Quantum Computation (484)

Mario Berta, Herbert Wiklicky

m.berta@imperial.ac.uk
Autumn 2018

Continuous and Discrete Transformations

A function f and expressed it via "standard" function e_i.

$$f(x) = \sum_i f_i e_i(x)$$

$$\sin(x) = x - \frac{x^3}{3!} + \frac{x^5}{5!} - \ldots + (-1)^n \frac{x^{2n+1}}{(2n+1)!} \pm \ldots$$

Continuous Transformation for functions:

$$g(s) = \int_0^\infty f(t) e^{st} dt \quad \text{(Laplace)}$$

Discrete Transformations for vectors:

$$y_j = \sum_i x_i e^{ij}$$

Discrete Fourier Transformation

Given a vector of N complex numbers $(x_0, x_1, x_2, \ldots, x_{N-1})^T$.
The Discrete Fourier Transformation (DFT) is a vector of N complex numbers $(y_0, y_1, y_2, \ldots, y_{N-1})^T$.

The DTF then corresponds to a function $\mathbf{F} : \mathbb{C}^N \to \mathbb{C}^N$:

$$\mathbf{F} : (x_0, x_1, x_2, \ldots, x_{N-1})^T \mapsto (y_0, y_1, y_2, \ldots, y_{N-1})^T$$

such that

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{2\pi i \frac{jk}{N}}$$

The Quantum Fourier Transformation (QFT) operates with $N = 2^n$

$$\mathbf{F} : \sum_{j=0}^{2^n-1} x_j |j\rangle \mapsto \sum_{k=0}^{2^n-1} y_k |k\rangle = \sum_{k=0}^{2^n-1} \frac{1}{\sqrt{2^n}} \left(\sum_{j=0}^{2^n-1} x_j e^{2\pi i \frac{jk}{2^n}} \right) |k\rangle$$

Evaluating Polynomials

In order to evaluate a **polynomial** of degree $N-1$

$$P(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_{N-1} x^{N-1} = \sum_{i=0}^{N-1} a_i x^i$$

at N points $x_0, x_1, x_2, \ldots, x_{N-1}$ we can use the **Vandermonde matrix** $\mathbf{V}(x_0, x_1, x_2, \ldots, x_{N-1})$.

$$\begin{pmatrix} 1 & x_0 & x_0^2 & \ldots & x_0^{N-1} \\ 1 & x_1 & x_1^2 & \ldots & x_1^{N-1} \\ 1 & x_2 & x_2^2 & \ldots & x_2^{N-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_{N-1} & x_{N-1}^2 & \ldots & x_{N-1}^{N-1} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_{N-1} \end{pmatrix} = \begin{pmatrix} P(x_0) \\ P(x_1) \\ P(x_2) \\ \vdots \\ P(x_{N-1}) \end{pmatrix}$$

Roots of Unity

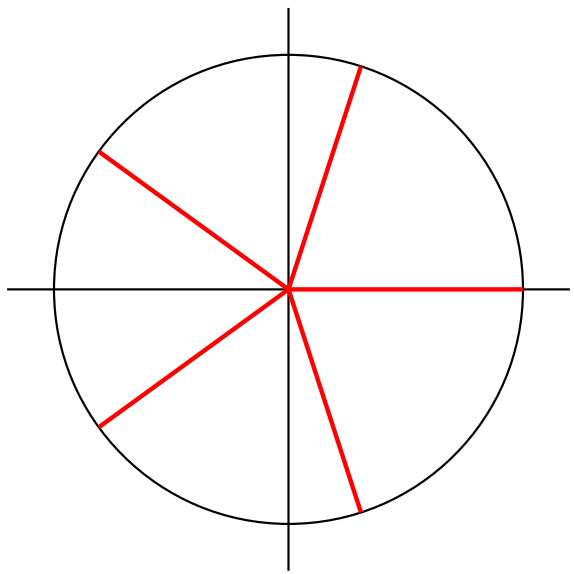
We need to consider the Mth root of unity for $M = 2^m$.

$$\omega^M = 1$$

or $\forall k = 0, 1, 2, \ldots, M - 1$

$$\omega = e^{2\pi i \frac{k}{M}}$$

Geometrically we can represent the roots of unity as:



Vandermonde and Roots of Unity

Consider the "first" root of unity $\omega = e^{\frac{2\pi i}{M}}$ then for all $k = 0, 1, 2, \ldots, M-1$ its powers ω^k are also roots of unity.

