Quantum algorithms for factorization and other problems

Pierre-Alain Fouque

Centre Inria de l'Université de Rennes

Contents

Basic Circuits

Quantum Hadamard Gates

A very important gate

1. Gate H: $|0\rangle \mapsto \frac{|0\rangle+|1\rangle}{\sqrt{2}} \quad |1\rangle \mapsto \frac{|0\rangle-|1\rangle}{\sqrt{2}}$
2. By linearity, $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, $\mathsf{H}|\psi\rangle = \alpha\mathsf{H}|0\rangle + \beta\mathsf{H}|1\rangle$
   $\mathsf{H}|\psi\rangle = \frac{\alpha}{\sqrt{2}}(|0\rangle + |1\rangle) + \frac{\beta}{\sqrt{2}}(|0\rangle - |1\rangle) = \frac{\alpha+\beta}{\sqrt{2}}|0\rangle + \frac{\alpha-\beta}{\sqrt{2}}|1\rangle$

Quantum Hadamard Gates

A very important gate

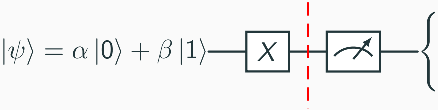
1. Gate H: $|0\rangle \mapsto \frac{|0\rangle+|1\rangle}{\sqrt{2}} \quad |1\rangle \mapsto \frac{|0\rangle-|1\rangle}{\sqrt{2}}$
2. By linearity, $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, $\mathsf{H}|\psi\rangle = \alpha\mathsf{H}|0\rangle + \beta\mathsf{H}|1\rangle$
   $\mathsf{H}|\psi\rangle = \frac{\alpha}{\sqrt{2}}(|0\rangle + |1\rangle) + \frac{\beta}{\sqrt{2}}(|0\rangle - |1\rangle) = \frac{\alpha+\beta}{\sqrt{2}}|0\rangle + \frac{\alpha-\beta}{\sqrt{2}}|1\rangle$
3. Matrix version: $M_{\mathsf{H}} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

   $$M_{\mathsf{H}}|0\rangle = M_{\mathsf{H}}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{|0\rangle + |1\rangle}{\sqrt{2}}.$$

   Similarly for $M_{\mathsf{H}}|1\rangle$.
4. Eg., if $|\psi\rangle = i|0\rangle + (2+i)|1\rangle$, compute $M_{\mathsf{H}}|\psi\rangle$?

Some Quantum Circuits

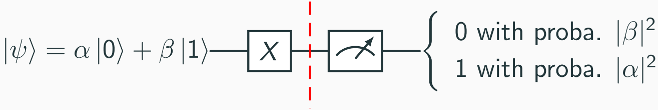
$$X|\psi\rangle = \beta|0\rangle + \alpha|1\rangle$$



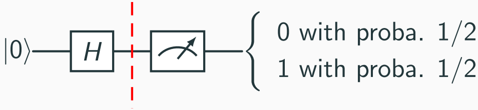
$$\begin{cases} 0 \text{ with proba. } |\beta|^2 \\ 1 \text{ with proba. } |\alpha|^2 \end{cases}$$

Some Quantum Circuits

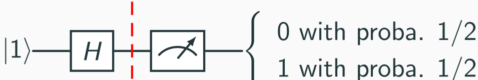
$$X|\psi\rangle = \beta|0\rangle + \alpha|1\rangle$$



$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$



$$H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$



2-qubits $\Rightarrow$ 4 possibilities

2-qubit

- $|\psi\rangle = \alpha\,|0.0\rangle + \beta\,|0.1\rangle + \gamma\,|1.0\rangle + \delta\,|1.1\rangle$, with $\alpha, \beta, \gamma, \delta \in \mathbb{C}$
- $|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1$
- $\begin{pmatrix} a \\ b \end{pmatrix} \otimes \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} ac \\ ad \\ bc \\ bd \end{pmatrix}$ and $|0\rangle \otimes |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = |0.0\rangle$

Vectors

$$|0.0\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix},\ |0.1\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix},\ |1.0\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix},\ |1.1\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix},\ |\psi\rangle = \begin{pmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{pmatrix}$$

Operations on qubits

- Addition of qubits: $|\phi\rangle = (1+3i)|0\rangle + 2i|1\rangle$ and $|\psi\rangle = 3|0\rangle + (1-i)|1\rangle$,

$$|\phi\rangle + |\psi\rangle = (4+3i)|0\rangle + (1+i)|1\rangle$$

  For 2 2-qubits: $(|1.0\rangle + |0.1\rangle) + (|1.0\rangle - |0.1\rangle) = 2|1.0\rangle$

- Multiplication of 2 1-qubit is a 2-qubit: $|\phi\rangle \cdot |\psi\rangle$

$$((1+3i)|0\rangle + 2i|1\rangle) \otimes (3|0\rangle + (1-i)|1\rangle)$$
$$(1+3i)\cdot 3 \cdot |0\rangle|0\rangle + (1+3i)\cdot(1-i)|0\rangle|1\rangle + 6i\cdot|1\rangle|0\rangle + ...$$
$$(3+9i)|0.0\rangle + (4+2i)|0.1\rangle + 6i|1.0\rangle + (2+2i)|1.1\rangle$$

CNOT Gate: controlled gate with 2-qubit

If … then … else …

- $|0.0\rangle \mapsto |0.0\rangle, |0.1\rangle \mapsto |0.1\rangle, |1.0\rangle \mapsto |1.1\rangle, |1.1\rangle \mapsto |1.0\rangle$
- If $|0.0\rangle = \begin{pmatrix}1\\0\\0\\0\end{pmatrix}$, $|0.1\rangle = \begin{pmatrix}0\\1\\0\\0\end{pmatrix}$, $|1.0\rangle = \begin{pmatrix}0\\0\\1\\0\end{pmatrix}$, $|1.1\rangle = \begin{pmatrix}0\\0\\0\\1\end{pmatrix}$,

  $M = \begin{pmatrix}1 & 0 & 0 & 0\\0 & 1 & 0 & 0\\0 & 0 & 0 & 1\\0 & 0 & 1 & 0\end{pmatrix}$, the upper left submatrix is the identity performed on the first line, the bottom right submatrix is the inversion operation performed on the second line

Quantum Circuit

where A is a unitary $A^* A = I_n$

Theorem
Every n-qubit quantum gate can be realized with a circuit using only CNOT and 1-qubit gates

Quantum Circuit

$|\psi\rangle \xrightarrow{/^{n}} \boxed{A} \xrightarrow{/^{n}} A|\psi\rangle$ where A is a unitary $A^*A = I_n$

Theorem
Every n-qubit quantum gate can be realized with a circuit using only CNOT and 1-qubit gates

Theorem (Solovay-Kitaev)
There is an infinite number of 1-qubit gates, and every such gate can be approximated with only H, T, and CNOT gates

The T gate: $|0\rangle \mapsto |0\rangle$ and $|1\rangle \mapsto e^{i\pi/4}|1\rangle$: $T = e^{i\pi/8}\begin{pmatrix} e^{-\pi/8} & 0 \\ 0 & e^{\pi/8} \end{pmatrix}$

Quantum Circuit

where A is a unitary $A^*A = I_n$

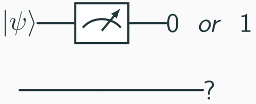
Theorem
Every n-qubit quantum gate can be realized with a circuit using only CNOT and 1-qubit gates

Theorem (Solovay-Kitaev)
There is an infinite number of 1-qubit gates, and every such gate can be approximated with only H, T, and CNOT gates

Theorem: Toffoli (CCNOT) is a universal gate

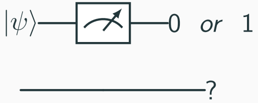
- Toffoli gate is invertible: $(|a.b.c\rangle \mapsto |a.b.c \oplus (ab)\rangle)$:
  $T|a.b.1\rangle = |a.b.NAND(a,b)\rangle$
- Any classical circuit using N gates in the set AND, OR, NOT (universal gates for classical circuits) can be computed using $O(N)$ Toffoli gates

Partial Measurement of a 2-qubit

- $|\psi\rangle = \alpha\,|0.0\rangle + \beta\,|0.1\rangle + \gamma\,|1.0\rangle + \delta\,|1.1\rangle$, $|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1$
- 

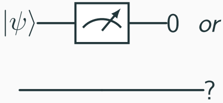
- If one measures the first qubit as 1, what is the second qubit ?

Partial Measurement of a 2-qubit

- $|\psi\rangle = \alpha\,|0.0\rangle + \beta\,|0.1\rangle + \gamma\,|1.0\rangle + \delta\,|1.1\rangle$, $|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1$
- 

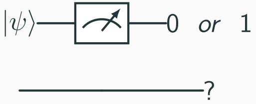
- If one measures the first qubit as 1, what is the second qubit ?
- E.g., If $|\psi\rangle = \frac{\sqrt{2}}{2}\,|0.0\rangle + \frac{1}{2}\,|0.1\rangle + \frac{1}{2}\,|1.1\rangle$, then if we observe $|1\rangle$ on the first qubit, the second is $|1\rangle$.

