Quantum Computation

Ahto Buldas   Aleksandr Lenin

Dec 2, 2019

Finding the Period of a Function

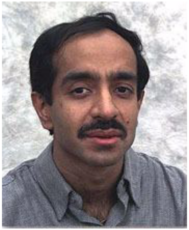
Peter Shor showed in 1994 that by using a quantum computer, it is possible to efficiently (in time $O(m^2)$) find the *period* of a wide class of functions $f\colon \mathbb{Z} \to \mathbb{Z}_{2^m}$.

The period of f is the least positive integer λ such that $f(x+\lambda) = f(x)$ for every argument x.

Shor's algorithm was one of the first quantum algoriths with serious practical consequences:

Efficient breakage of RSA and Elliptic curve cryptosystems with quantum computers

Searching from Unsorted Databases



Lov Grover showed in 1996 that quantum computers are able to:

- Search data from N-element unsorted databases in time $O(\sqrt{N})$.
- Find collisions for N-output hash functions in time $O(\sqrt[3]{N})$

In classical computational model:

- Searching from N-element unsorted database takes $O(N)$ time ($O(\log N)$ for sorted data).
- Finding collisions for N-output hash functions takes $O(\sqrt{N})$ time.

Factoring of $n = pq$ via Quantum Period Finding

The order $\mathrm{ord}_n(a)$ of $a \in \mathbb{Z}_n^*$ is the period of $f(x) = a^x \mod n$.

Repeat the next cycle until success:

1. Random element $a \leftarrow \mathbb{Z}_n^*$ is picked.
2. The period r of $f(x) = a^x \mod n$ is found with success probability $\frac{1}{\ln n}$ using quantum computer.
3. Using a and r, a non-trivial $\sqrt{1}$ is found with probability $\frac{1}{2}$.
4. The modulus n is factored via $\sqrt{1}$.

Finding Non-Trivial $\sqrt{1}$ via $\mathrm{ord}_n(\cdot)$

Lemma 1: If $p > 2$ is prime, $p - 1 = 2^d \cdot p'$, where p' is odd, the 2^d divides the order of exactly half of the elements of $\mathbb{Z}_p^*$.

Proof: Let g be a generator of $\mathbb{Z}_p^*$, $a = g^k \in \mathbb{Z}_p^*$, and $r = \mathrm{ord}_p(a)$.

If k is odd, then $g^{kr} = 1$ and $\mathrm{ord}_p(g) = p - 1 = |\mathbb{Z}_p^*|$ imply $p - 1 \mid kr$ and hence $2^d \mid r$.

If k is even, then $(g^k)^{\frac{p-1}{2}} = (g^{p-1})^{k/2} = 1^{k/2} = 1$ implies $r \mid \frac{p-1}{2}$ and hence $2^d \nmid r$. □

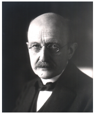
Lemma 2: If $n = pq$, where $p > q > 2$ are prime, then $r = \mathrm{ord}_n(a)$ are even and $a^{\frac{r}{2}} \not\equiv -1 \pmod{n}$ for at least half of the elements $a \in \mathbb{Z}_n^*$.

Proof: It follows from CRT that $\mathbb{Z}_n^* \cong \mathbb{Z}_p^* \times \mathbb{Z}_q^*$ and picking $a \leftarrow \mathbb{Z}_n^*$ is equivalent to picking a random vector $(a_p, a_q) \in \mathbb{Z}_p^* \times \mathbb{Z}_q^*$, where $a_p \leftarrow \mathbb{Z}_p^*$ and $a_q \leftarrow \mathbb{Z}_q^*$ are independent random variables.

If $a \sim (a_p, a_q)$, then by $\mathrm{ord}_n(a) = \mathrm{lcm}(\mathrm{ord}_p(a_p), \mathrm{ord}_q(a_q))$ we have that $\mathrm{ord}_n(a)$ can be odd only if $\mathrm{ord}_p(a_p)$ and $\mathrm{ord}_q(a_q)$ are both odd, the probability of which does not exceed $\frac{1}{4}$.

