A log-depth in-place quantum Fourier transform that rarely needs ancillas

[arXiv:2505.00701]

Greg Kahanamoku-Meyer [1] John Blue [1] Thiago Bergamaschi [2] Craig Gidney [3] Isaac Chuang [1]

[1]MIT [2]Berkeley [3]Google

January 28, 2026

Outline

Structure of the quantum Fourier transform

Outline

Structure of the quantum Fourier transform

Building a log-depth QFT with no ancillas

Outline

Structure of the quantum Fourier transform

Building a log-depth QFT with no ancillas

Why it's wrong

Outline

Structure of the quantum Fourier transform

Building a log-depth QFT with no ancillas

Why it's wrong

Why it's OK to be wrong sometimes

Outline

Structure of the quantum Fourier transform

Building a log-depth QFT with no ancillas

Why it's wrong

Why it's OK to be wrong sometimes

How to make it correct, if you really care about that (boo!)

Outline

Structure of the quantum Fourier transform

Building a log-depth QFT with no ancillas

Why it's wrong

Why it's OK to be wrong sometimes

How to make it correct, if you really care about that (boo!)

Structure of the quantum Fourier transform

Classic definition of QFT on n qubits:

$$|\Phi_x\rangle \equiv \mathrm{QFT}_{2^n} |x\rangle = \sum_{z=0}^{2^n-1} e^{2\pi i x z / 2^n} |z\rangle$$

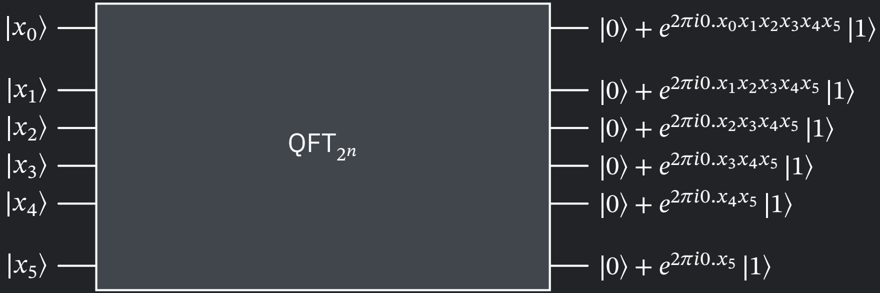
Structure of the quantum Fourier transform

Classic definition of QFT on n qubits:

$$|\Phi_x\rangle \equiv \mathrm{QFT}_{2^n} |x\rangle = \bigotimes_{j=0}^{n-1} \left(|0\rangle + e^{2\pi i 0.x_j x_{j+1} \ldots x_{n-1}} |1\rangle\right)$$

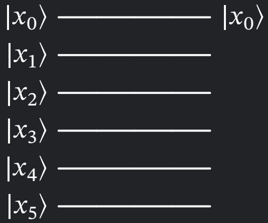
where $0.x_j x_{j+1} \cdots = 2^j x / 2^n \bmod 1$ is a binary fraction consisting of the bits of x.

Structure of the QFT



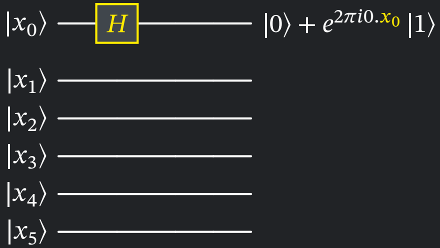
The quantum Fourier transform

Example: QFT_{2^6}



The quantum Fourier transform

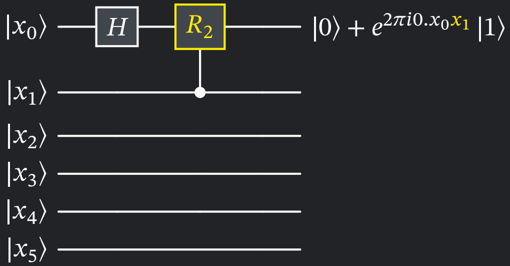
Example: QFT_{2^6}



The quantum Fourier transform

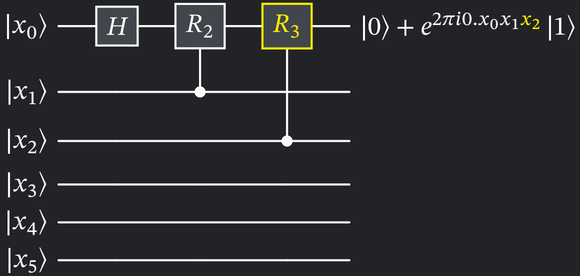
Example: QFT_{2^6}

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



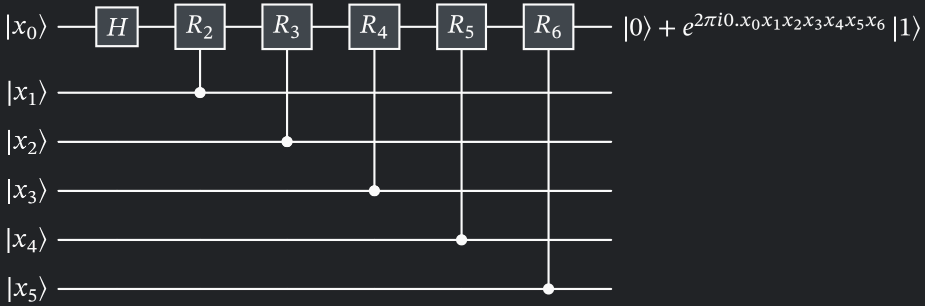
Example: QFT_{2^6}

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



Example: QFT_{2^6}

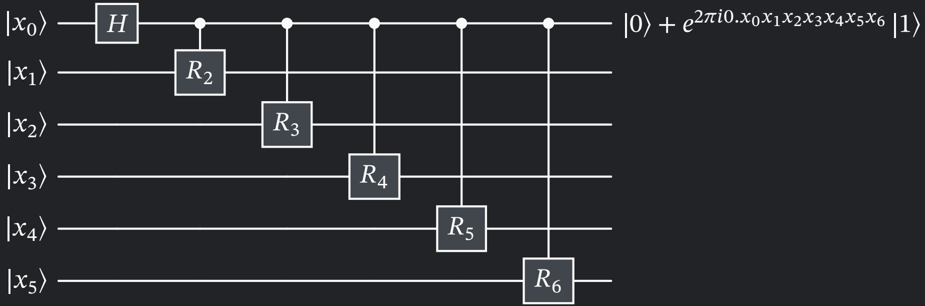
$$R_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{pmatrix}$$



The quantum Fourier transform

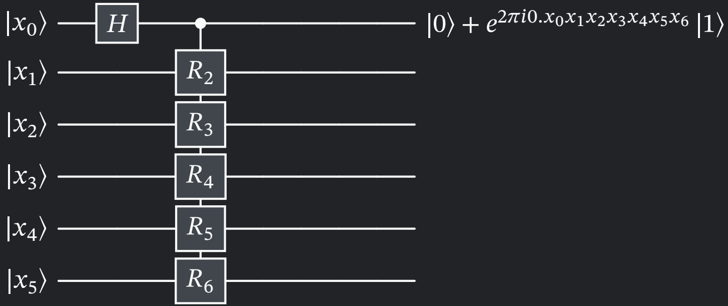
Example: QFT_{2^6}

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



The quantum Fourier transform

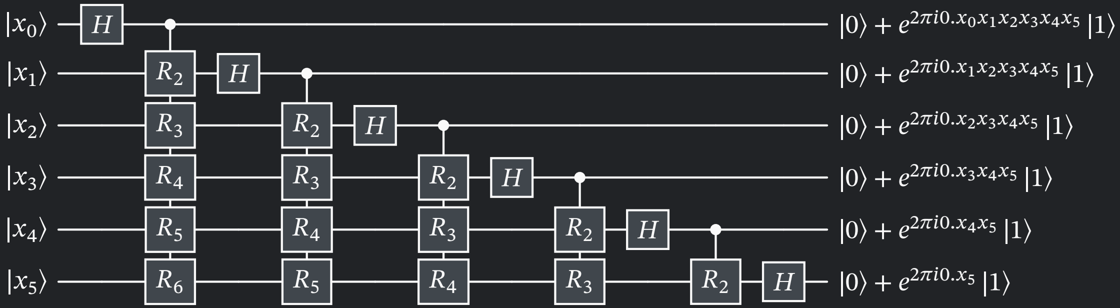
Example: QFT_{2^6} $\qquad R_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{pmatrix}$