Partial Measurement of a 2-qubit

- $|\psi\rangle = \alpha|0.0\rangle + \beta|0.1\rangle + \gamma|1.0\rangle + \delta|1.1\rangle$, $|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1$
- 

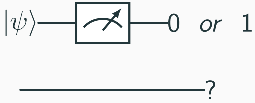
- If one measures the first qubit as 1, what is the second qubit ?
- E.g., If $|\psi\rangle = \frac{\sqrt{2}}{2}|0.0\rangle + \frac{1}{2}|0.1\rangle + \frac{1}{2}|1.1\rangle$, then if we observe $|1\rangle$ on the first qubit, the second is $|1\rangle$.
- If we observe $|0\rangle$, as $|\psi\rangle = \frac{|0\rangle}{2} \cdot (\sqrt{2}|0\rangle + |1\rangle) + \frac{1}{2}|1\rangle|1\rangle$, the second qubit is $\sqrt{\frac{2}{3}}|0\rangle + \frac{1}{\sqrt{3}}|1\rangle$

Partial Measurement of a 2-qubit

- $|\psi\rangle = \alpha\,|0.0\rangle + \beta\,|0.1\rangle + \gamma\,|1.0\rangle + \delta\,|1.1\rangle$, $|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1$
- 

- If one measures the first qubit as 1, what is the second qubit ?
- E.g., If $|\psi\rangle = \frac{\sqrt{2}}{2}\,|0.0\rangle + \frac{1}{2}\,|0.1\rangle + \frac{1}{2}\,|1.1\rangle$, then if we observe $|1\rangle$ on the first qubit, the second is $|1\rangle$.
- If we observe $|0\rangle$, as $|\psi\rangle = \frac{|0\rangle}{2} \cdot (\sqrt{2}\,|0\rangle + |1\rangle) + \frac{1}{2}\,|1\rangle\,|1\rangle$, the second qubit is $\sqrt{\frac{2}{3}}\,|0\rangle + \frac{1}{\sqrt{3}}\,|1\rangle$
- More generally, $|\psi\rangle = |0\rangle \cdot (\alpha\,|0\rangle + \beta\,|1\rangle) + |1\rangle \cdot (\gamma\,|0\rangle + \delta\,|1\rangle)$, and if one measures $|0\rangle$ for the first qubit, the second is $\frac{\alpha}{\sqrt{|\alpha|^2+|\beta|^2}}\,|0\rangle + \frac{\beta}{\sqrt{|\alpha|^2+|\beta|^2}}\,|1\rangle$

Partial Measurement of a 2-qubit

- $|\psi\rangle = \alpha\,|0.0\rangle + \beta\,|0.1\rangle + \gamma\,|1.0\rangle + \delta\,|1.1\rangle$, $|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1$
- 

- If one measures the first qubit as 1, what is the second qubit ?
- E.g., If $|\psi\rangle = \frac{\sqrt{2}}{2}\,|0.0\rangle + \frac{1}{2}\,|0.1\rangle + \frac{1}{2}\,|1.1\rangle$, then if we observe $|1\rangle$ on the first qubit, the second is $|1\rangle$.
- If we observe $|0\rangle$, as $|\psi\rangle = \frac{|0\rangle}{2} \cdot (\sqrt{2}\,|0\rangle + |1\rangle) + \frac{1}{2}\,|1\rangle\,|1\rangle$, the second qubit is $\sqrt{\frac{2}{3}}\,|0\rangle + \frac{1}{\sqrt{3}}\,|1\rangle$
- Exo: If $|\psi\rangle = \frac{1}{5}(2\,|0.0.0\rangle - |0.0.1\rangle + 3\,|0.1.0\rangle + |0.1.1\rangle - 2\,|1.0.0\rangle + 2\,|1.0.1\rangle + \sqrt{2}\,|1.1.1\rangle)$, and we measure 0.0, what is the last qubit ?

First algorithm: Deutsch-Jozsa

Quantum oracle gate

Oracle

- Let $f : E \longrightarrow \mathbb{Z}/2\mathbb{Z}$ be a function
- $(\mathbb{Z}/2\mathbb{Z}, +) = (\{0, 1\}, \oplus)$
- $F : E \times \mathbb{Z}/2\mathbb{Z} \longrightarrow E \times \mathbb{Z}/2\mathbb{Z}, \quad (x, y) \longmapsto (x, y \oplus f(x))$, is a bijection

Quantum oracle gate

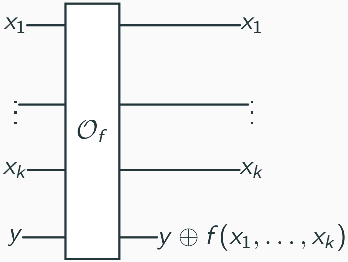
Oracle

- Let $f : E \longrightarrow \mathbb{Z}/2\mathbb{Z}$ be a function
- $(\mathbb{Z}/2\mathbb{Z}, +) = (\{0, 1\}, \oplus)$
- $F : E \times \mathbb{Z}/2\mathbb{Z} \longrightarrow E \times \mathbb{Z}/2\mathbb{Z}, \quad (x, y) \longmapsto (x, y \oplus f(x))$, is a bijection
- Proof: $F^{-1} = F$, $F(F(x, y)) = F(x, y \oplus f(x)) = (x, y)$

Quantum oracle gate

Oracle

- Let $f : E \longrightarrow \mathbb{Z}/2\mathbb{Z}$ be a function
- $(\mathbb{Z}/2\mathbb{Z}, +) = (\{0,1\}, \oplus)$
- $F : E \times \mathbb{Z}/2\mathbb{Z} \longrightarrow E \times \mathbb{Z}/2\mathbb{Z}, \quad (x, y) \longmapsto (x, y \oplus f(x))$, is a bijection
- Proof: $F^{-1} = F$, $F(F(x, y)) = F(x, y \oplus f(x)) = (x, y)$
- Deutsch-Jozsa Oracle $f : (\mathbb{Z}/2\mathbb{Z})^k \longrightarrow \mathbb{Z}/2\mathbb{Z}$:



Deutsch-Jozsa problem

Goal

- Let $f : \{0, 1\} \longrightarrow \{0, 1\}$.
- There are 4 such functions: two are constant and two are balanced (0 and 1 are taken the same number of times)
  $f_0 = \begin{cases} 0 \mapsto 0 \\ 1 \mapsto 0 \end{cases}$ $f_1 = \begin{cases} 0 \mapsto 1 \\ 1 \mapsto 1 \end{cases}$ $f_2 = \begin{cases} 0 \mapsto 0 \\ 1 \mapsto 1 \end{cases}$ $f_3 = \begin{cases} 0 \mapsto 1 \\ 1 \mapsto 0 \end{cases}$
- **Decide** if f is constant or balanced ?

Deutsch-Jozsa problem

Goal

- Let $f : \{0,1\} \longrightarrow \{0,1\}$.
- There are 4 such functions: two are constant and two are balanced (0 and 1 are taken the same number of times)

$$f_0 = \begin{cases} 0 \mapsto 0 \\ 1 \mapsto 0 \end{cases} \quad f_1 = \begin{cases} 0 \mapsto 1 \\ 1 \mapsto 1 \end{cases} \quad f_2 = \begin{cases} 0 \mapsto 0 \\ 1 \mapsto 1 \end{cases} \quad f_3 = \begin{cases} 0 \mapsto 1 \\ 1 \mapsto 0 \end{cases}$$

- **Decide** if f is constant or balanced ?
- Classically, ask 2 queries ($f(0)$ and $f(1)$), quantumly 1 query !

Deutsch-Jozsa problem

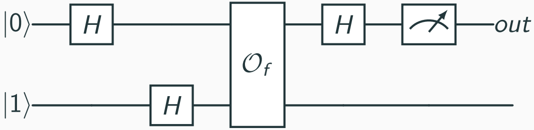
Goal

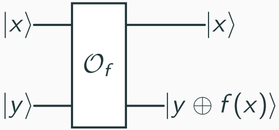
- Let $f : \{0,1\} \longrightarrow \{0,1\}$.
- There are 4 such functions: two are constant and two are balanced (0 and 1 are taken the same number of times)
  $f_0 = \begin{cases} 0 \mapsto 0 \\ 1 \mapsto 0 \end{cases}$ $f_1 = \begin{cases} 0 \mapsto 1 \\ 1 \mapsto 1 \end{cases}$ $f_2 = \begin{cases} 0 \mapsto 0 \\ 1 \mapsto 1 \end{cases}$ $f_3 = \begin{cases} 0 \mapsto 1 \\ 1 \mapsto 0 \end{cases}$
- **Decide** if f is constant or balanced ?
- Classically, ask 2 queries ($f(0)$ and $f(1)$), quantumly 1 query !

Exponential gap: Let $f : \{0,1\}^n \longrightarrow \{0,1\}$ and we have the promise f is either balanced or constant.

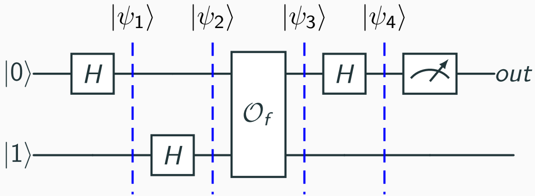
Classically, one need at most $2^{n-1} + 1$ queries, while only 1 quantumly !

