Quantum Mechanics & Quantum Computation

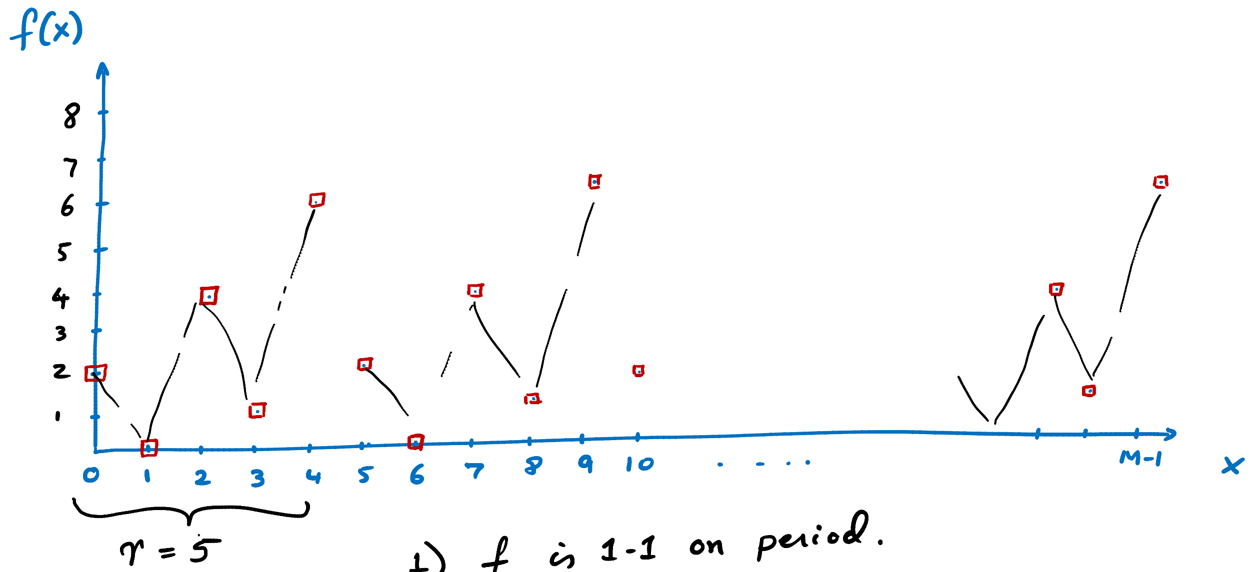
Umesh V. Vazirani
University of California, Berkeley

Lecture 10: Quantum Factoring

Period Finding

Period finding

Input: f: {0, 1, …, M-1} → S, such that for all x, f(x) = f(x+r).
Challenge: Find r.

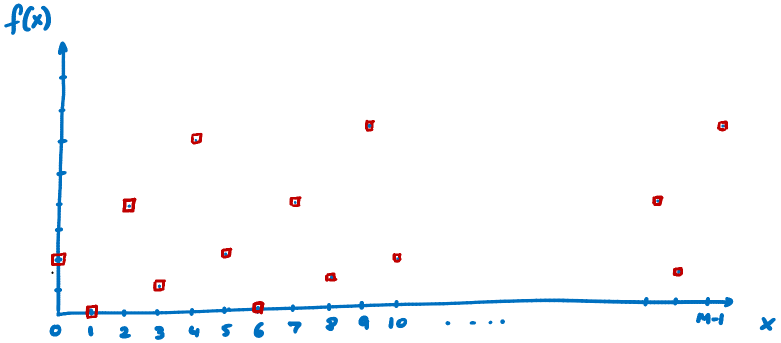


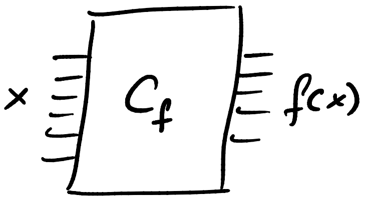
$M = 100$
$M/r = 20$

1) f is 1-1 on period.
2) r divides M.
2') $\frac{M}{r} \gg r$. $M \gg r^2$.

Period finding

Input: f: {0, 1, …, M-1} → S, such that for all x, f(x) = f(x+r).
Challenge: Find r.





M 1000 digit number.

$M \sim 10^{1000}$

$r \sim \sqrt{M}$

r 500 digit number.

$\sqrt{r}$ inputs suffice to see a collision!

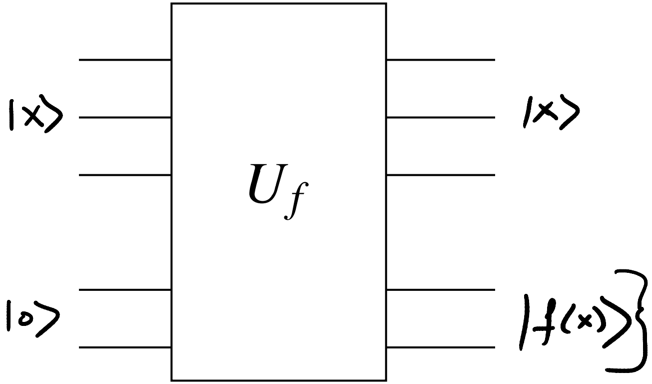
Birthday paradox

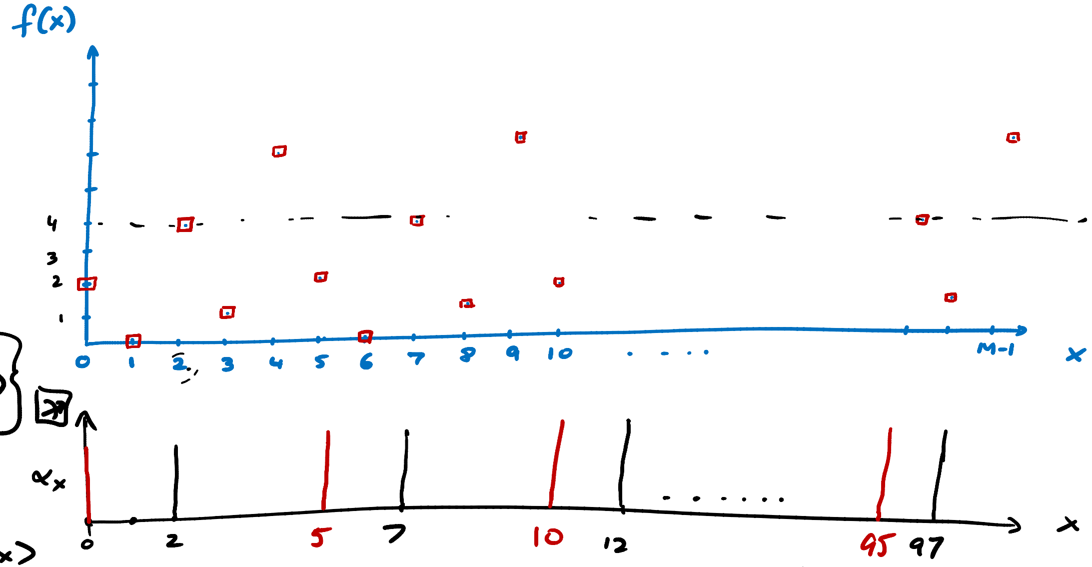
$\sqrt{r}$ 250 digit number

$\sqrt{r} \sim 10^{250}$.

