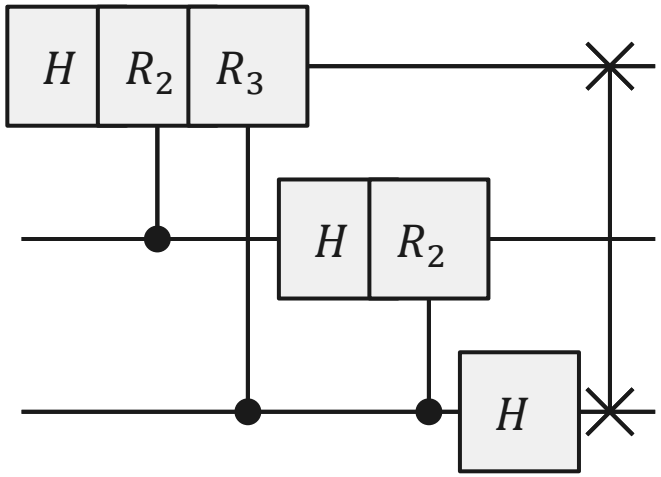
SAJID Lab
Smart & Advanced Junction of Intelligent Devices

EEE 6516 · QUANTUM COMPUTING

The Quantum Fourier Transform

From the DFT of signals and systems to a circuit of n(n+1)/2 gates

Chapter 6 · Lecture 12



Sajid Muhaimin Choudhury

Copyright © 2026 Sajid Muhaimin Choudhury. All rights reserved.

Today

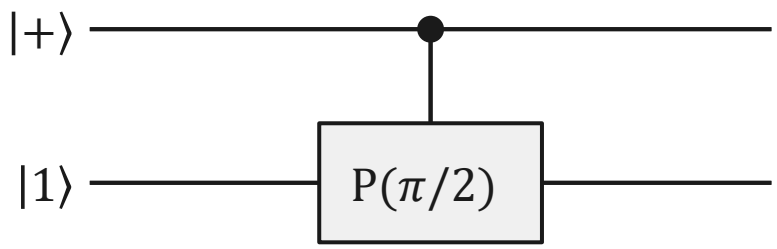
1. **Recap: kickback**
2. **The QFT**
3. **Product form**
4. **The circuit**
5. **What it cannot do**
6. **Kickback with U**

By the end of this lecture you can

- write the QFT as a DFT on the amplitudes, with its sign and normalisation
- derive the product form and read off the binary fraction on each qubit
- build the QFT circuit from H and controlled-R_k, count its gates, use QFTGate safely
- explain why the QFT does not speed up the FFT, and what C(U) does to an eigenvector

YOUR TURN · RECALL

Recap: a controlled phase on $|+\rangle|1\rangle$



Recall · 45 seconds

What does the controlled-$\mathrm{P}(\pi/2)$ do to $|+\rangle|1\rangle$? Control: qubit 0.

A $|+\rangle|1\rangle$: nothing changes

B $|+\rangle(i|1\rangle)$: the target changes

C $\frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)|1\rangle$

D $|-\rangle|1\rangle$

1 The quantum Fourier transform

Which Fourier transform does a register of qubits compute?

The QFT is a DFT on the amplitudes

DFT (signals and systems)

$$X_k = \sum_{j=0}^{N-1} x_j \, e^{-2\pi \, ijk/N}$$

Quantum Fourier transform, N = 2^n

$$\mathrm{QFT}|j\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi \, ijk/N} |k\rangle$$

The QFT acts on the 2^n amplitudes of an n-qubit register, in textbook order.

Plus sign and $1/\sqrt{N}$: it is $\sqrt{N}$ times the engineering inverse DFT.

Symmetric normalisation makes it unitary: a legitimate gate.