Deutsch-Jozsa Quantum Circuit ($n = 1$)

- 

- with 

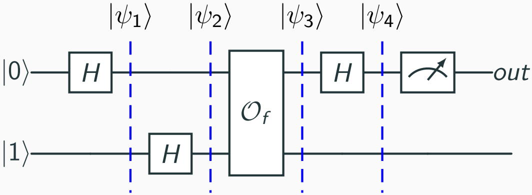
Deutsch-Jozsa Quantum Circuit ($n = 1$)

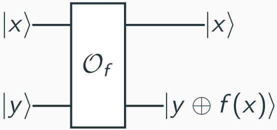
- 

$|\psi_1\rangle = (|0\rangle + |1\rangle).\,|1\rangle,$

$|\psi_2\rangle = (|0\rangle + |1\rangle).(|0\rangle - |1\rangle) = 0.0 - 0.1 + 1.0 - 1.1$

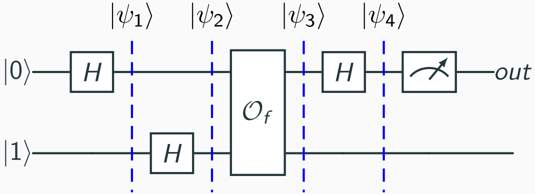
Deutsch-Jozsa Quantum Circuit ($n = 1$)

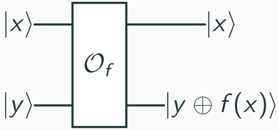




- $|\psi_2\rangle = 0.0 - 0.1 + 1.0 - 1.1,$

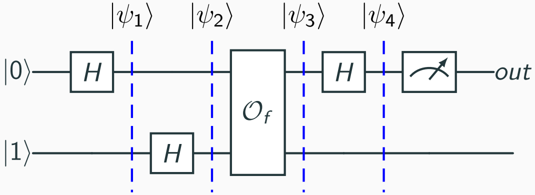
Deutsch-Jozsa Quantum Circuit ($n = 1$)

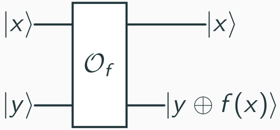




- $|\psi_2\rangle = 0.0 - 0.1 + 1.0 - 1.1$,
- $|\psi_3\rangle = \underbrace{0.(0 \oplus f(0)) - 0.(1 \oplus f(0))}_{A} + \underbrace{1.(0 \oplus f(1)) - 1.(1 \oplus f(1))}_{B}$
- $A = \begin{cases} 0.0 - 0.1 \text{ if } f(0) = 0 \\ -(0.0 - 0.1) \text{ if } f(0) = 1 \end{cases}$ so $A = (-1)^{f(0)}(0.0 - 0.1)$

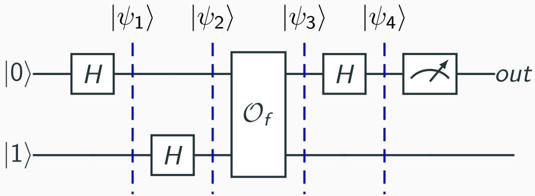
Deutsch-Jozsa Quantum Circuit ($n = 1$)





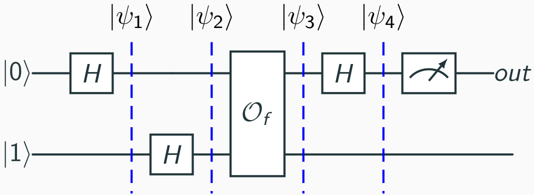
- $|\psi_2\rangle = 0.0 - 0.1 + 1.0 - 1.1$,
- $|\psi_3\rangle = \underbrace{0.(0 \oplus f(0)) - 0.(1 \oplus f(0))}_{A} + \underbrace{1.(0 \oplus f(1)) - 1.(1 \oplus f(1))}_{B}$
- $A = (-1)^{f(0)}(0.0 - 0.1)$ and $B = (-1)^{f(1)}(1.0 - 1.1)$
- $|\psi_3\rangle = (-1)^{f(0)}(0.0 - 0.1) + (-1)^{f(1)}(1.0 - 1.1)$

Deutsch-Jozsa Quantum Circuit ($n = 1$)

- 

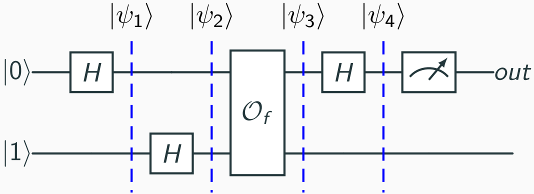
- $|\psi_3\rangle = (-1)^{f(0)}(0.0 - 0.1) + (-1)^{f(1)}(1.0 - 1.1)$
- $|\psi_4\rangle = (-1)^{f(0)}((0+1).0 - (0+1).1) + (-1)^{f(1)}((0-1).0 - (0-1).1)$
- $|\psi_4\rangle = (-1)^{f(0)}(0.0 - 0.1 + 1.0 - 1.1) + (-1)^{f(1)}(0.0 - 0.1 - 1.0 + 1.1)$

Deutsch-Jozsa Quantum Circuit ($n = 1$)

- 

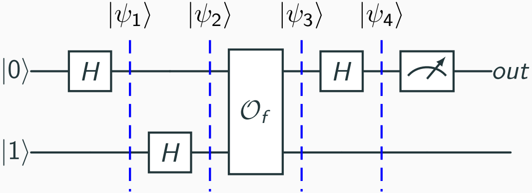
- $|\psi_4\rangle = (-1)^{f(0)}(0.0 - 0.1 + 1.0 - 1.1) + (-1)^{f(1)}(0.0 - 0.1 - 1.0 + 1.1)$

Deutsch-Jozsa Quantum Circuit ($n = 1$)

- 

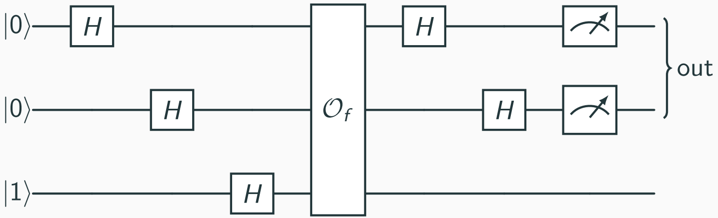
- $|\psi_4\rangle = (-1)^{f(0)}(0.0 - 0.1 + 1.0 - 1.1) + (-1)^{f(1)}(0.0 - 0.1 - 1.0 + 1.1)$
- $|\psi_4\rangle = ((-1)^{f(0)} + (-1)^{f(1)})0.0 + (-(-1)^{f(0)} - (-1)^{f(1)})0.1 + ((-1)^{f(0)} - (-1)^{f(1)})1.0 + (-(-1)^{f(0)} + (-1)^{f(1)})1.1$

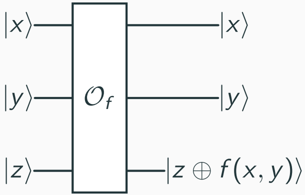
Deutsch-Jozsa Quantum Circuit ($n = 1$)

- 

- $|\psi_4\rangle = (-1)^{f(0)}(0.0 - 0.1 + 1.0 - 1.1) + (-1)^{f(1)}(0.0 - 0.1 - 1.0 + 1.1)$
- $|\psi_4\rangle = ((-1)^{f(0)} + (-1)^{f(1)})0.0 + (-(-1)^{f(0)} - (-1)^{f(1)})0.1 + ((-1)^{f(0)} - (-1)^{f(1)})1.0 + (-(-1)^{f(0)} + (-1)^{f(1)})1.1$
- If f is constant, $(-1)^{f(0)} + (-1)^{f(1)} = \pm 2$ and $(-1)^{f(0)} - (-1)^{f(1)} = 0$ and $(-1)^{f(0)} - (-1)^{f(1)} = 0$, so $|\psi_4\rangle = 0.0 - 0.1$ the measure of the first qubit 0 in both cases
- If f is balanced, check that the first bit is 1

Deutsch-Jozsa Circuit for $n = 2$





- Check that if f is constant, the final state before the measurement is $\pm |0.0\rangle \left| \frac{1}{\sqrt{2}}(0-1) \right\rangle$, and the 2 first bits are 0.0
- if f is balanced, the final state does not contain qubits starting with 0.0, so no measurement of these qubits will give 0.0.

Shor Algorithm

Arithmetic

- order of a: smallest positive integer r s.t. $a^r = 1 \bmod N$
- $r | \varphi(N)$ Lagrange Theorem in the group $(\mathbb{Z}/N\mathbb{Z})^*$
- r is the smallest period of the function $f : k \mapsto a^k \bmod N$

Arithmetic

- order of a: smallest positive integer r s.t. $a^r = 1 \bmod N$
- $r | \varphi(N)$ Lagrange Theorem in the group $(\mathbb{Z}/N\mathbb{Z})^*$
- r is the smallest period of the function $f : k \mapsto a^k \bmod N$

Assumptions

1. Assumption 1: $\mathrm{ord}(a) = r$ is even with proba. $1/2$
2. Fact: $(a^{r/2} - 1)(a^{r/2} + 1) = 0 \bmod N$

Arithmetic

- order of a: smallest positive integer r s.t. $a^r = 1 \bmod N$
- $r|\varphi(N)$ Lagrange Theorem in the group $(\mathbb{Z}/N\mathbb{Z})^*$
- r is the smallest period of the function $f : k \mapsto a^k \bmod N$

Assumptions

1. Assumption 1: $\mathrm{ord}(a) = r$ is even with proba. $1/2$
2. Fact: $(a^{r/2} - 1)(a^{r/2} + 1) = 0 \bmod N$
3. Assumption 2: $a^{r/2} + 1$ is not divisible by N for many a's
4. Under Assumption 1 and 2: $d = \gcd(a^{r/2} - 1, N)$ and $d' = \gcd(a^{r/2} + 1, N)$ are non-trivial factors of N

Arithmetic

- order of a: smallest positive integer r s.t. $a^r = 1 \bmod N$
- $r|\varphi(N)$ Lagrange Theorem in the group $(\mathbb{Z}/N\mathbb{Z})^*$
- r is the smallest period of the function $f : k \mapsto a^k \bmod N$

Assumptions

1. Assumption 1: $\mathrm{ord}(a) = r$ is even with proba. $1/2$
2. Fact: $(a^{r/2} - 1)(a^{r/2} + 1) = 0 \bmod N$
3. Assumption 2: $a^{r/2} + 1$ is not divisible by N for many a's
4. Under Assumption 1 and 2: $d = \gcd(a^{r/2} - 1, N)$ and $d' = \gcd(a^{r/2} + 1, N)$ are non-trivial factors of N
5. Recall: $\mathbb{Z}/N\mathbb{Z}$ is not an integral domain: $N = 6$, $2 \times 3 = 0 \bmod 6$

Arithmetic

- order of a: smallest positive integer r s.t. $a^r = 1 \bmod N$
- $r|\varphi(N)$ Lagrange Theorem in the group $(\mathbb{Z}/N\mathbb{Z})^*$
- r is the smallest period of the function $f : k \mapsto a^k \bmod N$

