) along the z-axis when the system is in the state $\left|\psi\right\rangle$. Colloquially, we write $\langle\sigma_z\rangle$ the "expectation value of z"; this is in fact the reason for the bra-ket notation.

§3.2 Higher Dimensions

In quantum mechanics in higher dimensions, say $\left|\psi\right\rangle \in \mathbb{C}^d$:

- the **observables** correspond to Hermitian matrices $A = A^\dagger$.
- the **outcomes** of measurements corresponding to A are the **eigenvalues** of A. We denote by $\left|i\right\rangle$ is the ith eigenvector of A with eigenvalue a_i. (id est $A\left|i\right\rangle = a_i \left|i\right\rangle$).

For example, the identity matrix id corresponds to not making an observation at all since the outcomes are all indistinguishable (all eigenvalues are 1).

Problem 3.2 (Homework 2.3)**.** Show that if $A = A^\dagger$ (meaning the matrix is Hermitian) then all eigenvalues a_i are real, and moreover if the eigenvectors corresponding to distinct eigenvalues are orthonormal, i.e. $\langle i \mid j\rangle = \delta_{ij}$ (Kronecker delta) if $a_i \neq a_j$.

Thus, suppose that we have a state

$$|\psi\rangle = \sum_{i=1}^{d} \psi_i |i\rangle$$

associated to the matrix A. Then the probability of observing a_i from A is $|\psi_i|^2 = p(i)$, and the expectation value of

$$\begin{aligned}
\langle\psi| A |\psi\rangle &= \left(\sum_j \overline{\psi} \langle j|\right) A \left(\sum_i \psi_i |i\rangle\right) \\
&= \sum_j \overline{\psi_j} \langle j| \sum_i \psi_i a_i |i\rangle \\
&= \sum_{i,j} \overline{\psi}_j \psi_i a_i \langle j|i\rangle \\
&= \sum_{i,j} \overline{\psi}_j \psi_i a_i \delta_{ij} \\
&= \sum_i |\psi_i|^2 a_i \\
&= \sum_i p(i) a_i \\
&= \langle A\rangle .
\end{aligned}$$

This is just the multivariable version of what we did earlier.

§3.3 Back to qubits

Recall that

$$\langle\psi|\psi\rangle = (\overline{\alpha}\ \overline{\beta}) \begin{pmatrix}\gamma \\ \delta\end{pmatrix} = \overline{\alpha}\gamma + \overline{\beta}\delta.$$

Definition 3.3. Define the **density matrix** corresponding to the state $|\psi\rangle$ to be $|\psi\rangle\langle\psi|$, which is a $d \times d$ matrix.

Remark 3.4. Density matrices are always denoted by the letter ρ.

Note that since the trace is invariant under cyclic permutations, we have

$$\langle\psi| A |\psi\rangle = \operatorname{Tr}(|\psi\rangle\langle\psi| A) = \operatorname{Tr}(\rho A).$$

Why introduce the density matrix? Density matrices allow mathematical description of states that are spin $|\rightarrow\rangle$ with probability $p_\uparrow$ or spin $|\leftarrow\rangle$ with probability $p_\downarrow$. Thus, we can now write

$$\rho = p_\uparrow |\uparrow\rangle\langle\uparrow| + p_\downarrow |\downarrow\rangle\langle\downarrow| .$$

Claim 3.5. If a system has probabilities $p_\uparrow$ and $p_\downarrow$ as above, then $\operatorname{Tr}(A\rho)$ gives the expectation value for outcomes of a measurement corresponding to A.

Indeed, consider probability distributions $\{p_i\}$ and $\{q_i\}$ for a random variable with outcomes a_i. Then

$$\langle A\rangle = p_0 \langle A\rangle_{p's} + p_1 \langle A\rangle_{q's}$$

where p_0 is the probability of getting the $\{p_i\}$ distribution and p_1 is the probability of getting the $\{q_i\}$ distribution.

For example,

$$\langle A \rangle = \operatorname{Tr}(\rho A) = p_\uparrow \operatorname{Tr}(\rho_\uparrow A) + p_\downarrow \operatorname{Tr}(\rho_\downarrow A) = p_\uparrow \langle\uparrow| A |\uparrow\rangle + p_\downarrow \langle\downarrow| A |\downarrow\rangle .$$

Example 3.6 (Fully Mixed State)

Suppose

$$\rho = \frac{1}{2}|\uparrow\rangle\langle\uparrow| + \frac{1}{2}|\downarrow\rangle\langle\downarrow| = \frac{1}{2}\begin{pmatrix}1\\0\end{pmatrix}(1\ 0) + \frac{1}{2}\begin{pmatrix}0\\1\end{pmatrix}(0\ 1) = \frac{1}{2}\mathrm{id}_2.$$

This is the so-called **fully mixed state**. One obtains the same result with y-up and y-down instead of x-up and x-down, and so on.

§3.4 More on Pauli matrices

Consider an arbitrary axis $\hat{\imath} = \begin{pmatrix} i_x \\ i_y \\ i_z \end{pmatrix}$, where $i_x^2 + i_y^2 + i_z^2 = 1$. We define the Pauli matrix for an arbitrary $\hat{\imath}$ by

$$\sigma_{\hat{\imath}} = i_x\sigma_x + i_y\sigma_y + i_z\sigma_z.$$

Problem 3.7 (Homework 2.4)**.** Show that $\sigma_{\hat{\imath}}^2 = \mathrm{id}$.

Now, recall the matrix exponential

$$e^A = \sum_k \frac{1}{k!}A^k.$$

Consider

$$e^{-i\theta/2\sigma}$$

where $\sigma^2 = \mathrm{id}$.

Problem 3.8 (Homework 2.5)**.** Show that

$$e^{-i\theta/2\sigma} = \cos(\theta/2)\mathrm{id} - i\sin(\theta/2)\sigma.$$

Fact 3.9. $e^{-i\theta/2\sigma_{\hat{\jmath}}}$ corresponds to rotation by θ about the $\hat{\jmath}$ axis.

§4 September 29, 2015

We say a state $|\psi\rangle$ is a **pure state**, versus a **mixed state** ρ represented by a density matrix.

Observe that pure state density matrices are idempotent, as

$$|\psi\rangle\langle\psi| \cdot |\psi\rangle\langle\psi| = |\psi\rangle\langle\psi|\psi\rangle\langle\psi| = |\psi\rangle\langle\psi| .$$

Problem 4.1 (Homework 3.1)**.** Let ρ be an operator (hence Hermitian with trace 1). Prove the converse, that

$$\rho^2 = \rho \implies \exists\psi : \rho = |\psi\rangle\langle\psi| .$$

Problem 4.2 (Homework 3.2)**.** If

$$\rho = p_\uparrow |\uparrow\rangle\langle\uparrow| + p_\downarrow |\downarrow\rangle\langle\downarrow|$$

then show that $\operatorname{Tr}\rho^2 = p_\uparrow^2 + p_\downarrow^2$.

§4.1 Multiple Qubits, and Tensor Products

Up til now the formalism has simply been bizarre, rather than pathological. However, multiple qubits are really going to be stranger. (Aside: why is quantum mechanics the way it is? Because the observations say so; no one really knows.)

Suppose we have two states A and B which are either ↑ and ↓ To do this, we introduce *tensor products.* (NB: after class, professor will post a guide to tensor products on website.)

Specifically, we consider a four-dimensional vector space $V_A \otimes V_B$ (where V_A and V_B are both $\mathbb{C}^2$) meaning we can consider elements such as $|\uparrow\rangle_A \otimes |\downarrow\rangle_B$; then flipping A about x-axis amounts to

$$(\sigma_x^A |\uparrow\rangle_A) \otimes |\downarrow\rangle_B = |\downarrow\rangle_A \otimes |\downarrow\rangle_B .$$

More generally, we can create linear operators $\operatorname{End}(V_A \otimes V_B)$ by simply taking $\operatorname{End}(V_A) \otimes \operatorname{End}(V_B)$, i.e. our linear operators are spanned by $T_1 \otimes T_2$ where $T_1 \in \operatorname{End}(V_A)$, $T_2 \in \operatorname{End}(V_B)$.

So, we can say "a tensor is a multilinear thing with slots that perches on a vector".

"Hope" is the thing with feathers -
That perches in the soul -
And sings the tune without the words -
And never stops - at all -

And sweetest - in the Gale - is heard -
And sore must be the storm -
That could abash the little Bird
That kept so many warm -

Ive heard it in the chillest land -
And on the strangest Sea -
Yet - never - in Extremity,
It asked a crumb - of me.

We can also take inner products; consider $||\rightarrow\rangle\rangle_B$ acting on the B slot. (Recall $|\rightarrow\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle + |\downarrow\rangle)$.) Thus, we have

$$|\psi\rangle_A \otimes \langle \rightarrow \mid \uparrow\rangle_B = \frac{1}{\sqrt{2}} |\uparrow\rangle_A .$$

Alternatively, we can write the tensor out explicitly in a basis, given vectors

$$\sum_i a_i |i\rangle_A \quad \text{and} \quad \sum_j b_j |j\rangle_B$$

which are vectors written in the $|i\rangle_A$ and $|j\rangle_B$ basis, their tensor is equal to

$$\sum_{i,j} a_i b_j \left(|i\rangle_A \otimes |j\rangle_B \right).$$

Similarly, we can view operators as matrices $C \otimes D$, which I won't write out.

§4.2 Basis Computation

Suppose we write a basis for $\mathbb{C}^2 \otimes \mathbb{C}^2$ by

$$|\uparrow\rangle_A \otimes |\uparrow\rangle_B = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad |\uparrow\rangle_A \otimes |\downarrow\rangle_B = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \quad |\downarrow\rangle_A \otimes |\uparrow\rangle_B = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \quad |\downarrow\rangle_A \otimes |\downarrow\rangle_B = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

Then it's trivial to verify that

$$\begin{aligned} \sigma_z^A \otimes \sigma_z^B &= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \\ \sigma_z^A \otimes \mathrm{id}^B &= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \\ \mathrm{id}^A \otimes \sigma_z^B &= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}. \end{aligned}$$

Of course, notice that $(\sigma_z^A \otimes \mathrm{id}^B)(\mathrm{id}^A \otimes \sigma_z^B) = (\sigma_z^A \otimes \sigma_z^B)$.

Problem 4.3 (Homework 3.3)**.** In the above basis, write out the 4×4 matrices corresponding to $\sigma_x^A \otimes \mathrm{id}^B$, $\mathrm{id}^A \otimes \sigma_x^B$, $\sigma_y^A \otimes \mathrm{id}^B$, $\mathrm{id}^A \otimes \sigma_y^B$, $\sigma_x^A \otimes \sigma_x^B$, $\sigma_y^A \otimes \sigma_y^B$, $\sigma_z^A \otimes \sigma_z^B$, $\sigma_x^A \otimes \sigma_y^B$, $\sigma_y^A \otimes \sigma_x^B$, $\sigma_y^A \otimes \sigma_z^B$.

§4.3 Entanglement

This is the central weirdness of quantum mechanics.