YOUR TURN · VOTE

Quick vote: the one-qubit QFT

Vote · 30 seconds

The one-qubit QFT ($N = 2$) acting on $|1\rangle$ gives

A $|0\rangle$

B $|+\rangle$

C $|-\rangle$

D $(|0\rangle + i|1\rangle)/\sqrt{2}$

YOUR TURN · CALCULATE

Your turn: the four-point QFT

$$\mathrm{QFT}_4 = \frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{bmatrix}$$

column j = input |j⟩; entry (k, j) = ½ i^{jk}

Pairs · 90 seconds

Compute $\mathrm{QFT}_4|1\rangle$ (that is, $|01\rangle$).

Compare with `np.fft.fft` and `np.fft.ifft` of (0, 1, 0, 0).

ANSWER

½(1, i, −1, −i): phases advance by a quarter turn

$$\mathrm{QFT}_4|1\rangle = \frac{1}{2}(|0\rangle + i|1\rangle - |2\rangle - i|3\rangle)$$

`np.fft.ifft` gives ¼(1, i, −1, −i): times $\sqrt{4} = 2$ it is the QFT.

`np.fft.fft` gives (1, −i, −1, i): divided by 2 it is $\mathrm{QFT}_4{}^{\dagger}|1\rangle$.

Every probability is ¼: the information sits entirely in the phases.

DERIVATION

The QFT is unitary

$$\langle j'|\mathrm{QFT}^{\dagger}\mathrm{QFT}|j\rangle = \frac{1}{N}\sum_{k=0}^{N-1} e^{2\pi\, i(j-j')k/N}$$

inner product of columns j′ and j

$$j = j': \quad \frac{1}{N}\cdot N = 1$$

every term equals 1

$$j \neq j': \quad \frac{1}{N}\,\frac{1-e^{2\pi\, i(j-j')}}{1-e^{2\pi\, i(j-j')/N}} = 0$$

geometric series; the numerator is 1 − 1 = 0

Orthonormal columns: the QFT is a gate, and its inverse QFT† has the minus sign.

COMMON MISTAKE

“The QFT is np.fft.fft”

✗ fft as the QFT

`np.fft.fft(x)`

minus sign, no normalisation

agrees on |000⟩, |100⟩, period-2 states

It is the inverse QFT, up to √N.

✓ ifft times √N

`np.fft.ifft(x) * np.sqrt(N)`

plus sign, symmetric factor

test with |001⟩: phases $e^{+2\pi\, ik/8}$

Equals the QFT on every input.

The two agree only on even inputs, $x_j = x_{(n-j)}$: test with an input that is not even, such as |001⟩.

2 The product form

Why can a transform on 2^n amplitudes be built from about n^2 gates?

DERIVATION

Deriving the product form

$$k = \sum_{l=1}^{n} k_l 2^{n-l}, \qquad \frac{k}{2^n} = \sum_{l=1}^{n} k_l 2^{-l}$$

write k in binary; k_1 is qubit 0

$$e^{2\pi\, ijk/2^n} = \prod_{l=1}^{n} e^{2\pi\, ijk_l 2^{-l}}$$

the exponent is a sum, so the exponential is a product

$$\mathrm{QFT}|j\rangle = \frac{1}{2^{n/2}} \bigotimes_{l=1}^{n} \left(|0\rangle + e^{2\pi\, ij2^{-l}}|1\rangle\right)$$

each sum over $k_l = 0,1$ is one qubit

$$j2^{-l} \equiv 0.j_{n-l+1} \ldots j_n \pmod 1$$

integer parts give $e^{2\pi\, i \cdot \text{integer}} = 1$

QFT|j⟩ is a product state: qubit l − 1 holds the binary fraction of the last l bits of j.

What each output qubit holds

QFT|$j_1 j_2 j_3$⟩, n = 3 (each factor over √2):

$$q_0\colon\ |0\rangle + e^{2\pi i\, 0.j_3}|1\rangle$$

$$q_1\colon\ |0\rangle + e^{2\pi i\, 0.j_2 j_3}|1\rangle$$

$$q_2\colon\ |0\rangle + e^{2\pi i\, 0.j_1 j_2 j_3}|1\rangle$$

Binary fractions

$$0.101 = \frac{1}{2} + \frac{1}{8} = \frac{5}{8}$$

$0.j_l \ldots j_m$ is a fixed-point fraction: 0.101 = ½ + ⅛ = ⅝.

