The Quantum Fourier Transform (QFT)

Sean Hallgren
Caltech

The usefulness of the QFT

- Main component in quantum algorithms:
  - Recursive Fourier Sampling
  - Simon's Problem
  - Factoring and discrete log
  - Hidden subgroup problem
  - Hidden coset problem
  - Solvable groups
  - Pell's equation

(Everything...)

Outline

- Part 1: The quantum Fourier transform (QFT)
  - Definition
  - How to compute it
- Part 2: Fourier Sampling
  - The hidden subgroup problem.
  - Primitive used in quantum algorithms.

Why is the QFT so useful?

- **Can be computed fast:**

  The (Q)FT is a unitary transformation on vector space of dim n

  – Classically in time $n \log n$

  – Quantum in time $\log^2 n$

  } an exponential speedup!

- There are limitations however:

  Exponential resources

  vs.

  Limited access

  – Limited ways to set up input (quantum states).

  – Limited ways to access output.

Definition of the QFT

- $F_G : \mathbb{C}^{|G|} \to \mathbb{C}^{|G|}$ is a unitary transformation defined w.r.t. some finite group G
- This talk: restrict to cyclic groups
  $\longrightarrow$ abelian groups follows from this
- Cyclic group $\mathbb{Z}_n$, n a positive integer.
  - $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$, addition modulo n.
- Example $\mathbb{Z}_5$:

$$\underbrace{\begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & \omega^1 & \omega^2 & \omega^3 & \omega^4 \\ 1 & \omega^2 & \omega^4 & \omega^1 & \omega^3 \\ 1 & \omega^3 & \omega^1 & \omega^4 & \omega^2 \\ 1 & \omega^4 & \omega^3 & \omega^2 & \omega^1 \end{pmatrix}}_{F_5} \cdot \underbrace{\begin{pmatrix} \phi_0 \\ \phi_1 \\ \phi_2 \\ \phi_3 \\ \phi_4 \end{pmatrix}}_{|\phi\rangle} = \underbrace{\begin{pmatrix} \hat{\phi}_0 \\ \hat{\phi}_1 \\ \hat{\phi}_2 \\ \hat{\phi}_3 \\ \hat{\phi}_4 \end{pmatrix}}_{|\hat{\phi}\rangle}$$

Definition (cont.)

$$
\begin{array}{ccc}
F_n & \cdot\ |\phi\rangle & = |\widehat{\phi}\rangle \\
\begin{pmatrix}
1 & 1 & 1 & 1 & \cdots & 1 \\
1 & \omega^1 & \omega^2 & \omega^3 & \cdots & \omega^{n-1} \\
1 & \omega^2 & \omega^4 & \omega^6 & \cdots & \omega^{2(n-1)} \\
1 & \omega^3 & \omega^6 & \omega^9 & \cdots & \omega^{3(n-1)} \\
\vdots & & & & & \\
1 & \omega^{n-1} & \omega^{2(n-1)} & \omega^{3(n-1)} & \cdots & \omega^1
\end{pmatrix}
& \cdot \begin{pmatrix} \phi_0 \\ \phi_1 \\ \phi_2 \\ \phi_3 \\ \vdots \\ \phi_{n-1} \end{pmatrix}
& = \begin{pmatrix} \widehat{\phi}_0 \\ \widehat{\phi}_1 \\ \widehat{\phi}_2 \\ \widehat{\phi}_3 \\ \vdots \\ \widehat{\phi}_{n-1} \end{pmatrix}
\end{array}
$$

Entry $i, j = \omega^{ij}$

Classical:

$|\phi\rangle$ is the input vector

$|\widehat{\phi}\rangle$ is the output vector

FFT in time $n \log n$

Quantum:

$|\phi\rangle$ and $|\widehat{\phi}\rangle$ are quantum states

QFT in time $\log^2 n$

Computing the QFT over cyclic groups

- Two cases:
  - Easier: $n = 2^m$.
  - Harder: n an arbitrary integer, e.g. a prime.

    Uses the power of 2 Fourier transform.

Computing the QFT over a power of 2

Cleve, Ekert, Macchiavello, Mosca 1996.