Evaluate a polynomial at $1 = \omega^0, \omega^1, \omega^2, \ldots, \omega^{M-1}$. For this we need to consider:

$$\mathbf{V}(\omega^0, \omega^1, \omega^2, \ldots, \omega^{M-1}) =$$

$$= \begin{pmatrix} 1 & 1 & 1 & \ldots & 1 \\ 1 & \omega^1 & \omega^2 & \ldots & \omega^{M-1} \\ 1 & \omega^2 & \omega^4 & \ldots & \omega^{2(M-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{M-1} & \omega^{(M-1)2} & \ldots & \omega^{(M-1)(M-1)} \end{pmatrix}$$

Discrete Fourier Transformation

We can define the **Discrete Fourier Transformation** also using the Vandermonde matrix of roots of unity.

$$\mathbf{F} = \frac{1}{\sqrt{M}}\mathbf{V}(\omega^0, \omega^1, \omega^2, \ldots, \omega^{M-1})$$

$$\mathbf{F}_{jk} = \frac{1}{\sqrt{M}}\omega^{jk} = \frac{1}{\sqrt{M}}e^{2\pi i \frac{jk}{M}}$$

The complex conjugate of roots of unity fulfil $(\omega^k)^* = \omega^{-k}$ thus:

$$\mathbf{F}^{\dagger}_{jk} = \frac{1}{\sqrt{M}}\omega^{-kj}$$

Therefore it follows directly that the DTF is a **unitary** matrix:

$$(\mathbf{F}\mathbf{F}^{\dagger})_{jk} = \frac{1}{M}\sum_{l=0}^{M-1}\omega^{jl}\omega^{-lk} = \frac{1}{M}\sum_{l=0}^{M-1}\omega^{-l(k-j)} = \begin{cases} 1 & \text{if } k = j \\ 0 & \text{if } k \neq j \end{cases}$$

Alternative Description

Consider the binary representation of $j \in \{0, 1, \ldots, 2^n - 1\}$

$$j = j_1 2^{n-1} + j_2 2^{n-2} + \ldots + j_{n-1} 2 + j_n = \sum_{k=0}^{n-1} j_{k+1} 2^{n-k-1}$$

then

$$\begin{aligned}
\mathbf{F}\,|\mathbf{j}\rangle &= \mathbf{F}\,|j_1 j_2 \cdots j_n\rangle = \\
&= \frac{1}{\sqrt{2^n}}(|0\rangle + e^{(2\pi i)0.j_n}\,|1\rangle) \otimes (|0\rangle + e^{(2\pi i)0.j_{n-1}j_n}\,|1\rangle) \otimes \ldots \\
&\quad \ldots \otimes (|0\rangle + e^{(2\pi i)0.j_2 \cdots j_{n-1}j_n}\,|1\rangle) \otimes (|0\rangle + e^{(2\pi i)0.j_1 j_2 \cdots j_{n-1}j_n}\,|1\rangle)
\end{aligned}$$

Proof: QFT via Fractional Rotations

$$
\begin{aligned}
\mathbf{F}\,|\mathbf{j}\rangle &= \frac{1}{\sqrt{2^n}} \sum_{k=0}^{N-1} e^{2\pi i \frac{jk}{2^n}}\,|\mathbf{k}\rangle \\
&= \frac{1}{\sqrt{2^n}} \sum_{k_1=0}^{1} \sum_{k_2=0}^{1} \cdots \sum_{k_n=0}^{1} e^{(2\pi i) j \left(\frac{k_1}{2^1} + \frac{k_2}{2^2} + \ldots + \frac{k_n}{2^n}\right)}\,|k_1 k_2 \ldots k_n\rangle \\
&= \frac{1}{\sqrt{2^n}} \sum_{k_1=0}^{1} \sum_{k_2=0}^{1} \cdots \sum_{k_n=0}^{1} \left(\bigotimes_{l=1}^{n} e^{(2\pi i) j \frac{k_l}{2^l}}\,|k_l\rangle \right) \\
&= \frac{1}{\sqrt{2^n}} \bigotimes_{l=1}^{n} \left(|0\rangle + e^{(2\pi i)\frac{j}{2^l}}\,|1\rangle \right)
\end{aligned}
$$