Consider the following element of the tensor product $\mathbb{C}^2 \otimes \mathbb{C}^2$:

$$|\Psi_-\rangle = \frac{1}{\sqrt{2}} |\uparrow\rangle_A \otimes |\downarrow\rangle_B - \frac{1}{\sqrt{2}} |\downarrow\rangle_A \otimes |\uparrow\rangle_B .$$

This is indeed normalized, because it has norm 1. We rewrite in the basis $|{\rightarrow}\rangle$ and $|{\leftarrow}\rangle$ as

$$\begin{aligned}|\Psi_-\rangle &= \frac{1}{\sqrt{2}}\frac{1}{\sqrt{2}}\left(|{\rightarrow}\rangle_A + |{\leftarrow}\rangle_A\right) \otimes \frac{1}{\sqrt{2}}\left(|{\rightarrow}\rangle_B - |{\leftarrow}\rangle_B\right) \\ &- \frac{1}{\sqrt{2}}\frac{1}{\sqrt{2}}\left(|{\rightarrow}\rangle_A - |{\leftarrow}\rangle_A\right) \otimes \frac{1}{\sqrt{2}}\left(|{\rightarrow}\rangle_B + |{\leftarrow}\rangle_B\right) \\ &= -\frac{1}{\sqrt{2}}\left(|{\rightarrow}\rangle_A \otimes |{\leftarrow}\rangle_B - |{\leftarrow}\rangle_A |{\rightarrow}\rangle_B\right).\end{aligned}$$

Ironically, this is the same result, with an overall phase of -1.

> "You could just write the answer? Ah, but not everyone is as swift as you. Mm? You trust me! It must still be early in the class."

Something is very pathological about this state $|\Psi_-\rangle$. If we make a measurement of the matrix A along the z-axis, then we know the spin of B along the z-axis. The same is true for measurements along the x-axis. So by solely looking at measurements on A, we can get information at B; this paradox is called *spooky action at a distance*, or in Einstein's tongue, *spukhafte Fernwirkung*. This is called **entanglement**

The state $|\Psi_-\rangle$ is called the **singlet state**.

Problem 4.4 (Homework 3.4)**.** Rewrite $|\Psi_-\rangle$ in the σ_y eigenbasis $|{\otimes}\rangle$, $|{\odot}\rangle$

Problem 4.5 (Homework 3.5)**.** Do again in the basis $|{\nearrow}\rangle$, $|{\swarrow}\rangle$.

§5 October 1, 2015

"Spooky action at a distance" is spooky but not at a distance. The idea: consider an entangled state such as the singlet state

$$|\Psi_-\rangle = \frac{1}{\sqrt{2}} \left(|{\uparrow}\rangle_A \otimes |{\downarrow}\rangle_B - |{\downarrow}\rangle_A \otimes |{\uparrow}\rangle_B \right).$$

In fact for any orthogonal basis (as we saw last time with x and y) it turns out that we have this entangled behavior. After an observation on A is made, then A's state is determined; thus, the state of B is known to A (i.e. A knows that B will get up or down). However, B does not know this information; A has no way of communicating this.

Anyways, more weird things:

§5.1 Triplet States

In addition to the singlet state, we have the three **triplet state**

$$|\Psi_+\rangle = \frac{1}{\sqrt{2}} \left(|{\uparrow}\rangle_A \otimes |{\downarrow}\rangle_B + |{\downarrow}\rangle_A \otimes |{\uparrow}\rangle_B \right).$$

We also define

$$\begin{aligned} |\Phi_+\rangle &= \frac{1}{\sqrt{2}}(|{\uparrow}\rangle_A \otimes |{\uparrow}\rangle_B + |{\downarrow}\rangle_A \otimes |{\downarrow}\rangle_B) \\ |\Phi_-\rangle &= \frac{1}{\sqrt{2}}(|{\uparrow}\rangle_A \otimes |{\uparrow}\rangle_B - |{\downarrow}\rangle_A \otimes |{\downarrow}\rangle_B). \end{aligned}$$

As the course goes on, we'll begin abusing notation more on more, for example simplifying $|\Phi_-\rangle$ to $\frac{1}{\sqrt{2}}(|{\uparrow\uparrow}\rangle - |{\downarrow\downarrow}\rangle)$ (thus omitting the A, B subscripts and the $\otimes$).

Problem 5.1 (Homework 3.6)**.** Rewrite each of the triplets in terms of the bases $\{|{\rightarrow}\rangle, |{\leftarrow}\rangle\}$ and $\{|{\otimes}\rangle, |{\odot}\rangle\}$. Identify the form of correlation along the x and y axes.

Problem 5.2 (Homework 3.7)**.** Find the result when $\sigma_z \otimes \sigma_z$ is applied to each of $|\Psi_-\rangle$, $|\Psi_+\rangle$, $|\Phi_-\rangle$, $|\Phi_+\rangle$.

Problem 5.3 (Homework 3.8)**.** Show that the singlet state is invariant (up to a global phase) under transformations of the form $U_A \otimes U_B$, where $U_A = \exp(-i\theta/2\sigma_{\hat{j}}^A)$ and $U_B = \exp(-i\theta/2\sigma_{\hat{j}}^B)$.

Problem 5.4 (Homework 3.9)**.** Show that the subspace of $\mathbb{C}^2 \otimes \mathbb{C}^2$ spanned by the triplet states is invariant under the same set of transformations.

§5.2 Group Theory Digression

In fact, the matrices $\exp(-i\theta/2\sigma_{\hat{j}})$ belongs to the group of special 2×2 unitary matrices, denoted $\mathrm{SU}(2)$. Here "special" means determinant 1, and unitary means $UU^\dagger = \mathrm{id}$. (Compare $\mathrm{SO}(3)$, the special orthogonal group in 3 real dimensions.)

Note $\sigma_x \notin \mathrm{SU}(2)$, since $\det \sigma_x = -1$.

In any case, given a group G, one can consider a faithful **representation** $G \to \mathrm{GL}(V)$, i.e. representing V by matrix groups. In this language, the triplet states span a three-dimensional **irreducible representation**, or **irrep** of $\mathrm{SU}(2)$. (In this language, the singlet state spans a one-dimensional irrep of $\mathrm{SU}(2)$.)

Remark 5.5. According to Lloyd: I think this is the best explanation of why quantum works. In QM we have unitary operators acting on complex vectors. Why? No one knows, but one explanation is that groups have symmetry. Things like the Schrödinger equation preserve the symmetry of translation, for example. Crudely, "the world has fundamental symmetries". The fundamental representations of these symmetry groups are things like SU(2), etc., so it should not be too surprising that things like SU(2) appear. The representation theory of groups kind of motivates this.

In short, quantum mechanics can be thought of as a manifestation of groups (reflecting the symmetry of the world) as unitary operators due to the purely mathematical work of representation theory.

§5.3 Measurement and reduced density matrices

Consider a state

$$|\psi\rangle = \sum_{i,j} \psi_{i,j} |i\rangle_A |j\rangle_B \in V_1 \otimes V_2$$

for finite dimensional spaces V_1, V_2 (which may not be qubits, so possibly dimension more than 2). Suppose we make a measurement on A alone, which we write as $M_A \otimes \mathrm{id}_B$. Thus the expected value of the output is

$$\begin{aligned}
\langle\psi|_{AB} M_A \otimes \mathrm{id}_B \,|\psi\rangle_{AB} &= \left(\sum_{i,j} \overline{\psi_{i,j}} \,\langle i| \otimes \langle j|\right) M_A \otimes \mathrm{id}_B \left(\sum_{i',j'} \psi_{i',j'} \,|i'\rangle \otimes |j'\rangle\right) \\
&= \sum_{i,j,i',j'} \overline{\psi_{i,j}} \psi_{i',j'} \langle i| M_A |i'\rangle \langle j| \mathrm{id}_B |j'\rangle \\
&= \sum_{i,j,i',j'} \overline{\psi_{i,j}} \psi_{i',j'} \langle i| M_A |i'\rangle \,\delta_{j,j'} \\
&= \sum_{i,j,i'} \overline{\psi_{i,j}} \psi_{i',j} \langle i| M_A |i'\rangle \\
&= \sum_{i,j,i'} \overline{\psi_{i,j}} \psi_{i',j} \,\mathrm{Tr}(\langle i| M_A |i'\rangle) \\
&= \sum_{i,j,i'} \overline{\psi_{i,j}} \psi_{i',j} \,\mathrm{Tr}(|i'\rangle \langle i| M_A) \\
&= \mathrm{Tr}(\sum_{i,j,i'} \overline{\psi_{i,j}} \psi_{i',j} \,|i'\rangle \langle i| M_A) \\
&= \mathrm{Tr}(\rho_A M_A).
\end{aligned}$$

where the subscripts A and B for $\langle i|$, $\langle j|$, $|i\rangle$, $|j\rangle$ have been left implicit, and

$$\rho_A \overset{\text{def}}{=} \sum_{i,i',j} \overline{\psi_{i,j}} \psi_{i',j} \,|i'\rangle \langle i|$$

is the **reduced density matrix** for A. This has the nice property that it depends only on the matrix A.

A key part of this class is learning how to compute ρ_A. Here is how. The idea is to use the **partial trace** [1]. For the purposes of this, if we write ψ_{AB} in the usual basis then

$$\mathrm{Tr}_B \sum_{i,i',j,j'} \overline{\psi_{i,j}} \psi_{i',j'} (|i'\rangle \otimes_A \langle i|) \otimes (|j'\rangle \otimes_B \langle j|) \overset{\text{def}}{=} \sum_{i,i',j,j'} \overline{\psi_{i,j}} \psi_{i',j'} (|i\rangle \otimes_A \langle i'|) \langle j|j'\rangle .$$

[1] See `https://en.wikipedia.org/wiki/Partial_trace`

Note this is an operator: the partial trace is a map $\operatorname{End}(\mathbb{C}^2 \otimes \mathbb{C}^2) \to \operatorname{End}(\mathbb{C}^2)$.

Problem 5.6 (Homework 3.10)**.** Compute the partial B trace of the four matrices $\left|\Psi_-\right\rangle\left\langle\Psi_-\right|$, $\left|\Psi_+\right\rangle\left\langle\Psi_+\right|$, $\left|\Phi_-\right\rangle\left\langle\Phi_-\right|$, $\left|\Phi_+\right\rangle\left\langle\Phi_+\right|$.

Problem 5.7 (Homework 3.11)**.** Let

$$\left|\psi\right\rangle_{AB} = \sqrt{\frac{2}{3}} \left|\uparrow\right\rangle_A \otimes \left|\downarrow\right\rangle_B - \frac{i}{\sqrt{3}} \left|\downarrow\right\rangle_A \otimes \left|\uparrow\right\rangle_B .$$

Compute the partial traces to A and B, respectively.

§6 October 6, 2015

Here and henceforth, tensor products are getting dropped at will.

This Thursday, Scott Aaronson is giving the guest lecture.

§6.1 CNOT Gate

Recall we had a CNOT gate from last time: in the basis we mentioned earlier $|0\rangle_A |0\rangle_B |0\rangle |0\rangle$, $|0\rangle |1\rangle$, $|1\rangle |0\rangle$, $|1\rangle |1\rangle$ then the corresponding unitary matrix U is

$$U_{\text{CNOT}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} \text{id} & 0 \\ 0 & \sigma_x \end{pmatrix}.$$

We saw we can use CNOT to copy a state if we know the state is either $|0\rangle$ or $|1\rangle$, for example

$$U_{\text{CNOT}} |x\rangle_A |0\rangle_B = |x\rangle_A |x\rangle_B .$$

§6.2 No-Cloning Theorem

It seems like copying is working just fine. However, suppose that now we have a probabilistic state

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle .$$

By linearity the image of $|\psi\rangle |0\rangle$ under U_{CNOT} is

$$\alpha |0\rangle |0\rangle + \beta |1\rangle |1\rangle .$$

This is an entangled state, and in fact not what we want: we really want $|\psi\rangle_A |\psi\rangle_B$, so we failed to clone the state $|\psi\rangle$.

