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*

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

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 facing 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!)

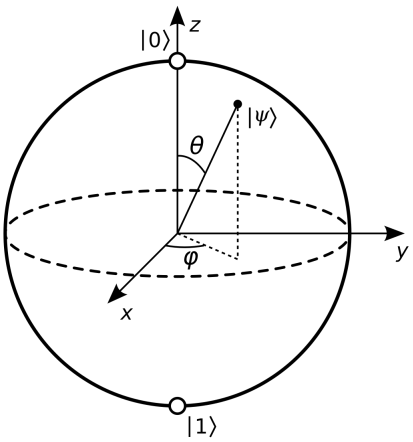


FIGURE 1. Bloch Sphere

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*:

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

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 $R_Z(\pi/4) \sim T$.*

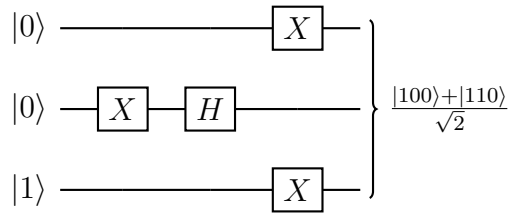
Theorem 6.1. *If $U \in \mathrm{U}_2(\mathbb{C})$, then*

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

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:

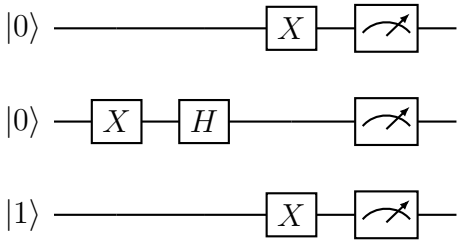


Breaking it down in steps:

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

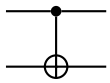
So, the probability that we get $|100\rangle$ or $|110\rangle$ is $1/2$ each, and 0 for every other state.

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*

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

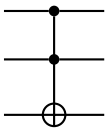
generates all gates, i.e., it generates $U_{2^n}(\mathbb{C})$.

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 $C^{n-1}U$.

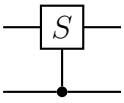
Note: These may be hard to create using only one-qubit gates and CNOT! See this Stack exchange post.

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

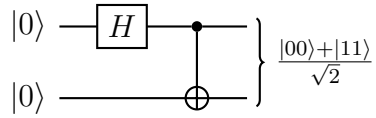
$$c^2 \left(\frac{1}{2} + \frac{3}{16} \right) = 1$$

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

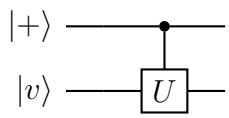
$$|0\rangle \otimes \left(\frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle\right),$$

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 ($(H \otimes \mathbb{I}) \circ \text{CNOT}$):

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

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

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

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

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

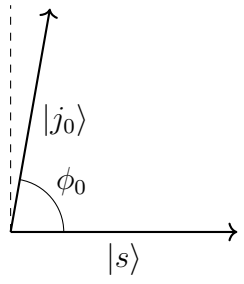
$$\mathbb{P}(\textit{getting } j_0 \mid \psi_k) = 1 - \mathcal{O}\left(\frac{1}{N}\right).$$

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

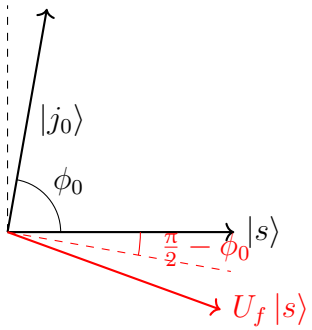
$$\langle j_0 \mid s \rangle = \frac{1}{2^{n/2}} \sum_{j \in \mathbb{F}_2^n} \langle j_0 \mid j \rangle = \frac{1}{2^{n/2}}.$$

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

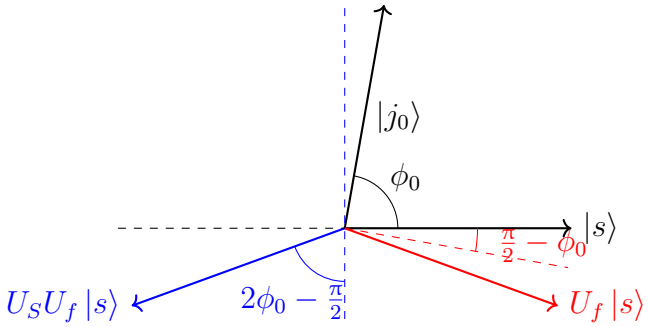


Then, by the inner product above, we have that $\phi_0 = \arccos(2^{-n/2})$.