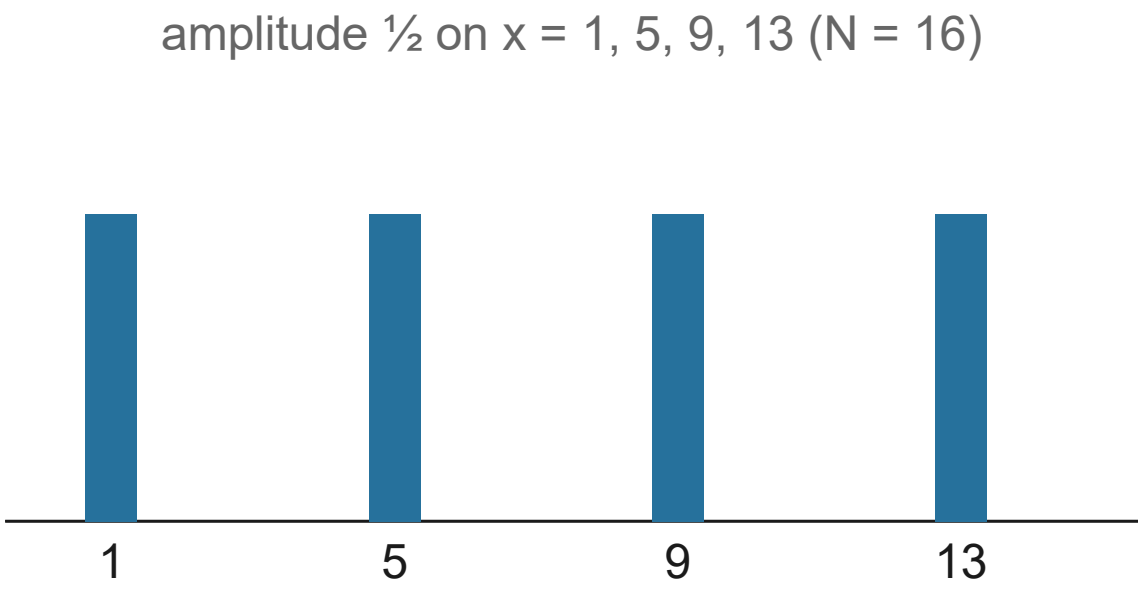
Qubit 0 sees only the last bit: phase 0 or ½ turn, so |+⟩ or |−⟩.

The last qubit sees all of j, resolved to $1/2^n$ of a turn.

The fractions come out in reverse bit order: the circuit will end with SWAPs.

YOUR TURN · PREDICT

Predict: the QFT of a periodic state



Predict · 45 seconds

Period $r = 4$, offset 1, in $N = 16$. Where are the peaks after the QFT?