Assumptions

1. Assumption 1: $\mathrm{ord}(a) = r$ is even with proba. 1/2
2. Fact: $(a^{r/2} - 1)(a^{r/2} + 1) = 0 \bmod N$
3. Assumption 2: $a^{r/2} + 1$ is not divisible by N for many a's
4. Under Assumption 1 and 2: $d = \gcd(a^{r/2} - 1, N)$ and $d' = \gcd(a^{r/2} + 1, N)$ are non-trivial factors of N

a=2	$(a, N) = 1$	$r = 4, 2^4 = 16 = 1 \bmod 15$	$(2^{4/2} - 1, 15) = 3$
a=3	no		
a=11	$(a, N) = 1$	$r = 2, 11^2 = 121 = 1 \bmod 15$	$(11^{2/2} - 1, 15) = 5$

Order and Oracle

- order of a: smallest positive integer r s.t. $a^r = 1 \mod N$
- $r|\varphi(N)$ Lagrange Theorem in the group $(\mathbb{Z}/N\mathbb{Z})^*$
- r is the smallest period of the function $f : k \mapsto a^k \mod N$
- Oracle $F : (k, 0) \mapsto (k, a^k \mod N)$
- E.g. $N = 15$ and $a = 2$, $r = 4$

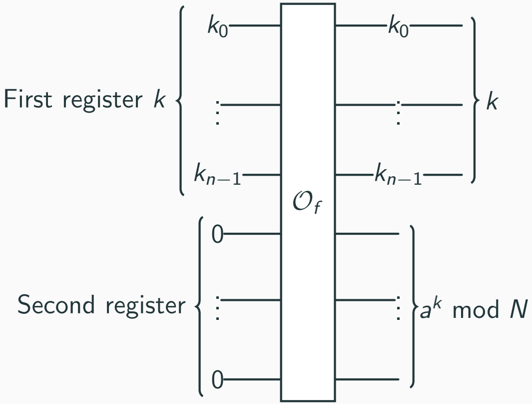
Order and Oracle

- order of a: smallest positive integer r s.t. $a^r = 1 \bmod N$
- $r|\varphi(N)$ Lagrange Theorem in the group $(\mathbb{Z}/N\mathbb{Z})^*$
- r is the smallest period of the function $f : k \mapsto a^k \bmod N$
- Oracle $F : (k, 0) \mapsto (k, a^k \bmod N)$
- E.g. $N = 15$ and $a = 2$, $r = 4$

$$
\begin{array}{llll}
(0,0) \overset{F}{\mapsto} (0,1) & (4,0) \overset{F}{\mapsto} (4,1) & (8,0) \overset{F}{\mapsto} (8,1) & (12,0) \overset{F}{\mapsto} (12,1) \\
(1,0) \overset{F}{\mapsto} (1,2) & (5,0) \overset{F}{\mapsto} (5,2) & (9,0) \overset{F}{\mapsto} (9,2) & (13,0) \overset{F}{\mapsto} (13,2) \\
(2,0) \overset{F}{\mapsto} (2,4) & (6,0) \overset{F}{\mapsto} (6,4) & (10,0) \overset{F}{\mapsto} (10,4) & (14,0) \overset{F}{\mapsto} (14,4) \\
(3,0) \overset{F}{\mapsto} (3,8) & (7,0) \overset{F}{\mapsto} (7,8) & (11,0) \overset{F}{\mapsto} (11,8) & (15,0) \overset{F}{\mapsto} (15,8)
\end{array}
$$

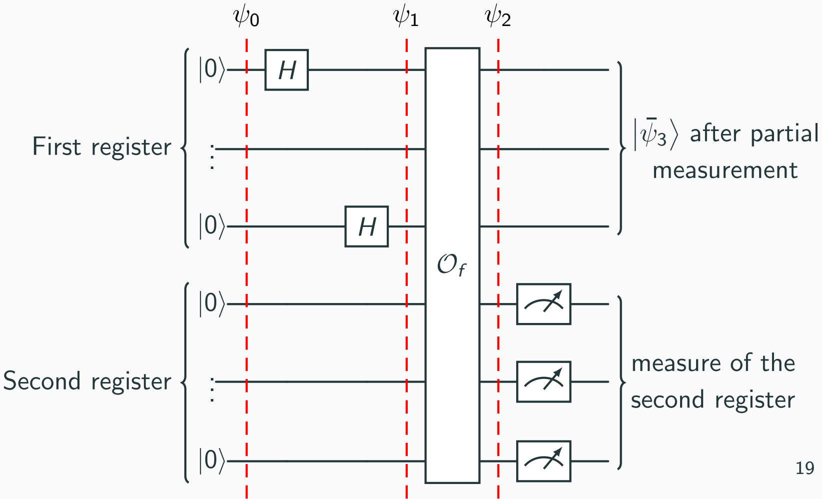
Oracle Circuit $2^n \geq N$

The oracle is composed of 2 registers: the first receives the integer k in binary with n bits, and the second, 0 on n bits. We write $|\underline{k}\rangle$ the register containing k written in binary. For instance, $|\underline{0}\rangle = |0.\dots0\rangle$ with n bits. The initial state is $|\underline{k}\rangle \otimes |\underline{0}\rangle$.

- 

Starting the Circuit $2^n \geq N$

- Initialization: $|\psi_0\rangle = |\underline{0}\rangle \otimes |\underline{0}\rangle$.
- Hadamard: $|\psi_1\rangle = H^{\otimes n}(|\underline{0}\rangle) \otimes |\underline{0}\rangle = \left(\frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} |\underline{k}\rangle\right) \otimes |\underline{0}\rangle$
- Oracle: $|\psi_2\rangle = \frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} |\underline{k}\rangle \otimes \left|\underline{a^k}\right\rangle$



Using the period to rewrite $|\psi_2\rangle$

- Assumption 3: $\mathrm{ord}(a) = r | 2^n$. This assumption is not true, and can be removed (see later)
- Under Assumption 3: $k = \alpha r + \beta$ with $0 \leq \beta < r$ and $0 \leq \alpha < 2^n/r$,

$$|\psi_2\rangle = \sum_{k=0}^{2^n-1} |\underline{k}\rangle \otimes |\underline{a^k}\rangle = \sum_{\beta=0}^{r-1} \left(\sum_{\alpha=0}^{2^n/r-1} |\underline{\alpha r + \beta}\rangle \right) \otimes |a^{\beta}\rangle$$

Using the period to rewrite $|\psi_2\rangle$

- Assumption 3: $\mathrm{ord}(a) = r | 2^n$. This assumption is not true, and can be removed (see later)
- Under Assumption 3: $k = \alpha r + \beta$ with $0 \leq \beta < r$ and $0 \leq \alpha < 2^n / r$,

$$|\psi_2\rangle = \sum_{k=0}^{2^n-1} |\underline{k}\rangle \otimes \left|\underline{a^k}\right\rangle = \sum_{\beta=0}^{r-1} \left(\sum_{\alpha=0}^{2^n/r-1} \left|\underline{\alpha r + \beta}\right\rangle \right) \otimes \left|a^{\beta}\right\rangle$$

- If we measure the second register, we get for a fixed β_0,

$$|\psi_3\rangle = \sum_{\alpha=0}^{2^n/r-1} |\alpha r + \beta_0\rangle \otimes \left|a^{\beta_0}\right\rangle$$

Using the period to rewrite $|\psi_2\rangle$

- Assumption 3: $\text{ord}(a) = r | 2^n$. This assumption is not true, and can be removed (see later)
- Under Assumption 3: $k = \alpha r + \beta$ with $0 \le \beta < r$ and $0 \le \alpha < 2^n/r$,

$$|\psi_2\rangle = \sum_{k=0}^{2^n-1} |\underline{k}\rangle \otimes |\underline{a^k}\rangle = \sum_{\beta=0}^{r-1} \left(\sum_{\alpha=0}^{2^n/r-1} |\underline{\alpha r + \beta}\rangle \right) \otimes |a^{\beta}\rangle$$

- If we measure the second register, we get for a fixed β_0,

$$|\psi_3\rangle = \sum_{\alpha=0}^{2^n/r-1} |\alpha r + \beta_0\rangle \otimes |a^{\beta_0}\rangle$$

- Assume we measure the first register, $|\alpha_0 r + \beta_0\rangle$ for fixed α_0 and β_0
- If we redo the computation, we will not the same β_0,
- We cannot do many measures of the first register ...

Example $N = 15$, $a = 2$

- $|\psi_0\rangle = |\underline{0}\rangle \otimes |\underline{0}\rangle$
- Hadamard Transform: $|\psi_1\rangle = (|\underline{0}\rangle + |\underline{1}\rangle + \ldots + |\underline{15}\rangle) \otimes |\underline{0}\rangle$
- Oracle: $|\psi_2\rangle = |\underline{0}\rangle \, . \left|\underline{a^0}\right\rangle + |\underline{1}\rangle \, . \left|\underline{a^1}\right\rangle + \ldots + |\underline{15}\rangle \, . \left|\underline{a^{15}}\right\rangle$

Example $N = 15$, $a = 2$

- $|\psi_0\rangle = |\underline{0}\rangle \otimes |\underline{0}\rangle$
- Hadamard Transform: $|\psi_1\rangle = (|\underline{0}\rangle + |\underline{1}\rangle + \ldots + |\underline{15}\rangle) \otimes |\underline{0}\rangle$
- Oracle: $|\psi_2\rangle = |\underline{0}\rangle \,.\, \left|\underline{a^0}\right\rangle + |\underline{1}\rangle \,.\, \left|\underline{a^1}\right\rangle + \ldots + |\underline{15}\rangle \,.\, \left|\underline{a^{15}}\right\rangle$
- Since $r = 4 | 2^4 = 16$, the values form a rectangular table

$$\begin{aligned} |\psi_2\rangle = \big(\, |\underline{0}\rangle + |\underline{4}\rangle + |\underline{8}\rangle + |\underline{12}\rangle \,\big) . \, |\underline{1}\rangle \, + \\ \big(\, |\underline{1}\rangle + |\underline{5}\rangle + |\underline{9}\rangle + |\underline{13}\rangle \,\big) . \, |\underline{2}\rangle \, + \\ \big(\, |\underline{2}\rangle + |\underline{6}\rangle + |\underline{10}\rangle + |\underline{14}\rangle \,\big) . \, |\underline{4}\rangle \, + \\ \big(\, |\underline{3}\rangle + |\underline{7}\rangle + |\underline{11}\rangle + |\underline{15}\rangle \,\big) . \, |\underline{8}\rangle \end{aligned}$$

- If we measure the second register, $|\underline{4}\rangle$, the first register is

$$\left|\widetilde{\psi_3}\right\rangle = |\underline{2}\rangle + |\underline{6}\rangle + |\underline{10}\rangle + |\underline{14}\rangle$$

- They are separated by the period $r = 4$, but how can we recover r ?

