NOTES ON QUANTUM COMPUTING

LUÍS R. A. FINOTTI

Contents

1. Qubits

Notation 1.1. The following notation is commonly used:

(1) *Qubit*:

$$|0\rangle \stackrel{\text{def}}{=} \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \qquad |1\rangle \stackrel{\text{def}}{=} \begin{pmatrix} 0 \\ 1 \end{pmatrix},$$
$$|+\rangle \stackrel{\text{def}}{=} \frac{\sqrt{2}}{2} \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \qquad |-\rangle \stackrel{\text{def}}{=} \frac{\sqrt{2}}{2} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$
$$|\mathrm{i}\rangle \stackrel{\text{def}}{=} \frac{\sqrt{2}}{2} \begin{pmatrix} 1 \\ \mathrm{i} \end{pmatrix}, \qquad |-\mathrm{i}\rangle \stackrel{\text{def}}{=} \frac{\sqrt{2}}{2} \begin{pmatrix} 1 \\ -\mathrm{i} \end{pmatrix}.$$

(2) *Quantum State*:

$$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}, \qquad \text{with } |\alpha|^2 + |\beta|^2 = 1,$$

where $|\alpha|^2$ is the probability of the qubit measuring as the 0 state and $|\beta|^2$ is the probability of the qubit measuring as the 1 state.

(3) *Dirac Notation* (and the *ket vector*):

$$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \alpha\,|0\rangle + \beta\,|1\rangle\,.$$

(4) We denote by $\oplus$ the addition in $\mathbb{F}_2$. E.g., if $x \in \mathbb{F}_2$, we have that

$$|x \oplus 1\rangle = \begin{cases} 1, & \text{if } x = 0; \\ 0, & \text{if } x = 1. \end{cases}$$

(So, this is example is like the *not* gate.)

(5)

$$|\psi(\theta, \phi)\rangle \stackrel{\text{def}}{=} \cos(\theta/2)\,|0\rangle + \mathrm{e}^{\mathrm{i}\phi} \sin(\theta/2)\,|1\rangle\,.$$

(See Section 4 below.)

(6) If $|\phi\rangle = \lambda\,|\psi\rangle$ with $|\lambda| = 1$, then $|\phi\rangle$ and $|\psi\rangle$ are *physically equivalent*. So we can disregard the overall phase.

2. Tensor Products

Notation 2.1. We denote, e.g.,

$$|010011\rangle \stackrel{\text{def}}{=} |0\rangle \otimes |1\rangle \otimes |0\rangle \otimes |0\rangle \otimes |1\rangle \otimes |1\rangle\,.$$

Also, as usual,

$$|0\rangle^{\otimes 5} \stackrel{\text{def}}{=} |00000\rangle\,.$$

Remark. If we have $\alpha\,|00\rangle + \beta\,|01\rangle + \gamma\,|10\rangle + \delta\,|11\rangle$, then

$$|\alpha|^2 = \text{probability of measuring } |00\rangle,$$
$$|\beta|^2 = \text{probability of measuring } |01\rangle,$$
$$|\gamma|^2 = \text{probability of measuring } |10\rangle,$$
$$|\delta|^2 = \text{probability of measuring } |11\rangle.$$

Definition 2.2. The *computational basis* is simply the induced basis of $(\mathbb{C}^2)^{\otimes n}$: $\{|i_1 i_2 \dots i_n\rangle \,:\, i_j \in \{0,1\}\}$. The order in qiskit is done via the binary representation (with unit digit coming *first*), e.g.,

$$\{|000\rangle\,, |100\rangle\,, |010\rangle\,, |110\rangle\,, |001\rangle\,, |101\rangle\,, |011\rangle\,, |111\rangle\}.$$

One can sometimes represent this basis (in this same order) as

$$\{|0\rangle_3\,, |1\rangle_3\,, |2\rangle_3\,, |3\rangle_3\,, \dots, |7\rangle_3\}.$$

3. Inner Product

We have the *inner product* in $(\mathbb{C}^2)^{\otimes n}$: if $|\psi\rangle = \sum_{x\in\mathbb{F}_2^n} \psi_x |x\rangle$ and $|\phi\rangle = \sum_{x\in\mathbb{F}_2^n} \phi_x |x\rangle$, then

$$\langle \psi \mid \phi \rangle \stackrel{\text{def}}{=} \sum_{x\in\mathbb{F}_2^n} \overline{\psi}_x \phi_x.$$

(So, it is simply the inner product that makes the computational basis *orthonormal*.)

Of course, for $x, y \in \mathbb{F}_2^n$, we have that $\langle x \mid y \rangle = \delta_{x,y}$.

Note that we denote by $\langle\psi|$ (the *bra vector* of ψ) the dual element of $|\psi\rangle$:

$$\langle\psi| = \sum_{x\in\mathbb{F}_2^n} \overline{\psi}_x \langle x| .$$

Hence,

$$\langle\psi| |\phi\rangle = \langle \psi \mid \phi \rangle.$$

4. Bloch Sphere

Reference: Bloch Sphere | Visualizing Qubits and Spin | Quantum Information

Note that if $|\rho| = 1$, then $|\psi\rangle \sim \rho |\psi\rangle$, as we don't care about the *overall* phase. So, if

$$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \alpha |0\rangle + \beta |1\rangle ,$$

then $|\alpha|^2 + |\beta|^2 = 1$, so

$$\alpha = \cos(\gamma) \mathrm{e}^{\mathrm{i}\delta},$$
$$\beta = \sin(\gamma) \mathrm{e}^{\mathrm{i}\epsilon},$$

with $\gamma, \delta, \epsilon \in \mathbb{R}$. Now,

$$\begin{aligned} |\psi\rangle &= \cos(\gamma)\mathrm{e}^{\mathrm{i}\delta}\,|0\rangle + \sin(\gamma)\mathrm{e}^{\mathrm{i}\epsilon}\,|1\rangle \\ &= \mathrm{e}^{\mathrm{i}\delta}\left(\cos(\gamma)\,|0\rangle + \mathrm{e}^{\mathrm{i}(\epsilon-\delta)}\sin(\gamma)\,|1\rangle\right) \\ &\sim \cos(\gamma)\,|0\rangle + \mathrm{e}^{\mathrm{i}(\epsilon-\delta)}\sin(\gamma)\,|1\rangle\,. \end{aligned}$$

So, we have that

$$(1) \qquad |\psi\rangle \sim |\psi(\theta,\phi)\rangle \stackrel{\text{def}}{=} \cos(\theta/2)\,|0\rangle + \mathrm{e}^{\mathrm{i}\phi}\sin(\theta/2)\,|1\rangle\,, \qquad \theta \in [0,\pi],\ \phi \in [0,2\pi].$$

Note that $\epsilon - \delta$ is the *relative phase*. Clearly, the relative phase does not change the probabilities.

Considering:

- θ the angle in $\mathbb{R}^3$ with the z-axis;
- ϕ the angle in $\mathbb{R}^3$ with the x-axis around the z-axis;

we get a sphere (with spherical coordinates and radius 1), the *Bloch sphere* (in Fig. 1 on the following page).

Let

$$\hat{\eta} = \begin{pmatrix} \sin(\theta)\cos(\phi) \\ \sin(\theta)\sin(\phi) \\ \cos(\theta) \end{pmatrix}$$

be a direction/point on the sphere (in spherical coordinates). Then, the spin operator in the direction of $\hat{\eta}$ (with angles θ and ϕ as above) the Bloch state $|\psi(\theta,\phi)\rangle$ is an eigenfunction with positive eigenvalue $\hbar/2$. (FIXME! Need details!)

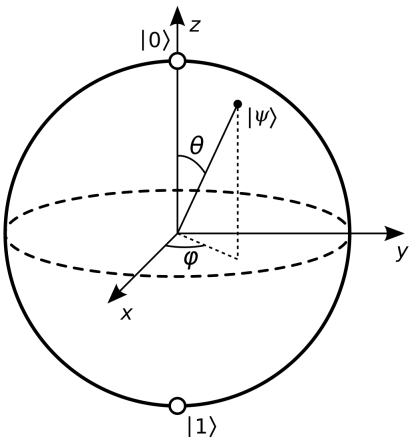


FIGURE 1. Bloch Sphere

5. GATES

Definition 5.1. A 1-qubit *gate* is simply an element of $\mathrm{U}_2(\mathbb{C})$ acting on a singe qubit. More gerenerally an n-qubit gate is an element of $U_{2^n}(\mathbb{C})$.

Notation 5.2. (1) *X Gate*: multiplication by:

$$X \stackrel{\text{def}}{=} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

It is basically the NOT gate, $|x\rangle \mapsto |x \oplus 1\rangle$. So, $\alpha|0\rangle + \beta|1\rangle \mapsto \beta|0\rangle + \alpha|1\rangle$.

(2) *Y Gate*: multiplication by:

$$Y \stackrel{\text{def}}{=} \begin{pmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix}$$

So, $\alpha|0\rangle + \beta|1\rangle \mapsto -\mathrm{i}\beta|0\rangle + \alpha\mathrm{i}|1\rangle \sim \beta|0\rangle - \alpha|1\rangle$.

(3) *Z Gate*: multiplication by:

$$Z \stackrel{\text{def}}{=} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

So, $\alpha|0\rangle + \beta|1\rangle \mapsto \alpha|0\rangle - \beta|1\rangle$, or $Z|x\rangle = (-1)^x|x\rangle$, for $x \in \mathbb{F}_2$. Note then that the Z gate is a *phase flip*.

(4) *Hadamard Gate*: multiplication by

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

Note that, with the Hadamard gate we have

$$|0\rangle \mapsto |+\rangle\,, \qquad |+\rangle \mapsto |0\rangle\,,$$
$$|1\rangle \mapsto |-\rangle\,, \qquad |-\rangle \mapsto |1\rangle\,.$$

So, it is a change of basis between $\{|0\rangle\,, |1\rangle\}$ and $\{|+\rangle\,, |-\rangle\}$ and back. Moreover:

$$|s\rangle \stackrel{\text{def}}{=} H^{\otimes n}\,|0\rangle^{\otimes n} = \sum_{x\in\mathbb{F}_2^n} \frac{1}{2^{n/2}}\,|x\rangle\,,$$

and hence it changes $|00\ldots0\rangle$ to one of equal probabilities, i.e., an equal (unbiased) superposition of all computational basis elements.

(5) We also have the S *gate* and T *gate*:

$$S \stackrel{\text{def}}{=} \begin{pmatrix} 1 & 0 \\ 0 & \mathrm{e}^{\mathrm{i}\pi/2} \end{pmatrix}, \qquad T \stackrel{\text{def}}{=} \begin{pmatrix} 1 & 0 \\ 0 & \mathrm{e}^{\mathrm{i}\pi/4} \end{pmatrix}$$

Remark. Note that if we have two gates U_1 and U_2, with $U_1 \sim U_2$, if they are affecting a single qubit, they can be exchanged without affecting the physical result, as they only add a global phase. On the other hand, if they come with a *controlled gate*, as seen in Section 8.4, then they introduce a relative phase and *cannot* be switched!

Remarks. (1) The X, Y, and Z gates can also be denoted by σ_1, σ_2, and σ_3, respectively, and are referred to as *Pauli gates*.

(2) Note that $Y = iXZ \sim XZ$.

(3) $XY \sim Z$, $YZ \sim X$, and $XZ \sim Y$.