$n = 2^m$

Basis vector $|a\rangle = |a_1 a_2 \cdots a_m\rangle$:

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

$$|a_1 a_2 \cdots a_m\rangle \xrightarrow{F_n} \sum_y \omega^{ay/2^m} |y_1 y_2 \cdots y_m\rangle$$

$$\vdots$$

$$(|0\rangle + \omega^{0.a_m}|1\rangle)(|0\rangle + \omega^{0.a_{m-1}a_m}|1\rangle)\cdots(|0\rangle + \omega^{0.a_1 a_2 \cdots a_m}|1\rangle)$$

$$\omega^{ay/2^m}|y_1 \cdots y_m\rangle =$$

$$\omega^{(0.a_m)y_1}|y_1\rangle \omega^{(0.a_{m-1}a_m)y_2}|y_2\rangle \cdots \omega^{(0.a_1 a_2 \cdots a_m)y_m}|y_m\rangle$$

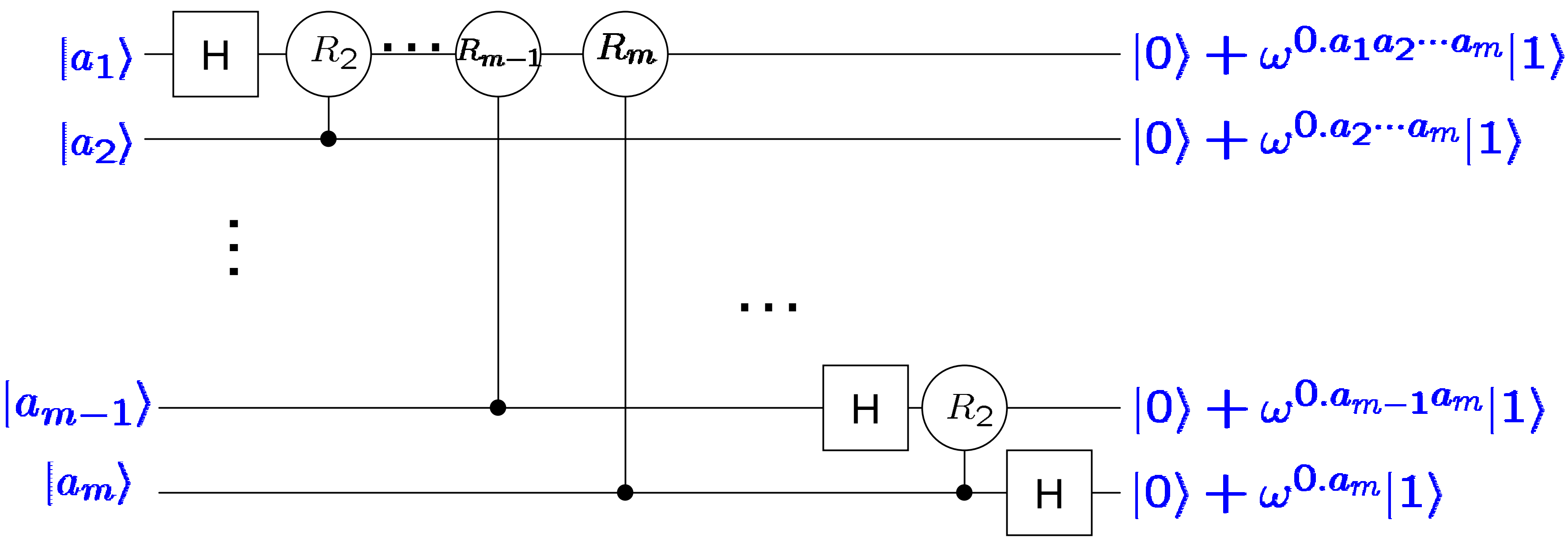
Computing the QFT over a power of 2: circuit

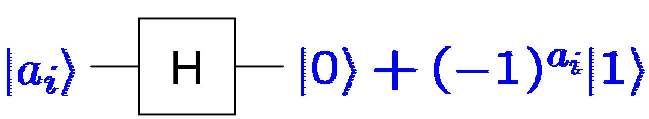
$$|a_1 a_2 \cdots a_m\rangle \longrightarrow \sum \omega^{ay/2^m} |y_1 y_2 \cdots y_m\rangle$$

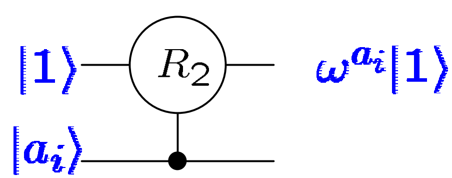
$$\|$$

$$(|0\rangle + \omega^{0.a_m}|1\rangle)(|0\rangle + \omega^{0.a_{m-1}a_m}|1\rangle)\cdots(|0\rangle + \omega^{0.a_1 a_2 \cdots a_m}|1\rangle)$$