A at k = 1, 5, 9, 13, like the input

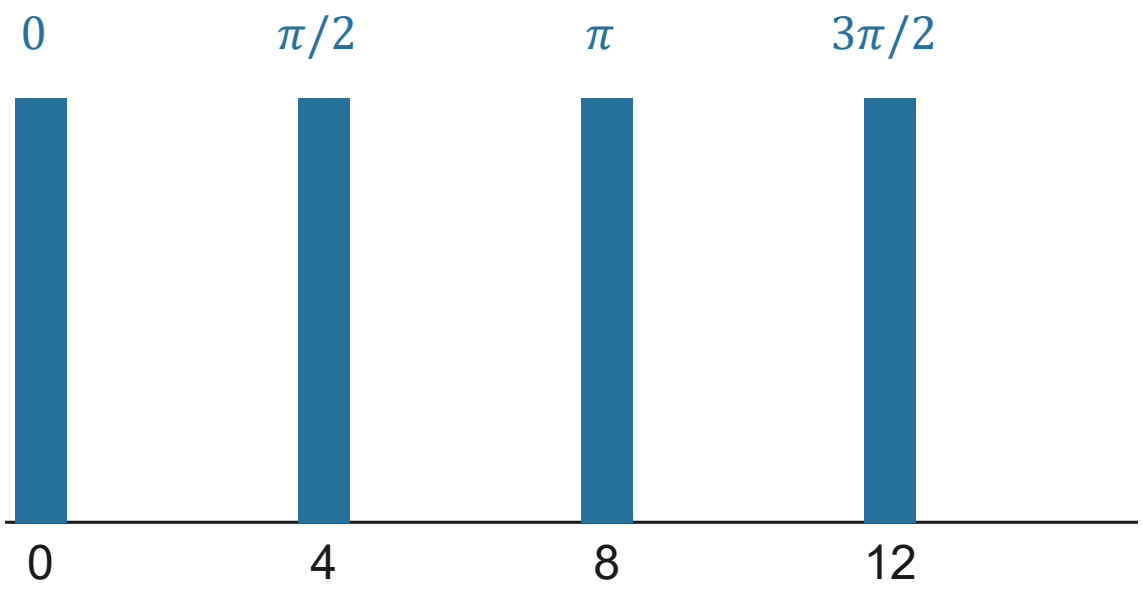
B at k = 0, 4, 8, 12, each with probability ¼

C only at k = 4

D spread evenly over all 16 outcomes

ANSWER

B: peaks at multiples of N/r = 4



outcome k; probability ¼; phase above each bar

$\frac{\sqrt{r}}{N} e^{2\pi\, i x_0 k/N} \sum_l e^{2\pi\, i l r k/N} = \frac{1}{\sqrt{r}} e^{2\pi\, i x_0 k/N}$ if k is a multiple of N/r, else 0

The offset x_0 moves into the phases; the probabilities do not depend on it.

From a few outcomes, N/r and hence the period r follow.

The QFT turns a period into peaks, and moves the offset into the phases.

3 The QFT circuit

Which gates write the binary fractions onto the qubits?

Two gates: H and controlled-R_k

Controlled-R_k

$$R_k = P\left(2\pi/2^k\right) = \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi\, i/2^k} \end{bmatrix}$$

Hadamard on a bit

$$H|j_l\rangle \propto |0\rangle + e^{2\pi\, i\, 0.j_l}|1\rangle$$

Controlled-R_k from a bit j_m

$$|1\rangle \rightarrow\ e^{2\pi\, i\, j_m/2^k}|1\rangle$$

H writes the first digit: $(-1)^j = e^{2\pi\, i\cdot 0.j}$.

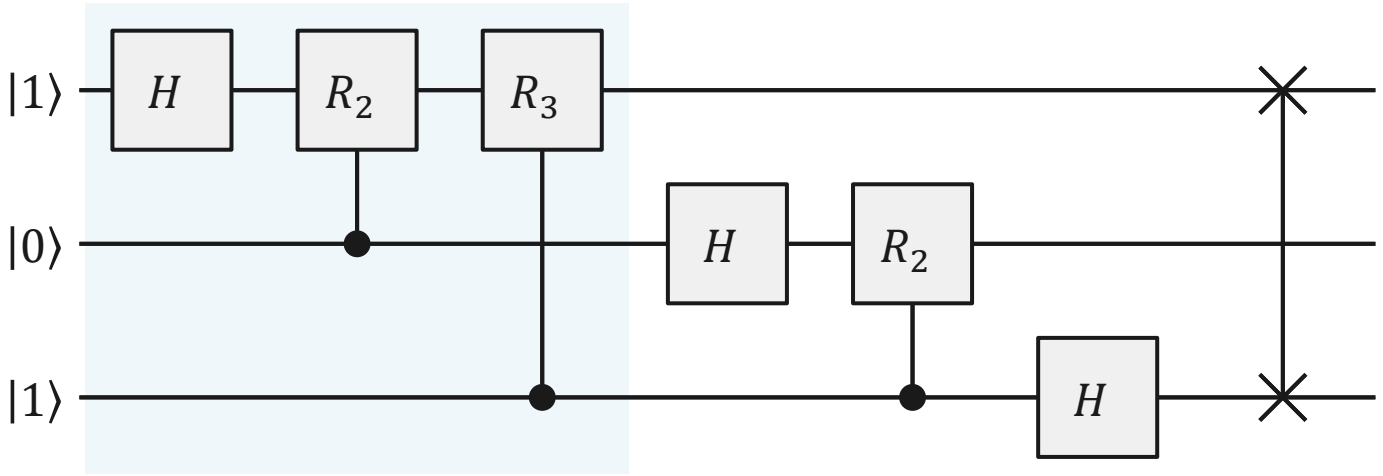
Each controlled-R_k appends one more digit, in position k.