(4) Note that all the matrices of these gates are their own inverses.

(5) In fact, they are all *unitary*, meaning $A^\dagger = A^{-1}$ (where $A^\dagger$ is the *adjoint*, i.e., the complex conjugate of the transpose of A). We shall denote the set of $n \times n$ unitary complex matrices by $\mathrm{U}_n(\mathbb{C})$.

(6) More over, quantum evolutions are *always* unitary, and therefore preserve inner products and norms.

(7) Note that $|+\rangle$ and $|-\rangle$ have the same probabilities for 0 and 1 (half for each), but after applying H (getting $|0\rangle$ and $|1\rangle$ respectively), they do not!

(8) Note that S and T introduce relative phases of $\pi/2$ and $\mathrm{i}/4$.

Theorem 5.3. *If $U \in \mathrm{U}_2(\mathbb{C})$, then*

$$U = \mathrm{e}^{\mathrm{i}\chi} \begin{pmatrix} \cos(\theta/2) & -\mathrm{e}^{\mathrm{i}\lambda}\sin(\theta/2) \\ \mathrm{e}^{\mathrm{i}\phi}\sin(\theta/2) & \mathrm{e}^{\mathrm{i}(\phi+\lambda)}\cos(\theta/2) \end{pmatrix},$$

for some $\chi, \theta, \phi, \lambda \in \mathbb{R}$. (Note that χ only affects the overall phase, so it is irrelevant.)

Remark. Most quantum algorithms start with $|s\rangle$ (equal probabilities) and then amplify the coefficient of the answer. Then, measuring will most likely give you the correct answer.

6. Rotations

We also have *rotations* around the X, Y, and Z angles:

$$R_X(\theta) \stackrel{\text{def}}{=} \exp\left(-\mathrm{i}\frac{\theta}{2}X\right) = \begin{pmatrix} \cos(\theta/2) & -\mathrm{i}\sin(\theta/2) \\ -\mathrm{i}\sin(\theta/2) & \cos(\theta/2) \end{pmatrix}$$

$$R_Y(\theta) \stackrel{\text{def}}{=} \exp\left(-\mathrm{i}\frac{\theta}{2}Y\right) = \begin{pmatrix} \cos(\theta/2) & -\sin(\theta/2) \\ \sin(\theta/2) & \cos(\theta/2) \end{pmatrix}$$

$$R_Z(\theta) \stackrel{\text{def}}{=} \exp\left(-\mathrm{i}\frac{\theta}{2}Z\right) = \begin{pmatrix} \mathrm{e}^{-\mathrm{i}\theta/2} & 0 \\ 0 & \mathrm{e}^{\mathrm{i}\theta/2} \end{pmatrix}$$

Note that if R is one of these, then:

- $R(0) = \mathbb{I}$;
- $R(\theta_1 + \theta_2) = R(\theta_1)R(\theta_2)$;
- $R(2\pi) = -\mathbb{I} \sim \mathbb{I}$.

Remark. Note that $R_Z(\pi/2) \sim S$ and $R_Z(\pi/4) \sim T$.

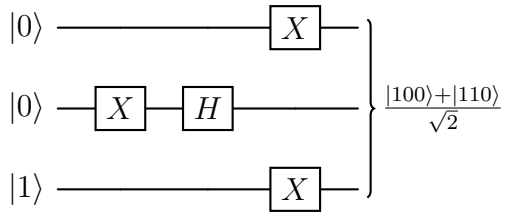
Theorem 6.1. *If $U \in \mathrm{U}_2(\mathbb{C})$, then*

$$U = \mathrm{e}^{\mathrm{i}\chi} R_X(\theta_1) R_Y(\theta_2) R_X(\theta_3),$$

for some $\chi, \theta_1, \theta_2, \theta_3 \in \mathbb{R}$. Moreover the X and Y can be replaces by any two of X, Y, and Z.

7. Quantum Circuits

Circuits apply gates to particular qubits. For instance:

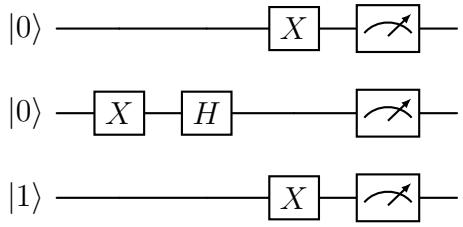


Breaking it down in steps:

$$\begin{aligned}
|001\rangle &\mapsto |011\rangle \\
&\mapsto |0\rangle \otimes \left(\frac{\sqrt{2}}{2} |0\rangle - \frac{\sqrt{2}}{2} |1\rangle \right) \otimes |1\rangle = \frac{\sqrt{2}}{2} |001\rangle + \frac{\sqrt{2}}{2} |011\rangle \\
&\mapsto \frac{\sqrt{2}}{2} |100\rangle + \frac{\sqrt{2}}{2} |110\rangle .
\end{aligned}$$

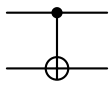
So, the probability that we get $|100\rangle$ or $|110\rangle$ is $1/2$ each, and 0 for every other state.

We can also add measurements to the circuit:



8. Multi-Qubit Gates

8.1. CNOT **Gate.** Here is the CNOT *Gate* (for *controlled not gate*) or *controlled NOT gate*: we have a control qubit and target qubit. If the control qubit is 1, then flip the value of the target bit. The graphical representation is



The dot is the control and the circle is the target. So, if the first qubit is the control and the second is the target, then this takes:

$$|00\rangle \mapsto |00\rangle\,,$$
$$|10\rangle \mapsto |11\rangle\,,$$
$$|01\rangle \mapsto |01\rangle\,,$$
$$|11\rangle \mapsto |10\rangle\,.$$

Or, we can represent:

$$\mathrm{CNOT}\,|x\rangle\,|y\rangle \stackrel{\text{def}}{=} \begin{cases} |x\rangle\,|y\rangle\,, & \text{if } x=0; \\ |x\rangle\,|y\oplus 1\rangle\,, & \text{if } x=1. \end{cases}$$

As a matrix:

$$\mathrm{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

Theorem 8.1. *On n qubits, the set*

$$\mathcal{G} \stackrel{\text{def}}{=} \{1\text{-}\textit{qubit gates on any qubit}\} \cup \{\mathrm{CNOT}\ \textit{on any two qubits}\}$$

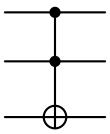
generates all gates, i.e., it generates $U_{2^n}(\mathbb{C})$.

Theorem 8.2. *We have that* $\dim_{\mathbb{R}} U_n(\mathbb{C})$ *is* $2n^2$ *(as an Euclidean space), so* $\dim_{\mathbb{R}} \mathrm{U}_{n^2}(\mathbb{C}) = 2\cdot(2^n)^2 = 2\cdot 2^{2n} = 2\cdot 4^n$.

8.2. **Multiple Control Gates.** We can have multiple controls for a gate. In that case, all control qubits must be $|1\rangle$ in order for the gate to be applied to the target qubit. For a gate U on n qubits, the notation for it is $C^{n-1}U$.

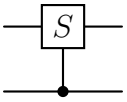
Note: These may be hard to create using only one-qubit gates and CNOT! See this Stack exchange post.

8.3. **Toffoli Gate.** The *Toffoli Gate* is C^2X, so it has two controls and one target. We only switch the target, i.e., apply X, when *both* controls are 1.



8.4. **Other Controlled Gates.** One can use the CNOT gate to produce other controlled gates: CY, CZ, CS, CH.

Here is a graphic representation:



9. Measuring Singular Qubits

If we have:

$$|\psi_0\rangle = \frac{1}{2}|00\rangle + \frac{1}{4}|01\rangle + \frac{\sqrt{2}}{2}|10\rangle + \frac{\sqrt{3}}{4}|11\rangle$$

and we measure the first qubit to be 1, then the new state is

$$|\psi_1\rangle = c \cdot \left(\frac{\sqrt{2}}{2} |10\rangle + \frac{\sqrt{3}}{4} |11\rangle \right),$$

with

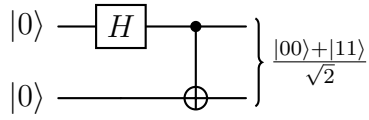
$$c^2 \left(\frac{1}{2} + \frac{3}{16} \right) = 1$$

due to probabilities. Hence, $c = 4/\sqrt{11}$ and

$$|\psi_1\rangle = \frac{4}{\sqrt{22}} |10\rangle + \frac{\sqrt{3}}{\sqrt{11}} |11\rangle .$$

10. Entanglement

Consider the circuit:



$$\begin{aligned} |00\rangle &\mapsto \frac{\sqrt{2}}{2} (|0\rangle + |1\rangle) \otimes |0\rangle = \frac{\sqrt{2}}{2} (|00\rangle + |10\rangle) \\ &\mapsto \frac{\sqrt{2}}{2} (|00\rangle + |11\rangle) . \end{aligned}$$

Hence, if the first qubit is measured as 0, then the second qubit must also be 0, and similarly if it is measured as 1, then the second must also be 1. So, these qubits are *entangled qubits*.

More precisely:

Definition 10.1. A state is *entangled state* if it cannot be factored as tensor products of individual qubits.

Example 10.2. We have that

$$\frac{\sqrt{3}}{2\sqrt{5}}|00\rangle + \frac{1}{2\sqrt{5}}|01\rangle + \frac{\sqrt{3}}{\sqrt{5}}|10\rangle + \frac{1}{\sqrt{5}}|11\rangle = \left(\frac{1}{\sqrt{5}}|0\rangle + \frac{2}{\sqrt{5}}|1\rangle\right) \otimes \left(\frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle\right)$$

so that state is *not* entangled. On the other hand

$$\frac{\sqrt{2}}{2}(|000\rangle + |011\rangle)$$

cannot be written as a tensor product, so it is. (Note that if we measure the second qubit, we know the state of the other two.)

Definition 10.3. (1) Qubits are *maximally entangled qubits* if measuring one of the qubits determine the other qubits.

(2) *Bell states* are some examples of maximally entangled qubits:

- $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$;
- $|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$;
- $|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$;
- $|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$.

(3) Qubits are *partially entangled* if measuring one of the qubits affect the probabilities for the other qubits. E.g., consider

$$|\psi\rangle = \frac{\sqrt{3}}{\sqrt{5}}|00\rangle + \frac{1}{\sqrt{5}}|01\rangle + \frac{1}{2\sqrt{5}}|10\rangle + \frac{\sqrt{3}}{2\sqrt{5}}|11\rangle.$$

If we measure the first qubit as 0, we get

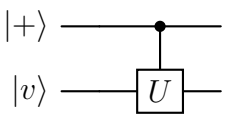
$$|0\rangle \otimes \left(\frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle\right),$$

while if we measure the first qubit as 1, we get

$$|1\rangle \otimes \left(\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle\right).$$

11. Phase Kickback

Consider:



and suppose the $|v\rangle$ is an *eigenstate* of U, meaning, $U|v\rangle = e^{i\theta}|v\rangle$. (Note that, due to normalization, all eigenvalues are of the form $e^{i\theta}$.)