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







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

Computing the QFT over cyclic groups

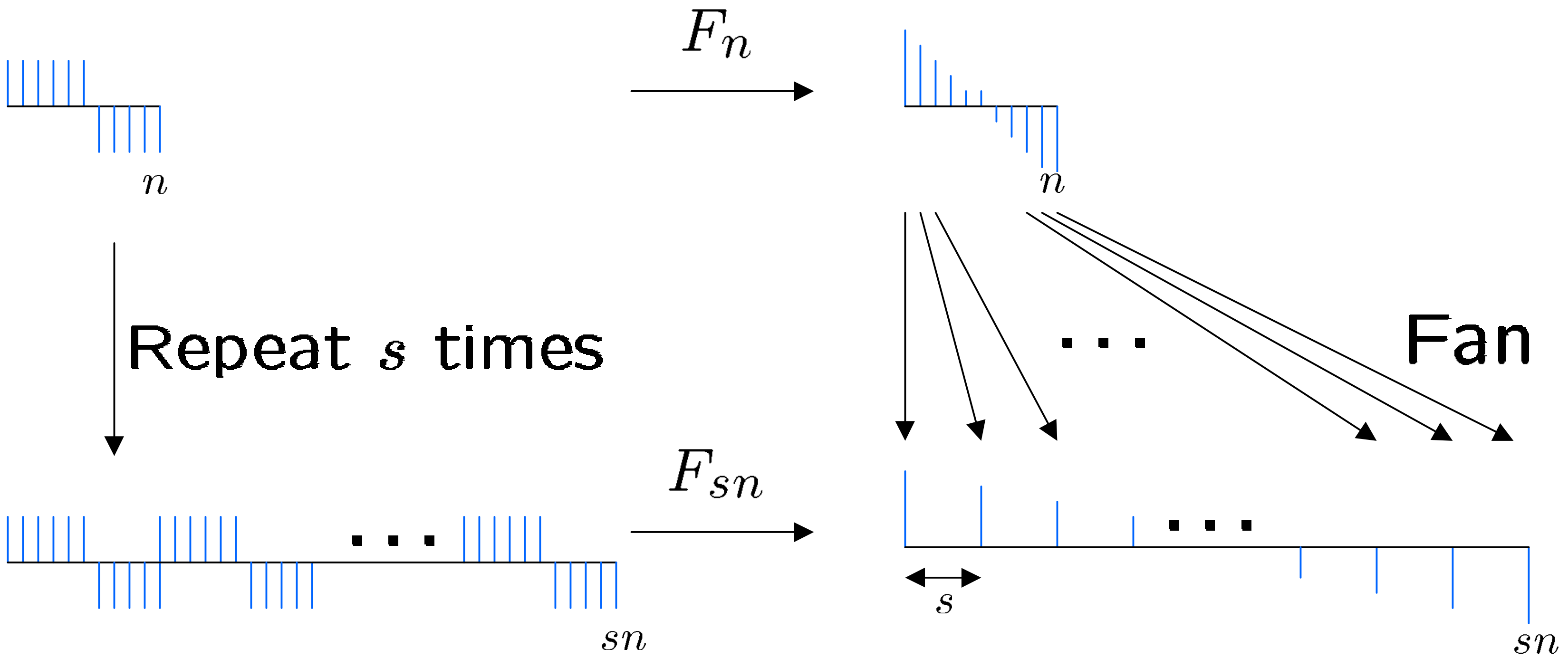
- Kitaev (1995)
- Hales, H. (2000) ← Today

- Parallel circuits:
  - Cleve, Watrous (2000)
  - Hales (2002, PhD Dissertation)

Two facts about the QFT

1) Repeated superposition

This diagram commutes.