In fact:

Theorem 6.1 (Baby No-Cloning Theorem)
Unitary operators cannot replicate qubits in the following sense: no unitary operator U can satisfy

$$U(|\psi\rangle |0\rangle) = |\psi\rangle |\psi\rangle .$$

Proof. First, note that unitary operators preserve the inner product, meaning

$$(\langle\phi| U^\dagger)(U |\psi\rangle) = \langle\phi|\psi\rangle$$

for any $|\phi\rangle$, $|\psi\rangle$.

Problem 6.2 (Homework 4.1)**.** Show that the converse is actually true too. That is, prove that if

$$(\langle\phi| U^\dagger)(U |\psi\rangle) = \langle\phi|\psi\rangle$$

for any $|\phi\rangle$, $|\psi\rangle$, then $U^\dagger U = \text{id}$, meaning U is unitary.

Now, assume for contradiction that

$$U(|\psi\rangle |0\rangle) = |\psi\rangle |\psi\rangle$$

for every ψ. Then in particular, we ought to have

$$(\langle\phi|_A \langle 0|_B)(|\psi\rangle_A |0\rangle_B) = (\langle\phi|_A \langle\phi|_B)(|\psi\rangle_A |\psi\rangle_B).$$

The left-hand side is $\langle\phi|\psi\rangle \langle 0|0\rangle = \langle\phi|\psi\rangle$ and the right-hand side is $\langle\phi|\psi\rangle \langle\phi|\psi\rangle$. These are clearly not equal in general. □

Problem 6.3 (Homework 4.2)**.** Show that no unitary can map

$$|\psi\rangle_A \otimes |0\rangle_B \otimes |0\rangle_C \mapsto |\psi\rangle_A \otimes |\psi\rangle_B \otimes |\text{junk}\rangle_C .$$

Here the "junk" is allowed to depend on ψ.

> My dad was a professor and claimed the following happened to him. He was giving a lecture and realized his pants were not zipped. Too embarrassed to re-zip them in the middle of lecture in front of everyone, he devises the following plan: in the middle of the lecture, he shouts "what's that out the window?" and while everyone is distracted he zips up his pants. All is well until he realizes that the students are still looking out the window; he looks outside and sees that there are two dogs screwing on the lawn outside.

§6.3 Entropy

The second law of thermodynamics concerns the entropy

$$S = -\sum_i p_i \log(p_i).$$

The quantum version of this, due to von Neumann:

$$\rho = \sum_i p_i |i\rangle \langle i| \implies S = -\operatorname{Tr}\rho\log\rho.$$

> Ah, calculus is just linear algebra anyways when you do it on Matlab!

Exercise 6.4. For unitary U we have $-\operatorname{Tr}(U\rho U^\dagger)\log(U\rho U^\dagger) = \operatorname{Tr}\rho\log\rho$.

So, entropy is "conversed"! Not too surprising in the quantum case, since U is reversible.

> . . . Luckily, I managed to make them reference my PhD thesis, because I was the referee. . . . there are probably several lessons there, but I don't know what they are.

§6.4 CNOT Again

One can check that CNOT does the following:

- $|{\rightarrow}\rangle_A |{\rightarrow}\rangle_B \mapsto |{\rightarrow}\rangle_A |{\rightarrow}\rangle_B$.
- $|{\rightarrow}\rangle_A |{\leftarrow}\rangle_B \mapsto |{\leftarrow}\rangle_A |{\leftarrow}\rangle_B$.
- $|{\leftarrow}\rangle_A |{\rightarrow}\rangle_B \mapsto |{\leftarrow}\rangle_A |{\rightarrow}\rangle_B$.
- $|{\leftarrow}\rangle_A |{\leftarrow}\rangle_B \mapsto |{\rightarrow}\rangle_A |{\leftarrow}\rangle_B$.

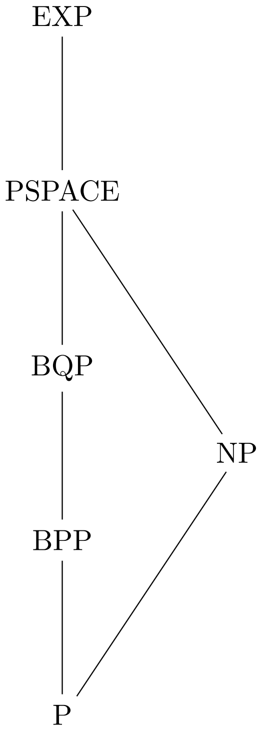
Problem 6.5 (Homework 4.3)**.** Repeat the above problem in the y-basis.

§7 October 8, 2015

> You can just put a Q in front of anything and ask what happens. . . this has been an effective strategy for generating papers for 20 years.

This is a guest lecture from Scott Aaronson. Thus all quotes from today are due to him, though they are possibly mangled by me.

Here is a hierarchy of complexity classes.



Here P has its usual meaning. BPP means "bounded-error probabilistic polynomial" which means polynomial runtime, but with a random source and such that the probability of outputting the correct answer is $\geq \frac{2}{3}$ (and hence by repeatedly running, arbitrarily close to 1).

> By the way, I apologize for the names. . . if we had been physicists we would have named them things like "quarks" or "black holes"

For example, it turns out that prime testing is BPP. But factoring is not known to be in P. For example, RSA depends on this.

In fact,

Conjecture 7.1. BPP is not P.

In fact, in the 1970's we showed that assuming Extended Riemann Hypothesis, testing primality is P. Unconditionally, we have a deterministic $n^{\log\log\log n}$ time for testing primes until about 2002, when the AKS algorithm was finally exhibited.

The NP means "nondeterministic polynomial time", which means that certificates can be checked in polynomial time. For example, factoring N is NP, because given the answer $p_1, \dots, p_n$ we can easily check whether $N = p_1 \dots p_n$ and whether each p_i is prime. On the other hand, actually finding a factorization is hard.

> I like to say that if we were physicists, we would have declared this [P $\neq$ NP] to be a law of nature . . . but we're mathematicians, so we have to call it a conjecture.

We also can consider NP-hard, NP-complete. Computational complexity theory took off in the 1970's when it turned out that tons and tons of NP problems are actually NP-complete.

> I think the Legend of Zelda is actually above NP complete, it's PSPACE-complete. . . . Pretty much any NP problem will be NP-complete unless it has a reason to be. That's sort of the rule of thumb.

Surprisingly, factoring is NP but not NP-hard. Factoring has "loads and loads of special properties" that make it different from the other NP problems. In fact, given P $\neq$ NP we know there must be NP problems which are not NP-complete; it seems like factoring might be such an example.

Actually, we know how to base cryptography on the factoring problem, and not on any other NP problem.

Other properties of factoring that make it special: Unlike e.g. Travelling Salesman, every number does have a unique prime factorization. So factoring has certificates even for "no" answers: in the question "does n have a prime factor ending in 7?" even the "no" answer can be verified in polynomial time.

Then we have BQP, which means "bounded-error quantum polynomial". We actually have a theorem

Theorem 7.2 (Simon)

There exists an oracle A such that BPP with oracle A is weaker than BQP with oracle A.

This was actually rejected from a major theoretical CS conference, but Peter Shor looked at this and exhibited the oracle A: modular exponentiation. Except we actually know what the oracle does! So in other words, Shor showed that the factoring problem is in BQP.

In particular, assuming factoring is not in BPP, then BQP is larger than BPP; quantum computers are stronger than classical ones.

PSPACE is the set of all decision problems that can be solved by a Turing machine using a polynomial amount of *space*; given $P(n)$ states, we have at most $2^{P(n)}$ time (by the way a Turing machine works) and so PSPACE is contained in EXP.

It has been shown that BQP is contained in PSPACE. (One can show "by hand" that BQP is in EXP by considering exponential vectors.) Thus, we can simulate a quantum computer in a classical one that, even if it requires exponential time, still uses a polynomial amount of memory.

In fact, it is open whether P is PSPACE.

By PSPACE, none of the probabilistic things make a difference: BPSPACE, BPPSPACE, BQPSPACE, NPSPACE are all the same.

It is also open whether NP is contained in BQP. However, it's been shown there exists an oracle A such that $\text{NP}^A \not\subset \text{BQP}^A$.

On the other hand, we can ask whether BQP is contained in NP: i.e. are there problems that quantum computers can solve but classical computers cannot even verify certificates to? This is open, but we actually suspect that such a problem might exist.

> For me, the biggest reason to do this [to build a quantum computer] is to disprove all the people who said it was impossible.

So far, as a couple of months ago, we have a simulation with six photons.

That being said, there exist conjectures which everyone believed to be true, with oracle-based evidence, and ended up being completely wrong. An example is interactive proofs, which people originally thought to be NP, but turns out to actually be PSPACE. For concreteness, suppose a super-intelligent being has solved the game chess. Not only does the alien want to just beat you at chess, it wants to prove to you that it knows how to play chess perfectly. To do this, it suffices to transform chess into an equivalent game (e.g. polynomials over a finite field) in which we "might as well" play randomly (i.e. for Black, playing randomly is an optimal strategy; no move gives Black an advantage). Then if the alien can always win on the equivalent game, this convinces us that the alien can play chess properly.

§8 October 15, 2015

> (Paraphrased) I asked the Chair "how do I get tenure?", and he responded, "well, just be the best person in the world in your field", which was very easy for me, because at the time I was the *only* person in the world in my field.

To cover:

- Deutsch-Jozsa Algorithm (first nontrivial quantum algorithm which gives a speed-up over physical computers)
- Quantum weirdness — Greenberger-Horne-Zeilinger state
- Quantum teleportation and super-dense coding

§8.1 Deustch-Jozsa

First, consider functions $f : \{0,1\} \to \{0,1\}$. There are $2^2 = 4$ such functions:

- Two constant functions, and
- Two **balanced** functions $x \mapsto x$ and $x \mapsto \neg x$. By balanced we mean that $|f^{-1}(0)| = |f^{-1}(1)|$.

More generally, 2^{2^m} functions from m bits to $\{0,1\}$.

Now, consider a box

$$(x,y) \overset{\boxed{f}}{\mapsto} (x, f(x) + y \mod 2).$$

Problem 8.1 (Homework 5.1)**.** Show that $\boxed{f}$ is reversible even if $f(x)$ is not, and exhibit its inverse.

Classically: given such a circuit $\boxed{f} : \{0,1\}^2 \to \{0,1\}$ as above, we need to use this box twice in order to decide for sure whether f is constant or balanced (just input 0 or 1).

More generally, if we have m-bit inputs, then we clearly require

$$2^{m-1} + 1$$

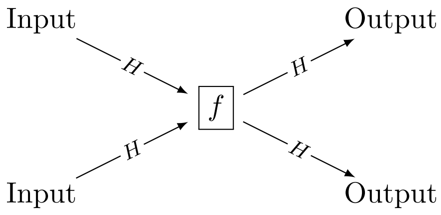
queries in order to prove that f is constant/balanced, since in the worst case we could get the same output 2^{m-1} times.