We then have

$$\begin{aligned}
|+\rangle \otimes |v\rangle &= \frac{\sqrt{2}}{2}\left(|0\rangle \otimes |v\rangle + |1\rangle \otimes |v\rangle\right) \\
&\mapsto \frac{\sqrt{2}}{2}\left(|0\rangle \otimes |v\rangle + |1\rangle \otimes U|v\rangle\right) \\
&= \frac{\sqrt{2}}{2}\left(|0\rangle \otimes |v\rangle + e^{i\theta}|1\rangle \otimes |v\rangle\right) \\
&= \frac{\sqrt{2}}{2}\left(|0\rangle + e^{i\theta}|1\rangle\right) \otimes |v\rangle .
\end{aligned}$$

So, $|v\rangle$ is unchanged (even though it was the target qubit), and a relative phase was applied to the control qubit.

So, if we apply a controlled gate to a target that is an eigenvector of this gate, the phase of the control qubit is changed. This is called *phase kickback*.

12. Superdense Coding

Alice can send Bob two classical bits using only one qubit. Alice and Bob start with a maximally entangled pair of qubits

$$|\psi_0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

Alice takes the first qubit and Bob the second. Then, when Alice applies the first operation (depending on which two bits she wants to send Bob) and Bob the last two ($(H \otimes \mathbb{I}) \circ \text{CNOT}$):

$$|\psi_0\rangle \xmapsto{\mathbb{I}^{\otimes 2}} \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \xmapsto{\text{CNOT}} \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) = |+\rangle \otimes |0\rangle \xmapsto{H\otimes\mathbb{I}} |00\rangle$$

$$|\psi_0\rangle \xmapsto{X\otimes\mathbb{I}} \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle) \xmapsto{\text{CNOT}} \frac{1}{\sqrt{2}}(|11\rangle + |01\rangle) = |+\rangle \otimes |1\rangle \xmapsto{H\otimes\mathbb{I}} |01\rangle$$

$$|\psi_0\rangle \xmapsto{\mathbb{I}\otimes Z} \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \xmapsto{\text{CNOT}} \frac{1}{\sqrt{2}}(|00\rangle - |10\rangle) = |-\rangle \otimes |0\rangle \xmapsto{H\otimes\mathbb{I}} |10\rangle$$

$$|\psi_0\rangle \xmapsto{\mathbb{I}\otimes XZ} \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \xmapsto{\text{CNOT}} \frac{1}{\sqrt{2}}(|01\rangle - |11\rangle) = |-\rangle \otimes |1\rangle \xmapsto{H\otimes\mathbb{I}} |11\rangle$$

13. Grover's Algorithm

Grover's algorithm is an *unstructured search*, meaning, no assumption on the data that might help with searching.

Problem statement: given a list $[x_0, x_1, \ldots, x_{N-1}]$ that we can query (i.e., given j we can read x_j from the list) and some y, find if there is j_0 such that $x_{j_0} = y$ and output j_0 if so.

Traditionally, the search is $\mathcal{O}(N)$, with expected number of queries and comparisons $(N+1)/2$.

Assumptions: Assume $N = 2^n$ (or pad the list) and that y is *guaranteed* to be in the list.

Recast: We have the binary representation:

$$\{0, 1, 2, \ldots, 2^n - 1\} \to \mathbb{F}_2^n$$

and so we can produce a function $f : \mathbb{F}_2^n \to \mathbb{F}_2$, where the domain corresponds to the binary representation of the index in the list, and the output is a boolean, such that:

$$f(j) = \begin{cases} 1, & \text{if } x_j = y; \\ 0, & \text{otherwise.} \end{cases}$$

So, we need to find j such that $f(j) = 1$.

Last assumption: We have access to an *oracle* (a quantum circuit) U_f on n qubits such that:

$$U_f \left|j\right\rangle = (-1)^{f(j)} \left|j\right\rangle = \begin{cases} -\left|j\right\rangle, & \text{if } f(j) = 1; \\ \left|j\right\rangle, & \text{otherwise.} \end{cases}$$

Hence, U_f allows us to check if j is the index for y in the list by checking for a phase change. (*Question:* Can we create such circuit in practice?)

Define

$$U_S \stackrel{\text{def}}{=} H^{\otimes n} \circ X^{\otimes n} \circ C^{n-1}Z \circ X^{\otimes n} \circ H^{\otimes n}.$$

Note that, for $x \in \mathbb{F}_2^n$, we have

$$C^{n-1}Z \left|x\right\rangle = \begin{cases} -\left|x\right\rangle, & \text{if } x = (1, 1, \ldots, 1); \\ \left|x\right\rangle, & \text{otherwise.} \end{cases}$$

Then, we have:

$$\begin{aligned} U_S \left|s\right\rangle &= H^{\otimes n} \circ X^{\otimes n} \circ C^{n-1}Z \circ X^{\otimes n} \circ H^{\otimes n} \circ H^{\otimes n} \left|0\right\rangle^{\otimes n} \\ &= H^{\otimes n} \circ X^{\otimes n} \circ C^{n-1}Z \circ X^{\otimes n} \left|0\right\rangle^{\otimes n} \\ &= H^{\otimes n} \circ X^{\otimes n} \circ C^{n-1}Z \circ \left|1\right\rangle^{\otimes n} \\ &= -H^{\otimes n} \circ X^{\otimes n} \left|1\right\rangle^{\otimes n} \\ &= -H^{\otimes n} \left|0\right\rangle^{\otimes n} \\ &= -\left|s\right\rangle . \end{aligned}$$

Note: If $\left|\psi\right\rangle$ is such that $\langle \psi \mid s \rangle = 0$, then $U_S \left|\psi\right\rangle = \left|\psi\right\rangle$.

Proof. Since $H^{\otimes n}$ is unitary, we have that

$$0 = \langle \psi \mid s \rangle = \langle H^{\otimes n} \left|\psi\right\rangle \mid H^{\otimes n} \left|s\right\rangle \rangle = \langle H^{\otimes n} \left|\psi\right\rangle \mid H^{\otimes s} H^{\otimes n} \left|0\right\rangle^{\otimes n} \rangle = \langle H^{\otimes n} \left|\psi\right\rangle \mid \left|0\right\rangle^{\otimes n} \rangle,$$

and hence the component of $H^{\otimes n} \left|\psi\right\rangle$ in $\left|0\right\rangle^{\otimes n}$ is 0.

So, the component of $X^{\otimes n} \circ H^{\otimes n} \left|\psi\right\rangle$ in $\left|1\right\rangle^{\otimes n}$ is 0, which implies that

$$C^{n-1}Z \circ X^{\otimes n} \circ H^{\otimes n} \left|\psi\right\rangle = X^{\otimes n} \circ H^{\otimes n} \left|\psi\right\rangle .$$

Therefore,

$$U_S \left|\psi\right\rangle = H^{\otimes n} \circ X^{\otimes n} \circ X^{\otimes n} \circ H^{\otimes n} \left|\psi\right\rangle = \left|\psi\right\rangle .$$

□

Summary:

$$\text{target state: } \left|j_0\right\rangle \qquad U_f \left|j\right\rangle = \begin{cases} -\left|j\right\rangle , & \text{if } j = j_0; \\ \left|j\right\rangle , & \text{otherwise (or } \langle j \mid j_0 \rangle = 0). \end{cases}$$

$$\text{initial state: } \left|s\right\rangle \qquad U_S \left|\psi\right\rangle = \begin{cases} -\left|\psi\right\rangle , & \text{if } \left|\psi\right\rangle = \left|s\right\rangle; \\ \left|\psi\right\rangle , & \text{if } \langle \psi \mid s \rangle = 0. \end{cases}$$

We define *Grover's oracle* as $G = -U_s U_f$.

Theorem 13.1 (Grover, 1996)**.** *Let k be a positive integer and let $|\psi_k\rangle \stackrel{\text{def}}{=} G^k |s\rangle$. Then, when measuring, we have*

$$\mathbb{P}(\textit{getting } j_0 \mid \psi_k) = |\langle j_0 \mid \psi_k \rangle|^2 = \sin^2\left((2k+1)\arcsin\left(2^{-n/2}\right)\right).$$

Corollary 13.2. *If we let*

$$k \stackrel{\text{def}}{=} \left\lfloor \frac{\pi}{4\arcsin(2^{-n/2})} - \frac{1}{2} \right\rceil \approx \frac{\pi}{4} 2^{n/2} = \frac{\pi}{4}\sqrt{N},$$

then

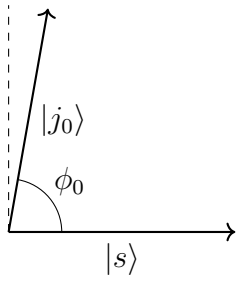
$$\mathbb{P}(\textit{getting } j_0 \mid \psi_k) = 1 - \mathcal{O}\left(\frac{1}{N}\right).$$

Takeaway: After about $\sqrt{N}$ queries, there is a very high probability we will get j_0 when measuring.

Proof of Grover's Theorem. Note that

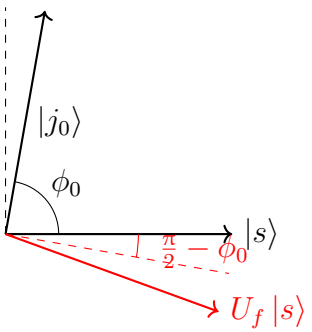
$$\langle j_0 \mid s \rangle = \frac{1}{2^{n/2}} \sum_{j \in \mathbb{F}_2^n} \langle j_0 \mid j \rangle = \frac{1}{2^{n/2}}.$$

Since this inner product is small, the vectors are almost perpendicular. Let ϕ_0 be the angle between them.

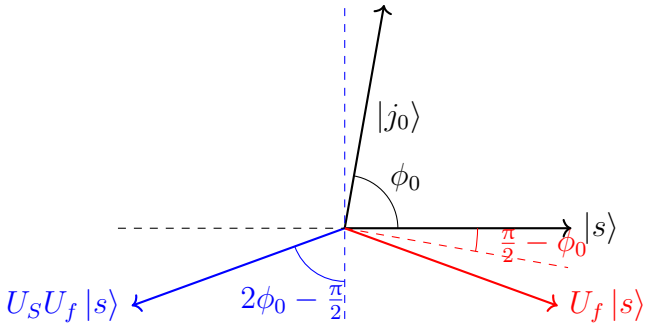


Then, by the inner product above, we have that $\phi_0 = \arccos(2^{-n/2})$.

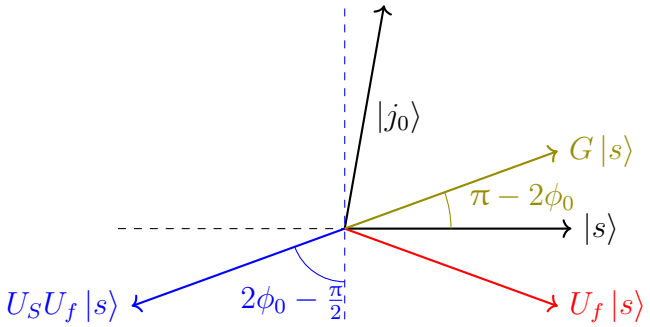
Note that U_S and U_f are *reflections*, so G is a rotation by some angle α. In the plane containing $|s\rangle$ and $|j_0\rangle$, U_f reflects on the line perpendicular to $|j_0\rangle$:



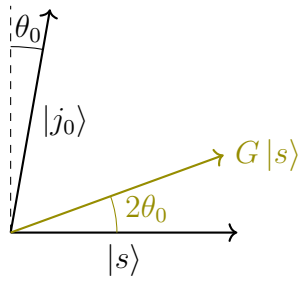
Similarly, U_S reflects on the line perpendicular to $|s\rangle$.