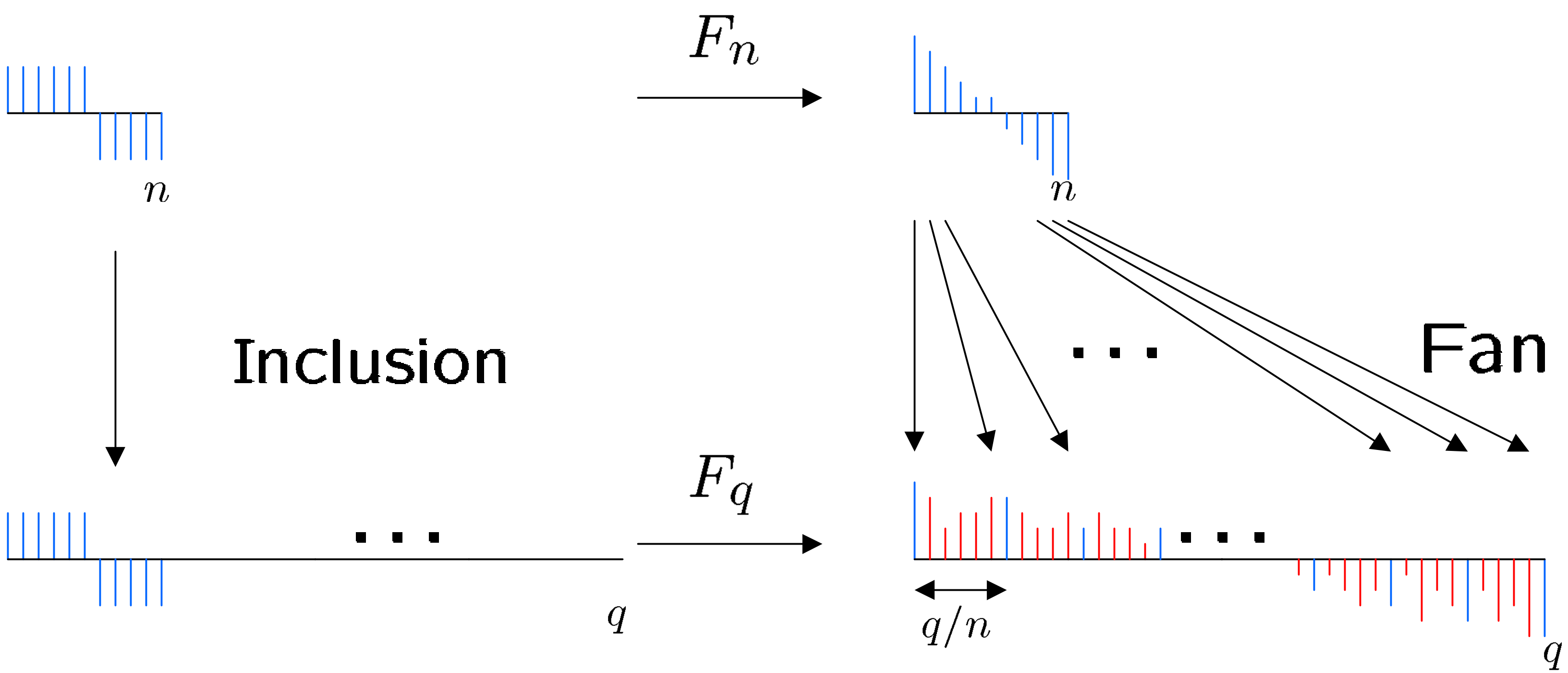


(Same superposition spaced out.)