R_k is not $R_z\left(2\pi/2^k\right)$: the global phase between them becomes relative once controlled.

Controlled-R_k is symmetric in its two qubits, like CZ (R_1 = Z).

WORKED EXAMPLE · STEP 1 OF 4

Worked example: the three-qubit QFT of |101⟩



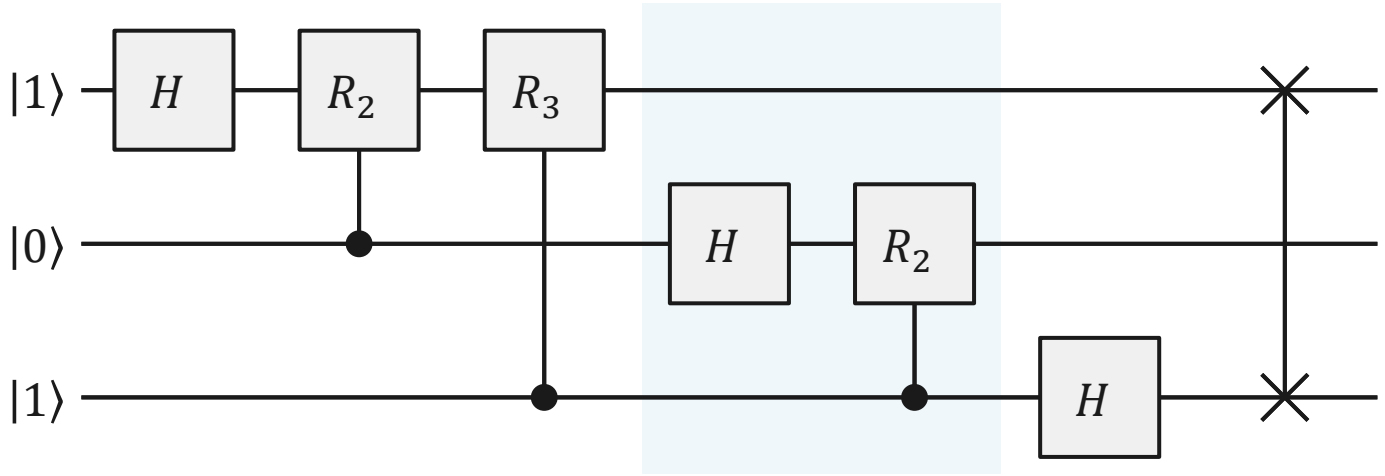
q_0: $|0\rangle + e^{2\pi\, i \cdot 5/8}|1\rangle$

1 H, then controlled-R_2 ($j_2 = 0$: nothing) and controlled-R_3 ($j_3 = 1$: +⅛): qubit 0 holds 0.101 = ⅝.

Before the next slide

What will qubit 1 hold?