Hence, we have:



Hence, G is a rotation of $\alpha = \pi - 2\phi_0$. Since ϕ_0 is close to $\pi/2$, we have that α is close to 0. So, we have:



Therefore, the angle for $|\psi_k\rangle \stackrel{\text{def}}{=} G^k\,|s\rangle$ is $2k\theta_0$. Hence, the angle between $|\psi_k\rangle$ and $|j_0\rangle$ is $\phi_0 - 2k\theta_0 = (2k+1)\phi_0 - k\pi$. Noting that

- $\phi_0 = \arccos(2^{-n/2})$,
- $\cos(x + \pi/2) = -\sin(x)$, and
- $\pi/2 - \arccos(\pi/x) = \arcsin(x)$,

we have

$$\begin{aligned} |\langle j_0 \mid \psi_k\rangle|^2 &= \cos^2((2k+1)\phi_0 - k\pi) \\ &= \cos^2(-(2k+1)(\pi/2 - \phi_0) + \pi/2) \\ &= \sin^2((2k+1)\arcsin(2^{-n/2})). \end{aligned}$$

□

14. Quantum Fourier Transform

(More of a quantum "subroutine".)

Lemma 14.1. *Let* $\zeta_N \stackrel{\text{def}}{=} \mathrm{e}^{2\pi\mathrm{i}/N}$*, with* $N \geq 2$*, and* $a \in \mathbb{R}$*. Then we have*

$$\sum_{b=0}^{N-1} \zeta_N^{ab} = \begin{cases} N, & \text{if } a \in \mathbb{Z} \text{ and } a \equiv 0 \pmod{N}; \\ 0, & \text{if } a \in \mathbb{Z} \text{ and } a \not\equiv 0 \pmod{N}; \\ \frac{\left(\zeta_N^a\right)^N - 1}{\zeta_N - 1}, & \text{if } a \notin \mathbb{Z}. \end{cases}$$

Proof. We have that $\zeta_N^a = 1$ if and only if $a \in \mathbb{Z}$ and $a \equiv 0 \pmod{N}$, in which case the result is trivial. So, suppose that $\zeta_N^a \neq 1$. Then:

$$\sum_{b=0}^{N-1} \left(\zeta_N^a\right)^b = \frac{\zeta_N^{aN} - 1}{\zeta_N^a - 1}.$$

If $a \in \mathbb{Z}$, then $\left(\zeta_N^a\right)^N = \left(\zeta_N^N\right)^a = 1$. □

14.1. **Discrete Fourier Transform.**

Definition 14.2. Let $f : \mathbb{Z}/N\mathbb{Z} \to \mathbb{C}$ and $\zeta \stackrel{\text{def}}{=} \mathrm{e}^{2\pi\mathrm{i}/N}$. Then the *Discrete Fourier Transform (DFT)* is defined as

$$\mathcal{F}(f)(z) \stackrel{\text{def}}{=} \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} \zeta_N^{xz} f(x).$$

It decomposes f into periodic functions.

Proposition 14.3. *We have:*

(1) $\mathcal{F}$ *is linear.*

(2) Parseval identity*: if*

$$\langle f_1 \mid f_2 \rangle \stackrel{\text{def}}{=} \sum_{x=0}^{N-1} \overline{f}_1(x) f_2(x),$$

then

$$\langle \mathcal{F}(f_1) \mid \mathcal{F}(f_2) \rangle = \langle f_1 \mid f_2 \rangle,$$

i.e., $\mathcal{F}$ *is unitary.*

(3) Let $k \in \mathbb{Z}/N\mathbb{Z}$ and define the translation

$$T_k(f)(x) \stackrel{\text{def}}{=} f(x-k).$$

Then,

$$T_k(\mathcal{F}(f))(z) = \zeta_N^{kz}\mathcal{F}(T_k(f))(z).$$

Proof. Let $\zeta_k \stackrel{\text{def}}{=} \mathrm{e}^{2\pi\mathrm{i}/k}$. For Parseval's identity, using Theorem 14.1 on the previous page we have:

$$\begin{aligned}
\langle \mathcal{F}(f_1) \mid \mathcal{F}(f_2)\rangle &= \sum_{x=0}^{N-1}\left[\frac{1}{\sqrt{N}}\sum_{x_1=0}^{N-1}\zeta_N^{-x_1x}\overline{f}_1(x_1)\right]\cdot\left[\frac{1}{\sqrt{N}}\sum_{x_2=0}^{N-1}\zeta_N^{x_2x}\overline{f}_2(x_2)\right]\\
&= \frac{1}{N}\sum_{x=0}^{N-1}\sum_{x_1,x_2=0}^{N-1}\zeta_N^{x(x_2-x_1)}\overline{f}_1(x_1)f_2(x_2)\\
&= \frac{1}{N}\sum_{x=0}^{N-1}\sum_{x_1=0}^{N-1}\overline{f}_1(x_1)f_2(x_1)\\
&= \frac{1}{N}N\sum_{x_1=0}^{N-1}\overline{f}_1(x_1)f_2(x_1)\\
&= \langle f_1 \mid f_2\rangle.
\end{aligned}$$

□

14.2. **Quantum Fourier Transform.**

Definition 14.4. Let $N \stackrel{\text{def}}{=} 2^n$, $\zeta_N \stackrel{\text{def}}{=} \mathrm{e}^{2\pi\mathrm{i}/N}$ and

$$|\psi\rangle = \sum_{x=0}^{N-1}\psi(x)\,|x\rangle_n\,, \quad \psi : \mathbb{Z}/N\mathbb{Z} \to \mathbb{C},\ \|\psi\| = 1.$$

Then,

$$\begin{aligned}
\mathrm{QFT}\,|\psi\rangle &\stackrel{\text{def}}{=} \sum_{z=0}^{2^n-1}\mathcal{F}(\psi)(z)\,|z\rangle_n\\
&= \frac{1}{2^{n/2}}\sum_{z=0}^{2^n-1}\left[\sum_{x=0}^{2^n-1}\zeta_{2^n}^{xz}\psi(x)\right]|z\rangle_n\\
&= \frac{1}{2^{n/2}}\sum_{x=0}^{2^n-1}\psi(x)\left[\sum_{z=0}^{2^n-1}\zeta_{2^n}^{xz}\,|z\rangle_n\right].
\end{aligned}$$

In particular,

$$\mathrm{QFT}\,|x\rangle_n = \frac{1}{2^{n/2}} \sum_{z=0}^{2^n-1} \zeta_{2^n}^{xz}\,|z\rangle_n$$

Also note that

$$\mathrm{QFT}^{-1}\,|x\rangle_n = \mathrm{QFT}^{\dagger}\,|x\rangle_n = \frac{1}{2^{n/2}} \sum_{z=0}^{2^n-1} \zeta_{2^n}^{-xz}\,|z\rangle_n$$

Indeed, using Lemma 14.1 again:

$$\begin{aligned}
\mathrm{QFT}^{-1}\,\mathrm{QFT}\,|x\rangle_n &= \frac{1}{2^{n/2}} \sum_{z=0}^{2^n-1} \zeta_{2^n}^{xz} \left[\frac{1}{2^{n/2}} \sum_{y=0}^{2^n-1} \zeta_{2^n}^{-yz}\,|y\rangle_n \right] \\
&= \frac{1}{2^n} \sum_{y=0}^{2^n-1} \left[\sum_{z=0}^{2^n-1} \zeta_{2^n}^{z(x-y)} \right] |y\rangle_n \\
&= |x\rangle_n .
\end{aligned}$$

Remark. One can compute $\mathcal{F}(f)$ from f using the fast Fourier transform in $\mathcal{O}(\log_2(N)N)$ time.

Fact: There are quantum circuits for the quantum Fourier transform using $\mathcal{O}(n^2) = \mathcal{O}((\log_2(N))^2)$ gates, using only 1-qubit gates and CNOT gates. (See Nielsen-Chuang pg. 217 for a "good" exact implementation.)

Definition 14.5. *Ancillas* (or ancilla qubits) are extra qubits used in the quantum circuit.

14.3. **Application: Adder Circuit.** We will need the following definition:

Definition 14.6. We define the P *gate*:

$$P(k)\,|x\rangle_n \stackrel{\text{def}}{=} \mathrm{e}^{2\pi \mathrm{i} x k/2^n}\,|x\rangle_n .$$

Remark. **Careful!** In qiskit we have

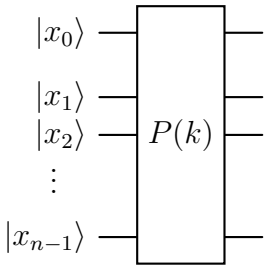
$$P(\theta) = \begin{pmatrix} 1 & 0 \\ 0 & \mathrm{e}^{\mathrm{i}\theta} \end{pmatrix}.$$

So here, $P(k)$ corresponds to qiskit's $P(\pi k)$!

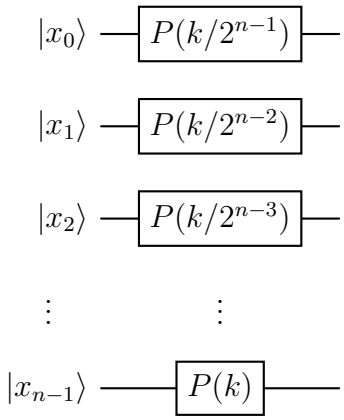
Hence, of $n = 1$ we have that

$$P(k) = \begin{pmatrix} 1 & 0 \\ 0 & \mathrm{e}^{\pi \mathrm{i} k} \end{pmatrix} = \mathrm{e}^{-\pi \mathrm{i} k/2} \begin{pmatrix} \mathrm{e}^{-\pi \mathrm{i} k/2} & 0 \\ 0 & \mathrm{e}^{\pi \mathrm{i} k/2} \end{pmatrix} = \mathrm{e}^{-\pi \mathrm{i} k/2} R_Z(\pi k/2)$$

Hence, we can easily implement the P gates. The circuit



which, as a multi-qubit gate, is the same as



Definition 14.7. For $k \in \mathbb{Z}/2^n\mathbb{Z}$, define the *plus k adder*

$$A_k \left|x\right\rangle_n \stackrel{\text{def}}{=} \left|x + k\right\rangle_n.$$

$$
\begin{aligned}
A_k \operatorname{QFT}^\dagger |x\rangle_n &= \frac{1}{2^{n/2}} \sum_{z=0}^{2^n-1} \zeta_{2^n}^{-xz} |z+k\rangle_n \\
&= \frac{1}{2^{n/2}} \sum_{z=0}^{2^n-1} \zeta_{2^n}^{-x(z-k)} |z\rangle_n \\
&= \frac{1}{2^{n/2}} \zeta_{2^n}^{xk} \sum_{z=0}^{2^n-1} \zeta_{2^n}^{-xz} |z\rangle_n \\
&= \zeta_{2^n}^{xk} \operatorname{QFT}^\dagger |x\rangle_n ,
\end{aligned}
$$

i.e.,

$$
(\operatorname{QFT} \circ A_k \circ \operatorname{QFT}^\dagger) |x\rangle_n = \zeta_{2^n}^{xk} |x\rangle_n = P(k) |x\rangle_n , \tag{2}
$$

or

$$
A_k = \operatorname{QFT}^\dagger \circ P(k) \operatorname{QFT} . \tag{3}
$$

(So, *shift* is turned in to *phase*)

So, using Eq. (3), and assuming that QFT can be implemented, we can also implement A_k.