However, we're going to show that with a *quantum* computer we can do this with just a *single* function call. Let's just do the case $f : \{0,1\} \to \{0,1\}$. Consider the Hadamard matrix

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

which sends $|0\rangle$ to $|{\rightarrow}\rangle$ and $|1\rangle$ to $|{\leftarrow}\rangle$. Observe that $H^2 = \mathrm{id}$.

Let's interpret this as an H gate: so consider the circuit



One might write this as the function

$$(H \otimes H) \circ \boxed{f} \circ (H \otimes H).$$

We fix the inputs $|0\rangle$ and $|1\rangle$, as follows:

$$\begin{tikzcd}
|0\rangle \arrow[dr, "H"] & & \text{Output} \\
& \boxed{f} \arrow[ur, "H"] \arrow[dr, "H"] & \\
|1\rangle \arrow[ur, "H"] & & \text{Output}
\end{tikzcd}$$

We claim that from the outputs of this, we can tell whether f is constant or balanced. There are about four cases to consider.

- If $f \equiv 0$, then f is identity, we check that the result is $|0\rangle$ and $|1\rangle$.
- If $f \equiv 1$, we have

  $$|0\rangle \xmapsto{H} |\rightarrow\rangle \xmapsto{\boxed{f}} |\rightarrow\rangle \xmapsto{H} |0\rangle$$

  $$|1\rangle \xmapsto[H]{} |\leftarrow\rangle \xmapsto{\boxed{f}} -|\leftarrow\rangle \xmapsto[H]{} -|1\rangle$$

  In summary, if f is constant then

  $$(|0\rangle, |1\rangle) \xmapsto{(H\otimes H)\circ\boxed{f}\circ(H\otimes H)} (|0\rangle, |1\rangle)$$

- If f is id, one can check that we get

  $$(|0\rangle, |1\rangle) \xmapsto{(H\otimes H)\circ\boxed{f}\circ(H\otimes H)} (|1\rangle, |0\rangle)$$

In fact, more generally, one check that for $x \in \{0,1\}$ we have

$$|x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \xmapsto{\boxed{f}} |x\rangle \otimes \frac{1}{\sqrt{2}}(|0 + f(x)\rangle) - |x\rangle \otimes \frac{1}{\sqrt{2}}(|1 + f(x)\rangle).$$

Problem 8.2 (Homework 5.2)**.** Consider $f : \{0,1\}^m \to \{0,1\}$ now, and define $\boxed{f} : \{0,1\}^{m+1} \to \{0,1\}^{m+1}$ defined by

$$(x_1, \dots, x_m, y) \xmapsto{\boxed{f}} (x_1, \dots, x_m, y + f(x_1, \dots, x_m)).$$

Show that inputting $|0\rangle \otimes \cdots \otimes |0\rangle \otimes |1\rangle$ into the circuit

$$H^{\otimes m+1} \circ \boxed{f} \circ H^{\otimes m+1}$$

is enough to determine whether f is constant or balanced. Possible hint: show that $\boxed{f}$ sends $|x_1\rangle \otimes \cdots \otimes |x_m\rangle \otimes |\leftarrow\rangle)$ to $(-1)^{f(x_1,\dots,x_m)} |x_1\rangle \otimes \cdots \otimes |x_m\rangle \otimes |\leftarrow\rangle)$.

§8.2 Greenberger-Horne-Zeilinger Paradox

Take the state

$$|\Psi\rangle_{\text{GHZ}} = \frac{1}{\sqrt{2}} \left(|0\rangle_A |0\rangle_B |0\rangle_C - |1\rangle_A |1\rangle_B |1\rangle_C \right).$$

Consider the following set of measurements:

$$\sigma_y^A \otimes \sigma_y^B \otimes \sigma_x^C, \quad \sigma_y^A \otimes \sigma_x^B \otimes \sigma_y^C, \quad \sigma_x^A \otimes \sigma_y^B \otimes \sigma_y^C, \quad \sigma_x^A \otimes \sigma_x^B \otimes \sigma_x^C.$$

Problem 8.3 (Homework 5.3)**.** (a) Show that

$$\langle\Psi|_{\text{GHZ}} \, \sigma_x^A \otimes \sigma_x^B \otimes \sigma_x^C \, |\Psi\rangle_{\text{GHZ}} = -1.$$

(Possible hint: $\sigma_x^A \otimes \sigma_x^B \otimes \sigma_x^C \, |\Psi\rangle_{\text{GHZ}} = - |\Psi\rangle_{\text{GHZ}}$.)

(b) Show that

$$\langle\Psi|_{\text{GHZ}} \, \sigma_y^A \otimes \sigma_y^B \otimes \sigma_x^C \, |\Psi\rangle_{\text{GHZ}} = 1.$$

(Possible hint: same trick as before.)

Something is weird about this. Let $S_X^A = \{\pm 1\}$ be the result of measuring by σ_x^A on the state, and define other variables similarly. Thus the possible results are $S_y^A S_y^B S_x^C$, $S_y^A S_x^B S_y^C$, $S_x^A S_y^B S_x^C$, $S_x^A S_x^B S_x^C$, with each variable being ±1, and with product $(-1)^3 \cdot 1 = -1$. However, the product of them all is 1, because of the squares!

What this means is that the values of the observations do not exist beforehand; in some sense they are "created" at the time of measurement.

§9 October 20, 2015

Today: superdense coding, and teleportation (plus time travel).

§9.1 Superdense Coding

This is quantum communication.

Assume Alice is trying to communicate with Bob by sending qubits. For every qubit Alice sends across a channel, it's been shown Bob can receive at most one bit of classical information.

But now suppose that Alice and Bob additionally both possess access to an entangled state

$$|\Psi_-\rangle_{AB} = \frac{1}{\sqrt{2}} \left(|0\rangle_A |1\rangle_B - |1\rangle_A |0\rangle_B \right).$$

We say they have one **e-bit** of shared entanglement.

We now claim that if Alice and Bob possess one e-bit, then Alice can send a qubit to transmit two classical bits. Note that Alice can transform $|\Psi_-\rangle_{AB}$ into any of the triplet states by acting on exactly one qubit, since

- Do nothing to get $|\Psi_-\rangle_{AB}$,
- Do σ_x^A to get $|\Phi_-\rangle_{AB}$,
- Do σ_z^A to get $|\Psi_+\rangle_{AB}$,
- Do σ_y^A to get $|\Psi_-\rangle_{AB}$.

Thus, the algorithm is:

- Perform an operation on the entangled state, and then
- Send her half of the entangled pair to Bob.

From here Bob recovers the qubits in his basis.

§9.2 Quiz Warmup

Problem 9.1 (Quiz Warmup 1)**.** Show how to do superdense coding when the initial entangled state is one of the other triplet states.

Problem 9.2 (Quiz Warmup 2)**.** Construct a quantum logic circuit (using single qubit rotations, one Hadamard, and one CNOT) that maps inputs $|0\rangle|0\rangle$, $|0\rangle|1\rangle$, $|1\rangle|0\rangle$, $|1\rangle|1\rangle$ to outputs $|\Psi_-\rangle_{AB}$, $|\Psi_+\rangle_{AB}$, $|\Phi_-\rangle_{AB}$, $|\Phi_+\rangle_{AB}$. (Hint: use Hadamard once, then feed into CNOT.)

Problem 9.3 (Quiz Warmup 3)**.** Show that the reverse circuit to the one in the previous problem allows one to distinguish between the two states.

> "The NSA would prefer for it not be possible to build a quantum computer. . . On the other hand, if it is possible to build a quantum computer, we would like the first one."

§9.3 Teleportation

Alice and Bob again share an entangled state $|\Psi_-\rangle_{AB}$. Moreover, Alice has a state $|\phi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$. The **Bell basis** of $\mathbb{C}^2 \otimes \mathbb{C}^2$ consists of the singlet and triplet state.

Now, Alice measures $|\phi\rangle_A$ and the first half of her entangled state, in the Bell basis, to get two classical bits k. Then, Bob will be able to recover the state $|\psi\rangle$ up to global base by applying a certain transformation U_k (depending on k).

Let $|\phi\rangle = (\alpha\,|0\rangle_B + \beta\,|1\rangle_B$. The key is the identity

$$\begin{aligned}
2\sqrt{2}\cdot(\alpha\,|0\rangle + \beta\,|1\rangle) \otimes |\Psi_-\rangle_{AB} =& (|0\rangle\,|1\rangle_A - |1\rangle\,|0\rangle_A) \otimes (\alpha\,|0\rangle_B + \beta\,|1\rangle_B) \\
&+ (|0\rangle\,|0\rangle_A - |1\rangle\,|1\rangle_A) \otimes (\alpha\,|0\rangle_B + \beta\,|1\rangle_B) \\
&+ (|0\rangle\,|0\rangle_A + |1\rangle\,|1\rangle_A) \otimes (\alpha\,|0\rangle_B + \beta\,|1\rangle_B) \\
&+ (|0\rangle\,|1\rangle_A + |1\rangle\,|1\rangle_A) \otimes (\alpha\,|0\rangle_B + \beta\,|1\rangle_B) \\
=& |\Psi_-\rangle *A \otimes \phi_B \\
&+ |\Phi_+\rangle *A \otimes -i\sigma_y^B \phi_B \\
&+ |\Phi_-\rangle *A \otimes \sigma_x^B \phi_B \\
&+ |\Phi_+\rangle *A \otimes \sigma_z^B \phi_B
\end{aligned}$$

Problem 9.4 (Quiz Warmup 4)**.** Verify this.

Thus, we can now use "spooky action at a distance". Specifically, Alice makes a measurement, and

- If she observes $|\Psi_-\rangle$, tells Bob to do nothing.
- If she observes $|\Phi_-\rangle$, tells Bob to apply σ_x.
- If she observes $|\Phi_+\rangle$, tells Bob to apply σ_y.
- If she observes $|\Psi_+\rangle$, tells Bob to apply σ_z.

§10 November 3, 2015

§10.1 Fast Fourier Transformation

Let $f(x)$ be a function from n bits to n bits. Then we can consider a discrete FFT which transforms $f(x)$ to

$$g(y) = \sum_{x=0}^{2^n-1} \exp\left(2\pi i xy/2^n\right)$$

The Fast Fourier Transform takes time $O(n2^n)$. Equivalently if $N = 2^n$ is the number of states then this is $O(N \log N)$ time.

Problem 10.1 (Homework 6.1)**.** Suppose $f(x) = e^{-i\omega x}$. What is the (discrete) fast Fourier transform of f?

§10.2 Quantum Fourier Transformation

The quantum Fourier transform (QFT) takes wave functions over n qubits to wave functions over n qubits as follows. Consider a function $f : \{0, \dots, 2^n - 1\} \to \mathbb{C}$ such that $\sum_x |f(x)|^2 = 1$ (normalization). The wave function is represent by

$$|\psi\rangle = \sum_{x=0}^{2^n-1} f(x) |x\rangle$$

and its **quantum Fourier transform** is defined as

$$|\psi\rangle \mapsto \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} \sum_{y=0}^{2^n-1} \exp\left(2\pi i xy/2^n\right) f(x) |y\rangle$$

which can be rewritten as

$$\frac{1}{2^{n/2}} \sum_{y=0}^{2^n-1} g(y) |y\rangle .$$

The factor $2^{-n/2} = 1/\sqrt{N}$ is another normalization factor. We will see this takes $O(n^2) = O(\log N)$ time to produce. But it would still take $O(2^n)$ time to actually extract the coefficient in front of each basis $|y\rangle$.

