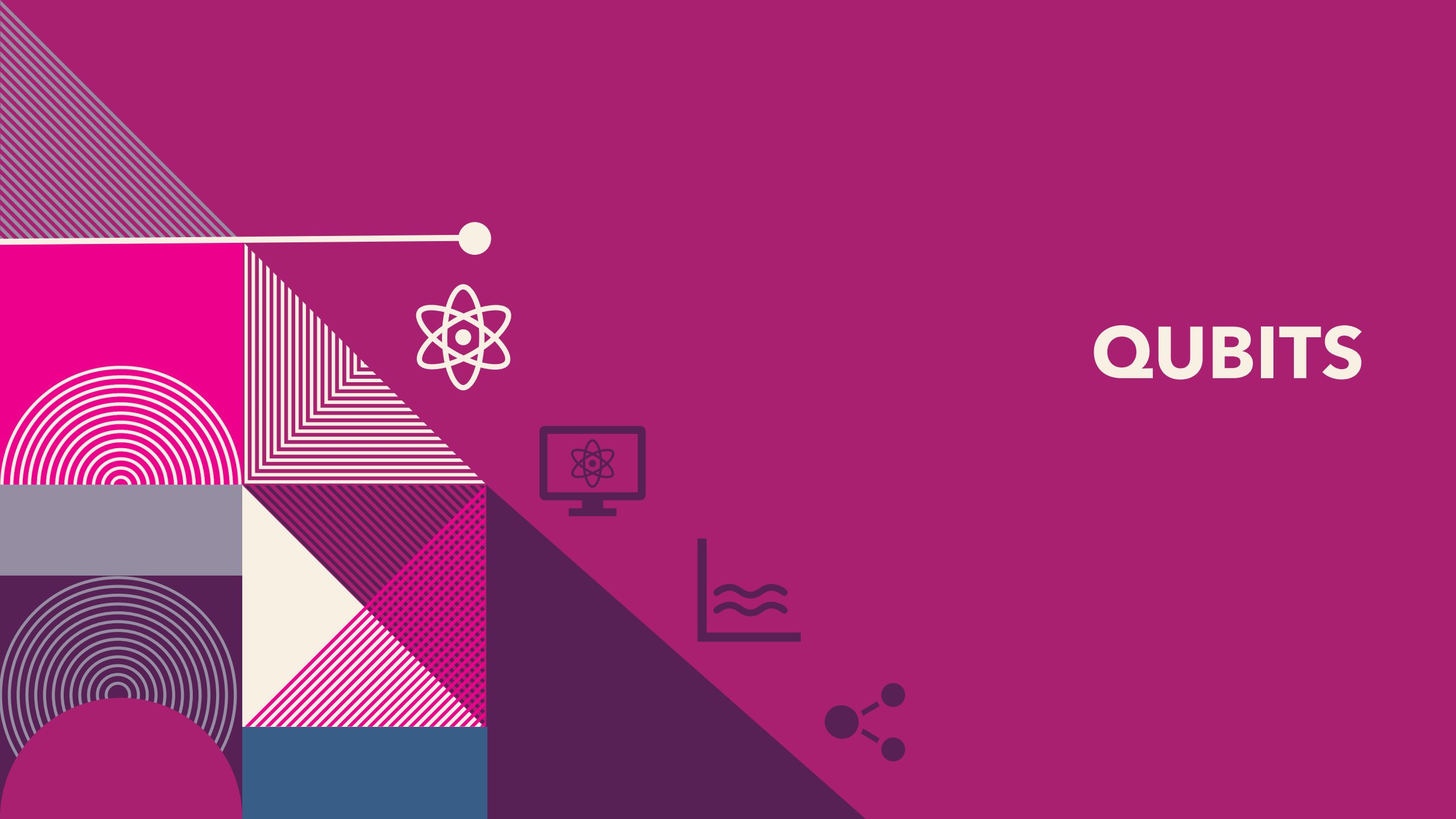
QUANTUM INTUITIONS: FROM QUBITS TO SHOR'S FACTORIZATION ALGORITHM

Mentor
Giovanni Manzini

Student
Silvia Mondin

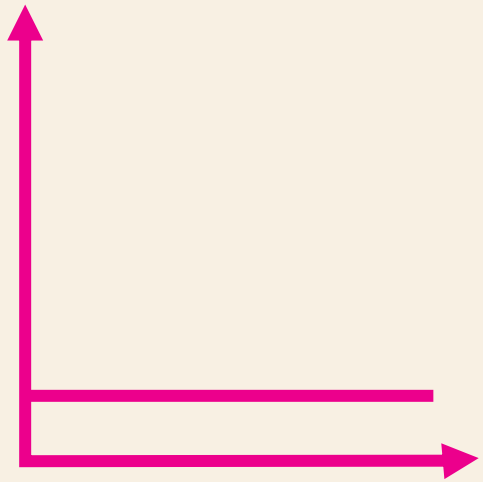
Date
15/05/2026

CONTENTS

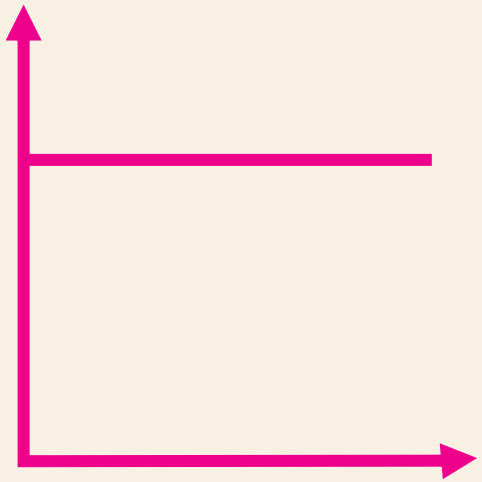

QUBITS

HOW TO REPRESENT INFORMATION: BITS…

- A bit can have one of two values: 0 and 1
- Represented by low and high voltages on wires



Low voltage
0



High voltage
1