Proof. Let

$$
x = x_0 + x_1 \cdot 2 + x_2 \cdot 2^2 + \cdots + x_{n-1} \cdot 2^{n-1} = \sum_{r=0}^{n-1} x_r 2^r .
$$

Then,

$$
\exp\left(\frac{2\pi \mathrm{i}}{2^n} xk\right) = \exp\left(k\pi \mathrm{i} \sum_{r=0}^{n-1} \frac{1}{2^{n-r-1}} x_r\right) \tag{4}
$$

Also, note that for a qubit x_r, we have

$$
R_Z(\theta) |x_r\rangle = \mathrm{e}^{-\mathrm{i}\theta/2} \mathrm{e}^{\mathrm{i}\theta x_r} |x_r\rangle .
$$

So,

$$
R_Z\left(\frac{k\pi}{2^{n-1-r}}\right) |x_r\rangle = \exp\left(-\frac{k\pi \mathrm{i}}{2^{n-r}}\right) \cdot \exp\left(\frac{k\pi \mathrm{i}}{2^{n-1-r}} x_r\right) |x_r\rangle .
$$

Therefore:

$$\begin{aligned}
\bigotimes_{r=0}^{n-1} R_Z\left(\frac{k\pi}{2^{n-1-r}}\right)|x_r\rangle &= \bigotimes_{r=0}^{n-1} \exp\left(-\frac{k\pi\mathrm{i}}{2^{n-r}}\right)\cdot\exp\left(\frac{k\pi\mathrm{i}}{2^{n-1-r}}x_r\right)|x_r\rangle \\
&= \left[\prod_{r=0}^{n-1}\exp\left(-\frac{k\pi\mathrm{i}}{2^{n-r}}\right)\cdot\prod_{r=0}^{n-1}\exp\left(\frac{k\pi\mathrm{i}}{2^{n-1-r}}x_r\right)\right]|x\rangle_n \\
&= \left[\exp\left(-\frac{k\pi\mathrm{i}}{2^n}\sum_{r=0}^{n-1}2^r\right)\cdot\exp\left(k\pi\mathrm{i}\sum_{r=0}^{n-1}\frac{1}{2^{n-1-r}}x_r\right)\right]|x\rangle_n \\
&= \exp\left(-\frac{(2^n-1)k\pi\mathrm{i}}{2^n}\right)\cdot\exp\left(\frac{2\pi\mathrm{i}}{2^n}xk\right)|x\rangle_n \\
&= \exp\left(-\frac{(2^n-1)k\pi\mathrm{i}}{2^n}\right)\cdot P(k)\,|x\rangle_n\,.
\end{aligned}$$

So, indeed the last circuit gives, up to a global phase, the $P(k)$ gate. □

15. Quantum Phase Estimation

15.1. **Fejér States.** What happens if we replace $k\in\mathbb{Z}$ in $A(k)$ by some $k\in\mathbb{R}$?

Definition 15.1. For n bits and $k\in\mathbb{R}$, define $|k\rangle_F$, the *k-th Fejér state* as

$$\begin{aligned}
|k\rangle_F &\stackrel{\text{def}}{=} \mathrm{QFT}^\dagger\circ P(k)\circ\mathrm{QFT}\,|0\rangle_n \\
&= \sum_{z=0}^{2^n-1}\exp\left(\pi\mathrm{i}(1-1/2)(k-z)\right)\frac{\sin(\pi(k-z))}{2^n\sin(\pi(k-z)/2^n)}\,|z\rangle_n\,.
\end{aligned}$$

Then, for $x\in\{0,1,\ldots,2^n-1\}$, we have

$$\mathbb{P}(x\mid|k\rangle_F) = |\langle x\mid k\rangle_F|^2 = \frac{\sin^2(\pi(k-x))}{4^n\sin^2(\pi(k-x)/2^n)},$$

the *Fejér kernel*.

Figure 2 on the facing page shows the graph of the Fejér kernel

$$\frac{\sin^2(\pi(k-x))}{4^n\sin^2(\pi(k-x)/2^n)}$$

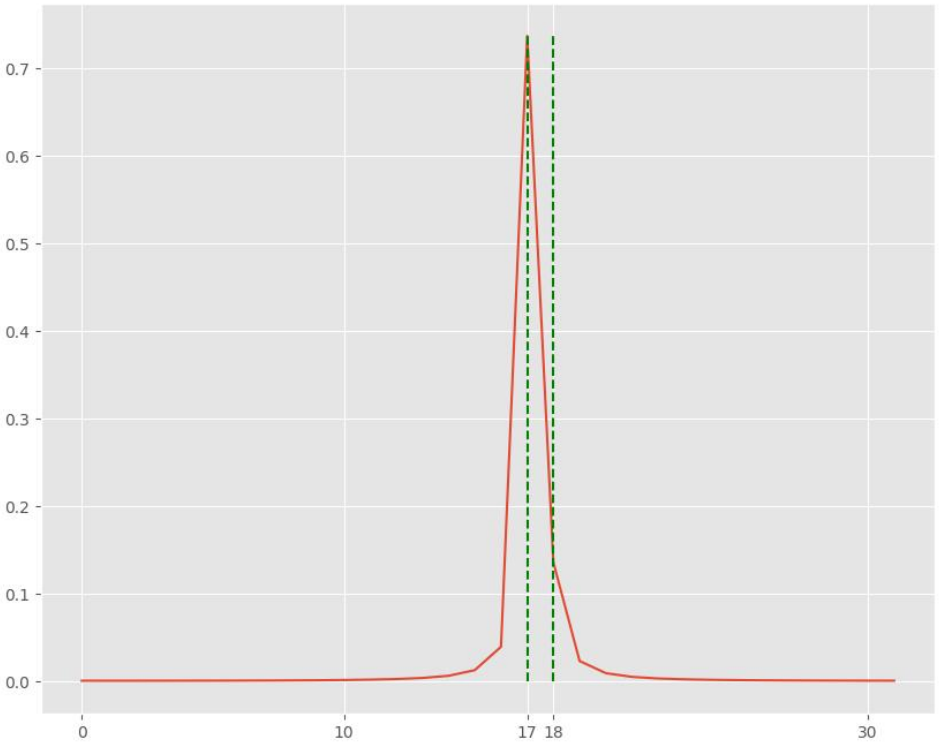


FIGURE 2. Ferjér kernel for $k = 17.3$ and $n = 5$.

for $n = 5$ and $k = 17.3$.

If we let $k = x_0 + r$, where $x_0 = \lfloor k \rceil$, so $r \in [-1/2, 1/2]$, then

$$\mathbb{P}(x_0 \mid |k\rangle_F) = \frac{\sin^2(\pi r)}{4^n \sin^2(\pi r/2^n)} \geq \frac{4}{\pi^2} \approx 0.41,$$

and in fact

$$\mathbb{P}(\lfloor x \rfloor \mid |k\rangle_F) + \mathbb{P}(\lceil x \rceil \mid |k\rangle_F) \geq \frac{8}{\pi^2} \approx 0.82.$$

15.2. **Quantum Phase Estimator/Digitizer.** Let $\mathcal{H}$ be the Hilbert space of m-qubit states. Given

- an implementation of an unitary operator U;
- an *eigenstate* $|\psi\rangle \in \mathcal{H}$ of U, with $U|\psi\rangle = \mathrm{e}^{2\pi\mathrm{i}\theta}|\psi\rangle$, with $0 \leq \theta < 1$;

we want to find or estimate θ.

Remark. Note that $|\psi\rangle \sim \mathrm{e}^{2\pi\mathrm{i}\theta}|\psi\rangle$, so physically there is no difference (and hence asking for θ, as is, is not a proper question). On the other hand, when we have a controlled gate CU given by

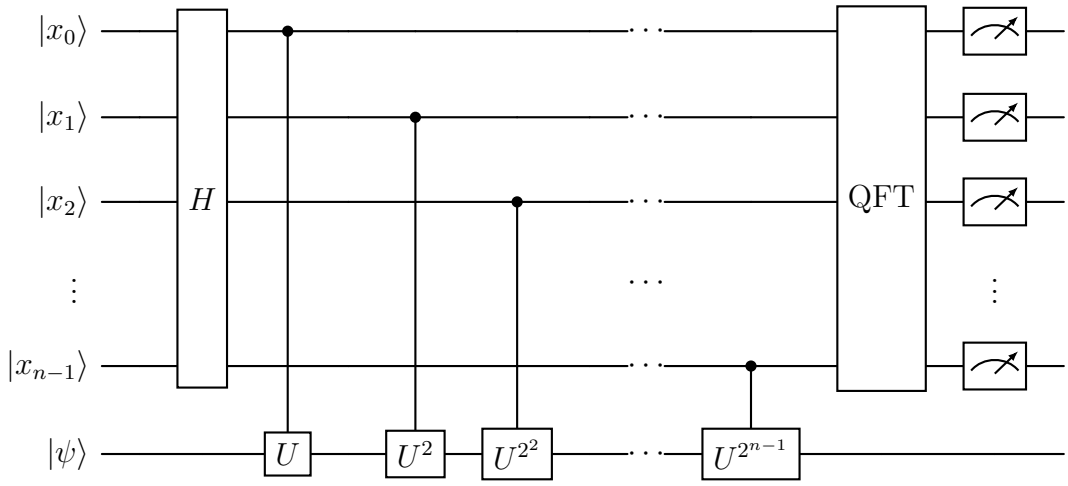
$$CU(|a\rangle|\psi\rangle) = |a\rangle U^a|\psi\rangle \quad (\text{for } a \in \mathbb{F}_2),$$

i.e.,

$$CU(\alpha|0\rangle|\psi\rangle + \beta|1\rangle|\psi\rangle) = \alpha|0\rangle|\psi\rangle + \beta\mathrm{e}^{2\pi\mathrm{i}\theta}|1\rangle|\psi\rangle,$$

then θ is relevant.

Definition 15.2. We define the n-qubit *quantum phase estimator* $\mathrm{QPE}|x\rangle_n|\psi\rangle$ as:



We then have that

$$\mathrm{QPE}|x\rangle_n|\psi\rangle = |x + 2^n\theta\rangle_F|\psi\rangle.$$

In particular,

$$\mathrm{QPE}|0\rangle_n|\psi\rangle = |2^n\theta\rangle_F|\psi\rangle.$$

Hence, measuring the first n qubits, we get either $\lfloor 2^n\theta \rfloor$ or $\lceil 2^n\theta \rceil$ with probability at least 82%. Pick the most likely $x_\theta \in \mathbb{Z}$ and then $\theta \approx x_\theta/2^n$.

16. Shor's Algorithm

Given $a \in \mathbb{Z}/N\mathbb{Z}$, with $\gcd(a, N) = 1$, f the order of $a \in \mathbb{Z}/N\mathbb{Z}^\times$. Classical methods are superpolynomial in $\log_2(N)$, with $\mathcal{O}\left((1+\epsilon)^{\log_2(N)}\right)$ for any $\epsilon > 0$.