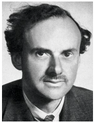
If $\mathrm{ord}_n(a)$ is even and $a^{\frac{r}{2}} \equiv -1 \pmod{n}$, then $(a_p)^{\frac{r}{2}} \equiv -1 \pmod{p}$ and $(a_q)^{\frac{r}{2}} \equiv -1 \pmod{q}$. Hence, $\mathrm{ord}_p(a_p) \nmid \frac{r}{2}$, and as $\mathrm{ord}_p(a_p) \mid r$, we have $2^d \mid \mathrm{ord}_p(a_p)$ and, analogously, $2^d \mid \mathrm{ord}_q(a_q)$, that by Lemma 1, happens with probability $\frac{1}{4}$. □

$\Rightarrow$ P$[a \leftarrow \mathbb{Z}_n^* \colon \mathrm{ord}_n(a)$ is even and $a^{\frac{\mathrm{ord}_n(a)}{2}}$ is non-trivial $\sqrt{1}] \geq \frac{1}{2}$

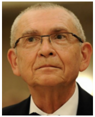


1900: Planck claimed that electromagnetic energy could only be be a multiple of an elementary unit $E = h\nu$

$\sim$1920: Schrdinger, Bohr, Heisenberg, et al. developed the foundations of quantum mechanics



$\sim$1930: Dirac, von Neumann and Hilbert created modern quantum mechanics



1980-1985: Manin, Benioff, Feynman, and Deutsch created the foundations of quantum computation

State Space

The state space of a closed physical system (electron, whole universe, etc.) is a complex vector space V with inner product $\langle \cdot, \cdot \rangle$, so called *Hilbert space*.

State of a physical system is represented by a *unit vector* $\Psi \in V$, i.e. $||\Psi|| = \sqrt{\langle \Psi, \Psi \rangle} = 1$.

All information about the system is in Ψ.

Dynamics

If $\Psi(t)$ is the state at t and $\Psi(t')$ is the state at later time t', then

$$\Psi(t') = U_{t,t'}\Psi(t) \ ,$$

where U is a *unitary* linear operator, i.e. $UU^\dagger = 1$, where $U^\dagger$ is the *Hermitian conjugate*: a unique operator U, so that for every $\Psi, \Psi' \in V$:

$$\langle U\Psi, \Psi' \rangle = \langle \Psi, U^\dagger \Psi' \rangle$$

Operator U depends on the described system.

$U_{t,t'}$ is the solution of a differential equation $\mathrm{i}\hbar\frac{\partial}{\partial t}\Psi = \mathcal{H}\Psi$, the *Schrödinger's equation*, integral from t to t'.

$\mathcal{H}$ is the *Hamiltoinian* operator that describes the energy of the system, $\hbar = \frac{h}{2\pi}$ is the reduced Planck konstant and i is the imaginary unit.

Measurement

Measurement of a physical quantity is descibed by a mutually ortogonal set $\{V_i\}$ of subspaces that generate the whole space V.

V_i are V_j orthogonal: $\langle \Psi_i, \Psi_j \rangle = 0$ for every $\Psi_i \in V_i$ ja $\Psi_j \in V_j$

Every subspace V_i is associated with possible measurement result r_i

If $P_i \colon V \to V_i$ is the projection operator of the corresponding result, then after measurement, with probability $p_i = ||P_i \Psi||^2$ the result is r_i and the state Ψ changes to

$$\Psi' = \frac{1}{||P_i \Psi||} P_i \Psi \quad .$$

Quantum Bit (*qubit*)

Two-dimensional complex vector space V with basis vectors $|0\rangle$ ja $|1\rangle$

A qubit can be in a state:

$$\Psi = \alpha|0\rangle + \beta|1\rangle \ ,$$

where $\alpha, \beta \in \mathbb{C}$ ja $|\alpha|^2 + |\beta|^2 = 1$.

$|0\rangle$ and $|1\rangle$ are orthogonal.

The corresponding measurement results are 0 and 1.

Measurement of Ψ gives:

- $|0\rangle$ with probability $|\alpha|^2$
- $|1\rangle$ with probability $|\beta|^2$.

For example, measuring $\Psi = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ gives 0 with probability $\frac{1}{2}$

Composition of Systems

Two *classical systems* with state sets S_1 and S_2 compose to a system with state set $S_1 \times S_2$ – *direct product*, the set of all ordered pairs (s_1, s_2) of states $s_1 \in S_1$ and $s_2 \in S_2$.

Two *quantum systems* with state spaces V_1 and V_2 compose to a system with state space $V_1 \otimes V_2$ (*tensor product*).