HOW TO REPRESENT INFORMATION: BITS…

- A bit can have one of two values: 0 and 1
- Represented by the state of a hydrogen atom

Ground State
0

Excited State
1

… AND QUBITS

- A qubit can be 0, 1 and all in between
- Represented by the state of a hydrogen atom

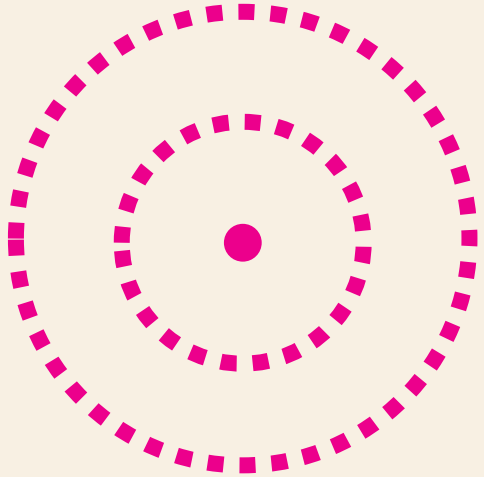
Ground State
$|0\rangle$

Excited State
$|1\rangle$

… AND QUBITS

- A qubit can be 0, 1 and all in between
- Represented by the state of a hydrogen atom