Period finding

Input: f: {0, 1, …, M-1} → S, such that for all x, f(x) = f(x+r).
Challenge: Find r.





$$\frac{1}{\sqrt{M}} \sum_{x=0}^{M-1} |x\rangle \underbrace{|f(x)\rangle}_{r} \xrightarrow{\text{measure}} \sum_{x=0}^{M-1} \alpha_x |x\rangle$$

$f(a) = 4$

Fourier sampling

$r = 5 \quad M = 100$

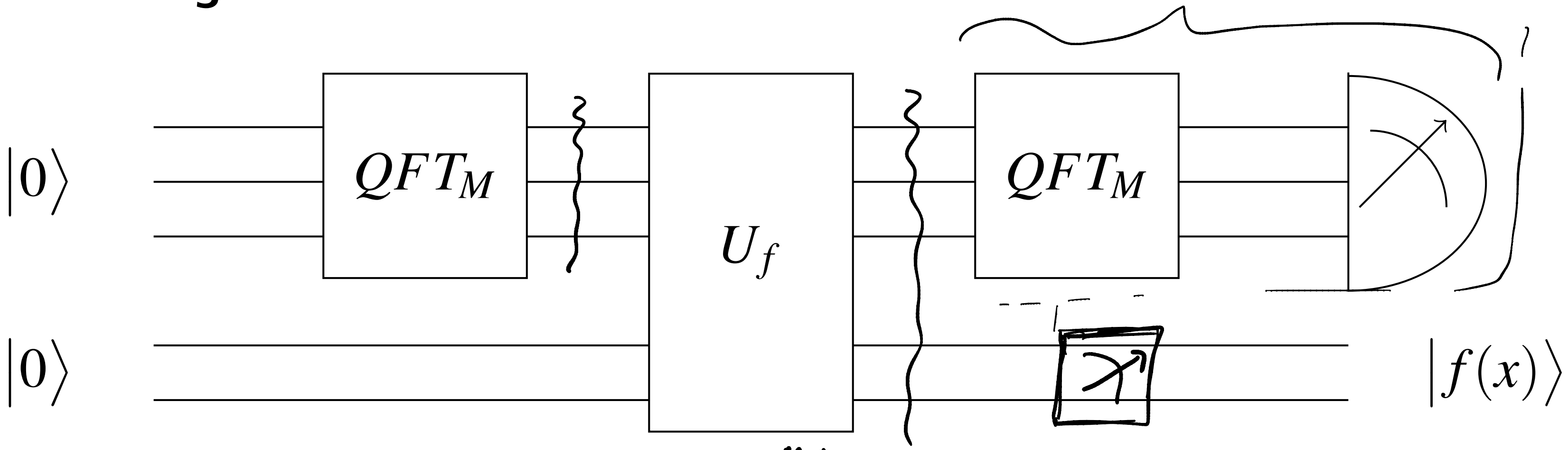
$$\sqrt{\frac{r}{M}} \sum_{j=0}^{\frac{M}{r}-1} |jr\rangle$$

Random mult of $\frac{M}{r} = \underline{\underline{20}}$

Output: $\left.\begin{matrix} 60 \\ 80 \end{matrix}\right\}$ $\gcd(60, 80) = 20$

Period finding

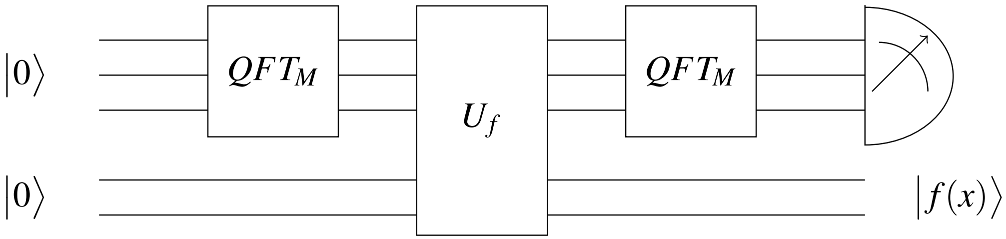
Input: f: {0, 1, …, M-1} → S, such that for all x, f(x) = f(x+r).
Challenge: Find r.



$$|0\rangle \xrightarrow{QFT_M} \frac{1}{\sqrt{M}}\sum_{x=0}^{M-1}|x\rangle \longrightarrow \frac{1}{\sqrt{M}}\sum_{x=0}^{M-1}|x\rangle\underbrace{|f(x)\rangle}_{f(x).}$$

Period finding

Input: f: {0, 1, …, M-1} → S, such that for all x, f(x) = f(x+r).
Challenge: Find r.



L

$M > 2r^2$

$\frac{M}{r} > 2r$

$\frac{L}{M} \sim \boxed{\frac{t}{r}?}$

$\cancel{L \quad \frac{tM}{r}}$

continued fractions.

Quantum Mechanics & Quantum Computation

Umesh V. Vazirani
University of California, Berkeley

Lecture 10: Quantum Factoring

Shor's Factoring Algorithm

$N = 60 = 2^2 \times 3 \times 5$

$N = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$

$N = P \cdot Q$

RSA cryptosystem

n = length of N in bits

$O(2^n)$

$2^{O(\sqrt[3]{n})}$

750 bit

200 decimal digits.

$N = 21$

$a \equiv b \pmod{N}$

$b = qN + \underline{\underline{a}}$

$3 \equiv 24 \pmod{21}$

$14 \equiv 35 \pmod{21}$

$20 \equiv -\underline{1} \pmod{21}$

$24 + 35 \pmod{21}$

$\equiv 3 + 14$

$\equiv 17 \pmod{21}$

$24 \times 30 \pmod{21}$

$\equiv 3 \times 9$

$\equiv 27 \equiv 6 \pmod{21}$

* Arithmetic (mod N) efficiently.