Let $\mathcal{L}(S)$ denote the complex vector space with basis S.

If $V_1 = \mathcal{L}(S_1)$ and $V_2 = \mathcal{L}(S_2)$, then

$$V_1 \otimes V_2 = \mathcal{L}(S_1 \times S_2) \ ,$$

i.e. tensor product is the complex vector spate whose basis vectors are all possible ordered pairs (s_1, s_2) of basis vectors $s_1 \in S_1$ and $s_2 \in S_2$.

Two-Bit Quantum Register

The state space is the four-dimensional space $V \otimes V$, where V is the state space of a qubit with basis vectors $|0\rangle$ and $|1\rangle$.

The basis vectors are $|00\rangle$, $|01\rangle$, $|10\rangle$, and $|11\rangle$.

Two-bit quantum register can be in the state:

$$\Psi = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle \ ,$$

where $\alpha, \beta, \gamma, \delta \in \mathbb{C}$ and $|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1$.

n-Bit Quantum Register

The state space is 2^n-dimensional space $\underbrace{V \otimes V \otimes \ldots \otimes V}_{n}$

The basis vectors are $|0..00\rangle, |0..01\rangle \ldots |1..11\rangle$.

Exponential growth of the dimension is the main reason why the behavior of quantum mechanical systems is hard to model with classical computers.

Entanglement

Vectors of $V \otimes V$ that are not representable in the form

$$\begin{aligned}\Psi &= (a|0\rangle + b|1\rangle) \otimes (c|0\rangle + d|1\rangle) \\ &= ac|00\rangle + ad|01\rangle + bc|10\rangle + bd|11\rangle\end{aligned}$$

where $|a|^2 + |b|^2 = |c|^2 + |d|^2 = 1$ are called *entangled states*.

Homework exercise: Show that the following state is entangled:

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

Einstein Podolsky Rosen (EPR) Paradox

Let XY be a two-bit quantum register that is in the state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

Alice takes the bit Y to Andromeda galaxy, X stays in Earth with Bob.

$X \longleftarrow \ldots \longleftarrow XY \longrightarrow \ldots \longrightarrow Y$

If Alice measures Y, then with probability $\frac{1}{2}$ she has 0 or 1.

With probability $\frac{1}{2}$ the state of the register immediately changes to $|00\rangle$ or to $|11\rangle$ and hence, *also X is now fixed*.

EPR paradox: How can X know immediately (faster than light) that Y has been measured?

Partial Measurement of a Quantum Register

If a part (e.g. Y) of a quantum register is measured, this cannot have any influence on the probability distributions of other parts (e.g. X).

Though Alice knows, what Bob gets when he measures X, but Bob does not know and for him, X is still random.

We say that X is in *mixed state*), that is a probabilistic combination of state vectors (*pure states*).

Principle of deferred measurement: all measurements during quantum computations can be postponed to the end of computations.

Principle of indirect measurement: if a qubit is not measured till the end of computation, then we can measure it right after creation.

Quantum Logic Gates

Quantum computations can be represented as a sequence of *quantum logic gates*.

m-bit quantum gate is a device that transforms input qubits $x_0, \ldots, x_{m-1}$ to output qubits $y_0, \ldots, y_{m-1}$.

The action of quantum gates is unitary and can be represented by *unitary matrices*.

A single-bit quantum gate is a represented by a unitary transform U with matrix $\begin{bmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{bmatrix}$) that converts the input qubit $\alpha|0\rangle + \beta|1\rangle$ to output qubit $\alpha'|0\rangle + \beta'|1\rangle$ so that:

$$\begin{bmatrix} \alpha' \\ \beta' \end{bmatrix} = \begin{bmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{bmatrix} \cdot \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} u_{00}\alpha + u_{01}\beta \\ u_{10}\alpha + u_{11}\beta \end{bmatrix}$$

Quantum NOT-gate

NOT-gate is defined by the operations on base vectors as follows:

$$\begin{aligned} \mathsf{NOT}(|0\rangle) &= |1\rangle \\ \mathsf{NOT}(|1\rangle) &= |0\rangle \end{aligned}$$

NOT-gate mixes the coefficients α and β of $\alpha|0\rangle + \beta|1\rangle$:

$$\mathsf{NOT}(\alpha|0\rangle + \beta|1\rangle) = \beta|0\rangle + \alpha|1\rangle \ ,$$

NOT-gate is represented by the matrix $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$.