The quantum Fourier transform

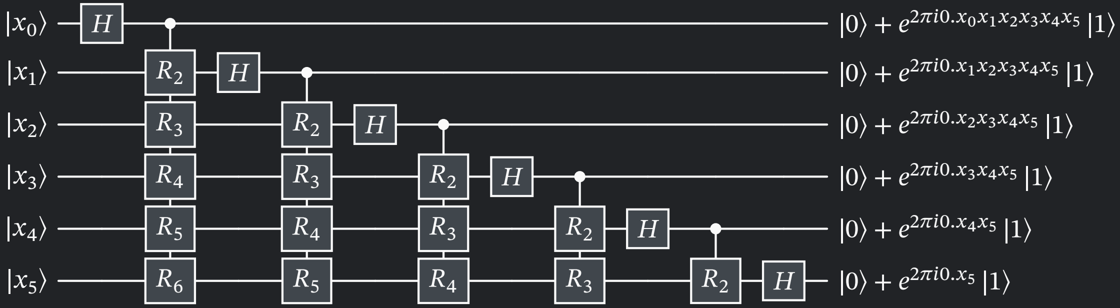
Example: QFT_{2^6}

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



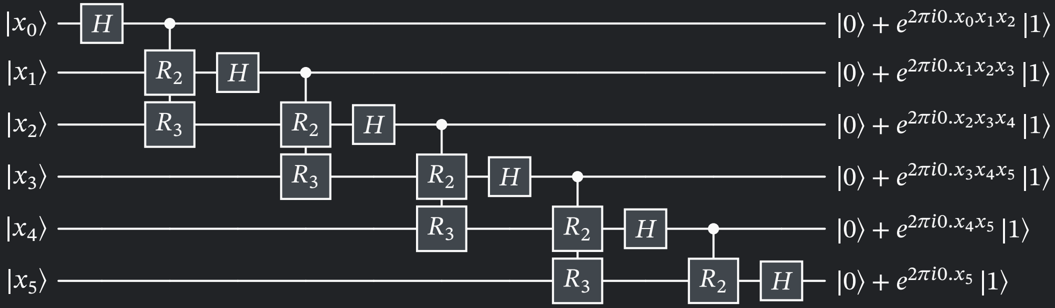
The quantum Fourier transform

Approximate QFT: truncate $0.x_j x_{j+1} \ldots$ after $m = O(\log(n/\epsilon))$ bits.



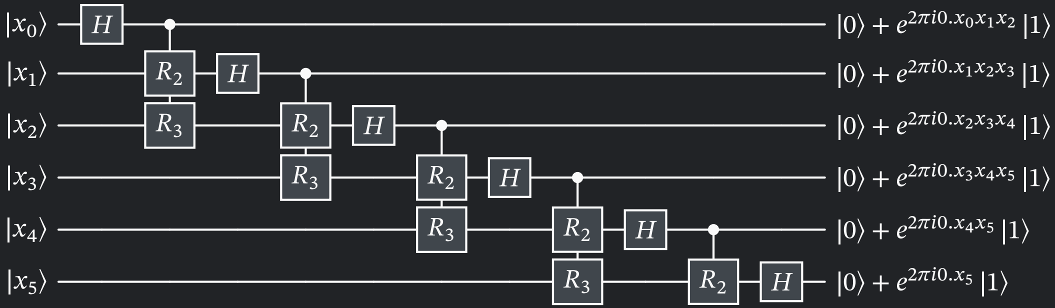
The quantum Fourier transform

Approximate QFT: truncate $0.x_j x_{j+1} \ldots$ after $m = O(\log(n/\epsilon))$ bits.



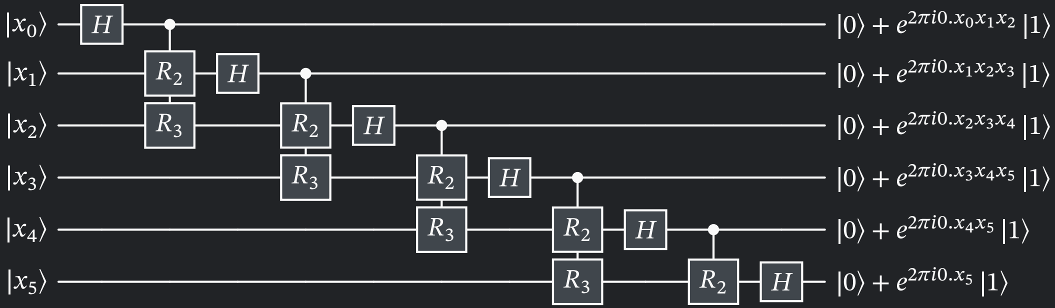
The quantum Fourier transform

😃 **Gate count:** $O(n \log n)$



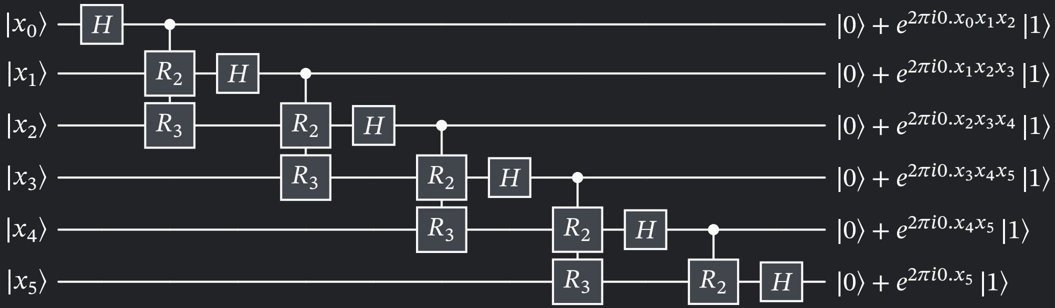
The quantum Fourier transform

😃 **Gate count:** $O(n \log n)$ 😃 **Ancillas:** 0



The quantum Fourier transform

😃 **Gate count:** $O(n \log n)$ 😃 **Ancillas:** 0 😢 **Circuit depth:** $O(n)$



How did I come to care about depth of the QFT?

How did I come to care about depth of the QFT?

How did I come to care about depth of the QFT?

GKM, Yao [arXiv:2403.18006]: **PhaseProduct** with...

- **Depth:** $O(n^\epsilon)$
- **Ancillas:** $O(n^{1-\epsilon})$

for any $0 < \epsilon \leq 1$

How did I come to care about depth of the QFT?

GKM, Yao [arXiv:2403.18006]: **PhaseProduct** with...

- **Depth:** $O(n^{\epsilon})$
- **Ancillas:** $O(n^{1-\epsilon})$

for any $0 < \epsilon \leq 1$

"Surely the QFT isn't the bottleneck" -me, 2023

Some existing (approximate) QFT constructions

Coppersmith '94

😢 Depth: $O(n)$

😃 Ancillas: 0

Some existing (approximate) QFT constructions

Coppersmith '94

😢 **Depth:** $O(n)$

😃 **Ancillas:** 0

Cleve + Watrous '00
(and follow-up works)

😃 **Depth:** $O(\log n)$

😢 **Ancillas:** $\widetilde{O}(n)$

Some existing (approximate) QFT constructions

Coppersmith '94

😢 **Depth:** $O(n)$

😃 **Ancillas:** 0

Cleve + Watrous '00
(and follow-up works)

😃 **Depth:** $O(\log n)$

😢 **Ancillas:** $\widetilde{O}(n)$

🤯 No construction with sublinear depth **and** sublinear ancilla count!

Outline

Structure of the quantum Fourier transform

Building a log-depth QFT with no ancillas

Why it’s wrong

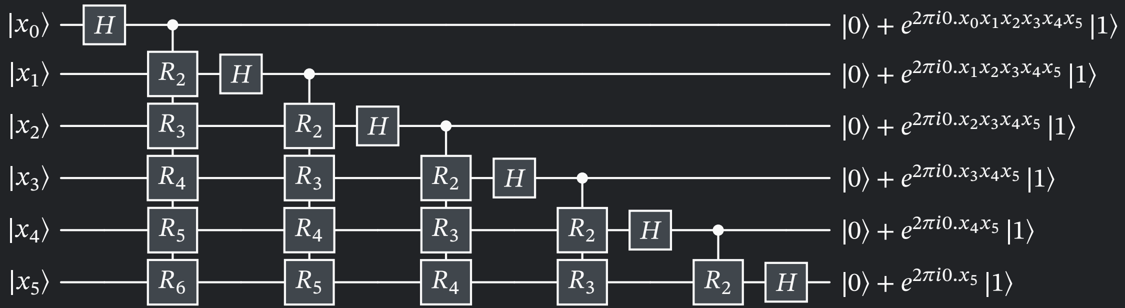
Why it’s OK to be wrong sometimes

How to make it correct, if you really care about that (boo!)