Two facts about the QFT

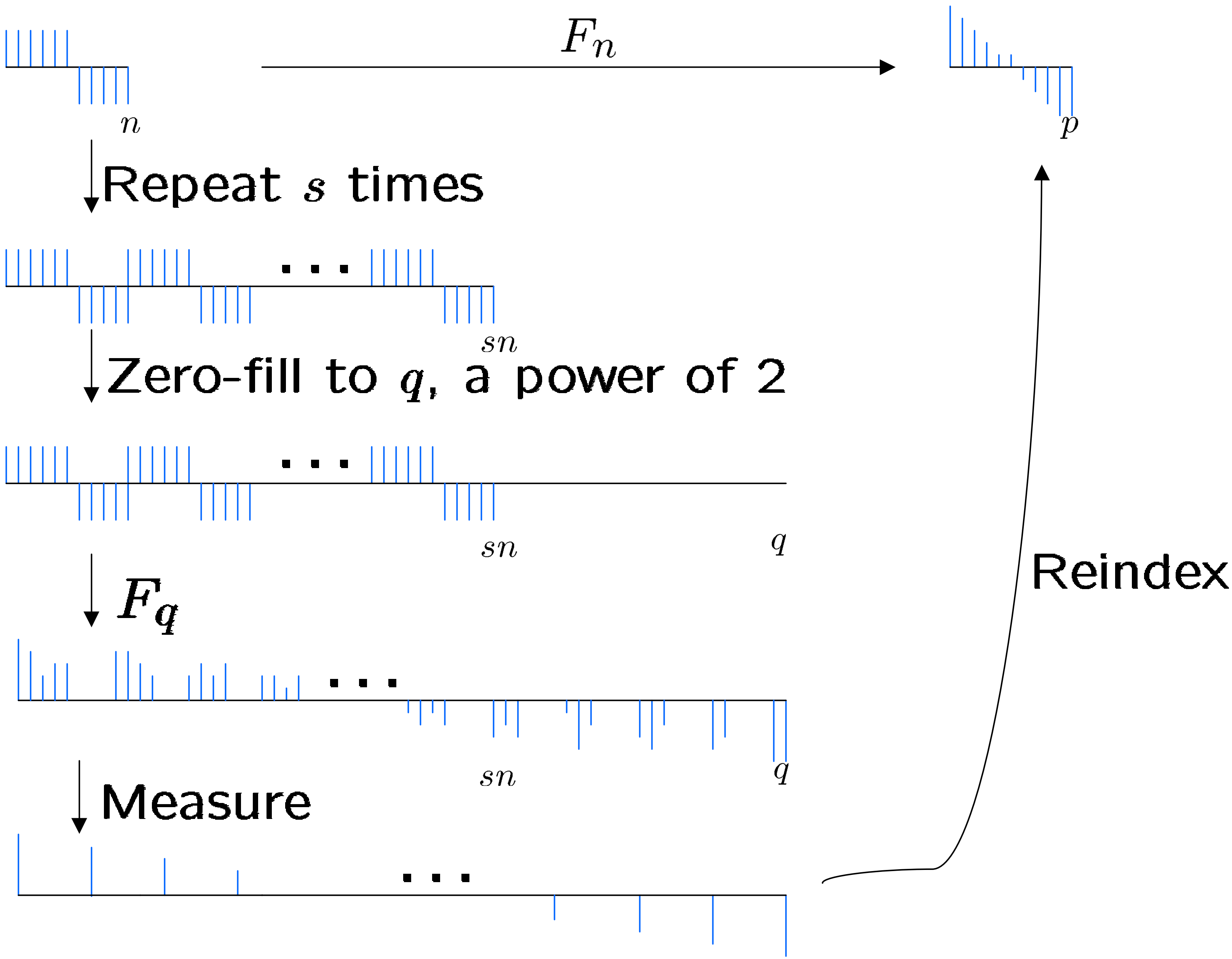
2) Zero-filling

This diagram commutes, but not as well.



Discard the red points.

Algorithm for QFT over cyclic groups



Parameters

Theorem (Approximating F_n)

Repeat the vector $s = \frac{\log^2 n}{\epsilon^4}$ times.

Choose $q = \frac{sn}{\epsilon^2}$.

Then the algorithm ϵ-approximates F_p and runs in time $O(m \log m \log\log m + \log^2 \frac{1}{\epsilon})$ $m = \log n$

Need a Fourier transform over a power of 2.

Two choices:

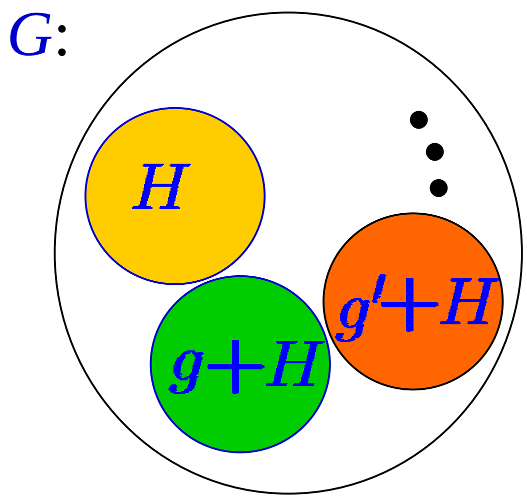
1) Coppersmith approximate circuit

2) Cleve, Watrous parallel circuit

Part 2: Quantum Fourier Sampling

The hidden subgroup problem (finite abelian groups)

Given $f : G \to$ Colors, constant and distinct on cosets of a subgroup H, find H.



Examples

- Factoring n: $G = \mathbb{Z}_m$, $m = \phi(n)$
- Discrete log: $G = \mathbb{Z}_{p-1} \times \mathbb{Z}_{p-1}$

Properites of the Fourier transform

finite group

Two properties of the FT over G:

1) subgroup $H \longrightarrow$ perp group $H^\perp$

$$\sum_{h\in H} |h\rangle \xrightarrow{F_G} \sum_{h'\in H^\perp} |h'\rangle$$

2) convolution $\longrightarrow$ pt. wise multiplication

$$|g\rangle * \sum_{h\in H} |h\rangle \xrightarrow{F_G} \sum_{h'} \alpha_{g,h'}|h'\rangle \bullet \sum_{h'\in H^\perp} |h'\rangle$$

$$\|$$

$$\sum_{h'\in H^\perp} \alpha_{g,h'}|h'\rangle$$

Creating a superposition on a coset

Given $f : G \to$ Colors, constant and distinct on cosets of a subgroup H, find H.