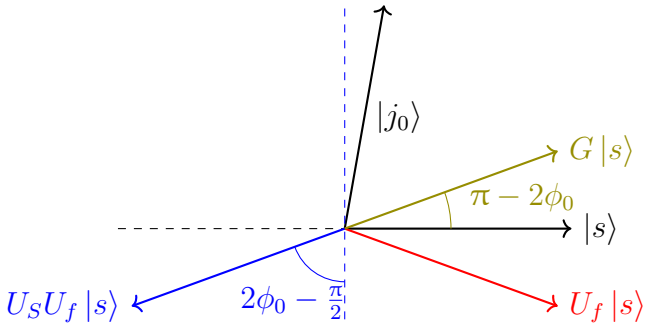
Note that U_S and U_f are *reflections*, so G is a rotation by some angle α. In the plane containing $|s\rangle$ and $|j_0\rangle$, U_f reflects on the line perpendicular to $|j_0\rangle$:



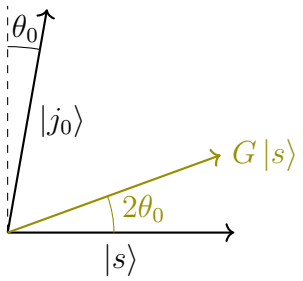
Similarly, U_S reflects on the line perpendicular to $|s\rangle$.



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* $N \geq 2$*. Then, for* $a \in \mathbb{Z}/N\mathbb{Z} \setminus \{0\}$ *such that* $N/\gcd(a,N) \geq 2$*, we have*

$$\sum_{b=0}^{N-1} \zeta_N^{ab} = 0.$$

Proof. Let $d \stackrel{\text{def}}{=} (a,N)$ and $a = da_1$, $N = dN_1$. Then, $\zeta_N^a = \mathrm{e}^{2\pi\mathrm{i}/N\cdot a} = \mathrm{e}^{2\pi\mathrm{i}/N_1\cdot a_1} \stackrel{\text{def}}{=} \zeta_{N_1}$. Since $\gcd(a_1, N_1) = 1$, we have that ζ_{N_1} is a *primitive* N_1-st root of unity and so

$$\Phi_{N_1}(X) \stackrel{\text{def}}{=} X^{N_1} - 1 = \prod_{i=0}^{N_1-1} (X - \zeta_{N_1}^i).$$

Hence, if $N_1 \geq 2$, we have that the coefficient of X^{N_1-1} in $\Phi_{N_1}(X)$ is 0. But this coefficient is simply

$$-\sum_{i=0}^{N_1-1} \zeta_{N_1}^i = -\sum_{i=0}^{N_1-1} \zeta_N^{ai} = 0.$$

Noting that $\zeta_{N_1}^{x+N_1} = \zeta_{N_1}^x$, we have that

$$\begin{aligned}
\sum_{b=0}^{N-1} \zeta_N^{ab} &= \sum_{b=0}^{N-1} \zeta_{N_1}^b \\
&= \sum_{b=0}^{N_1-1} \zeta_{N_1}^b + \sum_{b=N_1}^{2N_1-1} \zeta_{N_1}^b + \cdots + \sum_{b=(d-1)N_1}^{dN_1-1} \zeta_{N_1}^b \\
&= \sum_{b=0}^{N_1-1} \zeta_{N_1}^b + \sum_{b=0}^{N_1-1} \zeta_{N_1}^b + \cdots + \sum_{b=0}^{N_1-1} \zeta_{N_1}^b \\
&= 0 + 0 + \cdots + 0 = 0.
\end{aligned}$$

□

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 preceding page we have:

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

□

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. Let $\zeta_{2^n} \stackrel{\text{def}}{=} \mathrm{e}^{2\pi \mathrm{i}/2^n}$. We define the *P gate*:

$$P(k)\left|x\right\rangle_n \stackrel{\text{def}}{=} \zeta_{2^n}^{xk}\left|x\right\rangle_n .$$

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

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

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

i.e.,

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

or

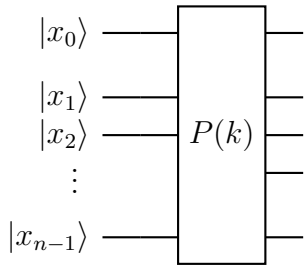
$$A_k = \operatorname{QFT}^\dagger \circ P(k) \operatorname{QFT} . \tag{3}$$

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

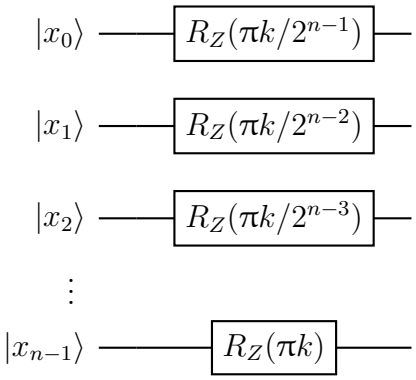
The P gate is easy to implement: remembering that

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

the circuit



up to a global phase factor, is the same as the n one-qubit gates



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. □

Notation

Index