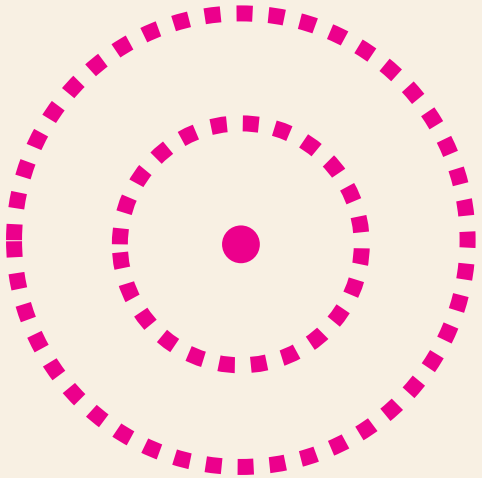
Ground State
$|0\rangle$



Superposition
$\alpha_0|0\rangle + \alpha_1|1\rangle$

Excited State
$|1\rangle$

SUPERPOSITION



Superposition
$\alpha_0|0\rangle + \alpha_1|1\rangle$

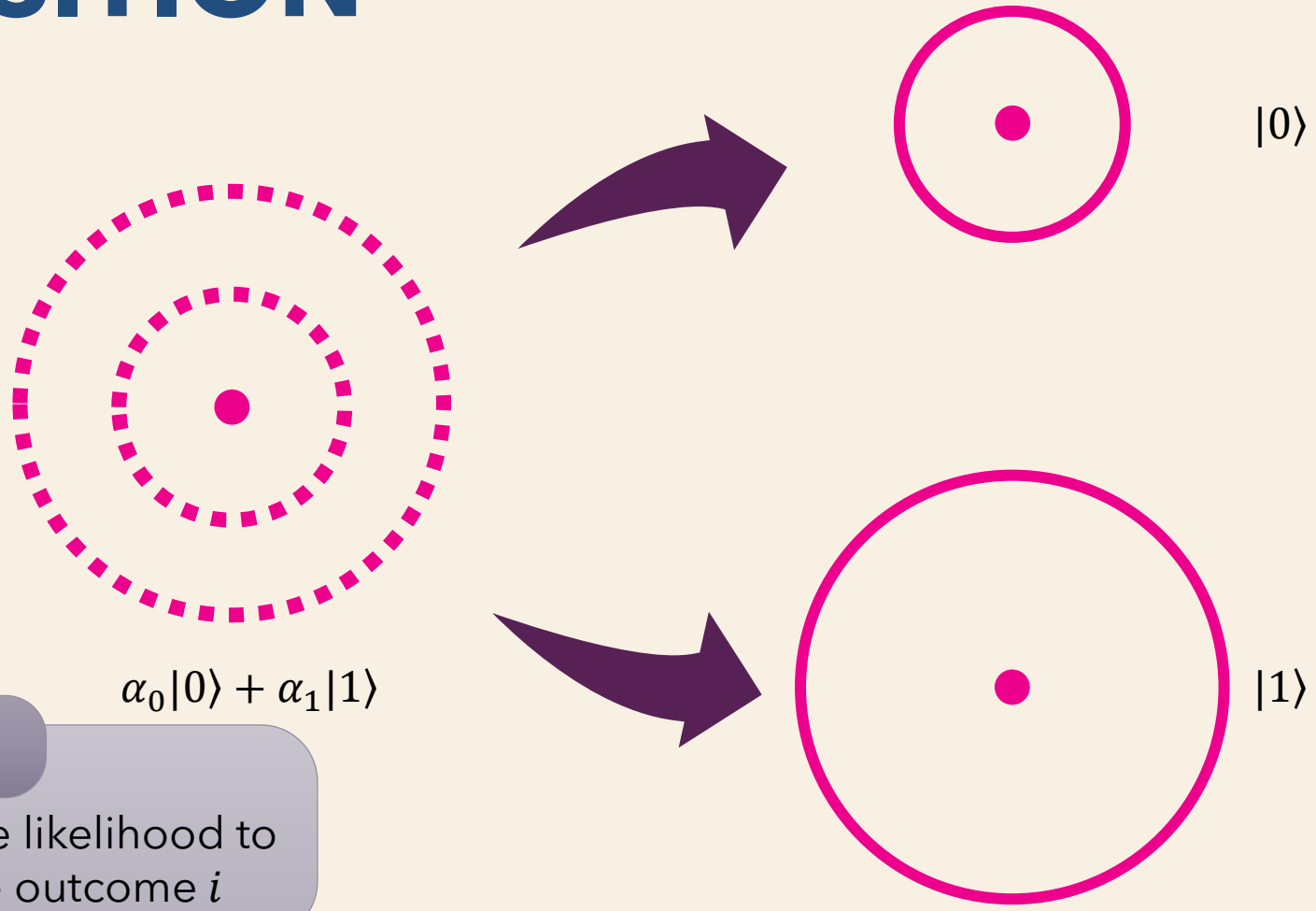
Superposition principle

If a quantum system can be in one of two states, then it can also be in any linear combination of the two possible states