Complex numbers

- $$1 + z + \ldots + z^{n-1} = \begin{cases} n & \text{if } z = 1 \\ \frac{1-z^n}{1-z} & \text{otherwise.} \end{cases}$$
- Crucial Lemma: $n > 0, j \in \mathbb{Z}$,

$$\frac{1}{n}\sum_{k=0}^{n-1} e^{2i\pi\frac{kj}{n}} = \begin{cases} 1 & \text{if } \frac{j}{n} \text{ is an integer} \\ 0 & \text{otherwise.} \end{cases}$$

Discrete Fourier Transform

Complex numbers

- $$1 + z + \ldots + z^{n-1} = \begin{cases} n & \text{if } z = 1 \\ \frac{1-z^n}{1-z} & \text{otherwise.} \end{cases}$$
- Crucial Lemma: $n > 0, j \in \mathbb{Z}$,

$$\frac{1}{n} \sum_{k=0}^{n-1} e^{2i\pi \frac{kj}{n}} = \begin{cases} 1 & \text{if } \frac{j}{n} \text{ is an integer} \\ 0 & \text{otherwise.} \end{cases}$$

Discrete Fourier Transform and Inverse

$$\widehat{F} \left|\underline{k}\right\rangle = \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} e^{2i\pi \frac{kj}{2^n}} \left|\underline{j}\right\rangle \text{ and } \widehat{F}^{-1} \left|\underline{k}\right\rangle = \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} e^{-2i\pi \frac{kj}{2^n}} \left|\underline{j}\right\rangle$$

Discrete Fourier Transform

Complex numbers

- $$1 + z + \ldots + z^{n-1} = \begin{cases} n & \text{if } z = 1 \\ \frac{1-z^n}{1-z} & \text{otherwise.} \end{cases}$$

- Crucial Lemma: $n > 0, j \in \mathbb{Z}$,

$$\frac{1}{n} \sum_{k=0}^{n-1} e^{2i\pi \frac{kj}{n}} = \begin{cases} 1 & \text{if } \frac{j}{n} \text{ is an integer} \\ 0 & \text{otherwise.} \end{cases}$$

Discrete Fourier Transform and Inverse

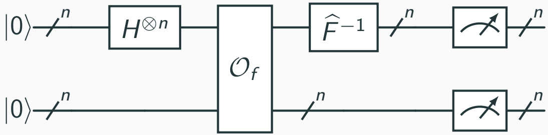
$$\widehat{F} \left| \underline{k} \right\rangle = \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} e^{2i\pi \frac{kj}{2^n}} \left| \underline{j} \right\rangle \text{ and } \widehat{F}^{-1} \left| \underline{k} \right\rangle = \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} e^{-2i\pi \frac{kj}{2^n}} \left| \underline{j} \right\rangle$$

The Discrete Fourier Transform is Linear and Unitary

$$\text{If } \left|\psi\right\rangle = \sum_{k=0}^{2^n-1} \alpha_k \left| \underline{k} \right\rangle, \text{ then } \widehat{F} \left|\psi\right\rangle = \sum_{k=0}^{2^n-1} \alpha_k \widehat{F} \left| \underline{k} \right\rangle$$

Shor Circuit

- Initialization: $|\psi_0\rangle = |\underline{0}\rangle \otimes |\underline{0}\rangle$.
- Hadamard: $|\psi_1\rangle = H^{\otimes n}(|\underline{0}\rangle) \otimes |\underline{0}\rangle = \left(\frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} |\underline{k}\rangle\right) \otimes |\underline{0}\rangle$
- Oracle: $|\psi_2\rangle = \frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} |\underline{k}\rangle \otimes \left|\underline{a^k}\right\rangle$



- Measure of the first register: $\left|\frac{2^n \ell}{r}\right\rangle$
- Allows (often) to get r (or a factor of r)

Computation

- After measuring the second register $\left|\bar{\psi}_3\right\rangle = \sum_{\alpha=0}^{2^n/r-1} \left|\underline{\alpha r + \beta_0}\right\rangle$

Computation

- After measuring the second register $|\bar{\psi}_3\rangle = \sum_{\alpha=0}^{2^n/r-1} |\underline{\alpha r + \beta_0}\rangle$
- Action of $\widehat{F}^{-1}$:

$$|\bar{\psi}_4\rangle = \widehat{F}^{-1} \left|\hat{\psi}_3\right\rangle = \sum_{\alpha=0}^{2^n/r-1} \widehat{F}^{-1} |\underline{\alpha r + \beta_0}\rangle$$

$$= \sum_{\alpha} \sum_{j=0}^{2^n-1} e^{-\frac{2i\pi(\alpha r+\beta_0)j}{2^n}} |\underline{j}\rangle = \sum_{j} \overbrace{\left(\sum_{\alpha} e^{-2i\pi \frac{\alpha j}{2^n/r}} \right)}^{0 \text{ or } 1} e^{-2i\pi \frac{\beta_0 j}{2^n}} |\underline{j}\rangle$$

$$= \sum_{j \text{ with } j/(2^n/r) \text{ integer}} e^{-2i\pi \frac{\beta_0 j}{2^n}} |j\rangle = \sum_{\ell=0}^{r-1} e^{-2i\pi \beta_0 \frac{\ell}{r}} \left| \frac{2^n \ell}{r} \right\rangle$$

Computation

- After measuring the second register $\left|\bar{\psi}_3\right\rangle = \sum_{\alpha=0}^{2^n/r-1} \left|\underline{\alpha r + \beta_0}\right\rangle$
- Action of $\widehat{F}^{-1}$:

$$\left|\bar{\psi}_4\right\rangle = \widehat{F}^{-1}\left|\hat{\psi}_3\right\rangle = \sum_{\alpha=0}^{2^n/r-1} \widehat{F}^{-1}\left|\underline{\alpha r + \beta_0}\right\rangle$$

$$= \sum_{\alpha}\sum_{j=0}^{2^n-1} e^{-\frac{2i\pi(\alpha r+\beta_0)j}{2^n}}\left|\underline{j}\right\rangle = \sum_{j} \overbrace{\left(\sum_{\alpha} e^{-2i\pi\frac{\alpha j}{2^n/r}}\right)}^{0 \text{ or } 1} e^{-2i\pi\frac{\beta_0 j}{2^n}}\left|\underline{j}\right\rangle$$

$$= \sum_{j \text{ with } j/(2^n/r) \text{ integer}} e^{-2i\pi\frac{\beta_0 j}{2^n}}\left|\underline{j}\right\rangle = \sum_{\ell=0}^{r-1} e^{-2i\pi\beta_0\frac{\ell}{r}}\left|\frac{2^n\ell}{r}\right\rangle$$

- Measure the first register: $\left|\frac{2^n\ell}{r}\right\rangle$, for $\ell \in \{0, 1, \ldots, r-1\}$
- We get $m = \frac{2^n\ell}{r}$ for one of the states $\left|\frac{2^n\ell}{r}\right\rangle$

Measure the first register

$m = \frac{2^n \ell}{r}$ **integer with n known and ℓ unknown**

- Divide m by 2^n to obtain the rational $x = \frac{m}{2^n} = \frac{\ell}{r}$
- If $x \in \mathbb{Z}$, we get no information on r, and we redo the quantum circuit
- If $\gcd(\ell, r) = 1$, then $\frac{\ell}{r}$ is irreducible and we get r.
- If $\gcd(\ell, r) \neq 1$, then $x = \frac{m}{2^n} = \frac{\ell'}{r'} = \frac{\ell}{r}$ and we get r' a factor of r. We redo the computation with $a' = a^{r'}$ which is of period r/r'.