This speed up is the key to good quantum algorithms: almost every quantum algorithm uses this in some way.

Problem 10.2 (Homework 6.2)**.** Show that the quantum Fourier tranform is unitary.

Problem 10.3 (Homework 6.3)**.** Show that the inverse QFT is given by

$$\sum_y g(y) |y\rangle \mapsto \frac{1}{2^{n/2}} \sum_{x,y} \exp(-2\pi i xy/2^n) g(y) |x\rangle .$$

We now take the time to write $x = x_n x_{n-1} \dots x_2 x_1$ in binary.

Problem 10.4 (Homework 6.4)**.** Expressing x binary notation, show that this is equivalent to

$$\begin{aligned} |x_n x_{n-1} \dots x_1\rangle \mapsto \frac{1}{2^{n/2}} & \left(|0\rangle + \exp(2\pi i \cdot 0.x_1) |1\rangle\right) \\ & \otimes \left(|0\rangle + \exp(2\pi i \cdot 0.x_2 x_1) |1\rangle\right) \\ & \otimes \dots \\ & \otimes \left(|0\rangle + \exp(2\pi i \cdot 0.x_n \dots x_1) |1\rangle\right) \end{aligned}$$

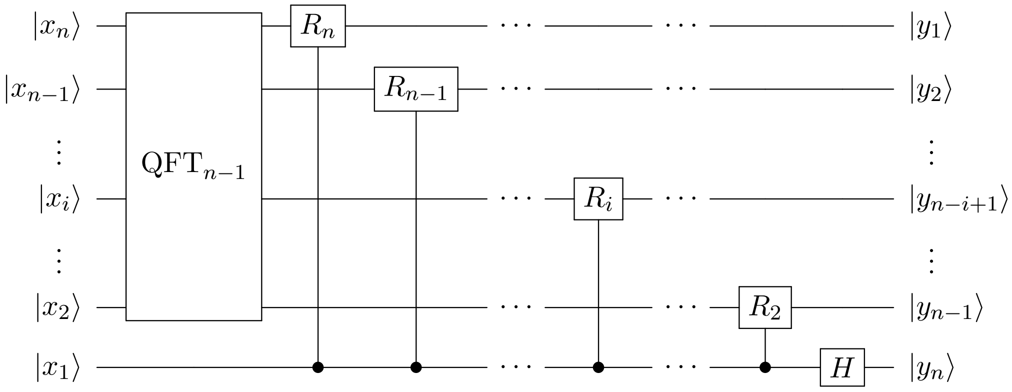
§10.3 The Circuit

We now draw the actual quantum circuit for the quantum Fourier Transform. Here it is for three qubits, just for concreteness.

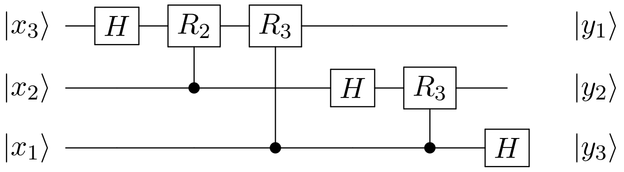
Abbreviating the controlled rotation

$$R_k = \begin{pmatrix} 1 & 0 \\ 0 & \exp(2\pi i/2^k) \end{pmatrix}$$

we can write the circuit (like Wikipedia does) as



If we write out the circuit explicitly for $n = 3$, we can rearrange the wires to give the more intuitive diagram



This was the diagram which was drawn in class; note that it's upside-down in comparison to the one given by Wikipedia. Use this one for the following homework problem:

Problem 10.5 (Homework 6.5)**.** Verify this works using the content of Homework 6.4.

§11 November 5, 2015

Problem 11.1 (Homework 6.6)**.** Show that

$$\mathrm{QFT}(|00\dots0\rangle) = \frac{1}{2^{n/2}} \sum_{x=0\dots0}^{1\dots1} |x\rangle .$$

Some digressions:

> "I do not recommend taking the exam on psilocybin, even if you are from Senior House"
>
> "There are a bunch of theorems of this form, due to me...why was that funny?"

§11.1 Digression on Flipping Bits

How much energy is required to flip a qubit?

For the classical case, most of the "loss of energy" takes place when we flip bits. There is a minimum amount of energy we need to dissipate to erase a bit, but currently our classical computers take much more energy than this. Specifically,

- A bit 0 has energy $E_0 = 0$, and
- A bit 1 has energy $E = \frac{1}{2}cv^2$.

So to erase a bit, $E_1 = \frac{1}{2}cv^2$ energy gets thermalized. This is $\gg k_B T \log 2$, the theoretical minimal threshold.

In qubits, a $|0\rangle$ has energy $E_0 = 0$ and a $|1\rangle$ has energy $E_1 = \hbar\omega$.

Now, consider a state

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + \exp(-i\omega t)\,|1\rangle).$$

We define the Hamiltonian

$$H = \frac{\hbar\omega}{2}(\mathrm{id} + \sigma_z).$$

This is contrived so that $H\,|0\rangle = 0$ and $H\,|1\rangle = \hbar\omega$. Then the expectation of E is

$$\langle E\rangle = \langle\psi|H|\psi\rangle$$

and the standard deviation is

$$\Delta E^2 = \langle\psi|H^2|\psi\rangle - (\langle\psi|H|\psi\rangle)^2$$

which is the "uncertainty in energy". The time to flip is

$$t = \pi/\omega = \frac{\pi\hbar}{E_1} = \frac{\pi\hbar}{2\,\langle E\rangle} = \frac{\pi\hbar}{2\Delta E}.$$

Theorem 11.2

The minimum time δt required to flip a qubit (take a quantum system from a state $|\psi(0)\rangle$ to an orthogonal state $|\psi(\Delta t)\rangle$) obeys

$$\langle E\rangle\,\Delta t \ge \frac{\pi\hbar}{2} \qquad \Delta E \Delta t \ge \frac{\pi\hbar}{2}.$$

§11.2 Atomic Clocks

Given an atom (say cesium) evolving according to the state

$$\frac{1}{\sqrt{2}}(|0\rangle + \exp(-i\omega t)\,|1\rangle)$$

according to t. This has only one bit of information, so it's not a terribly useful clock yet.

We add in an *oscillator* with frequency $\omega \approx \omega_0$ and we can count the number of oscillations at 10 GhZ, say. So the oscillator is the clock, but the atoms are providing the feedback: it will detect how much ω is drifting, and correct for this.

So starting with the state $|\uparrow\rangle$,

- Apply the oscillator field to rotate the spin to $|+\rangle$ in the co-rotating frame
- Wait for some time t
- Rotate back to $|\uparrow\rangle$
- Check to see if the state we get is actually $|\uparrow\rangle$, and if not how much it deviates. More precisely $\omega \neq \omega_0$ then spin is off by an angle $\Delta\theta = \Delta\omega \cdot t$.

§12 November 10, 2015

§12.1 Synopsis

Consider a unitary operator

$$U = \sum_j \exp(i\varphi_j) \left|j\right\rangle \left\langle j\right|$$

where $\left|j\right\rangle$ are eigenvectors of U and $\exp(i\varphi_j)$ are the eigenvalues.

Problem 12.1 (Homework 7.1)**.** Show $U^{-1} = U^\dagger$.

The **quantum phase algorithm** allows one to decompose an arbitrary vector $\left|\psi\right\rangle = \sum_j \psi_j \left|j\right\rangle$ into eigenvectors of U and find the corresponding eigenvalues.

In particular, the quantum phase algorithm will take

$$\sum_j \psi_J \left|j\right\rangle \left|0\dots 0\right\rangle = \left|\psi\right\rangle \left|0\dots 0\right\rangle \mapsto \sum_j \psi_j \left|j\right\rangle \left|\tilde{\varphi_j}\right\rangle$$

where there are n ancilla bits $\left|0\dots 0\right\rangle$. The $\tilde{\varphi_j}$ are estimates to φ_j, up to n bits of precision.

Fact 12.2. Any unitary operator can be written as $U = \exp(iA)$ where $A = A^\dagger$ is Hermitian and thus

$$U^\dagger = e^{-iA^\dagger} = e^{-iA}.$$

§12.2 The Quantum Phase Algorithm

Suppose we have U as described above (operating on m qubits). So of course

$$U^k \left|j\right\rangle = \exp(ik\varphi_j) \left|j\right\rangle.$$

First, assume $\left|\psi\right\rangle = \left|j\right\rangle$. The input is initially

$$\left|j\right\rangle \otimes \left|0\dots 0\right\rangle.$$

After the Hadamard, we have

$$\frac{1}{\sqrt{2^n}} \left|j\right\rangle \otimes \sum_{k=0}^{2^n-1} \left|k\right\rangle.$$

The controlled operators (applying depending on whether the bit fed into them is 0 or 1) then gives

$$\frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} \exp(ik\varphi_j) \left|j\right\rangle \otimes \left|k\right\rangle.$$

Discard the $\left|j\right\rangle$ now, to get

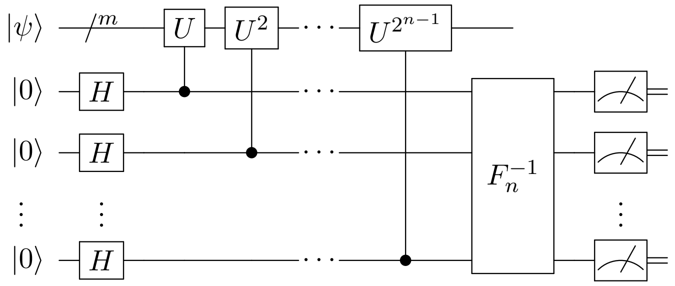
$$\frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} \exp(ik\varphi_j) \left|k\right\rangle.$$

This is a wave function, so we can extract the phase using the inverse quantum Fourier transform, and obtain

$$\frac{1}{2^n} \sum_{k,\ell} [\exp(2\pi ik \cdot (\varphi_j/2\pi - \ell/2^n)] \left|\ell\right\rangle.$$

Intuitively, we get $\approx |2^n \frac{\varphi_j}{2\pi}\rangle$. If $\ell/2^n = \varphi_j/2\pi$, then this isolates the specific phase: roots of unity filter.

In summary, the circuit is



Problem 12.3 (Homework 7.2, for Graduate Students)**.** Construct the output of the quantum phase estimation when $\frac{\varphi_j}{2\pi} \notin \frac{1}{2^n}\mathbb{Z}$ and provide a formula for the expected error in estimating $\frac{\varphi_j}{2\pi}$.

Note that classically, to find the eigenvectors/eigenvalues of a $2^n \times 2^n$ matrix takes $O(2^{3n})$ time. But in quantum it only takes $O(n^2)$ time.

§13 November 12, 2015

§13.1 Shor's Algorithm

Let $N = pq$ where p and q are prime numbers.

> "...aftertaste of burnt copper and arsenic ..."