Note that: $\dfrac{k}{2^n} = \dfrac{k_1 2^{n-1} + k_2 2^{n-2} + \ldots + k_n}{2^n}$

From Fractions to Binary Representations

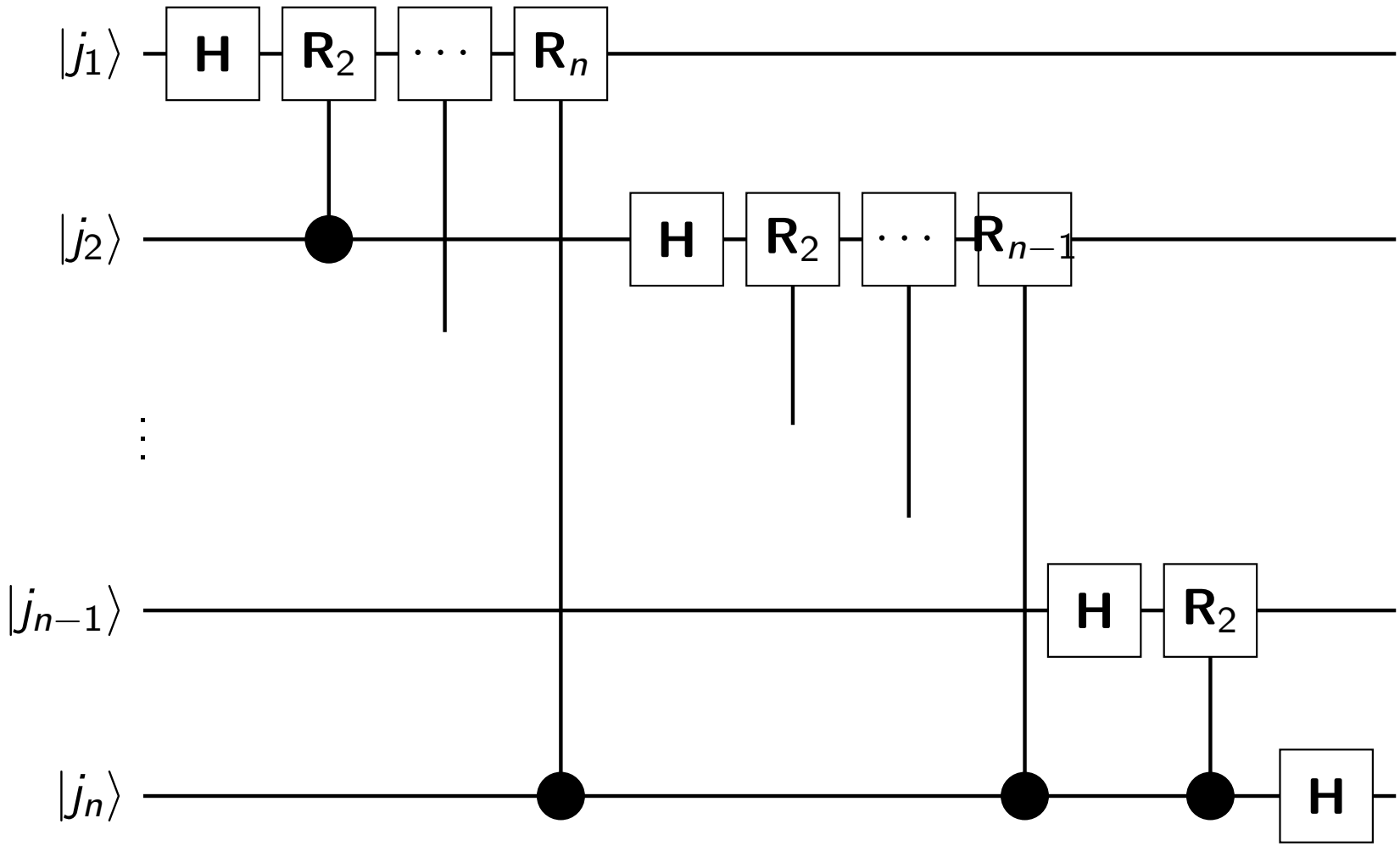
We can represent the fractions $\frac{j}{2^l}$ as a binary expression with some (irrelevant) integer part K before the binary point:

$$\frac{j}{2^l} = K + \frac{j_{n-(l-1)}}{2} + \ldots + \frac{j_{n-1}}{2^{l-1}} + \frac{j_n}{2^l} = K.j_{n-(l-1)} \cdots j_{n-1} j_n$$

$$\begin{aligned}
\mathbf{F}\,|\mathbf{j}\rangle &= \frac{1}{\sqrt{2^n}} \bigotimes_{l=1}^{n} \left(|0\rangle + e^{(2\pi i) K.j_{n-(l-1)} \cdots j_{n-1} j_n} |1\rangle \right) \\
&= \frac{1}{\sqrt{2^n}} \bigotimes_{l=1}^{n} \left(|0\rangle + e^{(2\pi i) 0.j_{n-(l-1)} \cdots j_{n-1} j_n} |1\rangle \right) \\
&= \frac{1}{\sqrt{2^n}} (|0\rangle + e^{(2\pi i) 0.j_n} |1\rangle) \otimes (|0\rangle + e^{(2\pi i) 0.j_{n-1} j_n} |1\rangle) \otimes \ldots \\
&\quad \ldots \otimes (|0\rangle + e^{(2\pi i) 0.j_2 \cdots j_{n-1} j_n} |1\rangle) \otimes (|0\rangle + e^{(2\pi i) 0.j_1 j_2 \cdots j_{n-1} j_n} |1\rangle)
\end{aligned}$$