* $\gcd(a, b)$

$\gcd(\underset{3\times 5}{\underset{\shortparallel}{15}}, \underset{3\times 7}{\underset{\shortparallel}{21}}) = 3.$

<u>Euclid's Alg</u>:

$21 = 1 \times \underline{15} + \underline{6}$

$15 = 2 \times \underline{6} + \underline{3}$

$6 = 2 \times 3 + \underline{0}$

Resources:

- Modular arithmetic.
- a = b (mod N). e.g. 3 = 15 (mod 12)
- “Algorithms” by Dasgupta, Papadimitriou, Vazirani

  www.cs.berkeley.edu/~vazirani/algorithms.html ✓

  Chapter 1: Modular Arithmetic
  Chapter 2 (2nd half): Fast fourier transform
  Chapter 10: Quantum factoring.

$N = 21$

$x^2 \equiv 1 \pmod{21}$

$x = 1$

$x = -1 \equiv 20 \pmod{21}$

$x = 8$

$x^2 = 8 \times 8 = 64 \pmod{21}$

$\equiv 1 \pmod{21}$

$x = -8 \equiv 13 \pmod{21}$

$13^2 \equiv 169 \equiv 1 \pmod{21}$

$8^2 \equiv 1 \mod 21$

$8^2 - 1^2 \equiv 0 \pmod{21}$

$\underset{3 \times 7}{\overset{\parallel}{21}}$ divides $(8+1)(8-1)$

$\gcd(21, \overset{9}{8+1}) = 3$

$\gcd(21, 7) = 7$

Find x:

$x \not\equiv \pm 1 \pmod{N}$ $\quad x \pm 1 \not\equiv 0 \pmod{N}$

but $x^2 \equiv 1 \pmod{N}$

N divides $(x+1)(x-1)$

N does not divide $(x \pm 1)$

$\gcd(N, x+1)$

$N = 21$

$x = 2$

$$2^0 \equiv 1 \pmod{21}$$
$$2^1 \equiv 2 \pmod{21}$$
$$2^2 = 4 \pmod{21}$$
$$2^3 = 8 \pmod{21}$$
$$2^4 \equiv 16 \pmod{21}$$
$$2^5 \equiv 11 \pmod{21}$$
$$2^6 \equiv 1 \pmod{21}$$

$$2^6 \equiv 2^3 \times 2^3$$
$$(\underbrace{2^3}_{=8})^2 \equiv 1 \pmod{21}$$

Pick x at random

$$x^0$$
$$x^1$$
$$\vdots$$
$$x^r \equiv 1 \pmod{N}$$

lucky : r is even.

$$(x^{r/2})^2 \equiv 1 \pmod{N}$$

luckier $x^{r/2} \not\equiv \pm 1 \pmod{N}$

Lemma: Let N be an odd composite, with at least two distinct prime factors, and let x be uniformly random between 0 and N-1. If gcd(x, N) = 1, then with probability at least ½, the order r of x (mod N) is even, and $x^{r/2}$ is a nontrivial square root of 1 (mod N)

$1 \equiv x^r \pmod{N}$

$N = 21$

$x = 2$

Period $= r = 6$

$(x^{r/2})^2 \equiv 1 \pmod N$

$$\frac{1}{\sqrt{M}} \sum_{a=0}^{M-1}$$

a	$f(a) = x^a \pmod N$
0	1
1	2
2	4
3	8
4	16
5	11
6	1
7	2
8	4
9	8
10	16
11	11
12	1
13	2
14	4
15	8

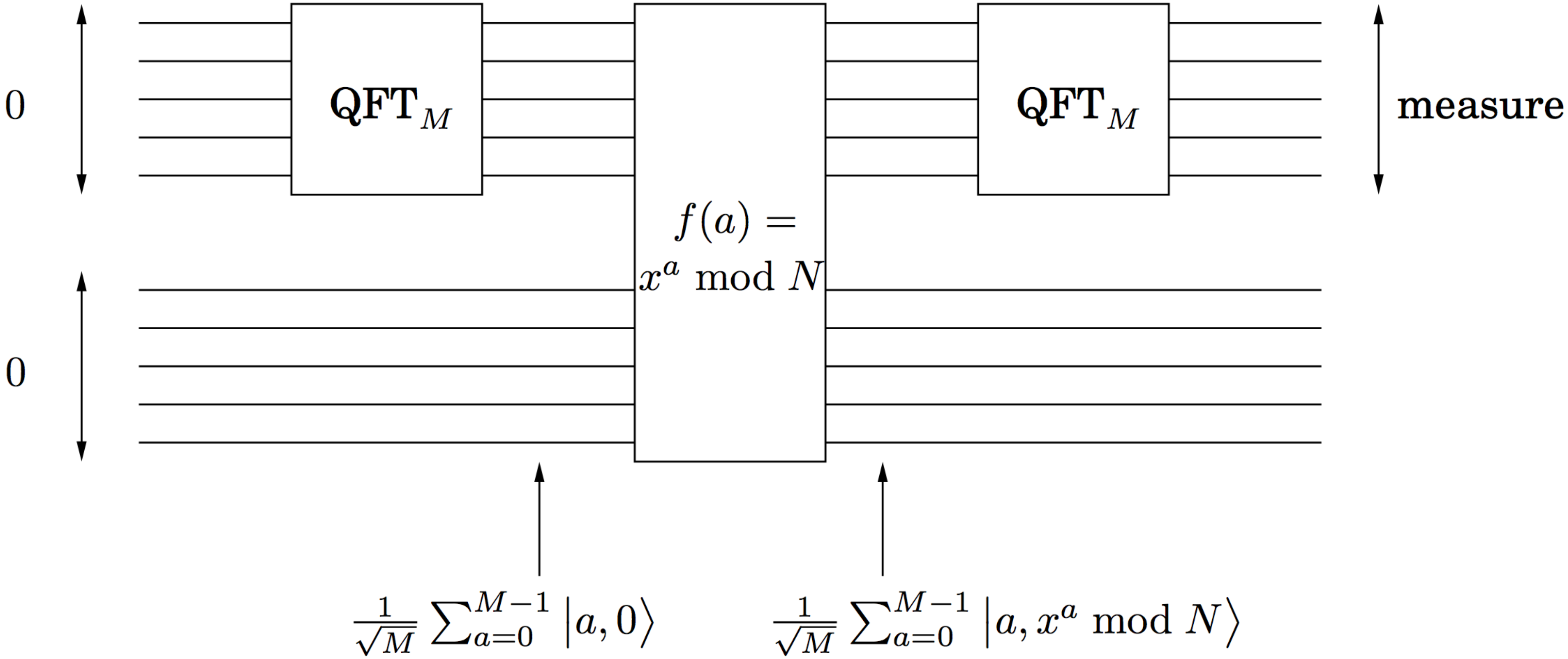
Fourier sampling

classically reconstruct period r.