$\mathsf{NOT}(\mathsf{NOT}(\Psi)) = \Psi$ for every state vector Ψ, because

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

Hadamard Gate

Hadamard gate is defined by the operations on base vectors as follows:

$$\begin{aligned} \mathsf{NOT}(|0\rangle) &= \frac{|0\rangle + |1\rangle}{\sqrt{2}} \\ \mathsf{NOT}(|1\rangle) &= \frac{|0\rangle - |1\rangle}{\sqrt{2}} \end{aligned}$$

Hadamard gate is represented by the matrix $H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$.

Homework exercise: Show that $HH = I$.

Phase Shift Gate

Phase shift gate is defined by the operations on base vectors as follows:

$$\begin{aligned}\mathsf{NOT}(|0\rangle) &= |0\rangle \\ \mathsf{NOT}(|1\rangle) &= e^{\mathrm{i}\phi}\beta|1\rangle\end{aligned}$$

Phase shift gate is represented by the matrix $R_\phi = \begin{bmatrix} 1 & 0 \\ 0 & e^{\mathrm{i}\phi} \end{bmatrix}$.

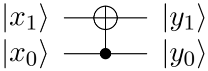
Homework exercise: Show that $R_\phi R_{-\phi} = I$.

Controlled Inversion or Quantum XOR-Gate

Defined by the operations on base vectors as follows:

$$\begin{array}{lllllll} |00\rangle & \mapsto & |00\rangle & \quad & |10\rangle & \mapsto & |11\rangle \\ |01\rangle & \mapsto & |01\rangle & \quad & |11\rangle & \mapsto & |10\rangle \end{array}$$

i.e., second bit is inverted if the first bit is set. Denoted by:



Controlled inversion gate is represented by the matrix:

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

Swap Gate

Defined by the operations on base vectors as follows:

$$\begin{array}{rclcrcl} |00\rangle & \mapsto & |00\rangle & \quad & |10\rangle & \mapsto & |01\rangle \\ |01\rangle & \mapsto & |10\rangle & \quad & |11\rangle & \mapsto & |11\rangle \end{array}$$

i.e., the order of the bits is inversed.

Represented by the matrix:

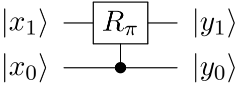
$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Controlled Phase Shift

Defined by the operations on base vectors as follows:

$$\begin{array}{lllllll} |00\rangle & \mapsto & |00\rangle & \quad & |10\rangle & \mapsto & |10\rangle \\ |01\rangle & \mapsto & |01\rangle & \quad & |11\rangle & \mapsto & e^{\mathrm{i}\phi}|11\rangle \end{array}$$

i.e., if the first bit is set, the phase of second qubit is shifted. Denoted by:

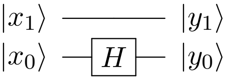


Represented by the matrix:

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{\mathrm{i}\phi} \end{bmatrix}$$

Example 1

Quantum circuit

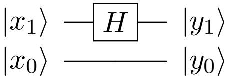


is represented by the matrix:

$$H \otimes I = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix}$$

Example 2

Quantum circuit

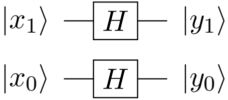


is represented by the matrix:

$$I \otimes H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix}$$

Example 3

Quantum circuit



is represented by the matrix:

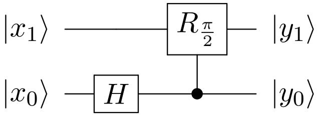
$$H \otimes H = \frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$

For example:

$$\begin{aligned} (H \otimes H)|00\rangle &= H|0\rangle \otimes H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ &= \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) \end{aligned}$$

Example 4

Quantum circuit



is represented by the matrix:

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \mathrm{i} \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & \mathrm{i} & 0 & -\mathrm{i} \end{bmatrix}$$

Non-Cloning Theorem

Cloner is a unitary operator with a state Φ, such that for every state Ψ we have $U\colon |\Psi\rangle|\Phi\rangle \mapsto |\Psi\rangle|\Psi\rangle$.