1) $|0,0\rangle \xrightarrow{F_G} \sum_{g\in G} |g,0\rangle \xrightarrow{f} \sum_{g\in G} |g, f(g)\rangle$

Measure

After measuring:

$$\sum_{h\in H} |g+h, f(g)\rangle$$

Rewrite as:

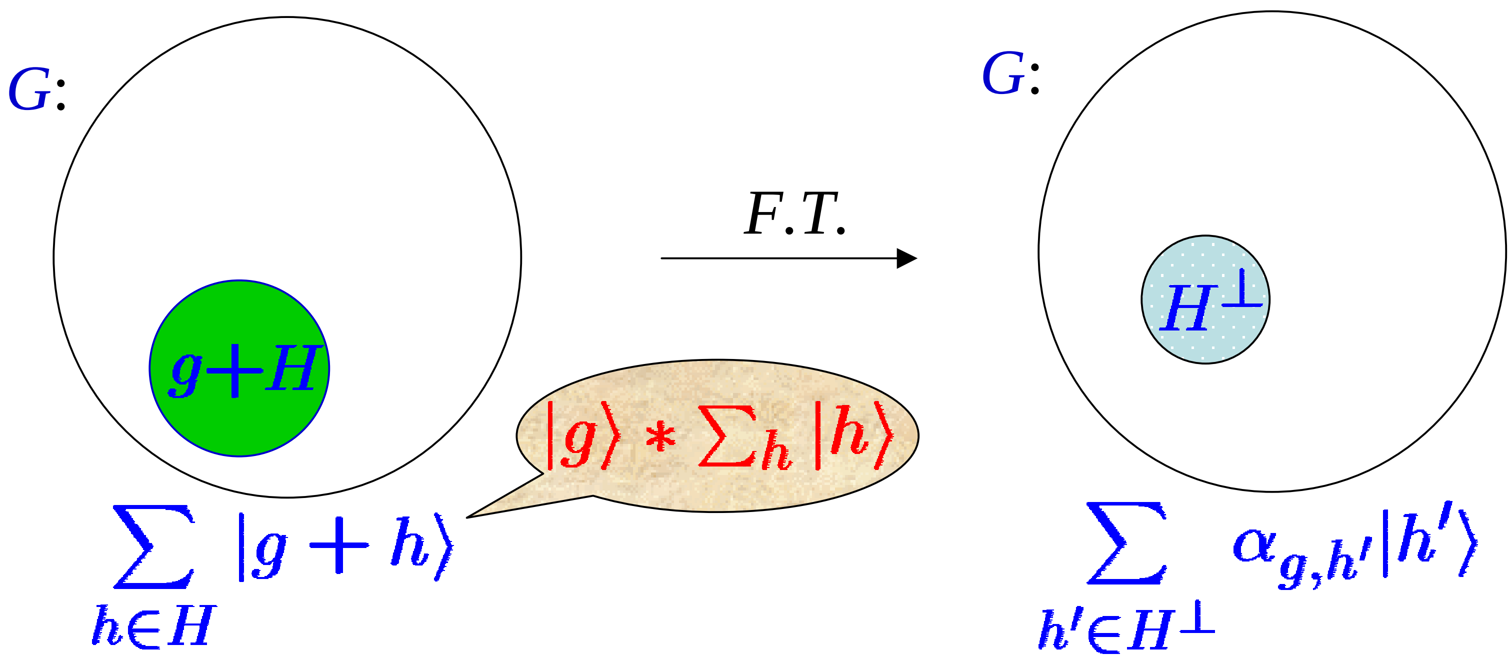
$$\sum_{h\in H} |g+h\rangle$$

The hidden subgroup problem algorithm

Given $f : G \to$ Colors, constant and distinct on cosets of a subgroup H, find H.

Algorithm:

2) Fourier sample:

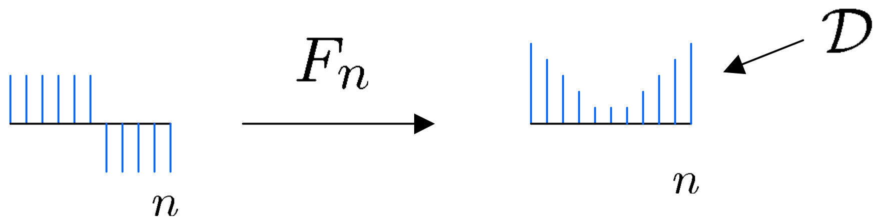


Measure a random element of *H?*.