$M > 2r^2$ $\qquad \frac{M}{r} > 2r$

$M > 2N^2$.

$M > 2N^2$


0
0
QFT$_M$
$f(a) =$
$x^a \bmod N$
QFT$_M$
measure
$\frac{1}{\sqrt{M}} \sum_{a=0}^{M-1} |a, 0\rangle$
$\frac{1}{\sqrt{M}} \sum_{a=0}^{M-1} |a, x^a \bmod N\rangle$

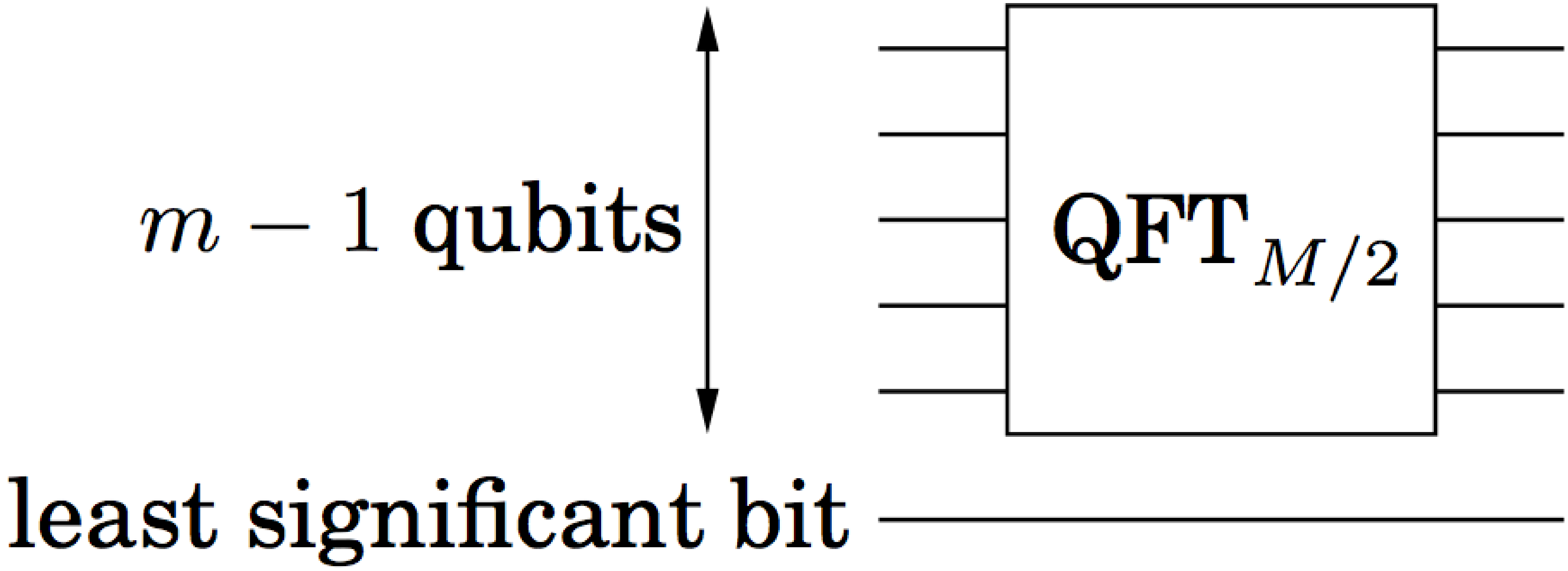
Quantum Mechanics & Quantum Computation

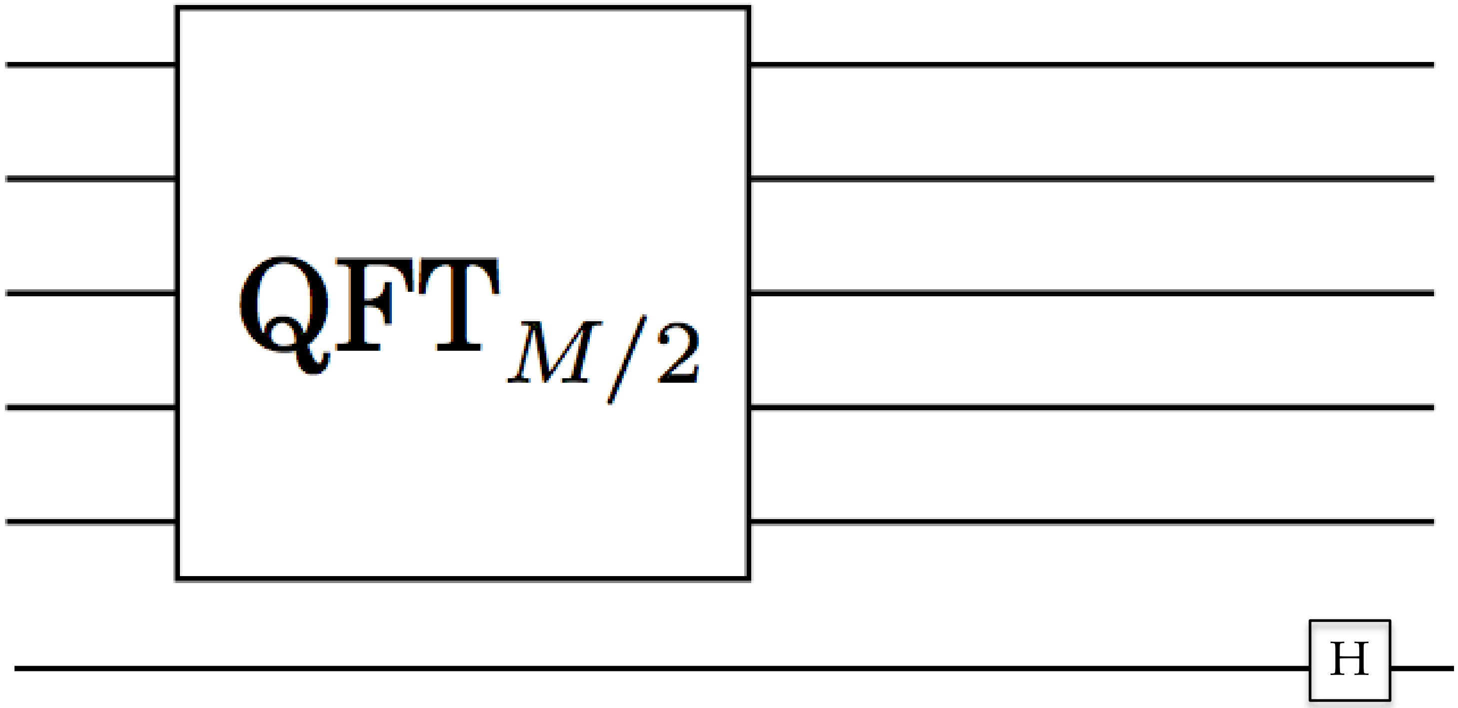
Umesh V. Vazirani
University of California, Berkeley