Worked example: the three-qubit QFT of |101⟩



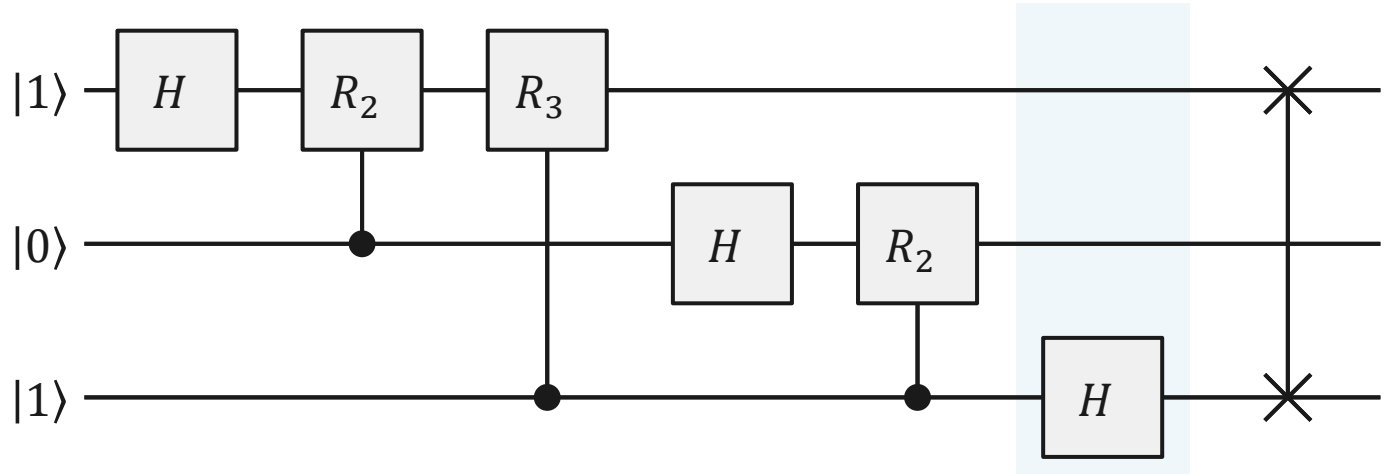
1 H, then controlled-R_2 ($j_2 = 0$: nothing) and controlled-R_3 ($j_3 = 1$: +⅛): qubit 0 holds 0.101 = ⅝.