Let $n \stackrel{\text{def}}{=} \lceil \log_2(N) \rceil$. Shor showed that one can implement

$$U_a \left|x\right\rangle_n = \begin{cases} \left|ax \bmod N\right\rangle_n, & \text{if } 0 \leq x < N; \\ \left|x\right\rangle_n, & \text{if } N \leq x < 2^n; \end{cases}$$

with $\mathcal{O}(n^2)$ gates and ancillas. Then, one can use QPE to compute the order.

16.1. **The Spectrum of U_a.** Suppose $\gcd(a, N) = 1$. Then for $x \geq N$, we have that $\left|x\right\rangle_n$ is an eigenstate of U_a, with eigenvalue 1.

Now, let $r \stackrel{\text{def}}{=} |a|$. Then, clearly we have that $x^r - 1$ is the minimal polynomial of U_a, so the eigenvalues of U_a are of the form $\mathrm{e}^{2\pi \mathrm{i} k/r}$, for $k \in \{0, 1, \ldots, r-1\}$.

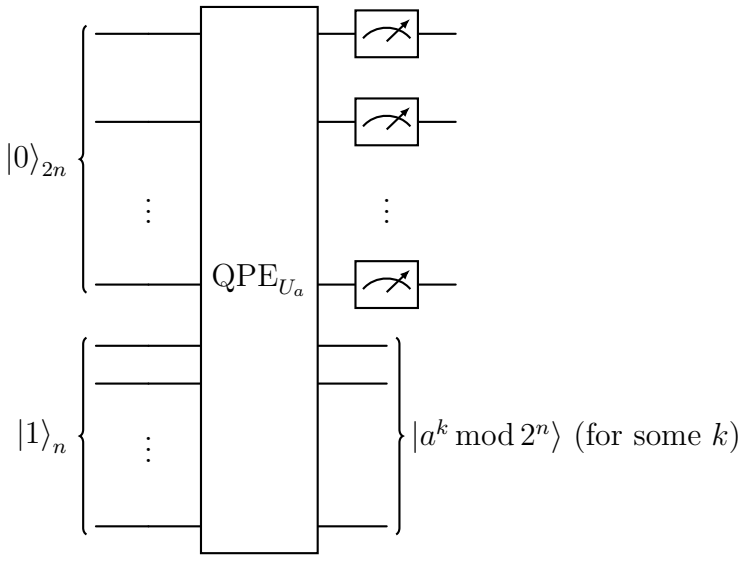
Let $\zeta_s \stackrel{\text{def}}{=} \mathrm{e}^{2\pi \mathrm{i}/r}$ and

$$\left|\phi_k\right\rangle \stackrel{\text{def}}{=} \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} \zeta_r^{ks} \left|a^s \bmod N\right\rangle$$

for $k \in \{0, 1, \ldots, r-1\}$. Then,

$$\begin{aligned} U_a \left|\phi_k\right\rangle &= \zeta_r^k \left|\phi_k\right\rangle; \\ \left\langle \phi_{k_1} \mid \phi_{k_2} \right\rangle &= \delta_{k_1, k_2}; \\ \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \left|\phi_k\right\rangle &= \left|1\right\rangle_n = \left|100\ldots0\right\rangle. \end{aligned}$$

Consider the circuit:



Since $U_{a^{2^k}}$ needs $\mathcal{O}(n^2)$ gates, we have that QPE_{U_a} needs $\mathcal{O}(n^3)$ gates.

Now:

$$\begin{aligned}
|a;n\rangle &\stackrel{\text{def}}{=} \mathrm{QPE}_{U_a}(|0\rangle_{2n}|1\rangle_n) \\
&= \mathrm{QPE}_{U_a}\left(|0\rangle_{2n}\frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}|\phi_k\rangle\right) \\
&= \frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}\mathrm{QPE}_{U_a}(|0\rangle_{2n}|\phi_k\rangle) \\
&= \frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}|2^{2n}k/r\rangle_F|\phi_k\rangle
\end{aligned}$$

So, for $0 \leq y < 2^{2n}$, we have

$$\mathbb{P}(y \mid |a;n\rangle) = \frac{1}{r}\sum_{k=0}^{r-1}\left|\langle y \mid 2^{2n}k/r\rangle_F\right|^2. \tag{5}$$

Now, for each k, the most likely y, i.e., the value that makes $\left|\langle y \mid 2^{2n}k/r\rangle_F\right|^2$ the largest, is the integer y closest to $2^{2n}k/r$, in which case we must have

$$\left|y - 2^{2n}\frac{k}{r}\right| \leq \frac{1}{2} \quad\Longleftrightarrow\quad \left|\frac{y}{2^{2n}} - \frac{k}{r}\right| \leq \frac{1}{2^{2n+1}}.$$

Lemma 16.1. *Let* $n \stackrel{\text{def}}{=} \lceil \log_2(N) \rceil \geq 2$. *Then, for a fraction* k/r *with* $0 \leq k < r < N$, *there is a unique* $y \in \{0, 1, 2, \ldots, 2^{2n} - 1\}$ *such that*

$$\left| \frac{y}{2^{2n}} - \frac{k}{r} \right| < \frac{1}{2^{2n+1}}.$$

Conversely, given $y \in \{0, 1, 2, \ldots, 2^{2n} - 1\}$, *if there exists* k/r *with* $0 \leq k < r < N$ *such that*

$$\left| \frac{y}{2^{2n}} - \frac{k}{r} \right| < \frac{1}{2^{2n+1}},$$

then this fraction k/r *is unique.*

Proof. We have

$$0 = \frac{0}{2^{2n}} \leq \frac{k}{r} \leq \frac{N-1}{N} = 1 - \frac{1}{N} \leq 1 - \frac{1}{2^n} < 1 - \frac{2}{2^{2n}} = \frac{2^{2n} - 2}{2^{2n}},$$

i.e.,

$$\frac{0}{2^{2n}} \leq \frac{k}{r} < \frac{2^{2n} - 2}{2^{2n}},$$

So, there $y_0 \in \{0, 1, \ldots, 2^{2n} - 2\}$ such that

$$\frac{y_0}{2^{2n}} \leq \frac{k}{r} < \frac{y_0 + 1}{2^{2n}}.$$

Thus, taking y as either y_0 or $y_0 + 1$, and hence $y \in \{0, 1, 2, \ldots, 2^{2n} - 1\}$, we can obtain

$$\left| \frac{y}{2^{2n}} - \frac{k}{r} \right| \leq \frac{1}{2} \frac{1}{2^{2n}} = \frac{1}{2^{2n+1}}.$$

On the other hand, the only way we get the equality is if

$$\frac{k}{r} = \frac{2y_0 + 1}{2^{2n+1}},$$

which would imply that $2^{2n+1} \mid r$ (since the fraction on the right is reduced), which is a contradiction, as $r \leq N \leq 2^n$. Thus, we have that there exists y with

$$\left| \frac{y}{2^{2n}} - \frac{k}{r} \right| < \frac{1}{2^{2n+1}}.$$

Now, suppose that we also have $y' \neq y$, with $y' \in \{0, 1, 2, \ldots, 2^{2n} - 1\}$, such that

$$\left| \frac{y'}{2^{2n}} - \frac{k}{r} \right| < \frac{1}{2^{2n+1}}.$$

Then,

$$\frac{1}{2^{2n}} \leq \left| \frac{y'}{2^{2n}} - \frac{y}{2^{2n}} \right| \leq \left| \frac{y'}{2^{2n}} - \frac{k}{r} \right| + \left| \frac{y}{2^{2n}} - \frac{k}{r} \right| < \frac{1}{2^{2n}},$$

which is a contradiction.

For the second part, assume that $k/r \neq k'/r'$, within the corresponding ranges and such that

$$\left| \frac{y}{2^{2n}} - \frac{k}{r} \right| < \frac{1}{2^{2n+1}}, \quad \left| \frac{y}{2^{2n}} - \frac{k'}{r'} \right| < \frac{1}{2^{2n+1}}.$$

Then, by the triangle inequality, we have that

$$\frac{1}{N^2} < \frac{1}{rr'} \leq \frac{|kr' - k'r|}{rr'} = \left| \frac{k}{r} - \frac{k'}{r'} \right| < \frac{1}{2^{2n}},$$

i.e., $N > 2^n$, or $\log_2(N) > n = \lceil \log_2(N) \rceil$, a contradiction. □

So, by Eq. (5), the first part of Theorem 16.1 and the previous section, when measuring the resulting $|a; n\rangle$, the first $2n$ qubits will correspond to some y close to some k/r. (If $y/2^{2n}$ is not close to any k/r, the probability in Eq. (5) is quite small!) Then, by the second part, this k/r is unique with

$$\left| \frac{y}{2^{2n}} - \frac{k}{r} \right| < \frac{1}{2^{2n+1}}.$$

We then can use *continued fractions* to find r: remember that there are $a_1, a_2, a_3, \ldots \in \mathbb{Z}$ such that

$$\frac{y}{2^{2n}} = [a_1, a_2, a_3, \ldots] \stackrel{\text{def}}{=} \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots}}}.$$

Then, if $[a_1, a_2, \ldots, a_n] = p_n/q_n$, then

$$\left| \frac{y}{2^{2n}} - \frac{p_n}{q_n} \right| < \frac{1}{2q_n^2}$$

Therefore, we use continued fractions until we get $\frac{1}{2q_n^2} \leq \frac{1}{2^{2n+1}}$ (with $q_n < N$ still). Then, we must have

$$\frac{k}{r} = \frac{p_n}{q_n},$$

We can then try to compute a^{q_n}. If we get 1, we found the order r! If not, we can try some small multiples that are still less than N. If that also fails, we can repeat the method of $|a^{q_n}|$. Alternatively, we could do another reading, which would likely give us another y with close $y/2^{2n}$ to (likely) another k/r, and find a new fraction p'_t/q'_t using continued fractions. If $q'_t s$ also does not work, but it is different from q_n, we know that $\operatorname{lcm}(q_n, q'_t) \mid r$.

17. Quantum Data Access Oracles

In classical data we often need functions $f : \mathbb{F}_2^n \to \mathbb{F}_2^d$, e.g., for lists, dictionaries, etc. How do we implement these on a quantum computer?

One possibility is to construct a *data access oracle*:

$$U_f \left|x\right\rangle_n \left|0\right\rangle_d \stackrel{\text{def}}{=} \left|x\right\rangle_n \left|f(x)\right\rangle_d .$$

(Note we do not specify $U_f \left|x\right\rangle_n \left|y\right\rangle_d$ for $y \neq 0$.) (How do we construct U_f?)

Alternatively, we could use *diagonal unitaries*:

$$\mathcal{D}_f \left|x\right\rangle_n \stackrel{\text{def}}{=} \mathrm{e}^{2\pi \mathrm{i}/2^d f(x)} \left|x\right\rangle_n$$

(seeing $f(x)$ as the integer corresponding to the one given by its binary representation). (How do we construct $\mathcal{D}_f$?)

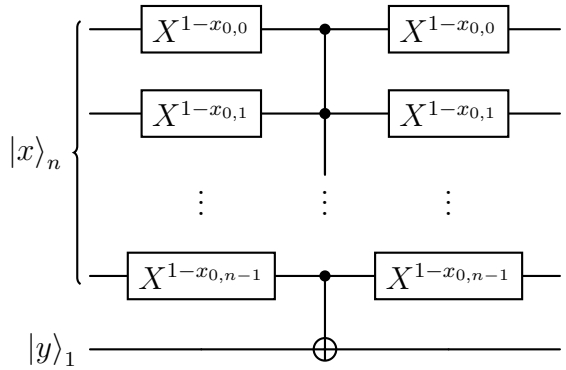
18. Implementing U_f

18.1. **Select QROM.** QROM means that f is in the circuit, not in the quantum computer.