Lecture 10: Quantum Factoring

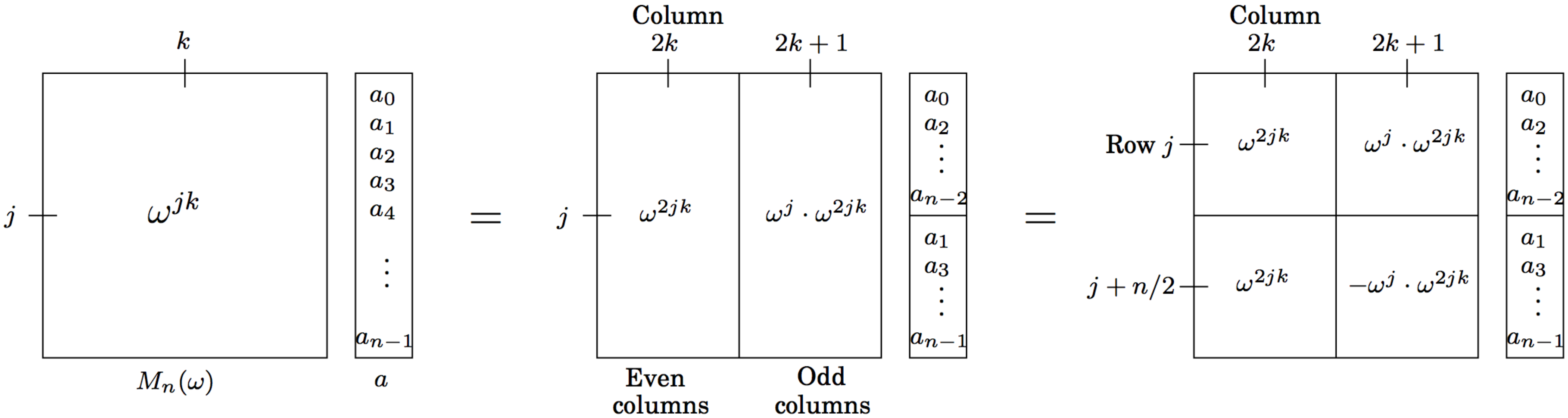
QFT Circuit

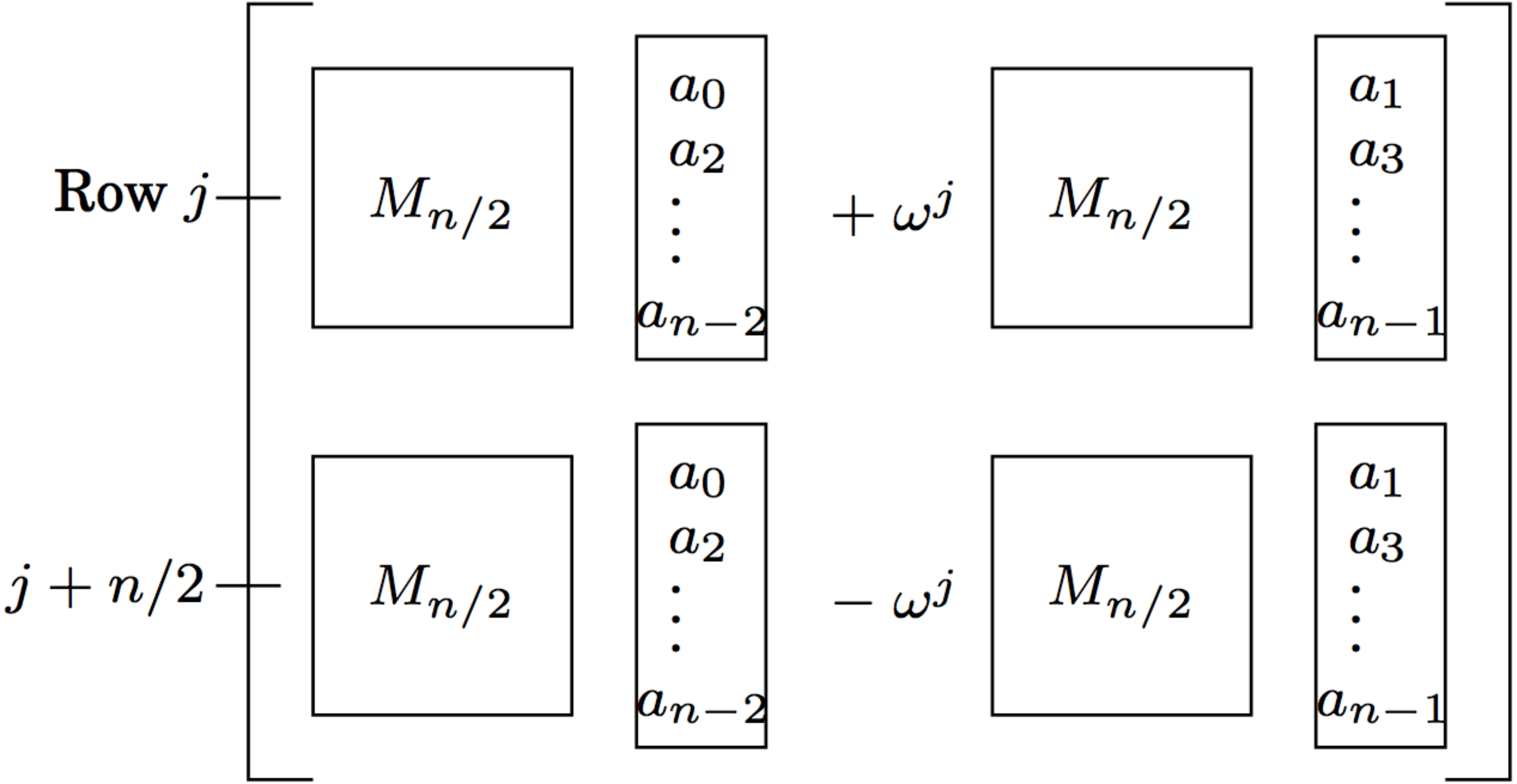
$$
\begin{bmatrix} \beta_0 \\ \beta_1 \\ \beta_2 \\ \vdots \\ \beta_{M-1} \end{bmatrix} = \frac{1}{\sqrt{M}} \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \cdots & \omega^{M-1} \\ 1 & \omega^2 & \omega^4 & \cdots & \omega^{2(M-1)} \\ & \vdots & & & \\ 1 & \omega^j & \omega^{2j} & \cdots & \omega^{(M-1)j} \\ & \vdots & & & \\ 1 & \omega^{(M-1)} & \omega^{2(M-1)} & \cdots & \omega^{(M-1)(M-1)} \end{bmatrix} \begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_{M-1} \end{bmatrix}
$$