- $\alpha_i \in \mathbb{C}$ is called the amplitude of state $|i\rangle$
- Constraint: $|\alpha_0|^2 + |\alpha_1|^2 = 1$

MEASUREMENT OF A SUPERPOSITION

- Cannot access to amplitudes
- Measurement gives a single bit of information i
- Probability to obtain i is $|\alpha_i|^2$
- The system collapses to a state $|i\rangle$



Note

α_i is the likelihood to have outcome i

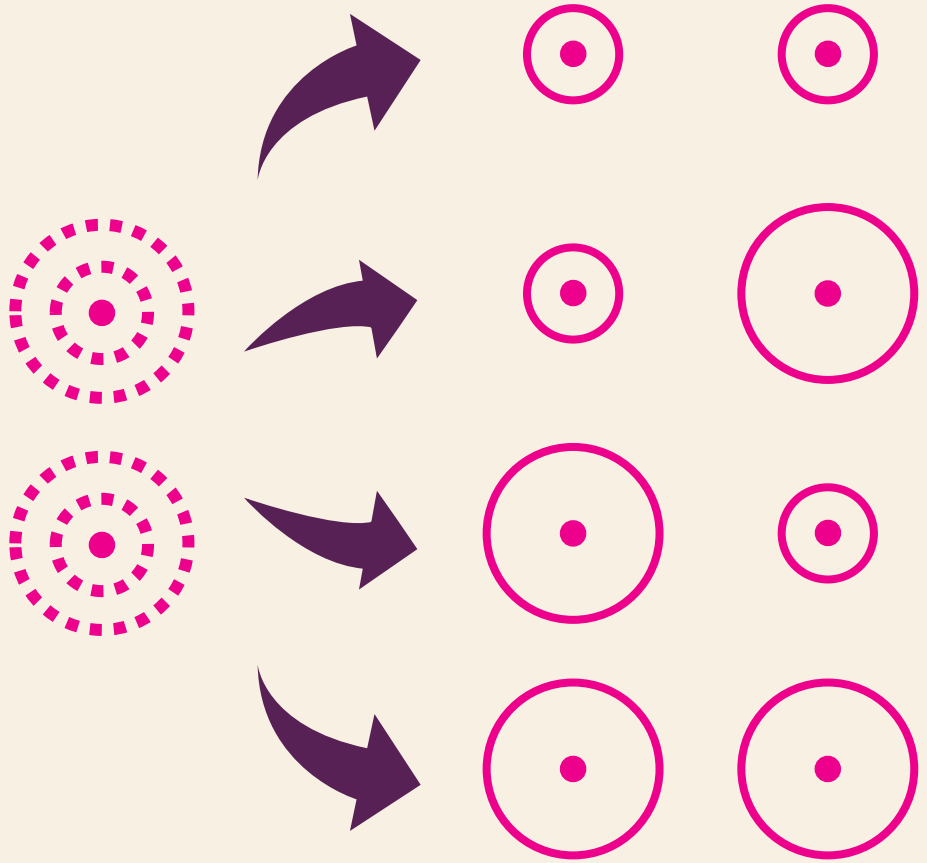
WHAT HAPPENS WITH n QUBITS?

- For simplicity $n = 2$ qubits
- The superposition is a linear combination of the four classical states

$$|\alpha\rangle = \alpha_{00}\,|00\rangle + \alpha_{01}\,|01\rangle + \alpha_{10}\,|10\rangle + \alpha_{11}\,|11\rangle$$

normalized so that $\sum_{x\in\{0,1\}^2}|\alpha_x|^2 = 1$

- The outcome of measurement is two bits jk, with probability $\left|\alpha_{jk}\right|^2$
- The system collapse to state $|jk\rangle$