Say, $|\Phi\rangle = |0\rangle$. In this case, $U\colon |0\rangle|0\rangle \mapsto |0\rangle|0\rangle$ and $U\colon |1\rangle|0\rangle \mapsto |1\rangle|1\rangle$. By the linearity of U:

$$U\colon \left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right)|0\rangle \quad\mapsto\quad \frac{1}{\sqrt{2}}|0\rangle|0\rangle + \frac{1}{\sqrt{2}}|1\rangle|1\rangle$$

On the other hand,

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

Simulating Classical Circuits

For every classical logic circuit (say, with AND- and NOT gates) that computes a function $f\colon \{0,1\}^n \to \{0,1\}^m$, there is a quantum circuit U that transforms a $(n+m)$-qubit quantum register in the following way:

$$U\colon |x\rangle|y\rangle \mapsto |x\rangle|y \oplus f(x)\rangle \quad ,$$

which means that $|x\rangle|0^m\rangle \mapsto |x\rangle|f(x)\rangle$.

Quantum Parrallelism

Hadamard gate $H^{\otimes n}$ converts $|0^n\rangle|0^m\rangle$ to the superposition

$$\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle|0^m\rangle \ ,$$

where $N = 2^n$. By applying U, we get a superposition

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

Analogous to classical parallel computation with 2^n *threads*, but threads are not separately accessible (no measurement!)

By measuring the output, one single value $y = f(x)$ is obtained. This is the same as classical computation where $x \leftarrow \{0,1\}^n$ and $y \leftarrow f(x)$.

Exchanging Information Between Threads

In classical computation, threads can exchange information in arbitrary way.

In quantum computation, such information exchange is limited.

For example, if all threads compute a one-bit output, there are no known ways how compute the product of those bits.

If this is possible, one can solve the so-called $\mathbf{NP}$-complete combinatorial problems efficiently with quantum computer.

This is widely belived (among complexity theoreticians) to be impossible.

Quantum Fourier Transform (QFT)

Classical Fourier Transform (FT) converts a vector $(x_0, \ldots, x_{N-1}) \in \mathbb{C}^N$ to vector $(y_0, \ldots, y_{N-1}) \in \mathbb{C}^N$ so that:

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{2\pi \mathrm{i} \frac{j\,k}{N}} \quad . \tag{1}$$

QFT converts $\sum_{i=0}^{N-1} x_i |i\rangle$ to state $\sum_{i=0}^{N-1} y_i |i\rangle$ using (1).

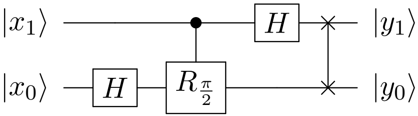
If $N = 2$, then $x_0|0\rangle + x_1|1\rangle$ maps to $\frac{x_0+x_1}{\sqrt{2}}|0\rangle + \frac{x_0-x_1}{\sqrt{2}}|1\rangle$. In matrix form:

$$\begin{bmatrix} y_0 \\ y_1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \cdot \begin{bmatrix} x_0 \\ x_1 \end{bmatrix} = H \cdot \begin{bmatrix} x_0 \\ x_1 \end{bmatrix} \quad .$$

Using the notation $\omega = e^{\frac{2\pi i}{N}}$, for $N = 4$ the QFT is represented by:

$$\frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 \\ 1 & \omega^2 & \omega^4 & \omega^6 \\ 1 & \omega^3 & \omega^6 & \omega^9 \end{bmatrix} = \frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{bmatrix}$$

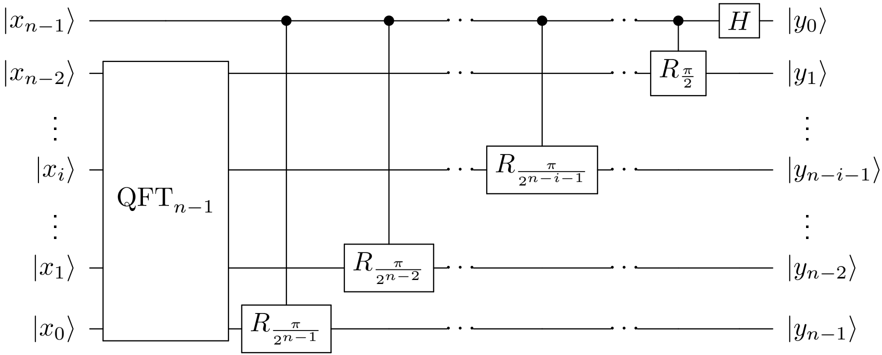
QFT_2 as a quantum circuit:



This corresponds to the next product of matrices:

$$\underbrace{\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}}_{\text{swap}} \cdot \underbrace{\begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix}}_{\text{second } H} \cdot \underbrace{\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & i \end{bmatrix}}_{\text{phase shift}} \cdot \underbrace{\begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix}}_{\text{first } H}$$

The next figure depicts a general recursive construction of QFT_n (if $N = 2^n$) using QFT_{n-1}. Schemes are presented without the last swap.