The block QFT

Example: QFT_{2^6}

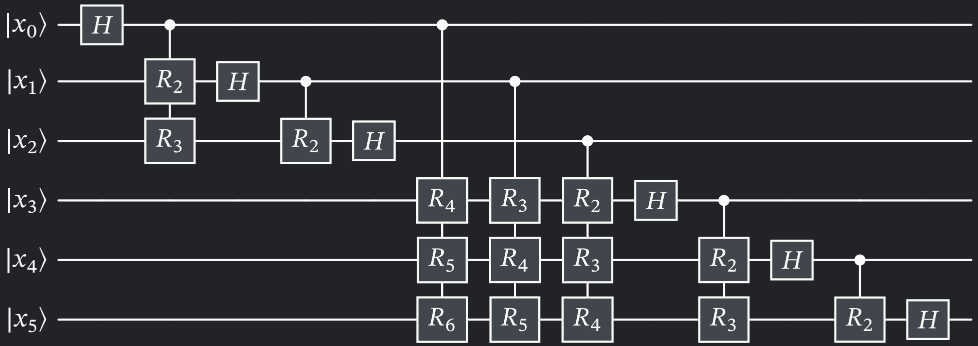
$$R_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{pmatrix}$$



The block QFT

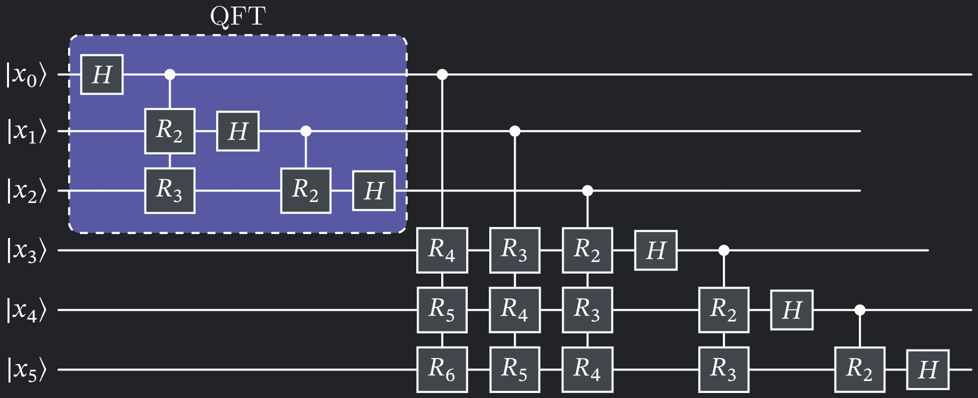
Example: QFT_{2^6}

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



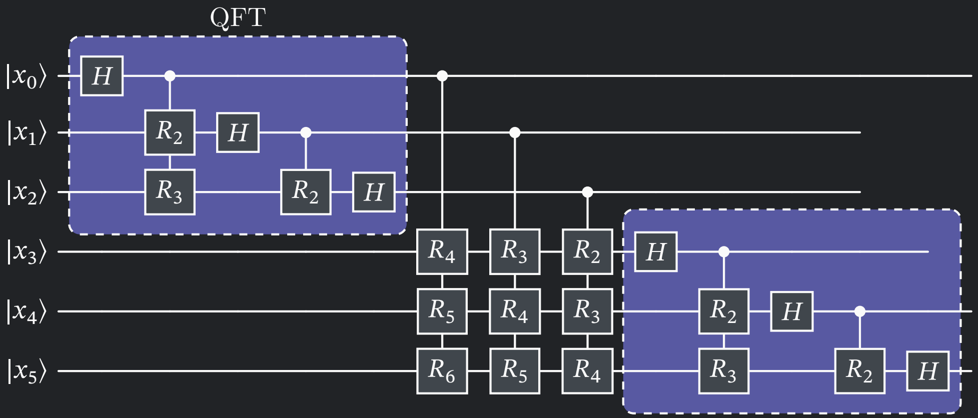
The block QFT

Example: QFT_{2^6} $\qquad R_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{pmatrix}$



The block QFT

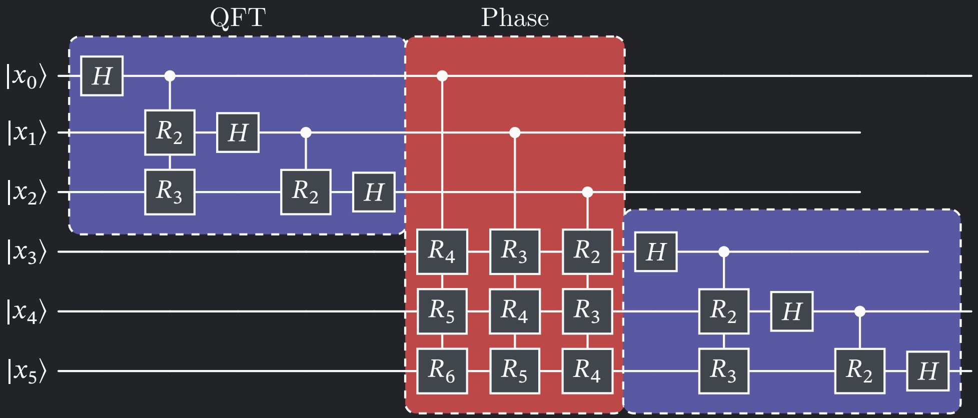
Example: QFT_{2^6} $\quad R_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{pmatrix}$



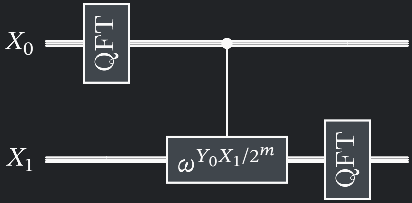
The block QFT

Example: QFT_{2^6}

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

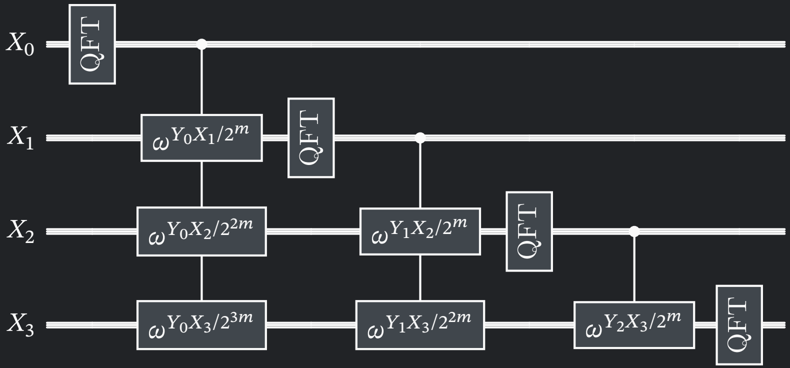


The block QFT



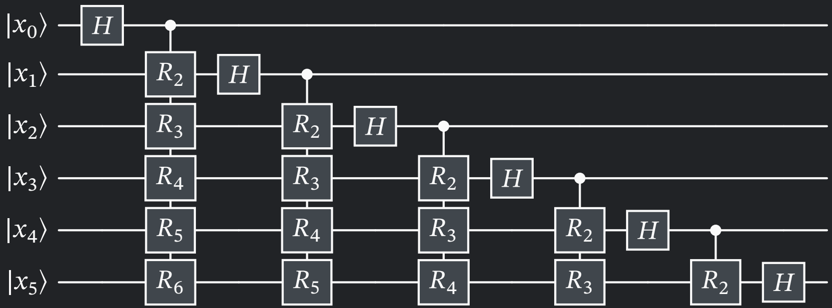
$$\omega = e^{2\pi i / 2^m}$$

The block QFT (exact!)

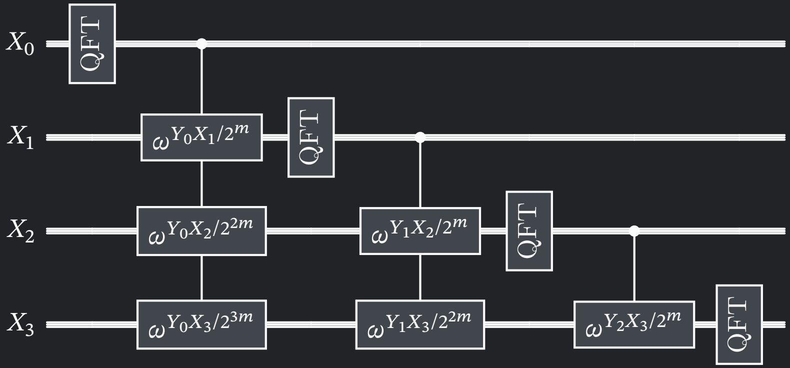


$$\omega = e^{2\pi i/2^m}$$

The regular QFT



The block QFT



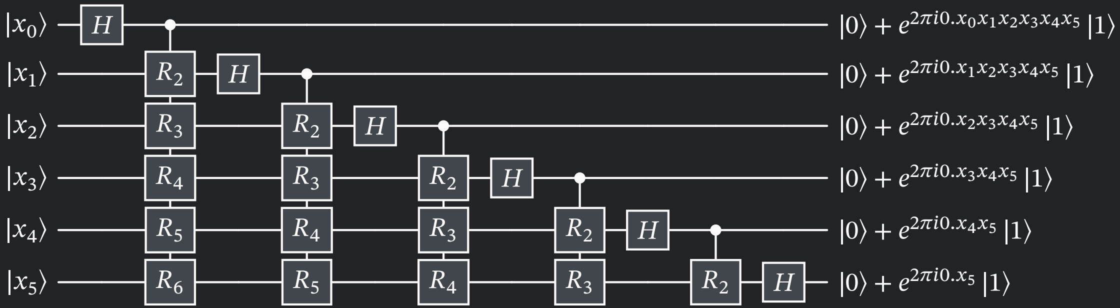
$$\omega = e^{2\pi i/2^m}$$

Same structure as non-block QFT!