Continued Fractions

Definition

- $a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\dots + \frac{1}{a_n}}}}$, noted $[a_0, a_1, \dots, a_n]$
- E.g., $[5, 2, 1, 4] = 5 + \frac{1}{2 + \frac{1}{1 + \frac{1}{4}}} = 5.3571428\dots$
- $[5] = 5, [5, 2] = \frac{11}{2} = 5.5, [5, 2, 1] = \frac{16}{3} = 5.33\dots$

Continued Fractions

Definition

- $a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\dots + \frac{1}{a_n}}}}$, noted $[a_0, a_1, \dots, a_n]$
- E.g., $[5, 2, 1, 4] = 5 + \frac{1}{2 + \frac{1}{1 + \frac{1}{4}}} = 5.3571428\dots$
- $[5] = 5, [5, 2] = \frac{11}{2} = 5.5, [5, 2, 1] = \frac{16}{3} = 5.33\dots$

Good Approximation by continued fractions

- $\pi = 3.14159\dots \approx \frac{314}{100}$ (denominator is large)
- $\frac{314}{100} = 3 + \frac{14}{100} = 3 + \frac{1}{\frac{100}{14}} = 3 + \frac{1}{7 + \frac{2}{14}} = 3 + \frac{1}{7 + \frac{1}{7}} = [3, 7, 7]$
- $[3, 7] = 3 + \frac{1}{7} = \frac{22}{7} = 3.1428$
- $[3, 7, 15, 1] = \frac{355}{113} = 3.14159292\dots$ (same order with 6 exact values instead of 2)

Example Shor with $N = 21$

- $N = 21$, $a = 2$, $2^n = 512 = 2^9$
- Circuit outputs $|427\rangle$, so $x = \frac{427}{512}$
- $\frac{427}{512} \approx \frac{4}{5}$ so order 5 ??
- $\frac{427}{512} = [0, 1, 5, 42, 2]$ and $[0, 1] = 1, [0, 1, 5] = \frac{5}{6}, [0, 1, 5, 42] = \frac{211}{253}$
- We keep the best fraction whose denominator is $\leq N$ and it gives r or a fraction of r

Example Shor with $N = 21$

- $N = 21,\ a = 2,\ 2^n = 512 = 2^9$
- Circuit outputs $|427\rangle$, so $x = \frac{427}{512}$
- $\frac{427}{512} \approx \frac{4}{5}$ so order 5 ??
- $\frac{427}{512} = [0, 1, 5, 42, 2]$ and $[0, 1] = 1, [0, 1, 5] = \frac{5}{6}, [0, 1, 5, 42] = \frac{211}{253}$
- We keep the best fraction whose denominator is $\leq N$ and it gives r or a fraction of r

Shor algorithm with arbitrary order

- $N = 21,\ a = 2,\ 2^n = 512 = 2^9 \geq N^2$
- $|\psi_0\rangle = |\underline{0}\rangle \otimes |\underline{0}\rangle$
- $|\psi_1\rangle = \sum_{k=0}^{r-1} |\underline{k}\rangle \otimes |\underline{0}\rangle$
- $|\psi_2\rangle = \sum_{k=0}^{r-1} |\underline{k}\rangle \otimes \left|\underline{a^k \bmod N}\right\rangle$
- $r = 6$ and $\frac{2^n \ell}{r} \notin \mathbb{Z}$

Example

The first two lines have 86 terms and 85 in the others

- The state $|\psi_2\rangle$ is not rectangular:

$$
\begin{aligned}
|\psi_2\rangle = &\frac{1}{\sqrt{512}}(|\underline{0}\rangle + |\underline{6}\rangle + \ldots + |\underline{504}\rangle + |\underline{510}\rangle)\,|\underline{1}\rangle \\
&+ \frac{1}{\sqrt{512}}(|\underline{1}\rangle + |\underline{7}\rangle + \ldots + |\underline{505}\rangle + |\underline{511}\rangle)\,|\underline{2}\rangle \\
&+ \frac{1}{\sqrt{512}}(|\underline{2}\rangle + |\underline{8}\rangle + \ldots + |\underline{506}\rangle)\,|\underline{4}\rangle \\
&+ \ldots \\
&+ \frac{1}{\sqrt{512}}(|\underline{5}\rangle + |\underline{11}\rangle + \ldots + |\underline{509}\rangle)\,|\underline{11}\rangle
\end{aligned}
$$

Example

The first two lines have 86 terms and 85 in the others

- The state $|\psi_2\rangle$ is not rectangular:

$$
\begin{aligned}
|\psi_2\rangle = & \frac{1}{\sqrt{512}}(|\underline{0}\rangle + |\underline{6}\rangle + \ldots + |\underline{504}\rangle + |\underline{510}\rangle)\,|\underline{1}\rangle \\
& + \frac{1}{\sqrt{512}}(|\underline{1}\rangle + |\underline{7}\rangle + \ldots + |\underline{505}\rangle + |\underline{511}\rangle)\,|\underline{2}\rangle \\
& + \frac{1}{\sqrt{512}}(|\underline{2}\rangle + |\underline{8}\rangle + \ldots + |\underline{506}\rangle)\,|\underline{4}\rangle \\
& + \ldots \\
& + \frac{1}{\sqrt{512}}(|\underline{5}\rangle + |\underline{11}\rangle + \ldots + |\underline{509}\rangle)\,|\underline{11}\rangle
\end{aligned}
$$

- measure the second register $|2\rangle$: $|\psi_3\rangle = |\underline{1}\rangle + |\underline{7}\rangle + \ldots + |\underline{511}\rangle$
- $|\psi_4\rangle = \hat{F}^{-1}\,|\psi_3\rangle = \sum_{\alpha=0}^{85} \hat{F}^{-1}\,|\underline{6\alpha+1}\rangle$
- $|\psi_4\rangle = \sum_{j=0}^{511} \left(\sum_{\alpha=0}^{85} e^{-2i\pi \frac{6\alpha j}{512}} \right) e^{-2i\pi \frac{j}{512}}\,|\underline{j}\rangle$

Example Shor with arbitrary order

$$|\psi_4\rangle = \frac{1}{\sqrt{512}} \sum_{j=0}^{511} \left(\frac{1}{\sqrt{86}} \sum_{\alpha=0}^{85} e^{-2i\pi \frac{6\alpha j}{512}} \right) e^{-2i\pi \frac{j}{512}} \left| \underline{j} \right\rangle$$

Now, $\Sigma(j) = \frac{1}{\sqrt{86}} \sum_{\alpha=0}^{85} e^{-2i\pi \frac{6\alpha j}{512}}$ does not take only 0 /1 values.

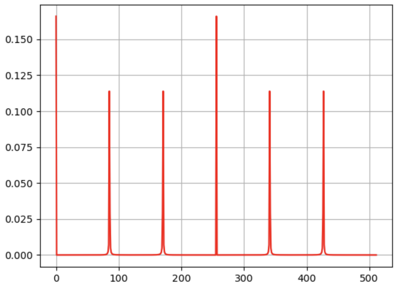
Example Shor with arbitrary order

$$|\psi_4\rangle = \frac{1}{\sqrt{512}}\sum_{j=0}^{511}\left(\frac{1}{\sqrt{86}}\sum_{\alpha=0}^{85} e^{-2i\pi\frac{6\alpha j}{512}}\right)e^{-2i\pi\frac{j}{512}}\left|\underline{j}\right\rangle$$

Now, $\Sigma(j) = \frac{1}{\sqrt{86}}\sum_{\alpha=0}^{85} e^{-2i\pi\frac{6\alpha j}{512}}$ does not take only 0 /1 values.

If we measure the first register, we get $|j\rangle$ with probability $|\Sigma(j)|^2$.

The proba. are ≈ 0, except when $j \approx \frac{2^n\ell}{r}$: for $\ell = 5$, $\frac{512\times 5}{6} = 426.66$.



j	p_j
422	0.00062...
423	0.00099...
424	0.00186...
425	0.00469...
426	0.02888...
427	**0.11389...**
428	0.00702...
429	0.00226...
430	0.00109...
431	0.00063...

Hardy-Wright Theorem

Theorem
Let $x \in \mathbb{R}$ and a rational $\frac{p}{q}$ such that

$$\left|x - \frac{p}{q}\right| < \frac{1}{2q^2}.$$

Then, $\frac{p}{q}$ is obtained as one of the continued fractions of x.

Hardy-Wright Theorem

Theorem
Let $x \in \mathbb{R}$ and a rational $\frac{p}{q}$ such that

$$\left|x - \frac{p}{q}\right| < \frac{1}{2q^2}.$$

Then, $\frac{p}{q}$ is obtained as one of the continued fractions of x.

Let m the closest integer to $\frac{2^n \ell}{r}$. So, $|m - \frac{2^n \ell}{r}| < \frac{1}{2}$.

If $x = \frac{m}{2^n}$, we get $|x - \frac{\ell}{r}| < \frac{1}{2^{n+1}}$.

As we set $2^n \geq N^2 \geq r^2$, $|x - \frac{\ell}{r}| < \frac{1}{2r^2}$.

Using Theorem, we obtain $\frac{\ell}{r}$ as one of the continued fractions of x.

Discrete Fourier Transform

Rewritting the Discrete Fourier Transform

Definition

- $\widehat{F}\,|\underline{k}\rangle = \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} e^{2i\pi \frac{k \cdot j}{2^n}} \,|\underline{j}\rangle$
- Factorization: $\widehat{F}\,|\underline{k}\rangle = \frac{1}{\sqrt{2^n}} \prod_{\ell=1}^{n} \left(|0\rangle + e^{2i\pi \frac{k}{2^\ell}} \,|\underline{1}\rangle \right)$

Rewritting the Discrete Fourier Transform

Definition

- $\widehat{F}\,|\underline{k}\rangle = \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} e^{2i\pi \frac{k \cdot j}{2^n}} \left|\underline{j}\right\rangle$
- Factorization: $\widehat{F}\,|\underline{k}\rangle = \frac{1}{\sqrt{2^n}} \prod_{\ell=1}^{n} \left(|0\rangle + e^{2i\pi \frac{k}{2^\ell}} |\underline{1}\rangle \right)$
- E.g. $n = 1$, $\widehat{F}\,|\underline{k}\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2i\pi \frac{k}{2}} |1\rangle \right)$.
  Hadamard Transform: $\widehat{F}\,|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $\widehat{F}\,|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

Rewritting the Discrete Fourier Transform

Definition

- $\widehat{F}\,|\underline{k}\rangle = \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} e^{2i\pi \frac{k \cdot j}{2^n}} \left|\underline{j}\right\rangle$
- Factorization: $\widehat{F}\,|\underline{k}\rangle = \frac{1}{\sqrt{2^n}} \prod_{\ell=1}^{n} \left(|0\rangle + e^{2i\pi \frac{k}{2^\ell}} |\underline{1}\rangle \right)$

Proof

- For each $|j\rangle$, show that the coefficient in both expressions is the same

Rewritting the Discrete Fourier Transform

Definition

- $\widehat{F}\,|\underline{k}\rangle = \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} e^{2i\pi \frac{k \cdot j}{2^n}} \left|\underline{j}\right\rangle$
- Factorization: $\widehat{F}\,|\underline{k}\rangle = \frac{1}{\sqrt{2^n}} \prod_{\ell=1}^{n} \left(|0\rangle + e^{2i\pi \frac{k}{2^\ell}} \,|\underline{1}\rangle \right)$

Proof

- For each $|j\rangle$, show that the coefficient in both expressions is the same
- Write $0 \leq j < 2^n$ in binary: $j = \sum_{\ell=0}^{n-1} j_\ell 2^\ell$ with $j_\ell = 0$ or 1.
  For $\underline{j} = j_{n-1} \ldots j_1 . j_0$, $\left|\underline{j}\right\rangle = |j_{n-1} \ldots j_2 . j_1 . j_0\rangle = |j_{n-1}\rangle \ldots |j_2\rangle . |j_1\rangle . |j_0\rangle$.