Period Finding with Shor's Algorithm

Let $F\colon |x,y\rangle \mapsto |x, y \oplus f(x)\rangle$ be a quantom circuit that computes an r-periodic function $f\colon \mathbb{Z} \to \mathbb{Z}_{2^m}$. Let $r < 2^{n-1}$ and $N = 2^{2n}$.

We use two quantum registers: $2n$-qubit X and m-qubit Y.

Shor's algorithm (initially, XY is in the state $\left|0^{2n}, 0^m\right\rangle$)

- S1 Using $H^{\oplus 2n}$ create the superposition $\Psi = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i, 0\rangle$
- S2 Using F compute the superposition $\Phi = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i, f(i)\rangle$
- S3 Measure the register Y (actually unnecessary!)
- S4 Apply QFT_{2n} to X
- S5 Measure X to obtain $|i_0\rangle$, where $i_0 \approx \lambda \frac{N}{r}$ ja $\lambda \in \mathbb{Z}_r$

$$\left|0^{2n}, 0^m\right\rangle \xrightarrow{H^{\oplus 2n}} \Psi \xrightarrow{F} \Phi \xrightarrow{\mathrm{QFT}_{2n}} \Phi_0 \xrightarrow{\mathcal{M}} |i_0, *\rangle \text{ kus } i_0 \approx \lambda \frac{N}{r}$$

Step S3: After Measuring Y

The result is $|*, k\rangle$, where $k = f(s)$ and s is chosen so that $s < r$.

A f is r-periodic, we obtain a superpositsiooni Φ' of $|x_j, k\rangle$, where $x_j = s + jr$. There are $p = \lceil N/r \rceil$ of such states. Hence:

$$\Phi' = \frac{1}{\sqrt{p}} \sum_{j=0}^{p-1} |s + jr, k\rangle \ .$$

Actually, S3 *unnecessary* because of the *deferred measurement principle*.

Register Y can be transported to Andromeda galaxy and measuring Y cannot have any influence over later measurements of X.

$$X \longleftarrow \ldots \longleftarrow XY \longrightarrow \ldots \longrightarrow Y$$

What happens if we measure X now?

The result is $|s + jr, k\rangle$.

If f is one to one in $\mathbb{Z}_r$, then s is uniformly distributed.

Also j is uniformly distributed on $\mathbb{Z}_p$.

Hence, if $\frac{N}{r} \in \mathbb{Z}$, then $s + jr$ is uniformly distributed on $\mathbb{Z}_N$ and does not contain any information about r.

If we repeat the experiment from S1, we get $|s' + j'r, k'\rangle$, where s' and j' are independent of s and j, and hence, $s' + j'r$ is independent of $s + jr$.

Therefore, repeating gives us nothing!

Step S4: QFT

"Filters out" the random shift s.

After applying QFT_{2n} we get:

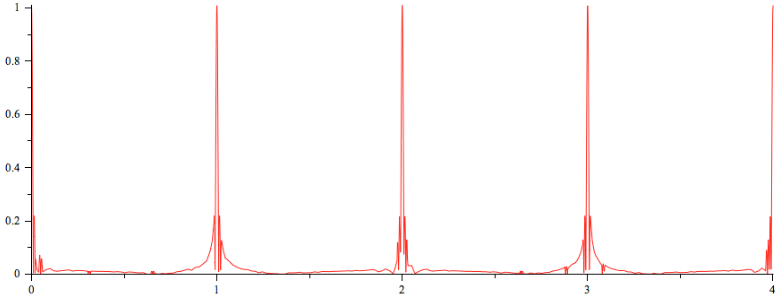
$$\begin{aligned}\Phi_0 &= \mathrm{QFT}_{2n}\Phi' = \frac{1}{\sqrt{pN}}\sum_{i=0}^{N-1}\left(\sum_{j=0}^{p-1} e^{2\pi\mathrm{i}\frac{i(s+jr)}{N}}\right)|i,k\rangle \\ &= \frac{1}{\sqrt{pN}}\sum_{i=0}^{N-1} e^{2\pi\mathrm{i}\frac{is}{N}}\left(\sum_{j=0}^{p-1} e^{2\pi\mathrm{i}\frac{ijr}{N}}\right)|i,k\rangle\end{aligned}$$