HOW TO REPRESENT A QUANTUM STATE

Example: Let $n = 2$

$$|\psi\rangle = \begin{bmatrix} \alpha_{00} \\ \alpha_{01} \\ \alpha_{10} \\ \alpha_{11} \end{bmatrix} \in \mathbb{C}^{2^2} = \mathbb{C}^4, \||\psi\rangle\|_2 = 1$$

Notation

We use the symbol $|\cdot\rangle$ to represent a superposition

Fact

An n-qubit state $|\psi\rangle$ is a unit vector in $\mathbb{C}^{2^n}$

Note

i-th value is the amplitude of state $|i\rangle$

HOW TO REPRESENT A QUANTUM STATE

Example: Let $n = 2$

$$|00\rangle = |0\rangle = \begin{bmatrix}1\\0\\0\\0\end{bmatrix}, \qquad |01\rangle = |1\rangle = \begin{bmatrix}0\\1\\0\\0\end{bmatrix},$$

$$|10\rangle = |2\rangle = \begin{bmatrix}0\\0\\1\\0\end{bmatrix}, \qquad |11\rangle = |3\rangle = \begin{bmatrix}0\\0\\0\\1\end{bmatrix}$$

Notation

We use the symbol $|\cdot\rangle$ to represent a superposition

Fact

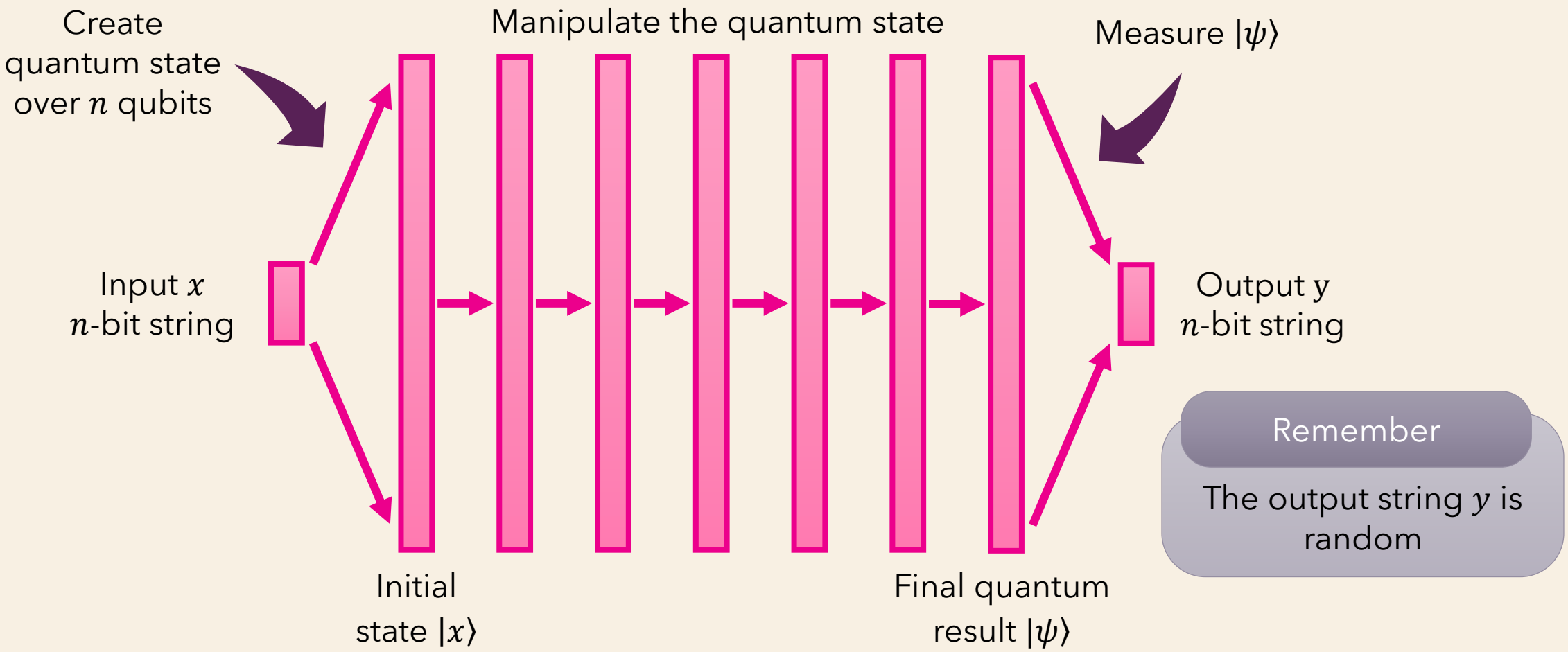
An n-qubit state $|\psi\rangle$ is a unit vector in $\mathbb{C}^{2^n}$