Definition 18.1. Given $x_0 \in \mathbb{F}_2^n$, we define the gate $C_{x_0}^n X$ by:

$$C_{x_0}^n X \left|x\right\rangle_n \left|y\right\rangle_1 = \begin{cases} \left|x\right\rangle_n \left|y\right\rangle_1, & \text{if } x \neq x_0, \\ \left|x\right\rangle_n \left|y+1\right\rangle_1, & \text{if } x = x_0. \end{cases}$$

If $x_0 = x_{0,0} + x_{0,1} \cdot 2 + c_{0,2} \cdot 2^2 + \cdots + c_{0,n-1} \cdot 2^{n-1}$, then we have the $C_{x_0}^n X$ is given by



The circuit above works by simply making $\left|x_0\right\rangle_n \mapsto \left|11\cdots1\right\rangle$ in the first step (and $\left|x\right\rangle$ does not give $\left|111\cdots1\right\rangle$ when $x \neq x_0$), then the control gates flips $\left|0\right\rangle$ to $\left|1\right\rangle$, and then undoing the first step.

Remark. Note that $C_{x_0}^n X$ is the same U_f for

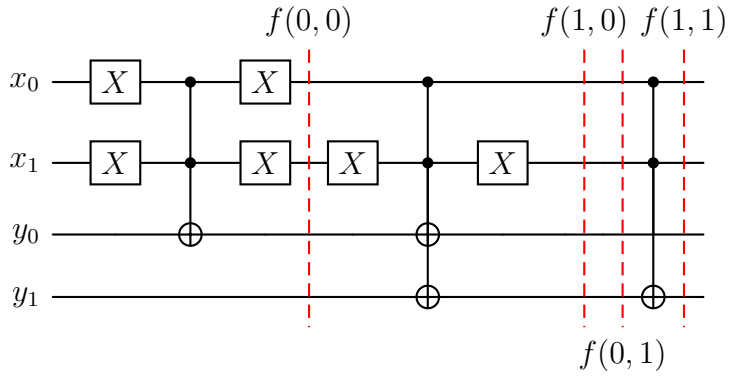
$$f(x) = \begin{cases} 0, & \text{if } x \neq x_0, \\ 1, & \text{if } x = x_0. \end{cases}$$

Then, to implement C_f, we just use various $C_{x_0}^n X$ flipping the corresponding qubits in the output. (See example below.)

Example 18.2. Consider

$$f(0,0) = (1,0), \qquad f(1,0) = (1,1),$$
$$f(0,1) = (0,0), \qquad f(1,1) = (0,1).$$

Here is C_f:



Remarks. (1) This naive implementation often have many cancellations of consecutive X gates.

(2) The state of the art implementation can be done with $\mathcal{O}(d2^n)$ H, S, and CX gates, and $\mathcal{O}(2^n)$ T gates.

(3) This select QROM is efficient when f has either few non-zero entries or if its *unstructured*.

(4) The size of the ancilla in this case is just d, so it is *shallow* (few ancillas).

(5) On the other hand, it is *long*.

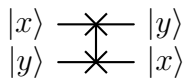
(6) Much better if the data is sparse, with many zeros.

18.2. **Swap QRAM.** QRAM means that the quantum computer knows f, not the circuit.

Definition 18.3. The *swap gate* SWAP is defined as

$$\text{SWAP} \left|x\right\rangle_1 \left|y\right\rangle_1 \stackrel{\text{def}}{=} \left|y\right\rangle_1 \left|x\right\rangle_1 .$$

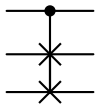
It is represented by:



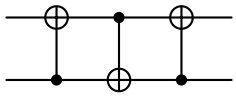
The *controlled swap gate* CSWAP is defined as

$$\text{CSWAP}\,|xyz\rangle = \begin{cases} |xyz\rangle\,, & \text{if } x = 0, \\ |xzy\rangle\,, & \text{if } x = 1. \end{cases}$$

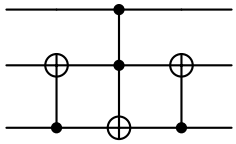
It is represented as



Note that SWAP can be implemented as



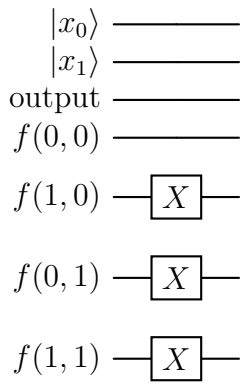
and CSWAP as



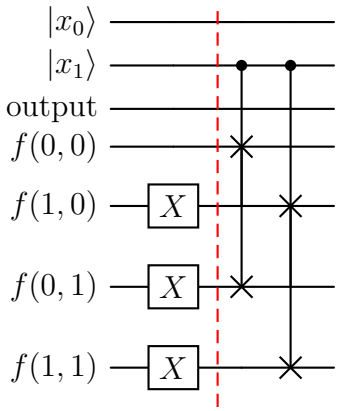
Example 18.4. Let's give an example of a QRAM swap with $n = 2$ and $d = 1$:

$$f(0,0) = 0, \qquad f(1,0) = 1$$
$$f(0,1) = 1, \qquad f(1,1) = 1$$

We first create the possible outputs in the last 2^n qubits, corresponding to $f(0,0)$, $f(1,0)$, $f(0,1)$, and $f(1,1)$ respectively:

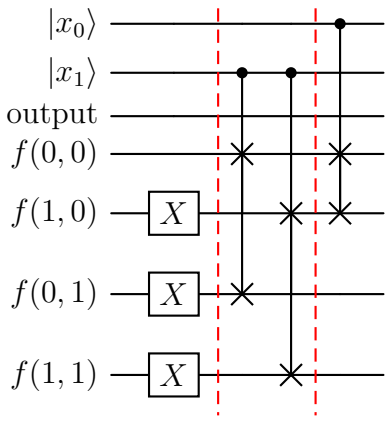


If the last qubit of the input is 1, we swap the correct output to the places where the last qubits were 0:

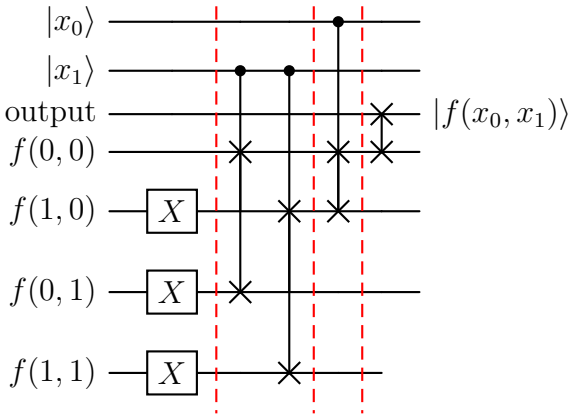


This makes the correct output $f(x_0, x_1)$ to be in the spots of $f(x_0, 0)$.

Then, if the first qubit is 1, we swap the correct output to where the first qubits were 0:



This makes then the correct output $f(x_0, x_1)$ to be in the spot of $f(0,0)$. At this point we could just measure the fourth qubit (corresponding to $f(0,0)$), but we could do a final swap to put it in the third spot:



Example 18.5. Here is a more complex example (without the final swap), the same as above:

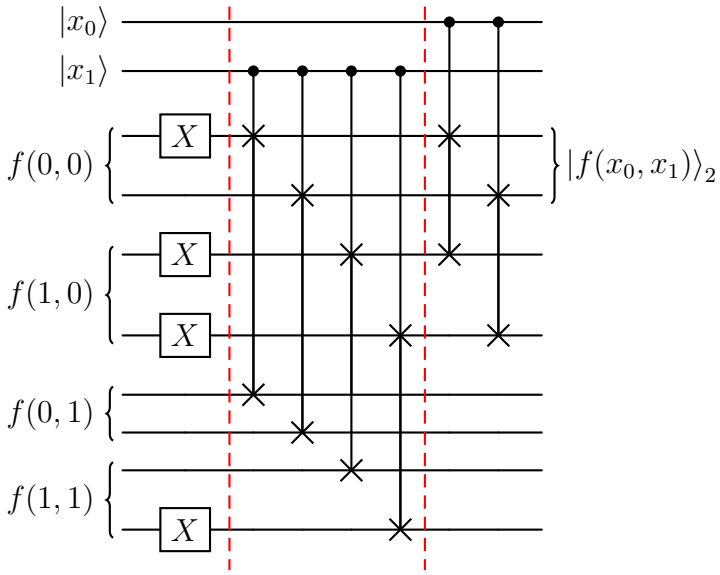
$$f(0,0) = (1,0), \qquad f(1,0) = (1,1),$$
$$f(0,1) = (0,0), \qquad f(1,1) = (0,1).$$

The steps are the same:

(1) set the correct outputs for $f(x_0, y_0)$ in their respective spots;

(2) place the result of $f(x_0, y_0)$ in the spots for $f(x_0, 0)$;
(3) place the result of $f(x_0, y_0)$ in the spots for $f(0, 0)$.

We have:



Remark. The ancilla needed in this method needs $2^n d$ qubits, so it is very *wide*, but is shallow (not long). Even the state of the art has $\mathcal{O}(d2^n)$ gates. (Much better if the data is sparse, with many zeros.)

18.3. **Select-Swap.** One can combine the two methods. We can select k qubits at the end of the input of f to obtain a function $g : \mathbb{F}_2^{n-k} \to \mathbb{F}_2^{d2^k}$:

$$g(x_0, \ldots, x_{n-k-1}) \stackrel{\text{def}}{=} (g_1(x_0, \ldots, x_{n-k-1}), \ldots, g_{2^k-1}(x_0, \ldots, x_{n-k-1})),$$

where $g_i : \mathbb{F}_2^{n-k} \to \mathbb{F}_2^d$ is defined as

$$g_i(x_0, \ldots, x_{n-k-1}) \stackrel{\text{def}}{=} f(x_0, \ldots, x_{n-k-1}, \text{“}k \text{ binary representation of } i\text{”}).$$

We can then use the select method for each g_i and then swap to get the correct answer in the $f(0, 0, \ldots, 0)$ spot.

This makes it so we need $d2^k$ ancillas, compared to the $d2^n$ of the swap method.