$m-1$ qubits
least significant bit
$\mathbf{QFT}_{M/2}$

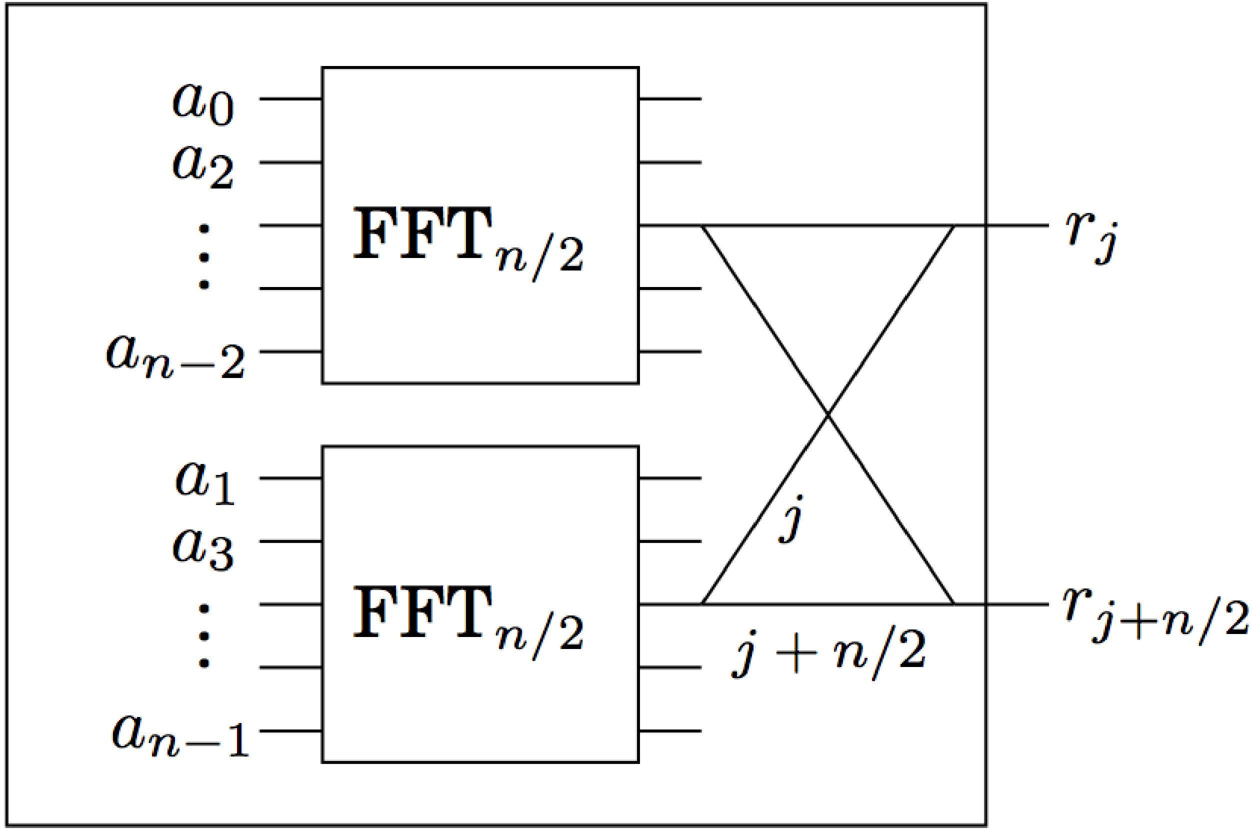

QFT$_{M/2}$
H

$$
\begin{bmatrix}
1 & 1 & 1 & \cdots & 1 \\
1 & \omega & \omega^2 & \cdots & \omega^{n-1} \\
1 & \omega^2 & \omega^4 & \cdots & \omega^{2(n-1)} \\
 & & \vdots & & \\
1 & \omega^j & \omega^{2j} & \cdots & \omega^{(n-1)j} \\
 & & \vdots & & \\
1 & \omega^{(n-1)} & \omega^{2(n-1)} & \cdots & \omega^{(n-1)(n-1)}
\end{bmatrix}
\begin{bmatrix}
a_0 \\
a_1 \\
\vdots \\
a_{n-1}
\end{bmatrix}
$$


k
j
ω^{jk}
a_0
a_1
a_2
a_3
a_4
a_{n-1}
$M_n(\omega)$
a
=
Column
$2k$
$2k+1$
j
ω^{2jk}
$\omega^j \cdot \omega^{2jk}$
a_0
a_2
a_{n-2}
a_1
a_3
a_{n-1}
Even columns
Odd columns
=
Column
$2k$
$2k+1$
Row j
$j+n/2$
ω^{2jk}
$\omega^j \cdot \omega^{2jk}$
ω^{2jk}
$-\omega^j \cdot \omega^{2jk}$
a_0
a_2
a_{n-2}
a_1
a_3
a_{n-1}