Notation

A basis state $i = 2^0 b_0 + 2^1 b_1 + \cdots + 2^{n-1} b_{n-1}$ can be denoted in binary $|b_{n-1} \ldots b_1 b_0\rangle$ or in decimal notation $|i\rangle$

QUANTUM ALGORITHMS

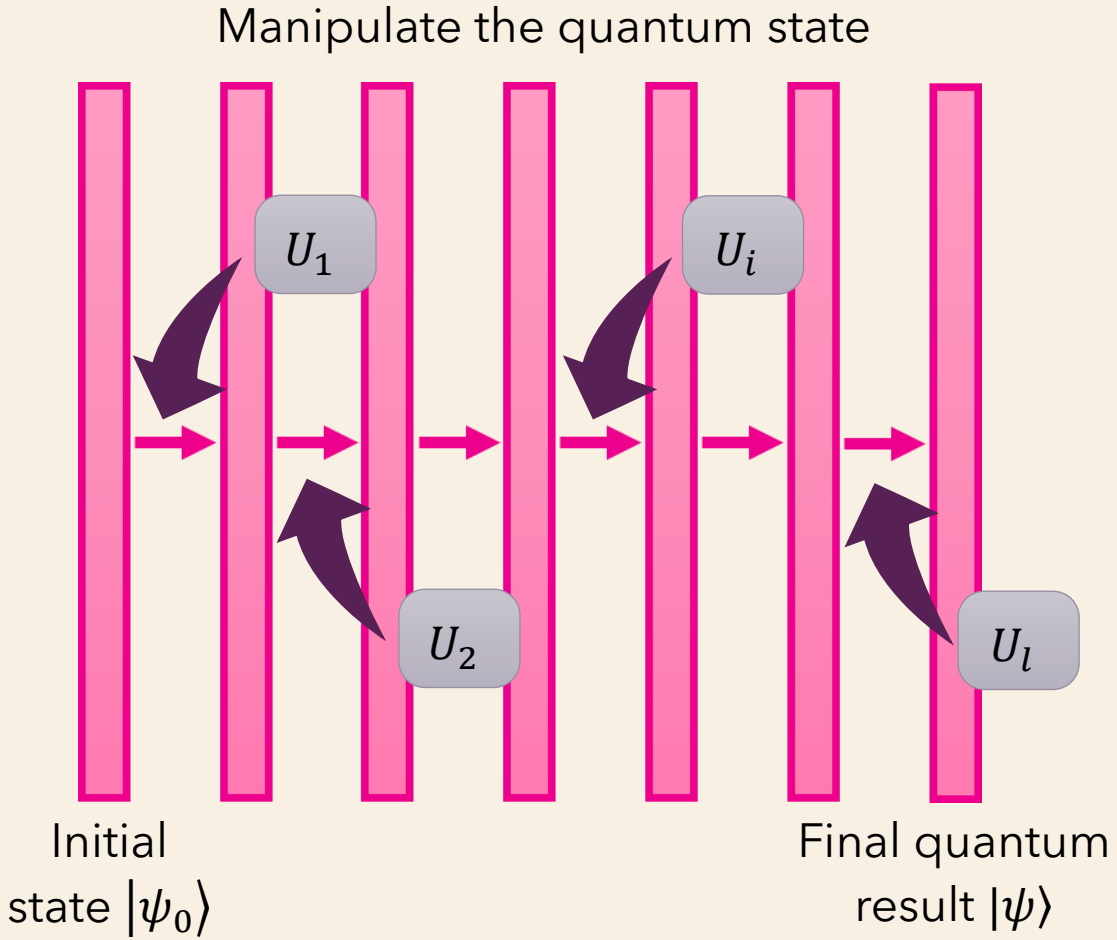
QUANTUM ALGORITHM



Remember

The output string y is random

QUANTUM ALGORITHM



- Apply a finite sequence of gates selected from a finite set
- All gates have an equivalent unitary matrix U_i on $\mathbb{C}^{2^n}$
- Linear transformations that preserve vector length
- The algorithm can be written as

$$|\psi\rangle = U_l U_{l-1} \dots U_1 |\psi_0\rangle$$

- l is the running time of the computation

ELEMENTARY QUANTUM GATES

- Hadamard gate:

$|0\rangle$

$|1\rangle$

$\alpha_0|0\rangle + \alpha_1|1\rangle$

$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$

$\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$

$\frac{\alpha_0 + \alpha_1}{\sqrt{2}}|0\rangle + \frac{\alpha_0 - \alpha_1}{\sqrt{2}}|1\rangle$

Note

Linearity of quantum physics

Equivalent matrix

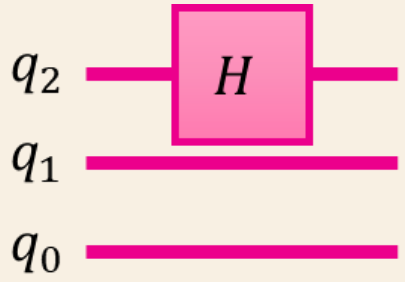
$$\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

APPLY HADAMARD GATE TO ONE OF n QUBITS

- For simplicity $n = 3$, the initial superposition is:

$$\alpha_{000}|000\rangle + \alpha_{001}|001\rangle + \alpha_{010}|010\rangle + \alpha_{011}|011\rangle$$
$$+\alpha_{100}|100\rangle + \alpha_{101}|101\rangle + \alpha_{110}|110\rangle + \alpha_{111}|111\rangle$$