Example 18.6. Consider

$$f(0,0,0,0) = (0,1,0) \quad f(1,0,0,0) = (1,0,0), \quad f(0,1,0,0) = (0,0,0) \quad f(1,1,0,0) = (1,1,0),$$
$$f(0,0,1,0) = (0,0,1) \quad f(1,0,1,0) = (0,0,1), \quad f(0,1,1,0) = (0,1,0) \quad f(1,1,1,0) = (0,1,0),$$
$$f(0,0,0,1) = (0,0,0) \quad f(1,0,0,1) = (1,1,0), \quad f(0,1,0,1) = (1,1,1) \quad f(1,1,0,1) = (0,0,0),$$
$$f(0,0,1,1) = (1,1,1) \quad f(1,0,1,1) = (0,1,0), \quad f(0,1,1,1) = (0,0,0) \quad f(1,1,1,1) = (0,1,0).$$

For $k = 2$, we have:

$$g_0(0,0) = (0,1,0), \qquad g_0(1,0) = (1,0,0),$$
$$g_0(0,1) = (0,0,0), \qquad g_0(1,1) = (1,1,0),$$

and

$$g_1(0,0) = (0,0,1), \qquad g_1(1,0) = (0,0,1),$$
$$g_1(0,1) = (0,1,0), \qquad g_1(1,1) = (0,1,0),$$

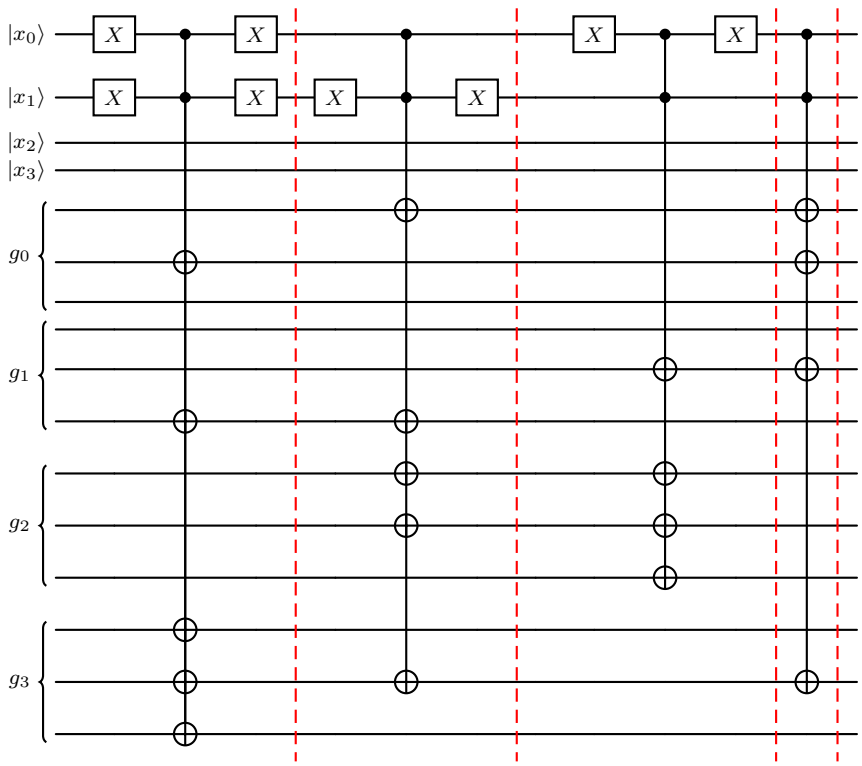
and

$$g_2(0,0) = (0,0,0), \qquad g_2(1,0) = (1,1,0),$$
$$g_2(0,1) = (1,1,1), \qquad g_2(1,1) = (0,0,0),$$

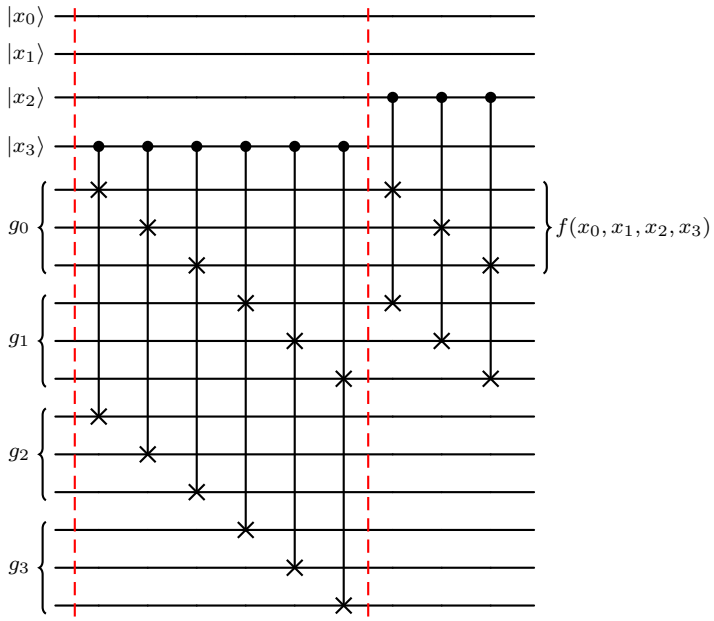
and

$$g_3(0,0) = (1,1,1), \qquad g_3(1,0) = (0,1,0),$$
$$g_3(0,1) = (0,0,0), \qquad g_3(1,1) = (0,1,0).$$

We then get:



followed by the swaps:



So,

$$U_f^{\text{Sel}-\text{Swap}} |x\rangle_n |0\rangle_{d2^k} = |x\rangle_n |f(x)\rangle_d |\text{garbage}\rangle_{d(2^k-1).}$$

The total cost is the cost of the 2^k select, plus the swap of k. So, the total gate cost is $\mathcal{O}(d2^k)$ and width $\mathcal{O}(2^{n-k} + d2^k)$. Choosing $k \approx n/2$, we get $\mathcal{O}\left(\sqrt{d2^n}\right)$.

Remark. If we restrict to H, T, S, and CX, then the T cost is only $\mathcal{O}\left(\sqrt{d2^n}\right)$. (A bit higher on the others.)

18.4. **Diagonal Unitary.** Given some $\theta : \mathbb{F}_2^n \to [0, 1)$, we might want

$$U_\theta |x\rangle_n = \mathrm{e}^{2\pi \mathrm{i}\theta(x)} |x\rangle_n .$$

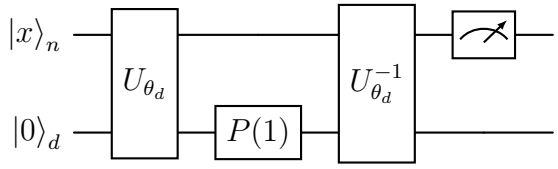
We can approximate it using data access oracles.

If $\epsilon > 0$ is the error, and in binary

$$\theta(x) = 0.\underbrace{y_0 y_1 \cdots y_d}_{\stackrel{\text{def}}{=} \theta_d(x)} y_{d+1} y_{d+2} \cdots$$

then $\theta_d : \mathbb{F}_2^n \to \mathbb{F}_2^d$ and $\left|\mathrm{e}^{2\pi \mathrm{i}\theta(x)} - \mathrm{e}^{2\pi \mathrm{i}\theta_d(x)}\right| \leq c/2^d < \epsilon$, for some constant c. So, we need $d \approx \log_2(1/\epsilon) + \mathcal{O}(1)$.

So, with the data access oracle U_{θ_d}, we can make



where the P gate is given as in Definition 14.6:

$$P(1) |x\rangle_n \stackrel{\text{def}}{=} P(1/2^{n-1}) |x_0\rangle \otimes P(1/2^{n-2}) |x_1\rangle \otimes \cdots \otimes P(1) |x_{n-1}\rangle .$$

This works since we get

$$\begin{aligned}
|x\rangle_n |0\rangle_d &\mapsto |x\rangle_n |\theta_d(x)\rangle_d \\
&\mapsto |x\rangle_n \mathrm{e}^{2\pi \mathrm{i}\theta_d(x)/2^d} |\theta_d(x)\rangle_d \\
&= \mathrm{e}^{2\pi \mathrm{i}\theta_d(x)/2^d} |0\rangle_n |\theta_d(x)\rangle_d \\
&\mapsto \left(\mathrm{e}^{2\pi \mathrm{i}\theta_d(x)/2^d} |0\rangle_n\right) |0\rangle_d \\
&\approx \left(\mathrm{e}^{2\pi \mathrm{i}\theta(x)} |0\rangle_n\right) |0\rangle_d .
\end{aligned}$$

One more observation. Let:

Definition 18.7. Given $\theta : \mathbb{F}_2^n \to [0,1)$ as above, a*multiplexer* of type Y (or X, or Z):

$$R_Y(\theta) |x\rangle_n |\psi\rangle_1 = |x\rangle_n R_Y(\theta(x)) |\psi\rangle_1 ,$$

with

$$R_Y(\theta) = \begin{pmatrix} \cos(\theta/2) & -\sin(\theta/2) \\ \sin(\theta/2) & \cos(\theta/2) \end{pmatrix}$$

as in Section 6.

These can also be done with data access oracles!

19. Quantum State Preparation

Given $\{\psi_x : x \in \mathbb{F}_2^n\} \subseteq \mathbb{C}^{2n}$, can we construct U_ψ such that $U_\psi |0\rangle_n = |\psi\rangle_n$?

Here is a construction that is not always the best, but always works and often is the best. We construct it inductively.

(1) Let $\psi_x = \mathrm{e}^{2\pi \mathrm{i}\theta(x)}\rho_x$, where $\rho_x \stackrel{\text{def}}{=} |\psi_x|$. Then, $|\psi\rangle = U_\theta |\rho\rangle$. (We can choose, for instance, $\theta(x) = 0$ if $\rho_x = 0$.) Since we can get U_θ, we may assume without loss of generality that $\psi_x \geq 0$ for all x.

(2) Let

$$\begin{aligned}|\psi\rangle_n &= \sum_{x\in\mathbb{F}_2^n} \psi_x |x\rangle_n \\ &= \sum_{y\in\mathbb{F}_2^{n-1}} \psi_{y0} |y\rangle_{n-1} |0\rangle + \psi_{y1} |y\rangle_{n-1} |1\rangle \\ &= |\chi\rangle_{n-1} \otimes (C(y) |0\rangle + S(y) |1\rangle),\end{aligned}$$

where

$$\begin{aligned}|\chi\rangle_{n-1} &\stackrel{\text{def}}{=} \sum_{y\in\mathbb{F}_2^{n-1}} \sqrt{\psi_{y0}^2 + \psi_{y1}^2}\, |y\rangle_{n-1}, \\ C(y) &\stackrel{\text{def}}{=} \frac{\psi_{y0}}{\sqrt{\psi_{y0}^2 + \psi_{y1}^2}}, \\ S(y) &\stackrel{\text{def}}{=} \frac{\psi_{y1}}{\sqrt{\psi_{y0}^2 + \psi_{y1}^2}}.\end{aligned}$$

(Note that if $\psi_{y0} = \psi_{y1} = 0$ above, we can just skip the term in the summation.)

Note that since $C(y), S(y) \geq 0$ and $C(y)^2 + S(y)^2 = 1$, there exists a unique $\theta(y) \in [0, \pi]$ such that $C(y) = \cos(\theta(y)/2)$ and $S(y) = \sin(\theta(y)/2)$.

Also,

$$\langle \chi \mid \chi \rangle = \sum_{y\in\mathbb{F}_2^{n-1}} \psi_{y0}^2 + \psi_{y1}^2 = \sum_{x\in\mathbb{F}_2^n} \psi_x^2 = \langle \psi \mid \psi \rangle = 1.$$

(3) If we can prepare $|\chi\rangle_{n-1}$, we can prepare $|\psi\rangle_n$, as

$$|\psi\rangle_n = (\mathbb{I} \otimes R_Y(\theta)) |\chi\rangle_{n-1} |0\rangle_1 .$$

(4) Finally, we can prepare any initial 1-qubit state, exactly as above, as given $|\psi\rangle_1 = a |0\rangle + b |1\rangle$ there is some θ such that $R_Y(\theta) |0\rangle = |\psi\rangle_1$.

Notation

Index