The quantum Fourier transform

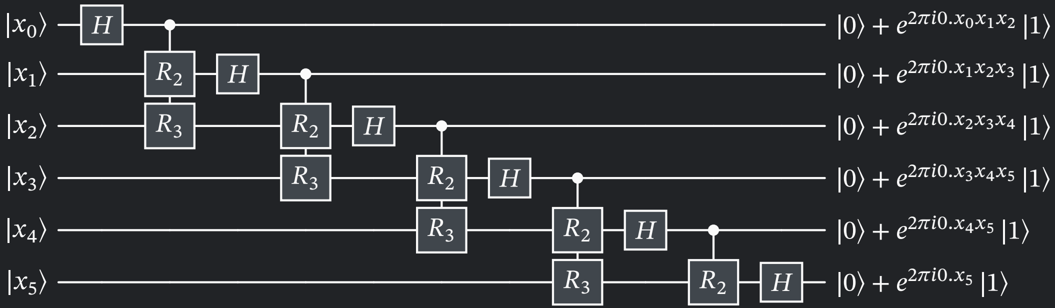
Example: QFT_{2^6}

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

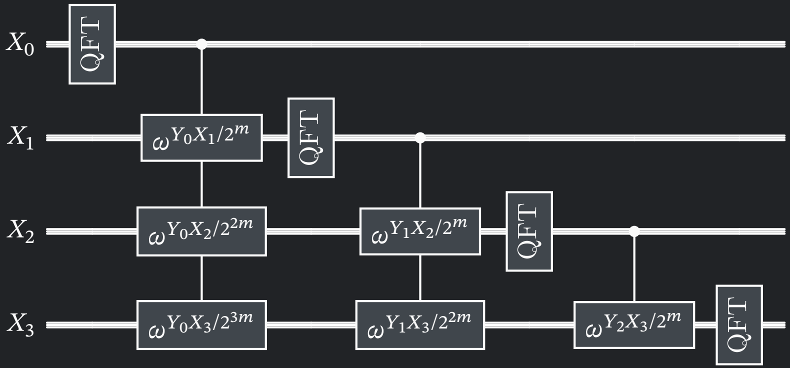


Example: approximate QFT_{2^6}

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

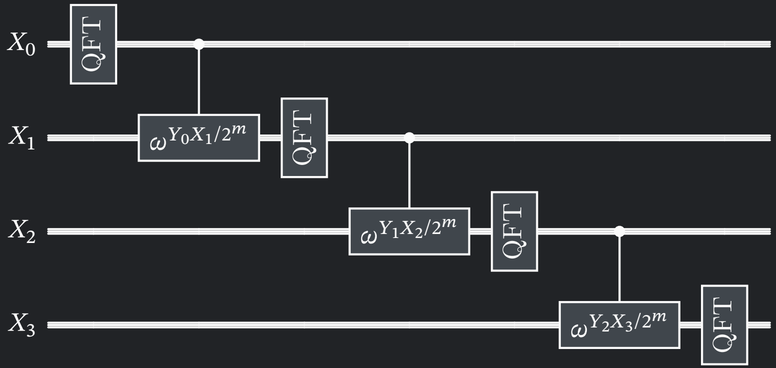


The block QFT



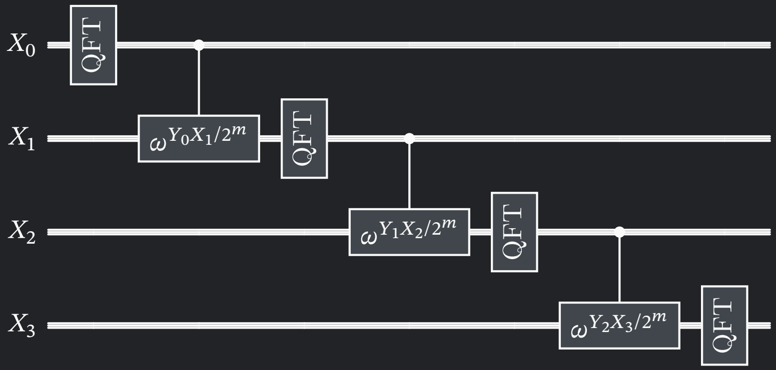
$$\omega = e^{2\pi i/2^m}$$

The approximate block QFT



$$\omega = e^{2\pi i / 2^m}$$

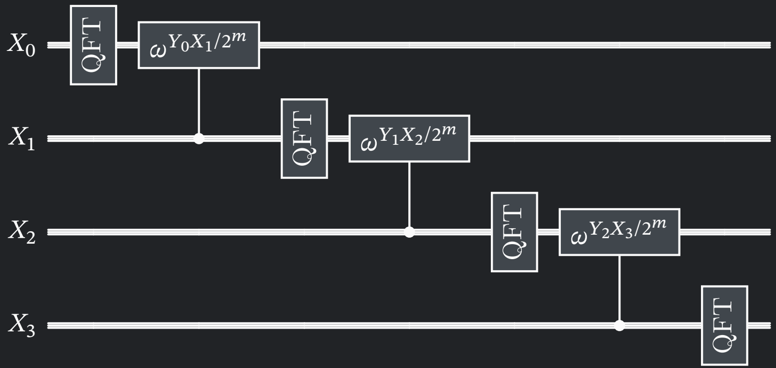
The approximate block QFT



$\omega = e^{2\pi i/2^m}$

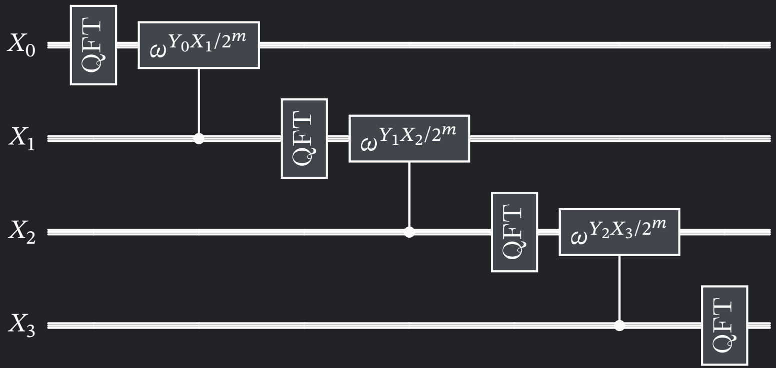
Approximation controlled by block size $m = O(\log(n/\varepsilon))$

The approximate block QFT



$$\omega = e^{2\pi i/2^m}$$

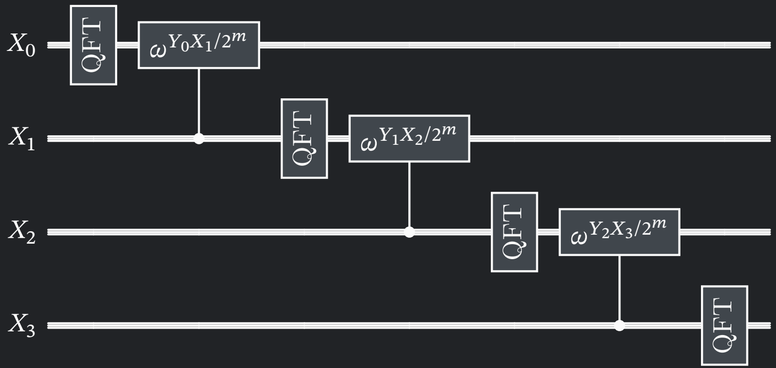
The approximate block QFT



$\omega = e^{2\pi i/2^m}$

Why linear depth?

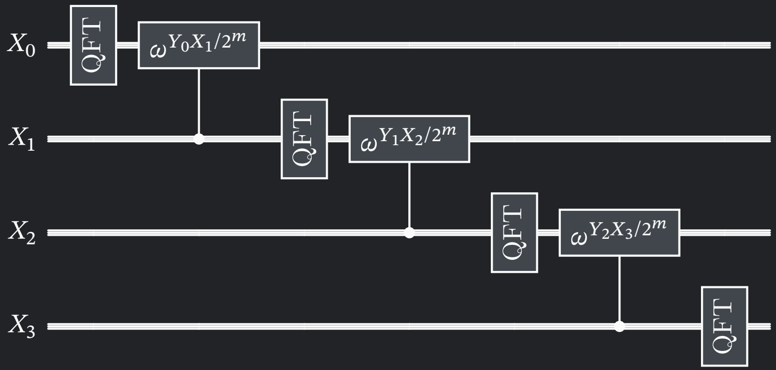
The approximate block QFT



$$\omega = e^{2\pi i/2^m}$$

Why linear depth? Need $|X_i\rangle$ for block $i-1$.