> "You just bought 2 tons of nitrogen fertilizer . . . people who bought this product also purchased these detonators."

Problem 13.1 (Homework 7.3)**.** Read up (e.g. Wikipedia) on RSA and be prepared to discuss how it works.

> "of course I'm going to look at people and see who's sweating..."

Shor used QFT to find p, q given N; there is a hidden periodicity in factoring that can be revealed using the quantum Fourier transform.

The first step is to transform factoring into the discrete logarithm problem: given N and x, find the smallest r such that $x^r \equiv 1 \pmod N$ (i.e. compute the order of $x \pmod N$).

We claim discrete logarithms let us do factoring. Pick x, say $x = 17$. After ensuring that $\gcd(x, N) = 1$ (otherwise, done), we use a quantum circuit.

So we have the following periodicity: if $x^r \equiv 1 \pmod N$ then $x^{ar} \equiv 1 \pmod N$. So we pick n such that $N^2 < 2^n < 2N^2$, and construct the state

$$\frac{1}{\sqrt{2^n}} \sum_{k=0\dots0}^{1\dots1} |k\rangle\,|0\rangle$$

and then compute

$$\frac{1}{\sqrt{2^n}} \sum_{k=0\dots0}^{1\dots1} |k\rangle\,|x^k \mod N\rangle$$

Anyways, $x^k \pmod N$ is periodic in k with period r. The quantum Fourier transform then lets us find r.

§14 November 17, 2015

Shor's algorithm uses a quantum computer on the **hidden subgroup problem** of determining the order of a given $x \pmod N$.

§14.1 Graph Isomorphism Problem

Let G and H be graphs of the same order n. Encode $|G\rangle$, $|H\rangle$. We can try to construct

$$\frac{1}{\sqrt{n!}} \sum_{\pi} |\pi(G)\rangle$$

and compare it to $\frac{1}{\sqrt{n!}} \sum_{\pi} |\pi(H)\rangle$. Unfortunately, it turns out we can only construct

$$|\psi_G\rangle_{AB} = \frac{1}{\sqrt{n!}} \sum_{\pi \in S_n} |\pi\rangle_A |\pi(G)\rangle_B$$

and the corresponding $|\psi_H\rangle_{AB}$.

Problem 14.1 (Homework 8.1)**.** What are the reduced density matrices for A and B above? In particular, does $\rho_B^G = \rho_B^H$? If so, why doesn't this provide a solution to graph isomorphism?

> Problems worthy of attack prove their worth by hitting back.

§14.2 Shor's Algorithm

Suppose we wish to factor N. Pick n so that $N^2 < 2^n < 2N^2$, and by modular exponentiation obtain the state

$$\frac{1}{\sqrt{2^n}} \sum_k |x\rangle \left|x^k \bmod N\right\rangle .$$

This takes $O(n^3)$ time, starting from $\frac{1}{\sqrt{2^n}} \sum_k |x\rangle |0\rangle$.

Suppose we make a measurement on the second register and get some value z for the second register. The entanglement goes away, and we obtain

$$\sum_{\substack{k \\ x^k \equiv z}} |k\rangle |z\rangle .$$

Thus, we get k_0, $k_0 + r$, $\dots$, or something. (The measurement of z is actually irrelevant.)

Now we discard the second register. Then the quantum Fourier transform gets us r. Thus using QFT on the first register, we arrive at

$$\frac{1}{2^n} \sum_{j,\ell} \exp\left(2\pi i \cdot \frac{j(k_0 + \ell r)}{2^n}\right) |j\rangle$$

For any fixed j the coefficient of $|j\rangle$ is positive if and only if $\frac{jr}{2^n}$ is close to an integer.

So, by measurement, we obtain a value of j such that $jr/2^n \approx s$, (here $s \in \mathbb{Z}$ is unknown, and $r \in \mathbb{Z}$ is what we want). Thus

$$\frac{j}{2^n} \approx \frac{s}{r}.$$

But $r < N$. So you can use continued fractions to compute both s and r, since $j/2^n$ is known.

Problem 14.2 (Homework 8.2)**.** Find continued fractions for e, π, $\sqrt{2}$. Construct the first five truncated rational approximations.

§15 November 24, 2015

§15.1 Sparse matrix completion

Problem: consider Netflix with N movies and M viewers. We want to "complete" the matrix A from incomplete information (ratings); this is *sparse matrix completion.*

Classical algorithms take $\text{poly}(MN)$ time while the quantum algorithm takes $(\log(MN))^2$ time.

Assume data is stored in quantum random access memory, in form

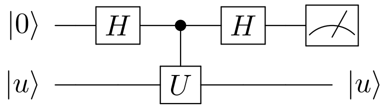
$$\begin{pmatrix} 0 & A \\ A^\dagger & 0 \end{pmatrix}.$$

We use phase estimation to find eigenvectors and eigenvalues, and claim there are only a few large eigenvalues. Intuitively each eigenvector with large eigenvalue is a "genre". Principal components of matrix.

Suppose your stated preferences are $\vec{b}^+ = (\dots)$. Apply quantum phase algorithm to decompose $\vec{b}$ in terms of principal components of $\tilde{A}$. Project $\vec{b}$ onto a superposition of movies in the same genre; then a measurement yields a movie, where movies liked by people have higher associated probability.

§15.2 Homework Problems

Problem 15.1 (Homework 9.1)**.** (Poor man's phase algorithm) Let U be unitary with eigenvector $|u\rangle$; thus $U|u\rangle = \exp(i\varphi)|u\rangle$. Consider the circuit



(1) We measure the top in the $|0\rangle$, $|1\rangle$ basis. Find the probability of obtaining $|1\rangle$.

(2) How many times do you have to repeat to estimate U to accuracy ε? (To be clear: we want the standard deviation of the Gaussian distribution to be ε.)

Both answers depend on φ.

Problem 15.2 (Homework 9.2)**.** Show that the controlled U operation

$$V = |0\rangle\langle 0| \otimes \text{id} + |1\rangle\langle 1| \otimes U$$

is unitary. (Show that $V^\dagger V = \text{id}$.)

§15.3 Grover's Algorithm

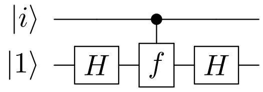
Unstructured database search. There are n items labeled $\{0, 1, \dots, n-1\}$ one of which is marked, say w. How many items do you have to sample to get it? Classically, in the worst case we need $n-1$ samples to deduce it and $n/2$ times to get a $\frac{1}{2}$ success rate.

For quantum algorithm, $\sqrt{n}$.

Indeed, classically we can test in the form

$$i \mapsto f(i) \equiv \begin{cases} 1 & i = w \\ 0 & \text{else.} \end{cases}$$

In the quantum situation consider $|i\rangle \mapsto (-1)^{f(i)} |i\rangle$. This comes from the circuit



Problem 15.3 (Homework 9.3)**.** Show that the above operation is given by $U_G = (\mathrm{id} - 2|w\rangle\langle w|)$.

Now, let $|\mathbf{1}\rangle = \frac{1}{\sqrt{n}} \sum_{i=0}^{n-1} |i\rangle$ be an "all-1" vector and define

$$U_{\mathbf{1}} = \mathrm{id} - 2|\mathbf{1}\rangle\langle\mathbf{1}|.$$

Problem 15.4 (Homework 9.4)**.** Take $n = 4$ and $w = 2$. Compute $U_{\mathbf{1}} U_G \mathbf{1}$. Can we find w from this?

§16 December 1, 2015

§16.1 Grover's search algorithm, continued

Let

$$|\mathbf{1}\rangle = \frac{1}{\sqrt{n}}\sum_{i=0}^{n-1}.$$

Remark 16.1. Observe that if $n = 2^m$, then $|\mathbf{1}\rangle$ is the output of taking $|0\dots0\rangle$ (m times) and passing it through m Hadamard operators, i.e.

$$H^{\otimes m}|0\dots0\rangle = |\mathbf{1}\rangle.$$

Again, we define

$$U_G = U_{|\mathbf{1}\rangle}U_w|\mathbf{1}\rangle.$$

Note that U_G never takes a state out of the subspace spanned by $|w\rangle$, $|\mathbf{1}\rangle$.

Also, note that

$$\langle\mathbf{1}|w\rangle = \frac{1}{\sqrt{n}}.$$

Consider the subspace H_ω By **Gram-Schmidt orthogonalization**, we can consider

$$|\widetilde{w}_{\mathbf{1}}\rangle = |\mathbf{1}\rangle - \langle w|\mathbf{1}\rangle|w\rangle$$

which is orthogonal to w, and normalize it to get

$$|w_{\mathbf{1}}\rangle = \frac{1}{\sqrt{1-1/n}}|\widetilde{w}_{\mathbf{1}}\rangle.$$

Now note that

$$\begin{aligned}\mathbf{1} &= \sqrt{1-1/n}\,|w_1\rangle + \frac{1}{\sqrt{n}}|w\rangle\\ |\mathbf{1}\rangle\langle\mathbf{1}| &= \langle w_1||w_1\rangle + \frac{1}{\sqrt{n}}\sqrt{1-\frac{1}{n}\sigma_x + \frac{1}{n}\sigma_z}\\ &= \frac{1}{2}(\mathrm{id}-\sigma_z) + \frac{1}{\sqrt{n}}\sqrt{1-\frac{1}{n}\sigma_x + \frac{1}{n}\sigma_z}.\end{aligned}$$

So one can compute

$$U_G = U_{\mathbf{1}}U_w = \exp\left(-i\frac{\theta}{2}\sigma_y\right)$$

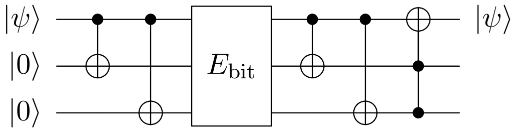
where $\cos(\frac{1}{2}\theta) = 1 - 2/n$ and $\sin(\frac{1}{2}\theta) = \frac{2}{\sqrt{n}}\sqrt{1-\frac{1}{n}}$.

So all we're doing is rotating. After ℓ iterations, we have $\ell\theta \approx \pi$.

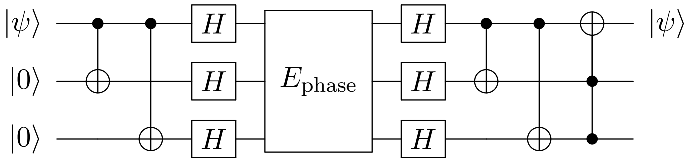
§17 December 3, 2015

§17.1 Error Correction

Classically, a error correcting code for one bit is 000 or 111 for 0 and 1, respectively. Quantum version for at most one σ_x flip:



This will restore the state $|\psi\rangle$ completely. Similarly,



is a code to deal with up to one σ_z rotation. (What about σ_y?)

§A December 10, 2015

§A.1 Review topics

- Classical logic and reversible computation.
- Quantum mechanics of single qubit, SU(2).
- Multiple qubits, tensor products, entanglements, reduced density matrices.
- Quantum circuits: for example, given a circuit and its input, compute the output of the circuit.
- No-cloning Theorem, teleportation, superdense coding.
- Quantum weirdness (Greenberger-Horne-Zeilinger).
- Simple quantum algorithms, Deutschz-Jozsa.
- Quantum Fourier transform (e.g. apply to a given)
- Phase estimation
- Shor's algorithm
- Grover search algorithm.
- A little on quantum error-correcting codes. (E.g. construct a code that corrects the following type of error.)