$\left|e^{2\pi\mathrm{i}\frac{is}{N}}\right| = 1$ and

$\left|\sum_{j=0}^{p-1} e^{2\pi\mathrm{i}\frac{ijr}{N}}\right| \approx \begin{cases} p & \text{if } \frac{ir}{N}\in\mathbb{Z}\text{, i.e. if } i \text{ is a multiple of } \frac{N}{r} \\ 0 & \text{if } \frac{ir}{N}\notin\mathbb{Z}\end{cases}$

Explanation:

$$\lim_{p\to\infty} \frac{1}{p} \sum_{j=0}^{p-1} e^{2\pi \mathrm{i} \alpha j} = \begin{cases} 1 & \text{if } \alpha \in \mathbb{Z} \\ 0 & \text{if } \alpha \notin \mathbb{Z} \end{cases} .$$



The graph of $g(\alpha) = \frac{1}{p} \sum_{j=0}^{p-1} e^{2\pi \mathrm{i}\alpha j}$ if $p = 100$.

Step S5: Measuring X

We obtain $i \approx \lambda \frac{N}{r}$ where $\lambda \in \mathbb{Z}_r$, i.e. $\left| \frac{i}{N} - \frac{\lambda}{r} \right| < 2^{-2n}$.

If $r, r' < 2^{n-1}$ ja $\frac{\lambda}{r} \neq \frac{\lambda'}{r'}$ then $\lambda r' \neq \lambda' r$ and thus

$$\left| \frac{\lambda}{r} - \frac{\lambda'}{r'} \right| = \frac{|\lambda r' - \lambda' r|}{rr'} \geq \frac{1}{rr'} \geq 4 \cdot 2^{-2n}$$

Hence, a rational approximation $\frac{a}{b}$ of $\frac{i}{N} = i \cdot 2^{-2n}$ with restriction $b < 2^{n-1}$ is uniquely defined.

The best rational approximation $\frac{a}{b}$ with $b < M$ can be found in time $O(\log M)$ by using *continued fractions*. If $M = 2^n$, then in time $O(n)$.

If $\gcd(\lambda, r) = 1$ then $b = r$. It is sufficient that λ is a *prime*.

This happens with probability about $\frac{1}{\ln r} = \frac{1}{O(n)}$ and hence $O(n)$ trials are sufficient to find r.

Continued Fractions

Denote

$$[a_0; a_1; \ldots; a_n] = a_0 + \frac{1}{a_1 + \frac{1}{\ldots + \frac{1}{a_n}}} = [a_0; a_1; \ldots; a_n - 1; 1]$$

Every rational number $x \geq 1$ can be represented with continued fractions. For example:

$$\begin{aligned}
\frac{31}{13} &= 2 + \frac{5}{13} = 2 + \frac{1}{\frac{13}{5}} = 2 + \frac{1}{2 + \frac{3}{5}} = 2 + \frac{1}{2 + \frac{1}{\frac{5}{3}}} = 2 + \frac{1}{2 + \frac{1}{1 + \frac{2}{3}}} \\
&= 2 + \frac{1}{2 + \frac{1}{1 + \frac{1}{\frac{3}{2}}}} = 2 + \frac{1}{2 + \frac{1}{1 + \frac{1}{1 + \frac{1}{2}}}} = [2; 2; 1; 1; 2] \\
&= 2 + \frac{1}{2 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1}}}}} = [2; 2; 1; 1; 1; 1]
\end{aligned}$$

Theorem: $[a_0; a_1; \ldots; a_n] = \frac{p_n}{q_n}$, where $p_0 = a_0$, $q_0 = 1$, $p_1 = 1 + a_0 a_1$, $q_1 = a_1$,

$$\begin{aligned} p_n &= a_n p_{n-1} + p_{n-2} \\ q_n &= a_n q_{n-1} + q_{n-2} \end{aligned}$$