The approximate block QFT

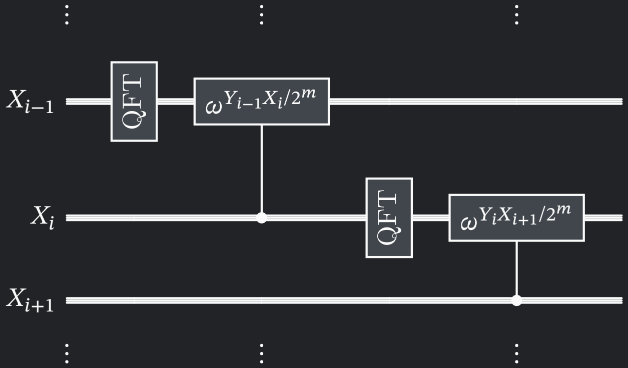


$\omega = e^{2\pi i / 2^m}$

Why linear depth? Need $|X_i\rangle$ for block $i-1$. … or can we somehow recover $|X_i\rangle$?

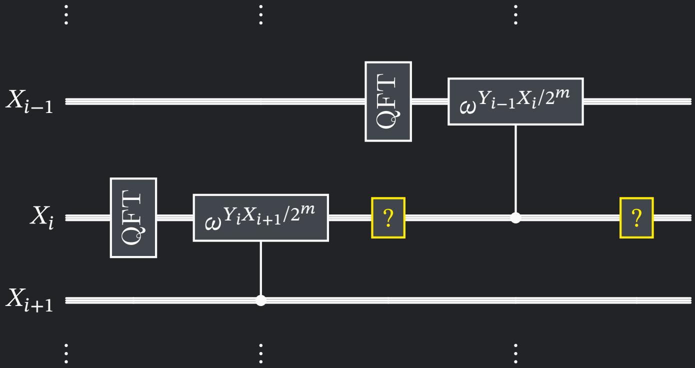
Lowering the depth

Can we somehow recover $|X_i\rangle$?



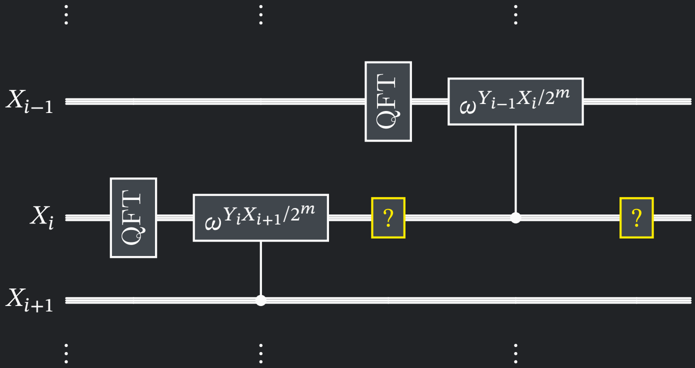
Lowering the depth

Can we somehow recover $|X_i\rangle$?



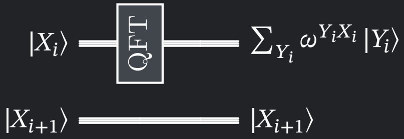
Lowering the depth

Can we somehow approximately recover $|X_i\rangle$?



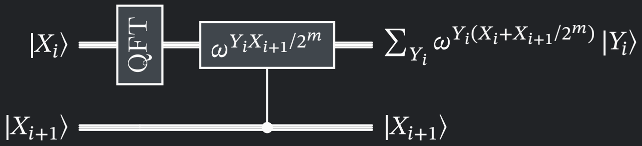
Lowering the depth

Can we somehow approximately recover $|X_i\rangle$?



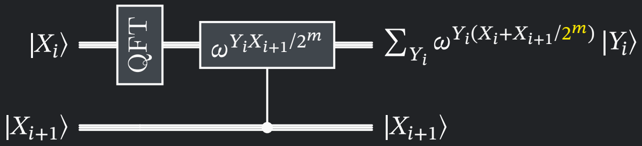
Lowering the depth

Can we somehow approximately recover $|X_i\rangle$?



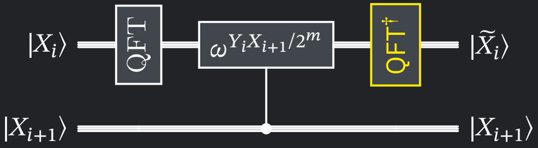
Lowering the depth

Can we somehow approximately recover $|X_i\rangle$?



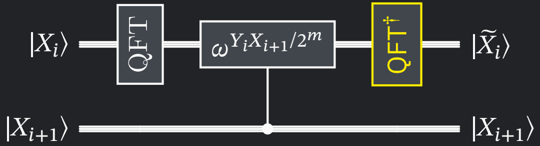
Lowering the depth

Can we somehow approximately recover $|X_i\rangle$?

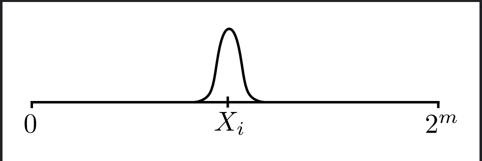


Lowering the depth

Can we somehow approximately recover $|X_i\rangle$?

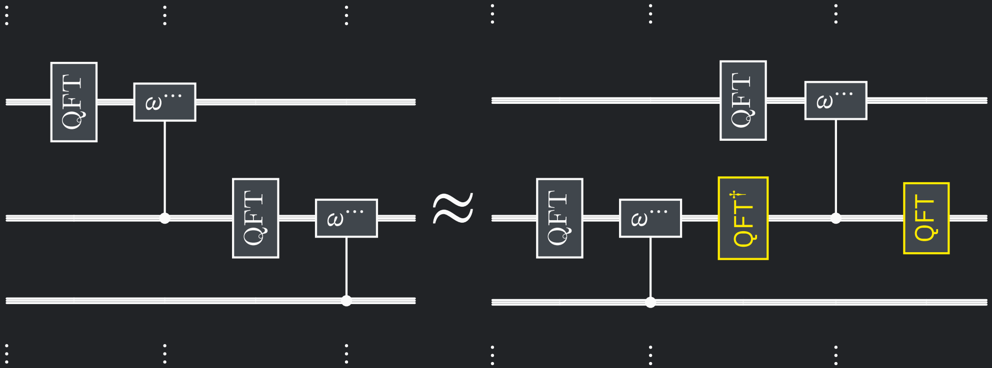


From **quantum phase estimation:**

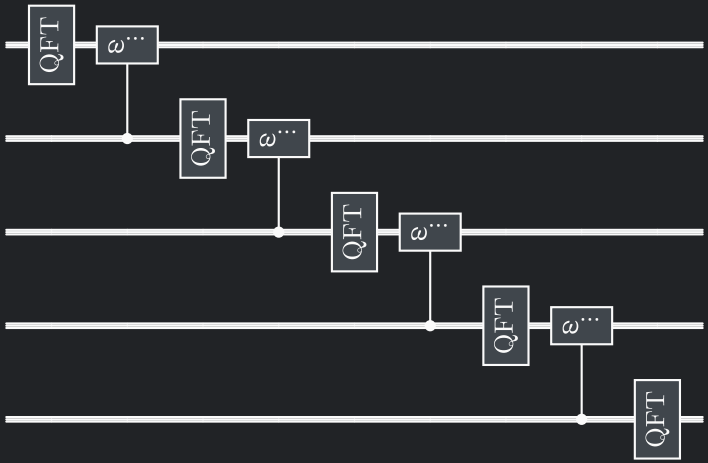


Lowering the depth

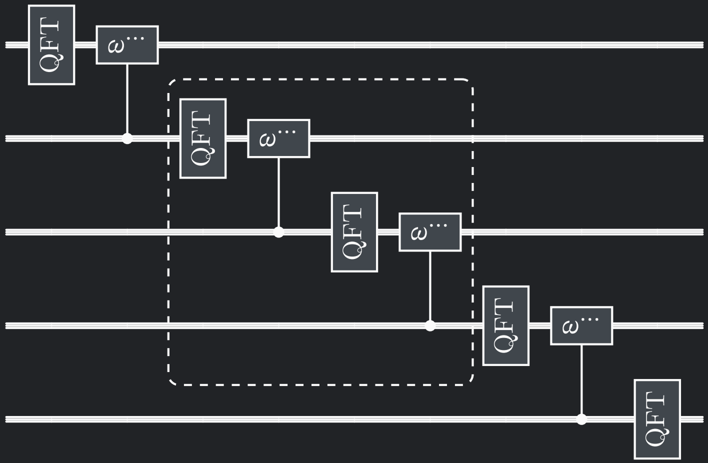
Claim:



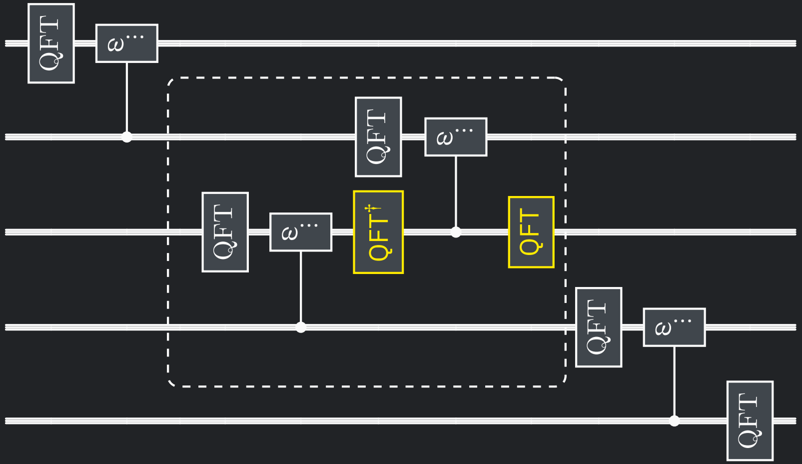
Rearranging gates…



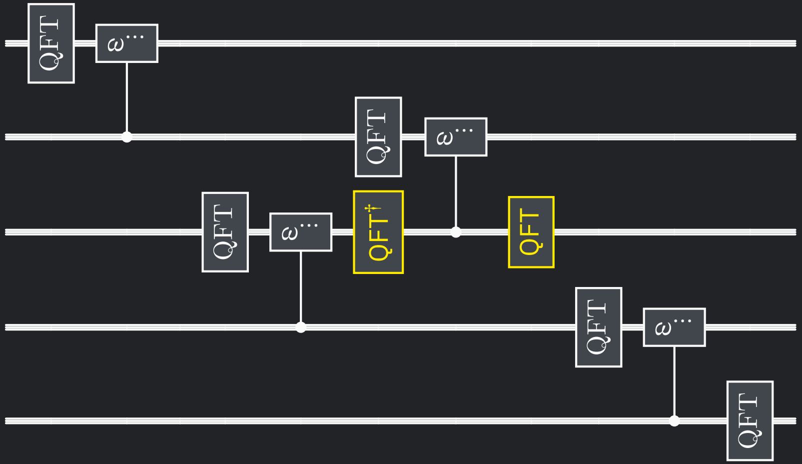
Rearranging gates...



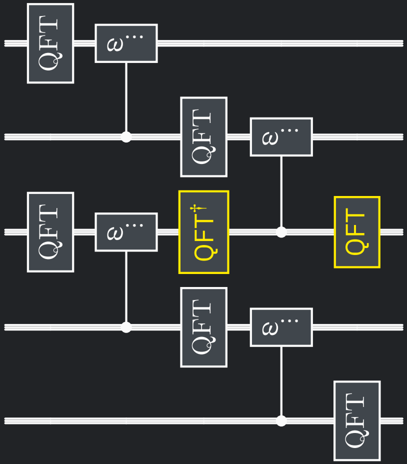
Rearranging gates...



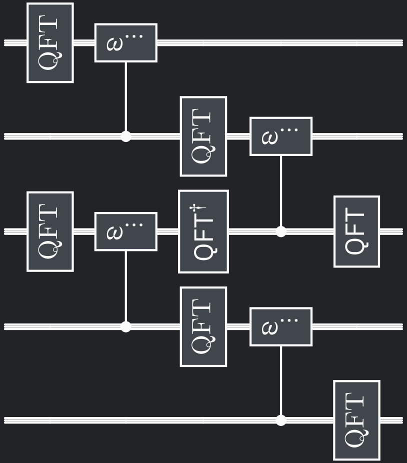
Rearranging gates...



Rearranging gates...

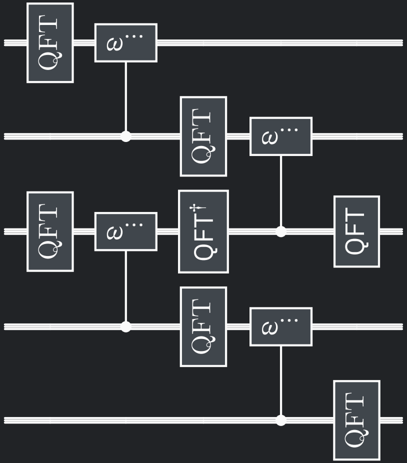


The low-depth block QFT



"If someone told me this approximates the QFT, I would probably believe them"
- Craig Gidney

The low-depth block QFT

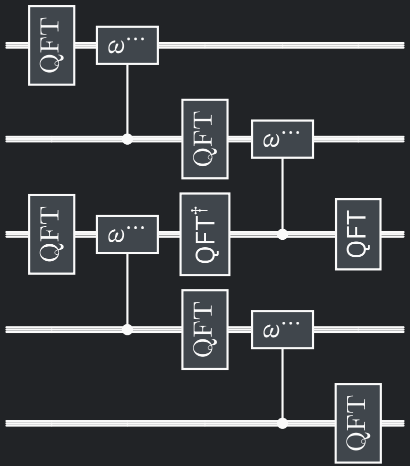


"If someone told me this approximates the QFT, I would probably believe them"
- Craig Gidney

Features:

- Depth $O(\log n/\epsilon)$

The low-depth block QFT

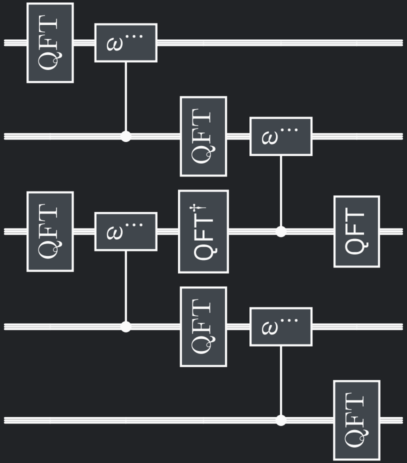


"If someone told me this approximates the QFT, I would probably believe them"
- Craig Gidney

Features:

- Depth $O(\log n/\epsilon)$
- No ancilla qubits

The low-depth block QFT

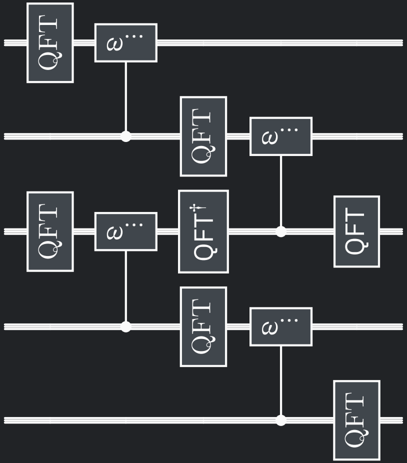


"If someone told me this approximates the QFT, I would probably believe them"
- Craig Gidney

Features:

- Depth $O(\log n/\epsilon)$
- No ancilla qubits
- Can be made *nearest-neighbor* local

The low-depth block QFT



"If someone told me this approximates the QFT, I would probably believe them"
- Craig Gidney

Features:

- Depth $O(\log n/\epsilon)$
- No ancilla qubits
- Can be made *nearest-neighbor* local
- Incorrect

Outline

Structure of the quantum Fourier transform

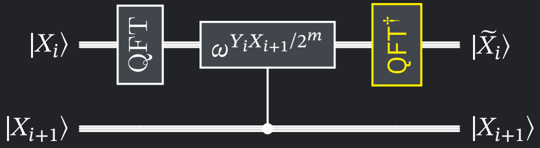
Building a log-depth QFT with no ancillas

Why it's wrong

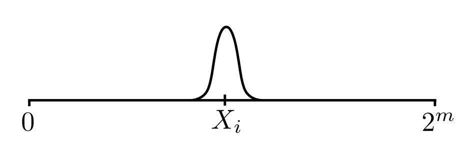
Why it's OK to be wrong sometimes

How to make it correct, if you really care about that (boo!)

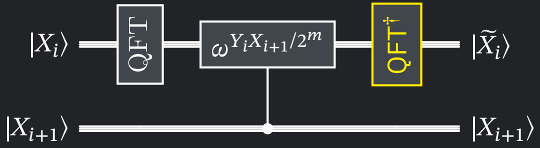
What went wrong?



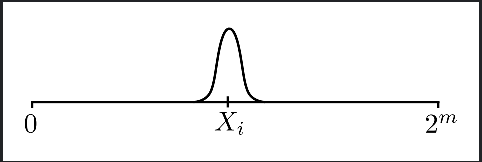
From **quantum phase estimation:**



What went wrong?

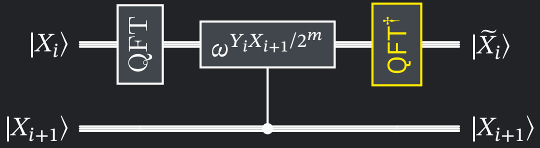


From **quantum phase estimation:**



What if X_i is close to 0 or 2^m?

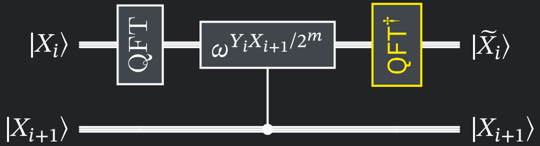
What went wrong?