Rewritting the Discrete Fourier Transform

Definition

- $\widehat{F}\,|\underline{k}\rangle = \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} e^{2i\pi\frac{k\cdot j}{2^n}} \left|\underline{j}\right\rangle$
- Factorization: $\widehat{F}\,|\underline{k}\rangle = \frac{1}{\sqrt{2^n}} \prod_{\ell=1}^{n} \left(|0\rangle + e^{2i\pi\frac{k}{2^\ell}} \,|\underline{1}\rangle \right)$

Proof

- For each $|j\rangle$, show that the coefficient in both expressions is the same
- Write $0 \leq j < 2^n$ in binary: $j = \sum_{\ell=0}^{n-1} j_\ell 2^\ell$ with $j_\ell = 0$ or 1.
  For $\underline{j} = j_{n-1}\dots j_1.j_0$, $\left|\underline{j}\right\rangle = |j_{n-1}\dots j_2.j_1.j_0\rangle = |j_{n-1}\rangle \dots |j_2\rangle . |j_1\rangle . |j_0\rangle$.
- For each term of the product, we take either $|0\rangle$ or $e^{2i\pi\frac{k}{2^\ell}} \,|1\rangle$.
  If we choose $|0\rangle$ every times, we get $|\underline{0}\rangle$. In the first term, if we choose $|0\rangle$, $\left|\underline{j}\right\rangle = |0...\rangle$, while if we choose $e^{2i\pi\frac{k}{2^\ell}} \,|1\rangle$, $\left|\underline{j}\right\rangle = |1...\rangle$.

Rewritting the Discrete Fourier Transform

Definition

- $\widehat{F}\,|\underline{k}\rangle = \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} e^{2i\pi\frac{k\cdot j}{2^n}} \left|\underline{j}\right\rangle$
- Factorization: $\widehat{F}\,|\underline{k}\rangle = \frac{1}{\sqrt{2^n}} \prod_{\ell=1}^{n} \left(|0\rangle + e^{2i\pi\frac{k}{2^\ell}} |\underline{1}\rangle \right)$

Proof

- For each $|j\rangle$, show that the coefficient in both expressions is the same
- Write $0 \leq j < 2^n$ in binary: $j = \sum_{\ell=0}^{n-1} j_\ell 2^\ell$ with $j_\ell = 0$ or 1.
  For $\underline{j} = j_{n-1} \ldots j_1 . j_0$, $\left|\underline{j}\right\rangle = |j_{n-1} \ldots j_2 . j_1 . j_0\rangle = |j_{n-1}\rangle \ldots |j_2\rangle . |j_1\rangle . |j_0\rangle$.
- For each term of the product, we take either $|0\rangle$ or $e^{2i\pi\frac{k}{2^\ell}} |1\rangle$.
  If we choose $|0\rangle$ every times, we get $|\underline{0}\rangle$. In the first term, if we choose $|0\rangle$, $\left|\underline{j}\right\rangle = |0...\rangle$, while if we choose $e^{2i\pi\frac{k}{2^\ell}} |1\rangle$, $\left|\underline{j}\right\rangle = |1...\rangle$.
- We can summarize both cases as $e^{2i\pi\frac{kj_{n-1}}{2^\ell}} |j_{n-1}\rangle$

Rewritting the Discrete Fourier Transform

- We can summarize these 2 cases as $e^{2i\pi\frac{kj_{n-1}}{2^\ell}}\left|j_{n-1}\right\rangle$

Rewritting the Discrete Fourier Transform

- We can summarize these 2 cases as $e^{2i\pi \frac{kj_{n-1}}{2^\ell}} \left|j_{n-1}\right\rangle$
- More generally, the ℓ term can be written as $e^{2i\pi \frac{kj_{n-\ell}}{2^\ell}} \left|j_{n-\ell}\right\rangle$, and

$$\prod_{\ell=1}^{n} \left(e^{2i\pi \frac{kj_{n-\ell}}{2^\ell}} \left|j_{n-\ell}\right\rangle \right) = \left(\prod_{\ell=1}^{n} e^{2i\pi \frac{kj_{n-\ell}}{2^\ell}} \right) \left|j_{n-1} \dots j_2 . j_1 . j_0\right\rangle$$

$$= e^{2i\pi k \cdot \sum_{\ell=1}^{n} \frac{j_{n-\ell}}{2^\ell}} \left|\underline{j}\right\rangle$$

$$= e^{2i\pi \frac{k}{2^n} \cdot \sum_{\ell=1}^{n} j_{n-\ell} 2^{n-\ell}} \left|\underline{j}\right\rangle$$

$$= e^{2i\pi \frac{k}{2^n} \cdot \sum_{\ell'=0}^{n-1} j_{\ell'} 2^{\ell'}} \left|\underline{j}\right\rangle$$

$$= e^{2i\pi \frac{k}{2^n} \cdot j} \left|\underline{j}\right\rangle$$

- The coefficient of $\left|\underline{j}\right\rangle$ is the same as the one of the DFT. Since it is true for all j, the two expressions are equivalent

Variant

We can write binary notation for $0 \leq x < 1$:

$$0..j_1.j_2 \ldots .j_n = \frac{j_1}{2} + \frac{j_2}{2^2} + \ldots \frac{j_n}{2^n} = \sum_{\ell=1}^{n} \frac{j_\ell}{2^\ell}$$

$0..j_1.j_2 \ldots .j_n$: the dots separate the bits, and .. represent 0.abc

E.g., $x = 0.625$ is written $x = 0..1.0.1$ since $0.625 = \frac{1}{2} + \frac{0}{4} + \frac{1}{8}$

Variant

We can write binary notation for $0 \leq x < 1$:

$$0..j_1.j_2\ldots j_n = \frac{j_1}{2} + \frac{j_2}{2^2} + \ldots \frac{j_n}{2^n} = \sum_{\ell=1}^{n} \frac{j_\ell}{2^\ell}$$

$0..j_1.j_2\ldots j_n$: the dots separate the bits, and .. represent 0.abc

E.g., $x = 0.625$ is written $x = 0..1.0.1$ since $0.625 = \frac{1}{2} + \frac{0}{4} + \frac{1}{8}$

Corollary
If $|\underline{k}\rangle = |k_{n-1}\ldots k_1.k_0\rangle$,

$$\hat{F}\,|\underline{k}\rangle = \frac{1}{\sqrt{2^n}} \prod_{\ell=1}^{n} \big(\,|0\rangle + e^{2i\pi 0..k_{\ell-1}\ldots k_0}\,|1\rangle\,\big).$$

$\hat{F}\,|\underline{k}\rangle = \frac{1}{\sqrt{2^n}}\big(\,|0\rangle + e^{2i\pi 0..k_0}\,|1\rangle\,\big) \otimes \big(\,|0\rangle + e^{2i\pi 0..k_1.k_0}\,|1\rangle\,\big) \otimes \cdots \otimes \big(\,|0\rangle + e^{2i\pi 0..k_{n-1}\cdots k_1.k_0}\,|1\rangle\,\big).$

Variant

Corollary

If $|\underline{k}\rangle = |k_{n-1} \dots k_1.k_0\rangle$, $\hat{F}\,|\underline{k}\rangle = \frac{1}{\sqrt{2^n}} \otimes_{\ell=1}^{n} \left(|0\rangle + e^{2i\pi 0..k_{\ell-1} \dots k_0} |1\rangle \right)$.

Variant

Corollary

If $|\underline{k}\rangle = |k_{n-1} \dots k_1.k_0\rangle$, $\hat{F}\,|\underline{k}\rangle = \frac{1}{\sqrt{2^n}} \otimes_{\ell=1}^{n} \left(|0\rangle + e^{2i\pi 0..k_{\ell-1}\dots k_0} |1\rangle \right)$.

Proof

For any integer p, $e^{2i\pi p} = 1$.

$$\begin{aligned}\frac{k}{2^\ell} &= \frac{k_{n-1}2^{n-1} + \dots + k_2 2^2 + k_1 2 + k_0}{2^\ell} \\ &= \underbrace{k_{n-1}2^{n-1-\ell} + \dots + k_\ell}_{\text{integer part}} + \underbrace{\frac{k_{\ell-1}}{2} + \dots + \frac{k_0}{2^\ell}}_{\text{fractional part}} \\ &= p + 0..k_{\ell-1}\dots k_0\end{aligned}$$

So, $e^{2i\pi \frac{k}{2^\ell}} = e^{2i\pi(p+0..k_{\ell-1}\dots k_0)}$.

Variant

Corollary

If $|\underline{k}\rangle = |k_{n-1}\ldots k_1.k_0\rangle$, $\hat{F}\,|\underline{k}\rangle = \frac{1}{\sqrt{2^n}} \otimes_{\ell=1}^{n} \left(|0\rangle + e^{2i\pi 0..k_{\ell-1}\ldots k_0}\,|1\rangle \right)$.