Proof: Induction on n:

- *Basis*: $[a_0] = a_0 = \frac{a_0}{1} = \frac{p_0}{q_0}$ and $[a_0; a_1] = a_0 + \frac{1}{a_1} = \frac{1+a_0 a_1}{a_1} = \frac{p_1}{q_1}$.
- *Step*: if the claim is true for $n-1$ then:

$$\begin{aligned} [a_0; \ldots; a_n] &= [a_0; a_1; \ldots; a_{n-1} + \frac{1}{a_n}] = \frac{\tilde{p}_{n-1}}{\tilde{q}_{n-1}} \\ &= \frac{(a_{n-1} + \frac{1}{a_n}) p_{n-2} + p_{n-3}}{(a_{n-1} + \frac{1}{a_n}) q_{n-2} + q_{n-3}} = \frac{p_{n-1} + p_{n-2}/a_n}{q_{n-1} + q_{n-2}/a_n} = \frac{p_n}{q_n} \end{aligned}$$

because $\tilde{p}_{n-2} = p_{n-2}$, $\tilde{q}_{n-2} = q_{n-2}$, $\tilde{p}_{n-3} = p_{n-3}$, $\tilde{q}_{n-3} = q_{n-3}$. □

Corollary: $p_n \geq p_{n-1} \geq \ldots \geq p_1 \geq p_0$ ja $q_n \geq q_{n-1} \geq \ldots \geq q_1 \geq q_0$.

Lemma: $q_n p_{n-1} - p_n q_{n-1} = (-1)^n$ for every $n > 0$.

Proof: Induction on n:

- *Basis*: $r_1 = q_1 p_0 - p_1 q_0 = a_0 a_1 - (1 + a_0 a_1) \cdot 1 = -1 = (-1)^1$.
- *Step*: If $r_{n-1} = q_{n-1} p_{n-2} - p_{n-1} q_{n-2} = (-1)^{n-1}$ then:

$$
\begin{aligned}
r_n &= q_n p_{n-1} - p_n q_{n-1} \\
&= (a_n q_{n-1} + q_{n-2}) p_{n-1} - (a_n p_{n-1} + p_{n-2}) q_{n-1} \\
&= -(q_{n-1} p_{n-2} - p_{n-1} q_{n-2}) = -r_{n-1} = -(-1)^{n-1} = (-1)^n
\end{aligned}
$$

□

Theorem: Let $x \in \mathbb{Q}$ ja $\frac{p}{q} = [a_0; a_1; \ldots; a_n] \in \mathbb{Q}$ (i.e. $\frac{p}{q} = \frac{p_n}{q_n}$) such that

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

Then there exist $a_{n+1}, \ldots, a_N$, so that $x = [a_0; a_1; \ldots; a_n; a_{n+1}; \ldots; a_N]$, i.e. the continued fraction of $\frac{p}{q}$ is the continued fraction of x.

Proof: Define δ so that $x = \frac{p_n}{q_n} + \frac{\delta}{2q_n^2}$. Then by (2) we have $|\delta| < 1$. Let

$$\lambda = 2 \cdot \frac{q_n p_{n-1} - p_n q_{n-1}}{\delta} - \frac{q_{n-1}}{q_n} \quad .$$

then ...

...

$$
\begin{aligned}
[a_0;\ldots;a_n;\lambda] &= \frac{\lambda p_n + p_{n-1}}{\lambda q_n + q_{n-1}} \\
&= \frac{2p_n \frac{q_n p_{n-1} - p_n q_{n-1}}{\delta} - q_{n-1}\frac{p_n}{q_n} + p_{n-1}}{2q_n \cdot \frac{q_n p_{n-1} - p_n q_{n-1}}{\delta}} \\
&= \frac{p_n}{q_n} + \frac{\delta}{2q_n^2} = x
\end{aligned}
$$

We choose n to be even and get $\lambda = \frac{2}{\delta} - \frac{q_{n-1}}{q_n} > 2 - 1 = 1$ Hence, there are $a_{n+1}, \ldots, a_N$ such that $\lambda = [a_{n+1};\ldots;a_N]$ and

$$x = [a_0;\ldots;a_n;\lambda] = [a_0;\ldots;a_n;a_{n+1};\ldots;a_N]$$

□