From **quantum phase estimation:**

What if X_i is close to 0 or 2^m?

What went wrong?



From **quantum phase estimation:**

Phase rotation that follows will be **wildly wrong!**

Outline

Structure of the quantum Fourier transform

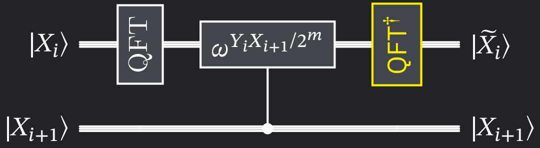
Building a log-depth QFT with no ancillas

Why it's wrong

Why it's OK to be wrong sometimes

How to make it correct, if you really care about that (boo!)

What went wrong?



From **quantum phase estimation:**

"Wraparound" error is negligible for the vast majority of X_i

How to measure error

Typical measures of error (e.g. diamond norm) consider the worst-case input

How to measure error

Typical measures of error (e.g. diamond norm) consider the worst-case input
This doesn't capture circuits that get it **mostly right**!

How to measure error

Typical measures of error (e.g. diamond norm) consider the worst-case input
This doesn't capture circuits that get it **mostly right**!

Definition: Optimistic quantum circuits (intuitive)

C is an **optimistic circuit** with error parameter ϵ for U if $\widetilde{U}$ induced by C has

$$\|(U|\phi\rangle - \widetilde{U}|\phi\rangle\|^2 < \epsilon$$

for **most** input states $|\phi\rangle$.

How to measure error

Typical measures of error (e.g. diamond norm) consider the worst-case input
This doesn't capture circuits that get it **mostly right**!

Definition: Optimistic quantum circuits

C is an **optimistic circuit** with error parameter ϵ for U if $\widetilde{U}$ induced by C has

$$\frac{1}{2^n} \sum_j \|(U - \widetilde{U}) |\phi_j\rangle \|^2 \leq \epsilon$$

for a set of orthonormal basis states $|\phi_j\rangle$.

How to measure error

Typical measures of error (e.g. diamond norm) consider the worst-case input
This doesn't capture circuits that get it **mostly right**!

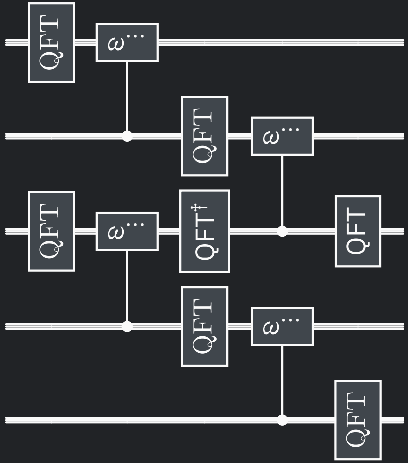
Definition: Optimistic quantum circuits

C is an **optimistic circuit** with error parameter ϵ for U if $\widetilde{U}$ induced by C has

$$\frac{1}{2^n}\sum_j \|(U-\widetilde{U})\,|\phi_j\rangle\,\|^2 \leq \epsilon$$

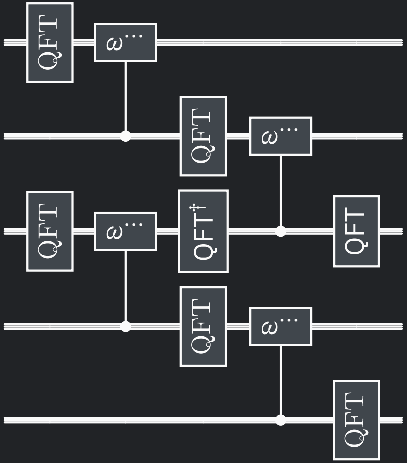
for **any** set of orthonormal basis states $|\phi_j\rangle$.

The low-depth block QFT



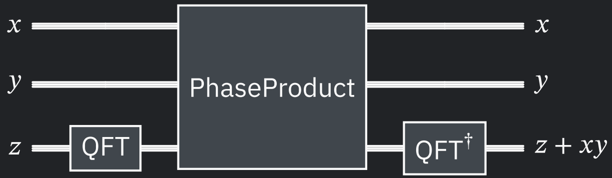
Theorem: this is an optimistic circuit for the quantum Fourier transform.

The low-depth block QFT



Theorem: this is an optimistic circuit for the quantum Fourier transform.

What should we do with it?

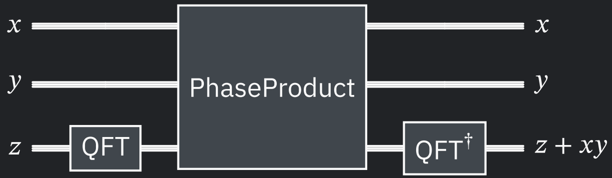


GKM, Yao '24:
PhaseProduct with...

- **Depth:** $O(n^{\epsilon})$
- **Ancillas:** $O(n^{1-\epsilon})$

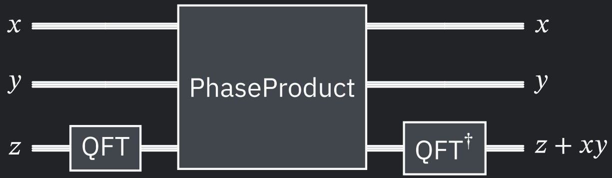
for any $0 < \epsilon \leq 1$

Using the optimistic QFT



Optimistic QFT + GKM, Yao '24:
Optimistic multiplier

Using the optimistic QFT

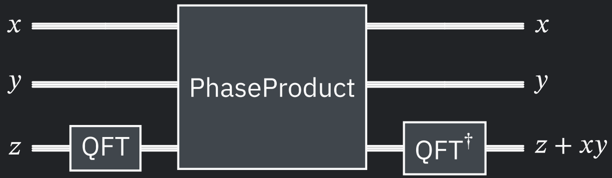


Optimistic QFT + GKM, Yao '24:
Optimistic multiplier with...

- **Depth:** $O(n^{\epsilon})$
- **Ancillas:** $O(n^{1-\epsilon})$

for any $0 < \epsilon \leq 1$

Using the optimistic QFT



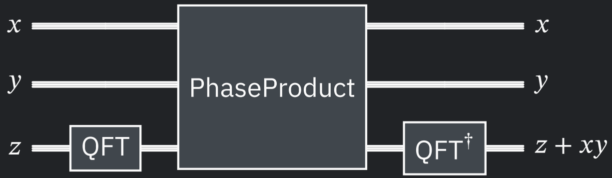
Optimistic QFT + GKM, Yao '24:
Optimistic multiplier with...

- **Depth:** $O(n^{\epsilon})$
- **Ancillas:** $O(n^{1-\epsilon})$

for any $0 < \epsilon \leq 1$

Theorem: using optimistic mult., Shor's algorithm still succeeds

Using the optimistic QFT



Optimistic QFT + GKM, Yao '24:
Optimistic multiplier with...

- **Depth:** $O(n^{\epsilon})$
- **Ancillas:** $O(n^{1-\epsilon})$

for any $0 < \epsilon \leq 1$

Theorem: using optimistic mult., Shor's algorithm still succeeds

Consequence: factoring in depth $O(n^{1+\epsilon})$ using $2n + O(n^{1-\epsilon})$ qubits

Want more factoring?

Come to the **factoring power hour** tomorrow (Thursday) at **Algorithms 6**!

Want more factoring?

Come to the **factoring power hour** tomorrow (Thursday) at **Algorithms 6**!

- 13:30-14:00 — GKM, **S. Ragavan**, V. Vaikuntanathan, **K. Van Kirk**,
  The Jacobi Factoring Circuit: Quantum Factoring in Sublinear Space and Depth

Want more factoring?

Come to the **factoring power hour** tomorrow (Thursday) at **Algorithms 6**!

- 13:30-14:00 — GKM, **S. Ragavan**, V. Vaikuntanathan, **K. Van Kirk**, *The Jacobi Factoring Circuit: Quantum Factoring in Sublinear Space and Depth*
- 14:00-14:30 — **GKM**, S. Ragavan, **K. Van Kirk**, *Parallel Spooky Pebbling Makes Regev Factoring More Practical*

Outline

Structure of the quantum Fourier transform

Building a log-depth QFT with no ancillas

Why it's wrong

Why it's OK to be wrong sometimes

How to make it correct, if you really care about that (boo!)

Worst to average case reduction

Optimistic circuits have small error on the vast majority of inputs $|\phi\rangle$.

Worst to average case reduction

Optimistic circuits have small error on the vast majority of inputs $|\phi\rangle$.

Let's **randomize** $|\phi\rangle$ before applying $\widetilde{U}$!

Worst to average case reduction

Optimistic circuits have small error on the vast majority of inputs $|\phi\rangle$.

Let's **randomize** $|\phi\rangle$ before applying $\widetilde{U}$!