You need to be able to rotate a single qubit around a given axis. You need to able to complete reduced density matrices.

§A.2 Classical and Quantum Logic

Reversible logic gates: Toffoli, Fredkin, CNOT, NOT, wire. Universal set of gates e.g. AND, OR, NOT, (COPY). Toffoli and Fredkin are universal on their own with suitable additional inputs.

In a qubit system, we have $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ and thus a state is given by $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$, where $|\alpha|^2 + |\beta|^2 = 1$.

The Pauli matrices are

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

As for SU(2), we consider a vector $\vec{\jmath} = j_1\sigma_x + j_2\sigma_y + j_3\sigma_z$, then

$$\exp(-i\theta/2\sigma_{\vec{\jmath}}) = \cos(\frac{1}{2}\theta)\mathrm{id} - i\sin(\frac{1}{2}\theta)\sigma_{\vec{\jmath}}.$$

to rotation by θ about the $\vec{\jmath}$ axis. (There *will* be a problem on this.)

A measurement corresponds to a Hermitian operator $A = A^\dagger$. The outcome of the measurement corresponds to an eigenvalue a_i of A and leaves the system in the corresponding eigenstate $|i\rangle$.

Two qubits, tensor products, operators $\sigma_A \otimes \sigma_B$. The singlet and triplet states. *Be able to take partial traces.*

No-cloning theorem. Superdense coding. "What should Alice do if she sees $|\Phi_+\rangle$?" (Write down answers for all four singlets.)

§A.3 Quantum Algorithms

Quantum Fourier Transform: $|x\rangle \mapsto \frac{1}{\sqrt{2^n}} \sum_{y=0\dots0}^{1\dots1} \exp\left(\frac{2\pi ixy}{2^n}\right) |y\rangle$. Finds periodicity in wave functions.

Shor's algorithm. Quantum phase algorithm. Grover's algorithm. Error correcting codes.

§B Notes for Exam

For the final exam we were permitted two pages of notes, double sided. On the next pages is a copy of the notes that I used. The condensing of material was done using `savetrees` (it actually could have fit on three pages with tighter line spacing).

18.435J Exam Notes

Evan Chen

December 15, 2015

1 Logic Gates

Universal set: Toffoli, Fredkin, CNOT, NOT, wire.-

- **Toffoli**: $[a, b, c] \mapsto [a, b, ab + c]$.
- **Fredkind**: Given abc, swaps b and c iff $a = 1$.

2 Rotation Matrices

The **Pauli matrices** are

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Normalized eigenvectors:

$$|\uparrow\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad |\downarrow\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$|\rightarrow\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \qquad |\leftarrow\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

$$|\otimes\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix} \qquad |\odot\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -i \end{pmatrix}.$$

As for SU(2), we consider a vector $\vec{\jmath} = j_1\sigma_x + j_2\sigma_y + j_3\sigma_z$, then

$$\exp(-i\theta/2\sigma_{\vec{\jmath}}) = \cos(\frac{1}{2}\theta)\mathrm{id} - i\sin(\frac{1}{2}\theta)\sigma_{\vec{\jmath}}.$$

to rotation by θ about the $\vec{\jmath}$ axis.

3 Spukhafte Fernwirkung

$$|\Psi_-\rangle = \frac{1}{\sqrt{2}} \left(|\uparrow\rangle_A \otimes |\downarrow\rangle_B - |\downarrow\rangle_A \otimes |\uparrow\rangle_B \right).$$

We also define

$$|\Psi_+\rangle = \frac{1}{\sqrt{2}} \left(|\uparrow\rangle_A \otimes |\downarrow\rangle_B + |\downarrow\rangle_A \otimes |\uparrow\rangle_B \right)$$
$$|\Phi_+\rangle = \frac{1}{\sqrt{2}} (|\uparrow\rangle_A \otimes |\uparrow\rangle_B + |\downarrow\rangle_A \otimes |\downarrow\rangle_B)$$
$$|\Phi_-\rangle = \frac{1}{\sqrt{2}} (|\uparrow\rangle_A \otimes |\uparrow\rangle_B - |\downarrow\rangle_A \otimes |\downarrow\rangle_B).$$

4 Reduced Density Matrices

Consider a state

$$|\psi\rangle = \sum_{i,j} \psi_{i,j} |i\rangle_A |j\rangle_B \in V_1 \otimes V_2$$

The **reduced density matrix** is

$$\rho_A \overset{\text{def}}{=} \sum_{i,i',j} \overline{\psi_{i,j}} \psi_{i',j} |i'\rangle \langle i|$$

Partial trace:

$$\mathrm{Tr}_B \sum_{i,i',j,j'} \overline{\psi_{i,j}} \psi_{i',j'} (|i'\rangle \otimes_A \langle i|) \otimes (|j'\rangle \otimes_B \langle j|)$$

$$\overset{\text{def}}{=} \sum_{i,i',j,j'} \overline{\psi_{i,j}} \psi_{i',j'} (|i\rangle \otimes_A \langle i'|) \langle j|j'\rangle.$$

Partial trace ρ_A for matrices:

$$\begin{bmatrix} a & b & c & d \\ e & f & g & h \\ i & j & k & l \\ m & n & o & p \end{bmatrix} \to \begin{bmatrix} a+f & c+h \\ i+n & k+p \end{bmatrix}$$

Derivation: the expected output applying $M_A \otimes \mathrm{id}_B$

$$\begin{aligned}
&\langle\psi|_{AB} M_A \otimes \mathrm{id}_B |\psi\rangle_{AB} \\
&= \left(\sum_{i,j} \overline{\psi_{i,j}} \langle i| \otimes \langle j| \right) M_A \otimes \mathrm{id}_B \left(\sum_{i',j'} \psi_{i',j'} |i'\rangle \otimes |j'\rangle \right) \\
&= \sum_{i,j,i',j'} \overline{\psi_{i,j}} \psi_{i',j'} \langle i| M_A |i'\rangle \langle j| \mathrm{id}_B |j'\rangle \\
&= \sum_{i,j,i',j'} \overline{\psi_{i,j}} \psi_{i',j'} \langle i| M_A |i'\rangle \delta_{j,j'} \\
&= \sum_{i,j,i'} \overline{\psi_{i,j}} \psi_{i',j} \langle i| M_A |i'\rangle \\
&= \sum_{i,j,i'} \overline{\psi_{i,j}} \psi_{i',j} \mathrm{Tr}(\langle i| M_A |i'\rangle) \\
&= \sum_{i,j,i'} \overline{\psi_{i,j}} \psi_{i',j} \mathrm{Tr}(|i'\rangle \langle i| M_A) \\
&= \mathrm{Tr}(\sum_{i,j,i'} \overline{\psi_{i,j}} \psi_{i',j} |i'\rangle \langle i| M_A) \\
&= \mathrm{Tr}(\rho_A M_A).
\end{aligned}$$

5 Deutsch-Jozsa

First, consider functions $f : \{0,1\}^m \to \{0,1\}$. Want to differentiate between constant and balanced.

Now, consider a box

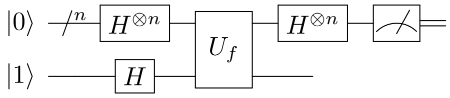
$$(x, y) \overset{\boxed{f}}{\mapsto} (x, f(x) + y \mod 2).$$

If we have m-bit inputs, then we clearly require

$$2^{m-1} + 1$$

queries in order to prove that f is constant/balanced, since in the worst case we could get the same output 2^{m-1} times.

In quantum, can do with one function call given an oracle $U_f : |x\rangle |y\rangle \mapsto |x\rangle |x + f(y)\rangle$.



Output:

$$\frac{1}{2^n} \sum_{y=0}^{2^n-1} \left[\sum_{x=0}^{2^n-1} (-1)^{f(x)} (-1)^{x \cdot y} \right] |y\rangle$$

where $x \cdot y$ is a dot product. The probability of measuring $|0\rangle^{\otimes n}$ is

$$\left| \frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{f(x)} \right|^2$$

which is 1 for constant and 0 if balanced.

6 Greenberger-Horne-Zeilinger Paradox

Take the state

$$|\Psi\rangle_{\text{GHZ}} = \frac{1}{\sqrt{2}} \left(|0\rangle_A |0\rangle_B |0\rangle_C - |1\rangle_A |1\rangle_B |1\rangle_C \right).$$

Consider the following set of measurements:

$$\sigma_y^A \otimes \sigma_y^B \otimes \sigma_x^C, \quad \sigma_y^A \otimes \sigma_x^B \otimes \sigma_y^C, \quad \sigma_x^A \otimes \sigma_y^B \otimes \sigma_y^C, \quad \sigma_x^A \otimes \sigma_x^B \otimes \sigma_x^C.$$

Compute

$$\langle\Psi|_{\text{GHZ}} \sigma_x^A \otimes \sigma_x^B \otimes \sigma_x^C |\Psi\rangle_{\text{GHZ}} = -1$$

and

$$\langle\Psi|_{\text{GHZ}} \sigma_y^A \otimes \sigma_y^B \otimes \sigma_x^C |\Psi\rangle_{\text{GHZ}} = 1.$$

(Possible hint: $\sigma_x^A \otimes \sigma_x^B \otimes \sigma_x^C |\Psi\rangle_{\text{GHZ}} = - |\Psi\rangle_{\text{GHZ}}$.)

Something is weird about this. Let $S_X^A = \{\pm 1\}$ be the result of measuring by σ_x^A on the state, and define other variables similarly. Thus the possible results are $S_y^A S_y^B S_x^C$, $S_y^A S_x^B S_y^C$, $S_x^A S_y^B S_x^C$, $S_x^A S_x^B S_x^C$, with each variable being ± 1, and with product $(-1)^3 \cdot 1 = -1$. However, the product of them all is 1, because of the squares!

What this means is that the values of the observations do not exist beforehand; in some sense they are "created" at the time of measurement.

7 Superdense coding

This is quantum communication.

Assume Alice is trying to communicate with Bob by sending qubits. For every qubit Alice sends across a channel, it's been shown Bob can receive at most one bit of classical information.

But now suppose that Alice and Bob additionally both possess access to an entangled state

$$|\Psi_-\rangle_{AB} = \frac{1}{\sqrt{2}} \left(|0\rangle_A |1\rangle_B - |1\rangle_A |0\rangle_B \right).$$

We say they have one **e-bit** of shared entanglement.

We now claim that if Alice and Bob possess one e-bit, then Alice can send a qubit to transmit two classical bits. Note that Alice can transform $|\Psi_-\rangle_{AB}$ into any of the triplet states by acting on exactly one qubit, since

- Do nothing to get $|\Psi_-\rangle_{AB}$,
- Do σ_x^A to get $|\Phi_-\rangle_{AB}$,
- Do σ_z^A to get $|\Psi_+\rangle_{AB}$,
- Do σ_y^A to get $|\Psi_-\rangle_{AB}$.

Thus, the algorithm is:

- Perform an operation on the entangled state, and then
- Send her half of the entangled pair to Bob.

From here Bob recovers the qubits in his basis.