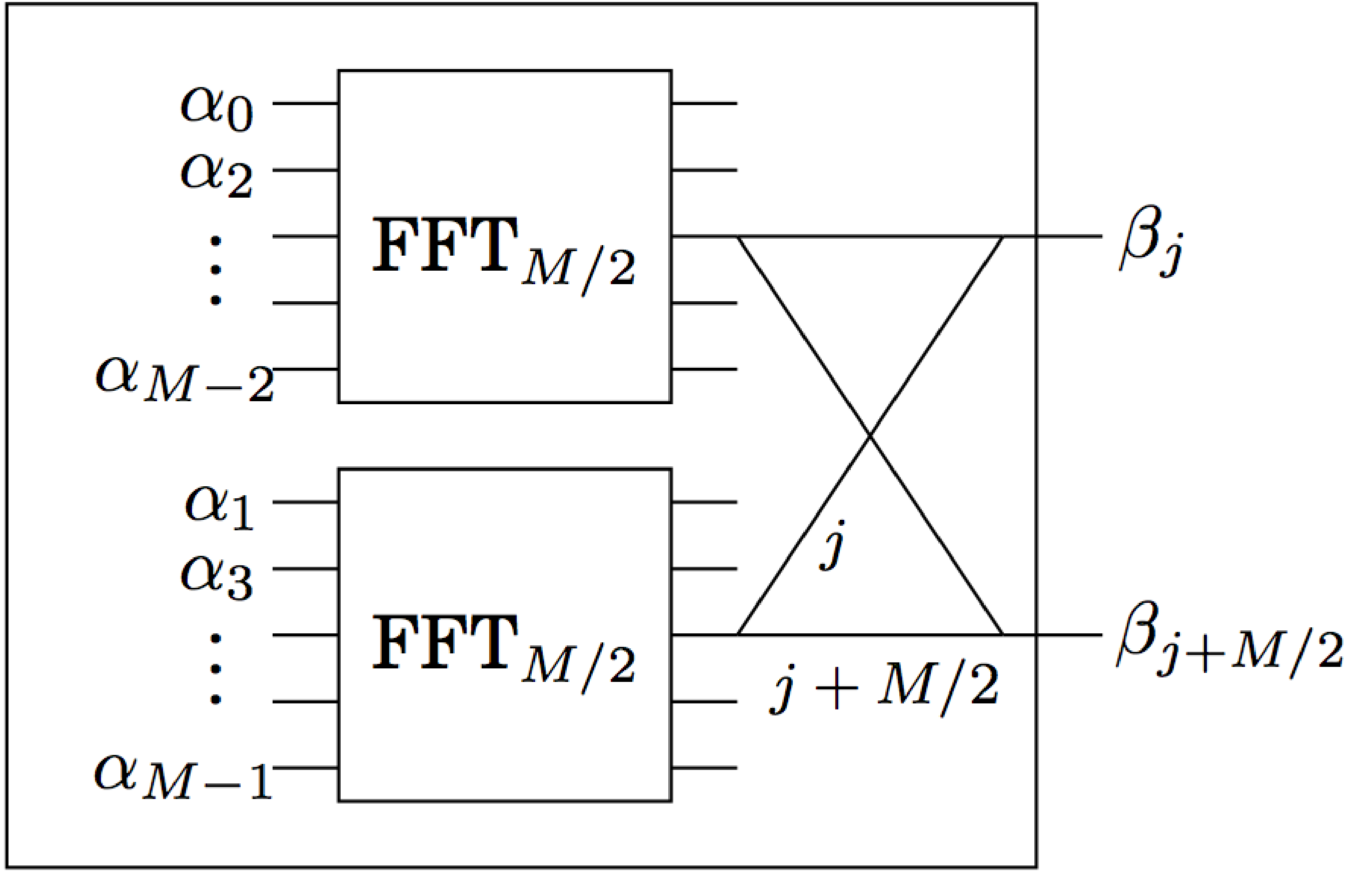

Row j
$j + n/2$
$M_{n/2}$
a_0
a_2
a_{n-2}
$+\,\omega^j$
$-\,\omega^j$
a_1
a_3
a_{n-1}

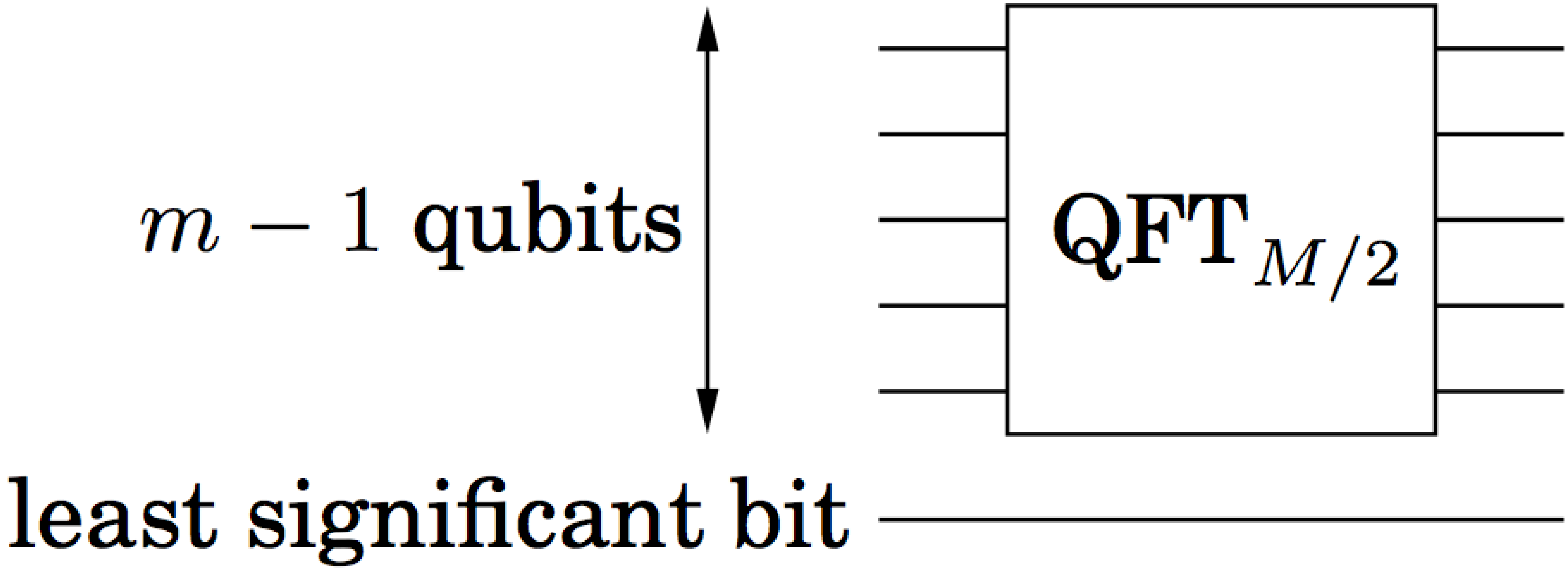
FFT$_n$ **(input:** $a_0, \ldots, a_{n-1}$**, output:** $r_0, \ldots, r_{n-1}$**)**