Classical

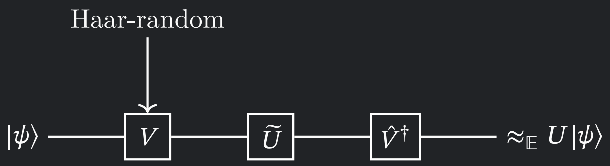
- Monte Carlo Integration
- Primality Testing
- Stochastic Gradient Descent
- And more ...

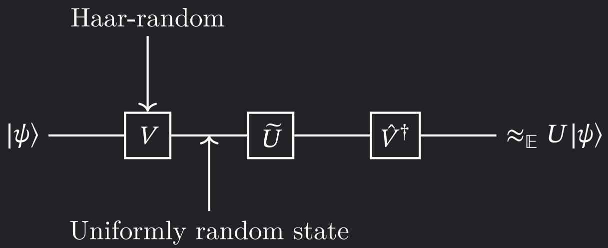
Quantum

- Gate synthesis
  - (Bocharov et al, 2014) [arXiv:1409.3552]
  - (Campbell, 2017) [arXiv:1612.02689]
- Hamiltonian Simulation
  - (Campbell, 2019) [arXiv:1811.08017]
  - (Nakaji et al, 2024) [arXiv:2302.14811]
- Quantum Signal Processing
  - (Martyn and Campbell, 2025) [arXiv:2409.03744]

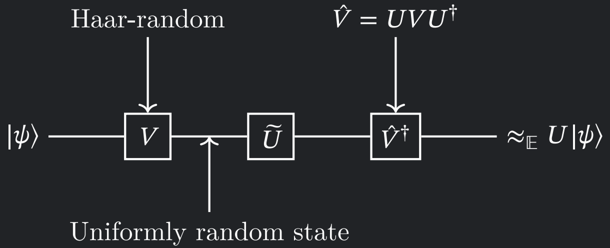
Randomizing the input

Randomizing the input

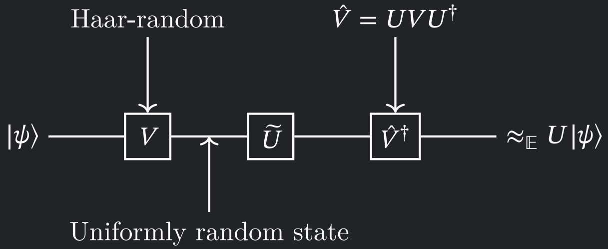



Haar-random
$|\psi\rangle$
V
$\widetilde{U}$
$\hat{V}^\dagger$
$\approx_{\mathbb{E}} U|\psi\rangle$
Uniformly random state

Randomizing the input



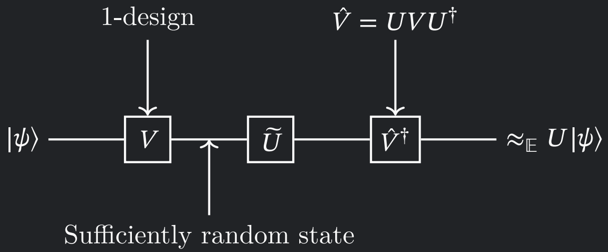
Randomizing the input



Problems:

- Haar-random unitaries are not feasible!

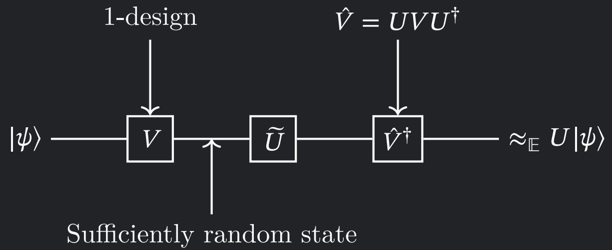
Randomizing the input



Problems:

- Haar-random unitaries are not feasible! $\Rightarrow$ only need a **1-design**!

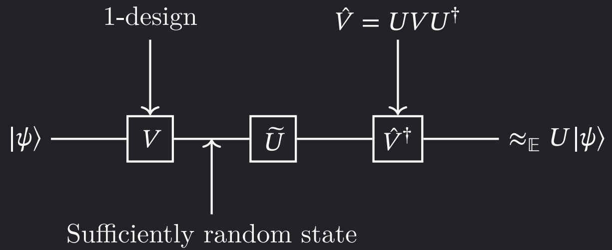
Randomizing the input



Problems:

- Haar-random unitaries are not feasible! ⇒ only need a **1-design**!
- Is $\hat{V}^\dagger$ going to be terrible?

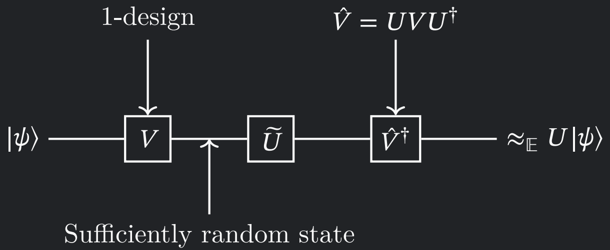
Randomizing the input



Problems:

- Haar-random unitaries are not feasible! $\Rightarrow$ only need a **1-design**!
- Is $\hat{V}^\dagger$ going to be terrible? $\Rightarrow$ not if we pick V carefully!

Randomizing the input



Problems:

- Haar-random unitaries are not feasible! $\Rightarrow$ only need a **1-design**!
- Is $\hat{V}^\dagger$ going to be terrible? $\Rightarrow$ not if we pick V carefully!

For **QFT:** exist V and $\hat{V}^\dagger$ with depth $O(\log n)$ using $O(n/\log n)$ ancillas!

Some previous approximate QFT constructions

Coppersmith '94

😢 **Depth:** $O(n)$

😃 **Ancillas:** 0

Cleve + Watrous '00
(and follow-up works)

😃 **Depth:** $O(\log n)$

😢 **Ancillas:** $\widetilde{O}(n)$

Our results

Optimistic QFT

Our results

Optimistic QFT

😃 **Depth:** $O(\log n)$

Our results

Optimistic QFT

😃 **Depth:** $O(\log n)$

🥳 **Ancillas:** 0

Our results

Optimistic QFT

😃 **Depth:** $O(\log n)$

🥳 **Ancillas:** 0

👫 **Locality:** nearest-neighbor

Our results

Optimistic QFT

😃 **Depth:** $O(\log n)$

🥳 **Ancillas:** 0

🧑‍🤝‍🧑 **Locality:** nearest-neighbor

🤷🏻‍♀️ **Error:** ϵ on most inputs

Our results

Optimistic QFT

😃 **Depth:** $O(\log n)$

🥳 **Ancillas:** 0

🧑‍🤝‍🧑 **Locality:** nearest-neighbor

🤷🏻‍♀️ **Error:** ϵ on most inputs

With randomized reduction

Our results

Optimistic QFT

😃 **Depth:** $O(\log n)$

🥳 **Ancillas:** 0

🧑‍🤝‍🧑 **Locality:** nearest-neighbor

🤷🏻‍♀️ **Error:** ϵ on most inputs

With randomized reduction

😃 **Depth:** $O(\log n)$

Our results

Optimistic QFT

😃 **Depth:** $O(\log n)$

🥳 **Ancillas:** 0

🧑‍🤝‍🧑 **Locality:** nearest-neighbor

🤷 **Error:** ϵ on most inputs

With randomized reduction

😃 **Depth:** $O(\log n)$

😄 **Ancillas:** $O(n/\log n)$

Our results

Optimistic QFT

😃 **Depth:** $O(\log n)$

🥳 **Ancillas:** 0

🧑‍🤝‍🧑 **Locality:** nearest-neighbor

🤷🏻‍♀️ **Error:** ϵ on most inputs

With randomized reduction

😃 **Depth:** $O(\log n)$

😄 **Ancillas:** $O(n/\log n)$

🧑‍🤝‍🧑 **Locality:** all-to-all

Our results

Optimistic QFT

😃 **Depth:** $O(\log n)$

🥳 **Ancillas:** 0

👫 **Locality:** nearest-neighbor

🤷🏻‍♀️ **Error:** ϵ on most inputs

With randomized reduction

😃 **Depth:** $O(\log n)$

😄 **Ancillas:** $O(n/\log n)$

👫 **Locality:** all-to-all

🤩 **Error:** $\leq \epsilon$ on **all** inputs

Our results

Optimistic QFT

😃 **Depth:** $O(\log n)$

🥳 **Ancillas:** 0

🧑‍🤝‍🧑 **Locality:** nearest-neighbor

🤷🏻‍♀️ **Error:** ϵ on most inputs

With randomized reduction

😃 **Depth:** $O(\log n)$

😄 **Ancillas:** $O(n/\log n)$

🧑‍🤝‍🧑 **Locality:** all-to-all*

🤩 **Error:** $\leq \epsilon$ on **all** inputs

*Bäumer et al. [2504.20832]: using **measurement** + **feed-forward** and $O(n)$ ancillas, can achieve nearest-neighbor connectivity

Thank you!

Greg Kahanamoku-Meyer
gkm@mit.edu

Collaborators:

John Blue

Thiago Bergamaschi

Craig Gidney

Ike Chuang