2 H on qubit 1 ($j_2 = 0$), then controlled-R_2 from qubit 2 (+¼): phase ¼ turn, |0⟩ + i|1⟩.

q_0: $|0\rangle + e^{2\pi\, i \cdot 5/8}|1\rangle$

q_1: $|0\rangle + i|1\rangle$

Worked example: the three-qubit QFT of |101⟩



q_0: $|0\rangle + e^{2\pi\, i \cdot 5/8}|1\rangle$

q_1: $|0\rangle + i|1\rangle$

q_2: $|0\rangle - |1\rangle$

1 H, then controlled-R_2 ($j_2 = 0$: nothing) and controlled-R_3 ($j_3 = 1$: +⅛): qubit 0 holds 0.101 = ⅝.

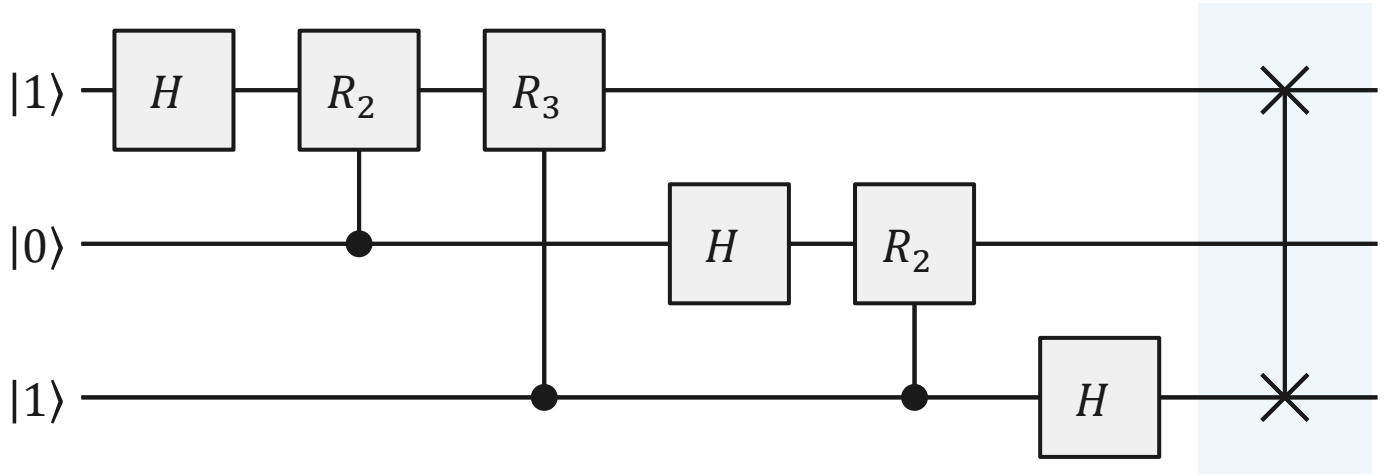
2 H on qubit 1 ($j_2 = 0$), then controlled-R_2 from qubit 2 (+¼): phase ¼ turn, $|0\rangle + i|1\rangle$.

3 H on qubit 2 ($j_3 = 1$): $|0\rangle - |1\rangle$.

Before the next slide

Which qubit holds which fraction now?

Worked example: the three-qubit QFT of |101⟩



q_0: $|0\rangle + e^{2\pi\, i \cdot 5/8}|1\rangle$

q_1: $|0\rangle + i|1\rangle$

q_2: $|0\rangle - |1\rangle$

out: $\dfrac{(|0\rangle - |1\rangle)(|0\rangle + i|1\rangle)\left(|0\rangle + e^{5\pi\, i/4}|1\rangle\right)}{2\sqrt{2}}$

1 H, then controlled-R_2 ($j_2 = 0$: nothing) and controlled-R_3 ($j_3 = 1$: +⅛): qubit 0 holds 0.101 = ⅝.

2 H on qubit 1 ($j_2 = 0$), then controlled-R_2 from qubit 2 (+¼): phase ¼ turn, $|0\rangle + i|1\rangle$.

3 H on qubit 2 ($j_3 = 1$): $|0\rangle - |1\rangle$.

4 SWAP qubits 0 and 2: fractions 0.1, 0.01, 0.101 in the order of the product form.

Cost: Θ(n²) gates against Θ(N log N)

n Hadamards + $\frac{n(n-1)}{2}$ controlled $R_k = \frac{n(n+1)}{2}$ gates, plus ⌊n/2⌋ SWAPs.

The FFT on the same $N = 2^n$ numbers needs $\Theta(n \cdot 2^n)$ operations.

Without the SWAPs: the DFT matrix with bit-reversed rows.

The exponential gap does not make a faster spectrum analyser (part five).

n	QFT gates + SWAPs	FFT $n \cdot 2^n$
3	6 + 1	24
10	55 + 5	10 240
30	465 + 15	≈ 3.2×10^{10}

SIMULATION

Simulation 6.1: the circuit equals the DFT matrix

```
for j in range(n):
    qc.h(j)
    for k in range(j + 1, n):
        qc.cp(2 * np.pi / 2 ** (k - j + 1), k, j)
for i in range(n // 2 if swaps else 0):
    qc.swap(i, n - 1 - i)
r.append(QFTGate(n), list(range(n))[::-1])
```

Hand-built circuit in textbook order: H, controlled phases, SWAPs.

QFTGate is LSB-first: apply it to the reversed qubits.

n	circuit	QFTGate	reversed
2	True	False	True
3	True	False	True
4	True	False	True

equal to the DFT matrix in textbook order

ifft · √N = QFT: `True`
fft / √N = QFT: `False`

YOUR TURN · VOTE

Quick vote: why no exponentially faster FFT?