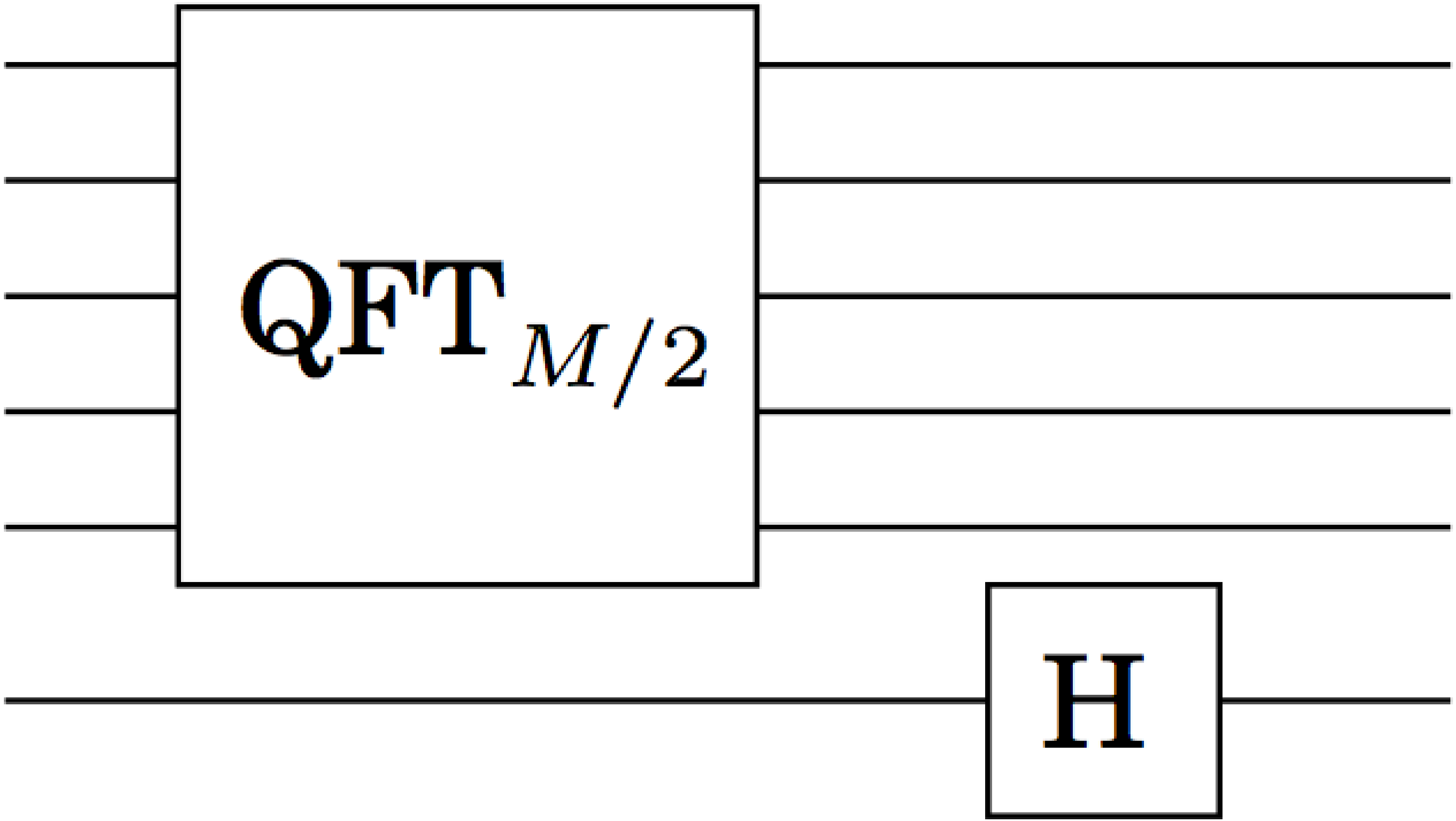
$$
\begin{bmatrix} \beta_0 \\ \beta_1 \\ \beta_2 \\ \vdots \\ \beta_{M-1} \end{bmatrix} = \frac{1}{\sqrt{M}} \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \cdots & \omega^{M-1} \\ 1 & \omega^2 & \omega^4 & \cdots & \omega^{2(M-1)} \\ & \vdots & & & \\ 1 & \omega^j & \omega^{2j} & \cdots & \omega^{(M-1)j} \\ & \vdots & & & \\ 1 & \omega^{(M-1)} & \omega^{2(M-1)} & \cdots & \omega^{(M-1)(M-1)} \end{bmatrix} \begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_{M-1} \end{bmatrix}
$$

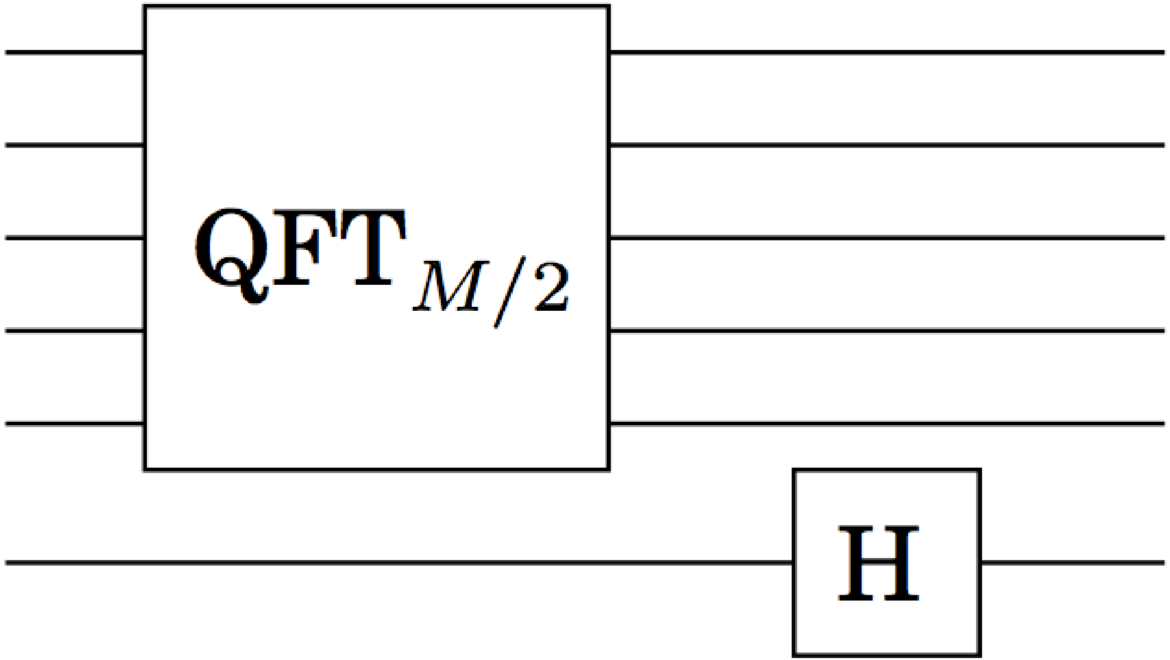
$\mathbf{FFT}_M$ (input: $\alpha_0, \ldots, \alpha_{M-1}$, output: $\beta_0, \ldots, \beta_{M-1}$)





$m - 1$ qubits
$\mathbf{QFT}_{M/2}$
least significant bit


$\mathrm{QFT}_{M/2}$
H



$\mathbf{QFT}_{M/2}$
H