8 Teleportation

Alice and Bob again share an entangled state $|\Psi_-\rangle_{AB}$. Moreover, Alice has a state $|\phi\rangle = \alpha |0\rangle + \beta |1\rangle$. The **Bell basis** of $\mathbb{C}^2 \otimes \mathbb{C}^2$ consists of the singlet and triplet state.

Now, Alice measures $|\phi\rangle_A$ and the first half of her entangled state, in the Bell basis, to get two classical bits k. Then, Bob will be able to recover the state $|\psi\rangle$ up to global base by applying a certain transformation U_k (depending on k).

Let $|\phi\rangle = (\alpha |0\rangle_B + \beta |1\rangle_B$. The key is the identity

$$\begin{aligned}
&2\sqrt{2} \cdot (\alpha |0\rangle + \beta |1\rangle) \otimes |\Psi_-\rangle_{AB} \\
=&(|0\rangle |1\rangle_A - |1\rangle |0\rangle_A) \otimes (\alpha |0\rangle_B + \beta |1\rangle_B) \\
&+ (|0\rangle |0\rangle_A - |1\rangle |1\rangle_A) \otimes (\alpha |0\rangle_B + \beta |1\rangle_B) \\
&+ (|0\rangle |0\rangle_A + |1\rangle |1\rangle_A) \otimes (\alpha |0\rangle_B + \beta |1\rangle_B) \\
&+ (|0\rangle |1\rangle_A + |1\rangle |1\rangle_A) \otimes (\alpha |0\rangle_B + \beta |1\rangle_B) \\
=& |\Psi_-\rangle * A \otimes \phi_B \\
&+ |\Phi_+\rangle * A \otimes -i\sigma_y^B \phi_B \\
&+ |\Phi_-\rangle * A \otimes \sigma_x^B \phi_B \\
&+ |\Phi_+\rangle * A \otimes \sigma_z^B \phi_B
\end{aligned}$$

Thus, we can now use "spooky action at a distance". Specifically, Alice makes a measurement, and

- If she observes $|\Psi_-\rangle$, tells Bob to do nothing.
- If she observes $|\Phi_-\rangle$, tells Bob to apply σ_x.
- If she observes $|\Phi_+\rangle$, tells Bob to apply σ_y.
- If she observes $|\Psi_+\rangle$, tells Bob to apply σ_z.

9 Quantum Fourier Transform

Consider a function $f : \{0, \ldots, 2^n - 1\} \to \mathbb{C}$ such that $\sum_x |f(x)|^2 = 1$ (normalization). The wave function is represent by

$$|\psi\rangle = \sum_{x=0}^{2^n-1} f(x) |x\rangle$$

and its **quantum Fourier transform** is defined as

$$|\psi\rangle \mapsto \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} \sum_{y=0}^{2^n-1} \exp\left(2\pi i x y / 2^n\right) f(x) |y\rangle$$

The inverse operation is

$$\sum_y g(y) |y\rangle \mapsto \frac{1}{2^{n/2}} \sum_{x,y} \exp(-2\pi i x y / 2^n) g(y) |x\rangle.$$

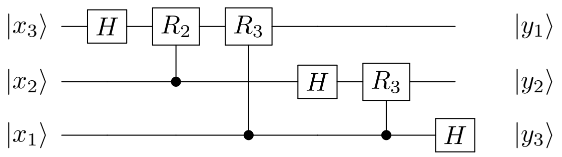
Expressing x binary notation, this is equivalent to

$$\begin{aligned}
|x_n x_{n-1} \ldots x_1\rangle \mapsto \frac{1}{2^{n/2}} &(|0\rangle + \exp(2\pi i \cdot 0.x_1) |1\rangle) \\
&\otimes (|0\rangle + \exp(2\pi i \cdot 0.x_2 x_1) |1\rangle) \\
&\otimes \ldots \\
&\otimes (|0\rangle + \exp(2\pi i \cdot 0.x_n \ldots x_1) |1\rangle)
\end{aligned}$$

Abbreviating the controlled rotation

$$R_k = \begin{pmatrix} 1 & 0 \\ 0 & \exp(2\pi i / 2^k) \end{pmatrix}$$

for $n = 3$ the circuit is given by



10 Quantum Phase Algorithm

Suppose we have U as described above (operating on m qubits). So of course

$$U^k |j\rangle = \exp(ik\varphi_j) |j\rangle .$$

First, assume $|\psi\rangle = |j\rangle$. The input is initially

$$|j\rangle \otimes |0 \dots 0\rangle .$$

After the Hadamard, we have

$$\frac{1}{\sqrt{2^n}} |j\rangle \otimes \sum_{k=0}^{2^n-1} |k\rangle .$$

The controlled operators (applying depending on whether the bit fed into them is 0 or 1) then gives

$$\frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} \exp(ik\varphi_j) |j\rangle \otimes |k\rangle .$$

Discard the $|j\rangle$ now, to get

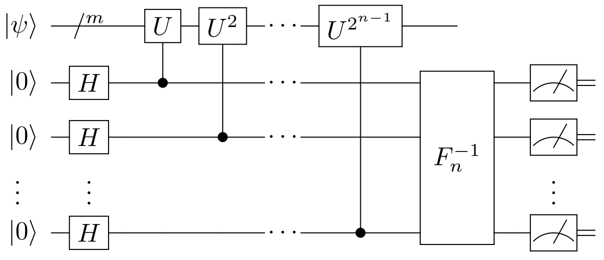
$$\frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} \exp(ik\varphi_j) |k\rangle .$$

This is a wave function, so we can extract the phase using the inverse quantum Fourier transform, and obtain

$$\frac{1}{2^n} \sum_{k,\ell} [\exp(2\pi ik \cdot (\varphi_j/2\pi - \ell/2^n)] |\ell\rangle .$$

Intuitively, we get $\approx |2^n \frac{\varphi_j}{2\pi}\rangle$. If $\ell/2^n = \varphi_j/2\pi$, then this isolates the specific phase: roots of unity filter.

In summary, the circuit is



11 Shor's Algorithm

Let $N = pq$ where p and q are prime numbers. Suppose we wish to factor N. Pick n so that $N^2 < 2^n < 2N^2$, and by modular exponentiation obtain the state

$$\frac{1}{\sqrt{2^n}} \sum_k |x\rangle |x^k \bmod N\rangle .$$

This takes $O(n^3)$ time, starting from $\frac{1}{\sqrt{2^n}} \sum_k |x\rangle |0\rangle$.

Suppose we make a measurement on the second register and get some value z for the second register. The entanglement goes away, and we obtain

$$\sum_{\substack{k \\ x^k \equiv z}} |k\rangle |z\rangle .$$

Thus, we get k_0, $k_0 + r$, …, or something. (The measurement of z is actually irrelevant.)

Now we discard the second register. Then the quantum Fourier transform gets us r. Thus using QFT on the first register, we arrive at

$$\frac{1}{2^n} \sum_{j,\ell} \exp\left(2\pi i \cdot \frac{j(k_0 + \ell r)}{2^n}\right) |j\rangle$$

For any fixed j the coefficient of $|j\rangle$ is positive if and only if $\frac{jr}{2^n}$ is close to an integer.

So, by measurement, we obtain a value of j such that $jr/2^n \approx s$, (here $s \in \mathbb{Z}$ is unknown, and $r \in \mathbb{Z}$ is what we want). Thus

$$\frac{j}{2^n} \approx \frac{s}{r}.$$

But $r < N$. So you can use continued fractions to compute both s and r, since $j/2^n$ is known.

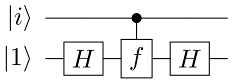
12 Grover's Search Algorithm

Unstructured database search. There are n items labeled $\{0, 1, \dots, n-1\}$ one of which is marked, say w. How many items do you have to sample to get it? Classically, $n/2$ times to get a $\frac{1}{2}$ success rate. For quantum algorithm, $\sqrt{n}$.

Indeed, classically we can test in the form

$$i \mapsto f(i) \equiv \begin{cases} 1 & i = w \\ 0 & \text{else.} \end{cases}$$

In the quantum situation consider $|i\rangle \mapsto (-1)^{f(i)} |i\rangle$. This comes from the circuit



Now, let $|\mathbf{1}\rangle = \frac{1}{\sqrt{n}} \sum_{i=0}^{n-1} |i\rangle$ be an "all-1" vector and define

$$U_\mathbf{1} = \mathrm{id} - 2 |\mathbf{1}\rangle \langle \mathbf{1}| .$$

Remark 1. Observe that if $n = 2^m$, then $|\mathbf{1}\rangle$ is the output of taking $|0 \dots 0\rangle$ (m times) and passing it through m Hadamard operators, i.e.

$$H^{\otimes m} |0 \dots 0\rangle = |\mathbf{1}\rangle .$$

Note that U_G never takes a state out of the subspace spanned by $|w\rangle$, $|\mathbf{1}\rangle$. Also, note that

$$\langle \mathbf{1} | w \rangle = \frac{1}{\sqrt{n}}.$$

Consider the subspace H_ω By **Gram-Schmidt orthogonalization**, we can consider

$$|\widetilde{w}_\mathbf{1}\rangle = |\mathbf{1}\rangle - \langle w | \mathbf{1} \rangle |w\rangle$$

which is orthogonal to w, and normalize it to get

$$|w_{\mathbf{1}}\rangle = \frac{1}{\sqrt{1-1/n}}\, |\widetilde{w}_{\mathbf{1}}\rangle .$$

Now note that

$$\begin{aligned}
\mathbf{1} &= \sqrt{1-1/n}\, |w_1\rangle + \frac{1}{\sqrt{n}} |w\rangle \\
|\mathbf{1}\rangle \langle \mathbf{1}| &= \langle w_1|\, |w_1\rangle + \frac{1}{\sqrt{n}} \sqrt{1-\frac{1}{n}\sigma_x + \frac{1}{n}\sigma_z} \\
&= \frac{1}{2}(\mathrm{id} - \sigma_z) + \frac{1}{\sqrt{n}} \sqrt{1-\frac{1}{n}\sigma_x + \frac{1}{n}\sigma_z}.
\end{aligned}$$

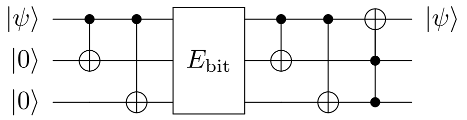
So one can compute

$$U_G = U_{\mathbf{1}} U_w = \exp\left(-i\frac{\theta}{2}\sigma_y\right)$$

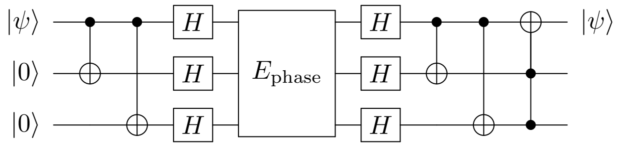
where $\cos(\frac{1}{2}\theta) = 1 - 2/n$ and $\sin(\frac{1}{2}\theta) = \frac{2}{\sqrt{n}}\sqrt{1-\frac{1}{n}}$. So all we're doing is rotating. After ℓ iterations, we have $\ell\theta \approx \pi$.

13 Error Correction

Classically, a error correcting code for one bit is 000 or 111 for 0 and 1, respectively. Quantum version for at most one σ_x flip:



This will restore the state $|\psi\rangle$ completely. Similarly,



is a code to deal with up to one σ_z rotation. (What about σ_y?)