3) (Classically) reconstruct H from the samples.

Quantum Fourier sampling

Fourier sample: compute the Fourier transform and measure:



$\mathcal{D}$ is a probability dist. on $\{0, 1, \ldots, n-1\}$

Structure of many quantum algorithms:

Repeat:

1) Set up some superposition
2) Fourier sample

3) Classical postprocessing

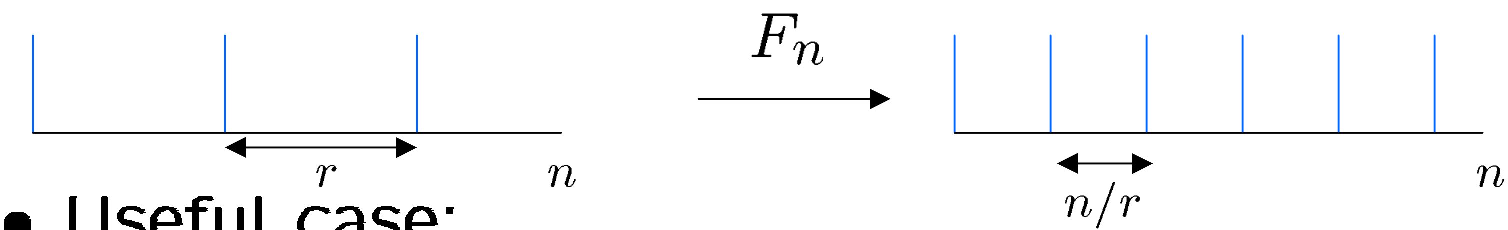
Example: period finding

Step 1: Set up periodic superposition using periodic function $f : \mathbb{Z} \to$ Colors.

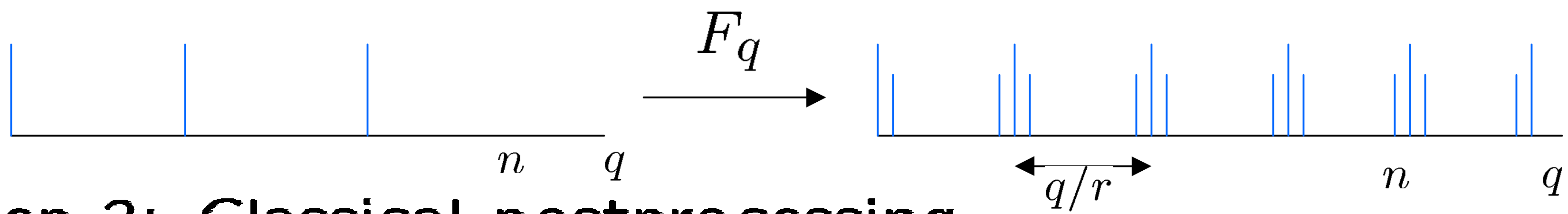
(factoring reduces to period finding)

Step 2: Fourier sample.

- Clean case:



- Useful case:



Step 3: Classical postprocessing

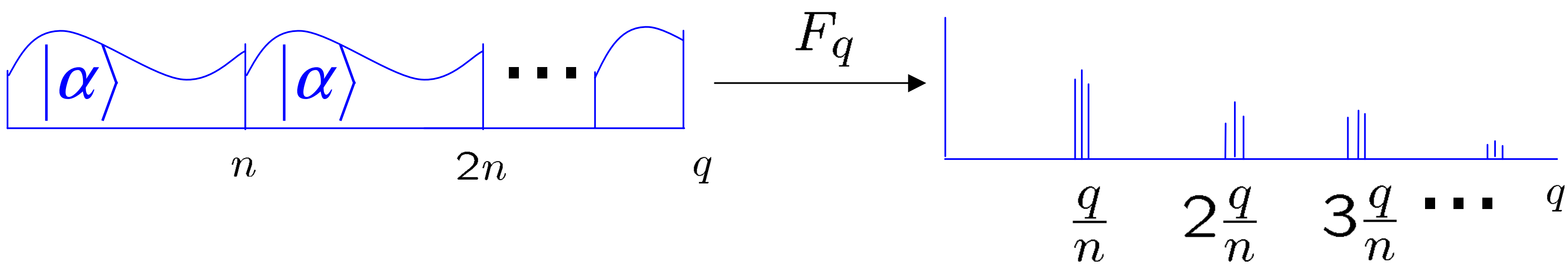
Theorem: useful Fourier sampling $\leq$ clean Fourier sampling

Fourier Sampling Theorem

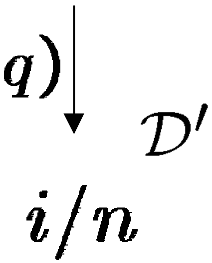
Arbitrary superposition $|\alpha\rangle$, with n **unknown**.