Vote · 45 seconds

The QFT needs $\Theta(n^2)$ gates; the FFT of $N = 2^n$ recorded samples needs $\Theta(n \cdot 2^n)$. Why does the QFT not give an exponentially faster way to compute the FFT of recorded data?

A It does: $\Theta(n^2)$ gates for any data set

B Quantum gates are slower, which cancels the gain

C Only noise prevents it; an error-free device would deliver it

D Loading the samples and reading out the spectrum cost too much

4 Kickback from an eigenvector

What does a controlled-U do when its target is an eigenvector?

DERIVATION

Controlled-U on an eigenvector

$$U|u\rangle = e^{2\pi i\varphi}|u\rangle, \qquad 0 \le \varphi < 1$$

eigenphase φ, measured in turns

$$\mathrm{C}(U)\frac{|0\rangle + |1\rangle}{\sqrt{2}}|u\rangle = \frac{|0\rangle|u\rangle + |1\rangle e^{2\pi i\varphi}|u\rangle}{\sqrt{2}}$$

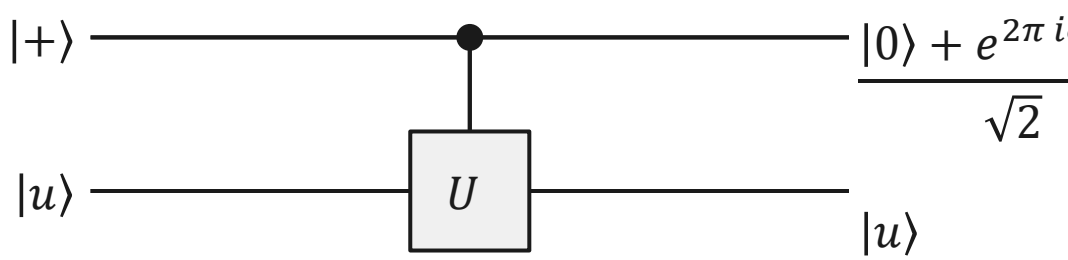
U acts only in the $|1\rangle$ branch

$$= \frac{|0\rangle + e^{2\pi i\varphi}|1\rangle}{\sqrt{2}}|u\rangle$$

factor out $|u\rangle$

The target is unchanged; the eigenvalue becomes a relative phase on the control.

From one kickback to many bits



One kickback writes φ onto one qubit: at most one bit, and only with a probability.

Powers U^{2^m} kick back $2^m\varphi$: the binary digits of φ, shifted.

Those are QFT-like phases: an inverse QFT reads them out (next week).

Phase estimation (Lecture 13)

$$t \text{ controls}, U, U^2, U^4, \ldots$$

$$\rightarrow \text{QFT}^\dagger \rightarrow t \text{ bits\ of } \varphi$$

Recap

1

The QFT

$\sqrt{N}$ × inverse DFT on the amplitudes; unitary; $\mathrm{QFT}_2 = H$

2

Product form

qubit l − 1 holds the fraction $0.j_{n-l+1} \ldots j_n$; periods become peaks

3

Circuit

H and controlled-R_k, then SWAPs: n(n+1)/2 gates; QFTGate on reversed qubits

4

Limits and kickback

loading and reading out are expensive; C(U) kicks the eigenphase back

Next week: Lecture 13

Phase estimation: reading an eigenphase to t bits

Read: handout 6.1–6.3 and 6.4 (phase estimation) before next week.

Exit ticket

Write $\mathrm{QFT}|110\rangle$ (n = 3) as a product of three one-qubit states, using the binary fractions.

Copyright © 2026 Sajid Muhaimin Choudhury. All rights reserved.

Rights and attributions

Copyright (c) 2026 Sajid Muhaimin Choudhury. All rights reserved.

Public edition of Lecture 12: The Quantum Fourier Transform. Release qc-2026-10-15, prepared 2026-10-15 from source revision 3df9449aa6.

This edition omits speaker notes, instructor-only material and every figure whose publication rights are not cleared for public distribution.