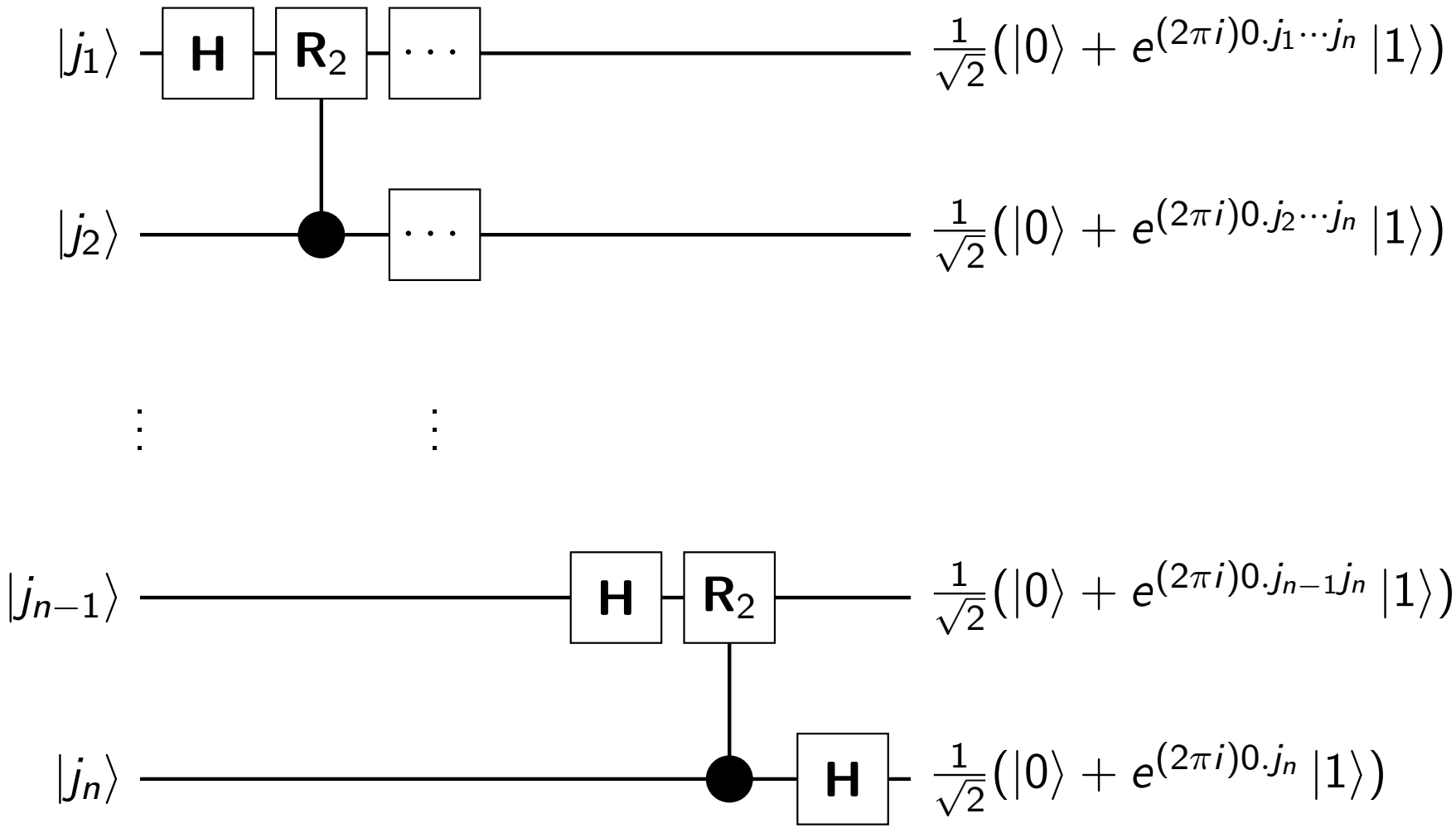
Quantum Fourier Circuit

Based on that there is a highly effective implementation of QFT which allows for fast Period Estimation, Factorisation, etc.