Suppose know $\mathcal{D}$.

Then $\mathcal{D} \approx \mathcal{D}'$:



C.F. expansion of (sample$/q$)



Situation:

n is unknown, have access to repeated $|\alpha\rangle$.

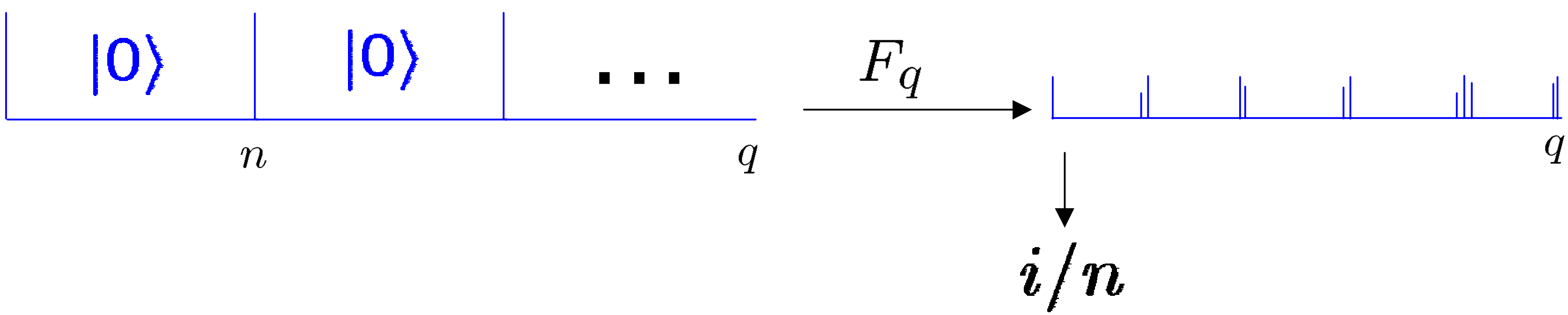
Example: Shor's Period Finding

Know:

What is $|\alpha\rangle$ for Shor's period finding algorithm?

Answer:

(uniform)



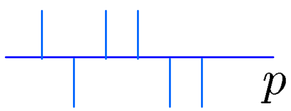
i uniformly dist.

Example: Legendre Symbol

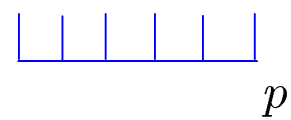
$\left(\frac{\cdot}{p}\right) : \mathbb{Z}_p \to \{\pm 1\}$ specifies whether an element is a square

Suppose can query values of the function, but p is **unknown**. Find p.

$$\sum_{x=0}^{p-1} \left(\frac{x}{p}\right) |x\rangle$$

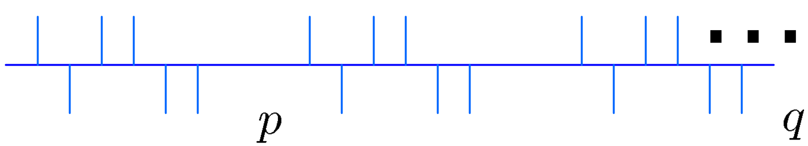


$$\xrightarrow{F_p}$$

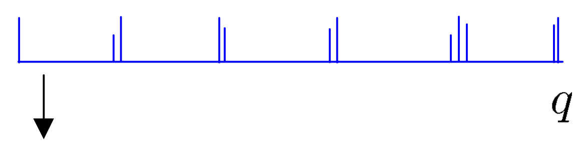


(uniform)

$$\sum_{x=0}^{q-1} \left(\frac{x}{p}\right) |x\rangle$$



$$\xrightarrow{F_q}$$



i/p $\quad i$ uniform

Conclusions

Fourier sampling theorem:

- Useful when not possible to use the clean group theoretic case directly.
- Fourier sampling is robust under group changes.
- Other examples:
  - Functions that are not distinct on cosets.
  - Alternate solution to Pell's equation.

Earlier in the talk:

- How to compute Fourier transforms over finite abelian groups
- The hidden subgroup problem