Proof

For any integer p, $e^{2i\pi p} = 1$.

$$\begin{aligned}\frac{k}{2^\ell} &= \frac{k_{n-1}2^{n-1} + \ldots + k_2 2^2 + k_1 2 + k_0}{2^\ell} \\ &= \underbrace{k_{n-1}2^{n-1-\ell} + \ldots + k_\ell}_{\text{integer part}} + \underbrace{\frac{k_{\ell-1}}{2} + \ldots + \frac{k_0}{2^\ell}}_{\text{fractional part}} \\ &= p + 0..k_{\ell-1}\ldots k_0\end{aligned}$$

So, $e^{2i\pi\frac{k}{2^\ell}} = e^{2i\pi(p+0..k_{\ell-1}\ldots k_0)}$.

Example

- for $\ell = 1$, $e^{2i\pi\frac{k}{2} = e^{2i\pi 0..k_0}}$
- for $\ell = 2$, $e^{2i\pi\frac{k}{4} = e^{2i\pi 0..k_1.k_0}}$ and for $\ell = n$, $e^{2i\pi\frac{k}{2^n} = e^{2i\pi 0..k_{n-1}\ldots k_1.k_0}}$

Quantum Circuit of the Discrete Fourier Transform

Gate R_k and controlled

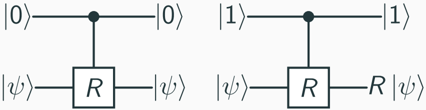
- $R_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{2i\pi}{2^k}} \end{pmatrix}$ 

- $R_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $R_1 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $R_2 = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$, $R_3 = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{i\pi}{4}} \end{pmatrix}$

Quantum Circuit of the Discrete Fourier Transform

Gate R_k and controlled

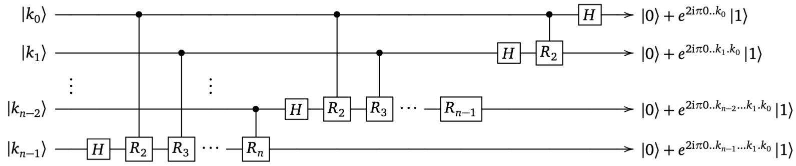
- $R_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{2i\pi}{2^k}} \end{pmatrix}$ 

- $R_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $R_1 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $R_2 = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$, $R_3 = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{i\pi}{4}} \end{pmatrix}$
- 

Gate R_k and controlled

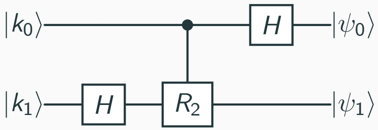
- $R_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{2i\pi}{2^k}} \end{pmatrix}$ 

- $R_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $R_1 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $R_2 = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$, $R_3 = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{i\pi}{4}} \end{pmatrix}$
- $n = 1$: $\psi_0 = H\left|k_0\right\rangle$: $\left|\psi_0\right\rangle = \left|0\right\rangle + \left|1\right\rangle$ if $k_0 = 0$, $\left|0\right\rangle - \left|1\right\rangle$ if $k_0 = 1$
  We get $\left|\psi_0\right\rangle = \left|0\right\rangle + e^{2i\pi 0..k_0}\left|1\right\rangle$ as $e^{2i\pi 0..1} = e^{i\pi} = -1$



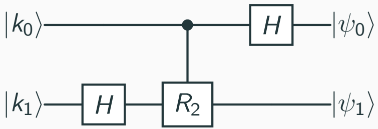
Quantum Circuit of the Discrete Fourier Transform

Case $n = 2$

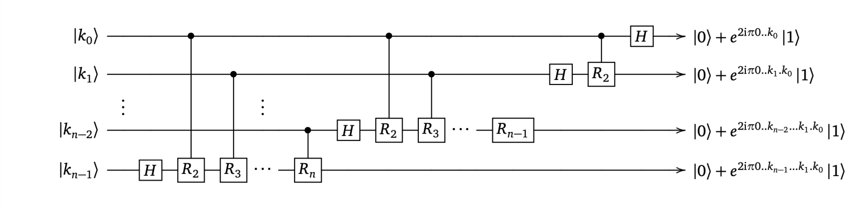
- 

- $|\psi_0\rangle$ is the same as in the case $n = 1$.
- If $|k_0\rangle = |0\rangle$, $|\psi_1\rangle = H|k_1\rangle = |0\rangle + e^{2i\pi\frac{k_1}{2}}|1\rangle$ (R_2 not active)
- If $|k_0\rangle = |1\rangle$, $|\psi_1\rangle = R_2(H|k_1\rangle) = R_2(|0\rangle + e^{2i\pi\frac{k_1}{2}}|1\rangle)$
  $|\psi_1\rangle = R_2|0\rangle + e^{2i\pi\frac{k_1}{2}}R_2|1\rangle = |0\rangle + e^{2i\pi\frac{k_1}{2}} \cdot e^{2i\pi\frac{1}{4}}|1\rangle$
- $|\psi_1\rangle = |0\rangle + e^{2i\pi\frac{k_1}{2}} \cdot e^{2i\pi\frac{k_0}{4}}|1\rangle$ and $e^{2i\pi\frac{k_1}{2}} \cdot e^{2i\pi\frac{k_0}{4}} = e^{2i\pi 0..k_1.k_0}$.

Case $n = 2$

- 

- $|\psi_0\rangle$ is the same as in the case $n = 1$.
- If $|k_0\rangle = |0\rangle$, $|\psi_1\rangle = H|k_1\rangle = |0\rangle + e^{2i\pi \frac{k_1}{2}}|1\rangle$ (R_2 not active)
- If $|k_0\rangle = |1\rangle$, $|\psi_1\rangle = R_2(H|k_1\rangle) = R_2(|0\rangle + e^{2i\pi \frac{k_1}{2}}|1\rangle)$
  $|\psi_1\rangle = R_2|0\rangle + e^{2i\pi \frac{k_1}{2}} R_2|1\rangle = |0\rangle + e^{2i\pi \frac{k_1}{2}} \cdot e^{2i\pi \frac{1}{4}}|1\rangle$
- $|\psi_1\rangle = |0\rangle + e^{2i\pi \frac{k_1}{2}} \cdot e^{2i\pi \frac{k_0}{4}}|1\rangle$ and $e^{2i\pi \frac{k_1}{2}} \cdot e^{2i\pi \frac{k_0}{4}} = e^{2i\pi 0..k_1.k_0}$.



Conclusion

Generalization

- HSP (Hidden Subgroup Problem): Let G a group and H a subgroup. The function f is constant on each coset of H, find H

Conclusion

Generalization

- HSP (Hidden Subgroup Problem): Let G a group and H a subgroup. The function f is constant on each coset of H, find H
- Shor's algorithm is for subgroup H of $G = \mathbb{Z}/\varphi(N)\mathbb{Z}$ and $H = \langle r \rangle$
- Simon's algorithm: $G = \mathbb{F}_2^n$ and $H = \{0, s\}$
- Kitaev: any Abelian Group G

Conclusion

Generalization

- HSP (Hidden Subgroup Problem): Let G a group and H a subgroup. The function f is constant on each coset of H, find H
- Shor's algorithm is for subgroup H of $G = \mathbb{Z}/\varphi(N)\mathbb{Z}$ and $H = \langle r \rangle$
- Simon's algorithm: $G = \mathbb{F}_2^n$ and $H = \{0, s\}$
- Kitaev: any Abelian Group G
- Non-abelian group: Kuperberg and Relation to Lattice problems

Conclusion

Generalization

- HSP (Hidden Subgroup Problem): Let G a group and H a subgroup. The function f is constant on each coset of H, find H
- Shor's algorithm is for subgroup H of $G = \mathbb{Z}/\varphi(N)\mathbb{Z}$ and $H = \langle r \rangle$
- Simon's algorithm: $G = \mathbb{F}_2^n$ and $H = \{0, s\}$
- Kitaev: any Abelian Group G
- Non-abelian group: Kuperberg and Relation to Lattice problems

New Results on factorization

- Shor algorithm: $O(n)$ qubits and $O(n^2 \log n)$ gates

Conclusion

Generalization

- HSP (Hidden Subgroup Problem): Let G a group and H a subgroup. The function f is constant on each coset of H, find H
- Shor's algorithm is for subgroup H of $G = \mathbb{Z}/\varphi(N)\mathbb{Z}$ and $H = \langle r \rangle$
- Simon's algorithm: $G = \mathbb{F}_2^n$ and $H = \{0, s\}$
- Kitaev: any Abelian Group G
- Non-abelian group: Kuperberg and Relation to Lattice problems

New Results on factorization

- Shor algorithm: $O(n)$ qubits and $O(n^2 \log n)$ gates
- Regev algorithm [R23]: $O(n^{3/2})$ qubits and $O(n^{3/2} \log n)$ gates

RV24 $O(n \log n))$ qubits and $O(n^{3/2} \log n)$ gates

Conclusion

Generalization

- HSP (Hidden Subgroup Problem): Let G a group and H a subgroup. The function f is constant on each coset of H, find H
- Shor's algorithm is for subgroup H of $G = \mathbb{Z}/\varphi(N)\mathbb{Z}$ and $H = \langle r \rangle$
- Simon's algorithm: $G = \mathbb{F}_2^n$ and $H = \{0, s\}$
- Kitaev: any Abelian Group G
- Non-abelian group: Kuperberg and Relation to Lattice problems

New Results on factorization

- Shor algorithm: $O(n)$ qubits and $O(n^2 \log n)$ gates
- Regev algorithm [R23]: $O(n^{3/2})$ qubits and $O(n^{3/2} \log n)$ gates

RV24 $O(n \log n))$ qubits and $O(n^{3/2} \log n)$ gates

C**F**S24 $o(n)$ qubits: RSA-2048, with 1730 qubits and $O(n^3)$ gates
For DL in $\mathbb{F}_p$ with a 2024-bit prime and 224-bit DL, 684 qubits

Conclusion

How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits by Gidney and Ekerå

Conclusion

How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits by Gidney and Ekerå

Further Reading

1. Quantum Computation and Quantum Information, Nielsen and Chuang.
2. Lecture Notes on Quantum Algorithms, A. Childs, `https://www.cs.umd.edu/~amchilds/qa/qa.pdf`