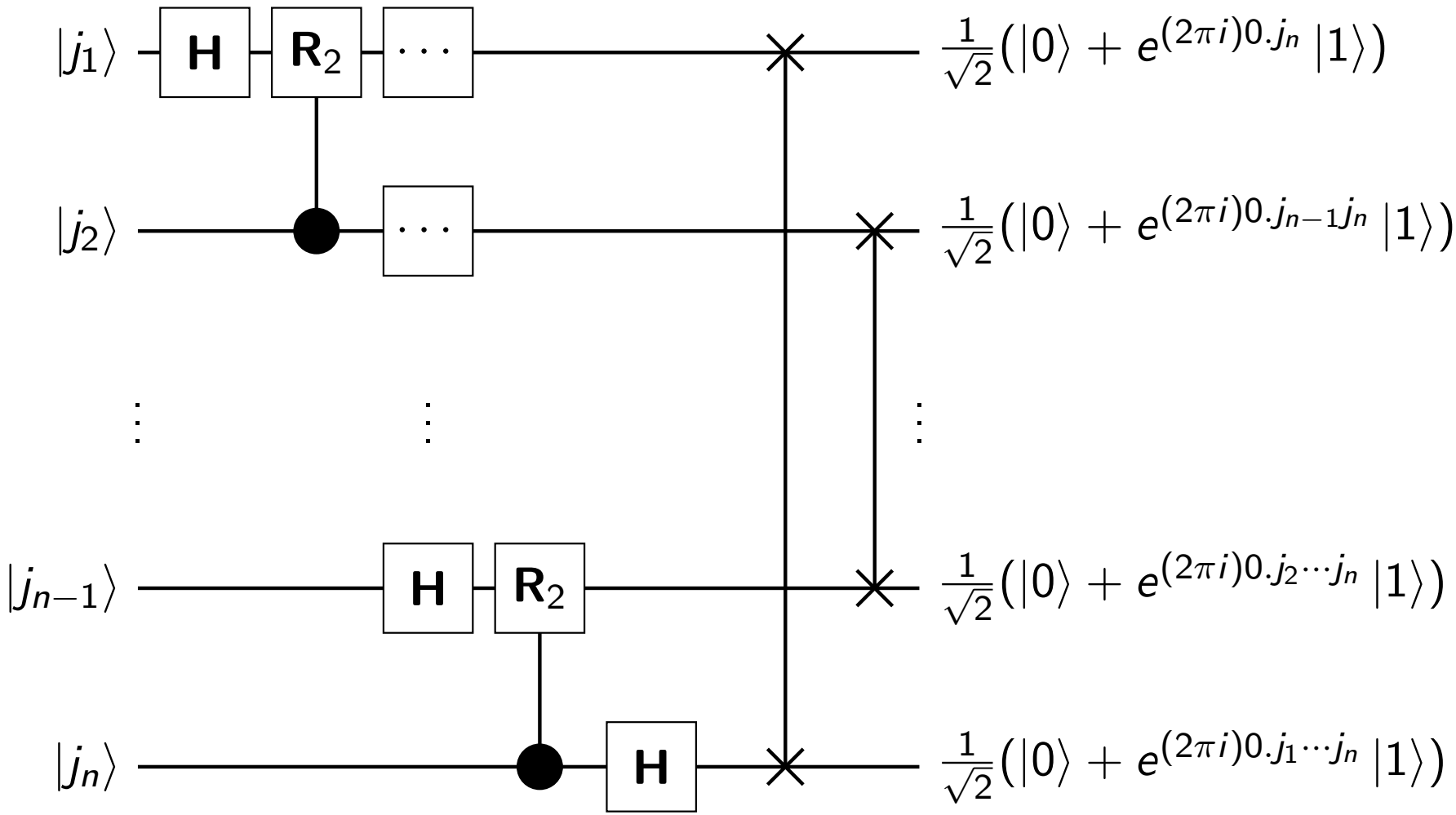
Order of Qubits

A technical problem: we get the wrong order of output qubits.



Additional Swapping

We need to add some swapping to get qubits into right positions.



QFT Complexity

The quantum circuit for QFT requires just Hadamard gates **H** and an additional type of 2-qubit gates $\mathbf{R}_k$ which implement a rotation (controlled phase shift):

$$\mathbf{R}_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i \frac{1}{2^k}} \end{pmatrix}$$

There are n Hadamard gates, $\frac{n(n-1)}{2}$ rotation gates and (about) $\frac{n}{2}$ swap gates at the end. Thus the complexity of QFT is n^2.

The best classical algorithms has complexity $2^n(\log 2^n)$, i.e. we have exponential speedup.

Working Steps of the Circuit

Starting with $|\mathbf{j}\rangle = |j_1 j_2 j_3 \dots j_n\rangle$. Applying, Hadamard gives:

$$(\mathbf{H}\,|j_1\rangle)\,|j_2 j_3 \dots j_n\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{(2\pi i)\frac{j_1}{2}}\,|1\rangle)\,|j_2 j_3 \dots j_n\rangle$$

Applying the controlled rotation $\mathbf{R}_2$ gives:

$$(\mathbf{R}_2\mathbf{H}\,|j_1\rangle)\,|j_2 j_3 \dots j_n\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{(2\pi i)(\frac{j_1}{2}+\frac{j_2}{2^2})}\,|1\rangle)\,|j_2 j_3 \dots j_n\rangle$$

The combined effect of all $\mathbf{R}_k$ to the first qubit are:

$$\begin{aligned}
&(\mathbf{R}_n\mathbf{R}_{n-1}\dots\mathbf{R}_2\mathbf{H}\,|j_1\rangle)\,|j_2 j_3 \dots j_n\rangle = \\
&= \frac{1}{\sqrt{2}}(|0\rangle + e^{(2\pi i)(\frac{j_1}{2}+\frac{j_2}{2^2}+\dots+\frac{j_n}{2^n})}\,|1\rangle)\,|j_2 j_3 \dots j_n\rangle \\
&= \frac{1}{\sqrt{2}}(|0\rangle + e^{(2\pi i)0.j_1 j_2 \dots j_n}\,|1\rangle)\,|j_2 j_3 \dots j_n\rangle
\end{aligned}$$