apply the Hadamard gate to only the first qubit:



Equivalent matrix

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 \end{bmatrix}$$

APPLY HADAMARD GATE TO ONE OF n QUBITS

- For simplicity $n = 3$, the initial superposition is:

$$\alpha_{000}|000\rangle + \alpha_{001}|001\rangle + \alpha_{010}|010\rangle + \alpha_{011}|011\rangle$$
$$+\alpha_{100}|100\rangle + \alpha_{101}|101\rangle + \alpha_{110}|110\rangle + \alpha_{111}|111\rangle$$

apply the Hadamard gate to only the first qubit:

$$\frac{\alpha_{000} + \alpha_{100}}{\sqrt{2}}|000\rangle + \frac{\alpha_{001} + \alpha_{101}}{\sqrt{2}}|001\rangle + \frac{\alpha_{010} + \alpha_{110}}{\sqrt{2}}|010\rangle + \frac{\alpha_{011} + \alpha_{111}}{\sqrt{2}}|011\rangle$$
$$+\frac{\alpha_{000} - \alpha_{100}}{\sqrt{2}}|100\rangle + \frac{\alpha_{001} - \alpha_{101}}{\sqrt{2}}|101\rangle + \frac{\alpha_{010} - \alpha_{110}}{\sqrt{2}}|110\rangle + \frac{\alpha_{011} - \alpha_{111}}{\sqrt{2}}|111\rangle$$

Equivalent matrix

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 \end{bmatrix}$$

APPLY HADAMARD GATE TO ONE OF n QUBITS

- For simplicity $n = 3$, the initial superposition is:

$$\alpha_{000}|000\rangle + \alpha_{001}|001\rangle + \alpha_{010}|010\rangle + \alpha_{011}|011\rangle$$
$$+\alpha_{100}|100\rangle + \alpha_{101}|101\rangle + \alpha_{110}|110\rangle + \alpha_{111}|111\rangle$$

apply the Hadamard gate to only the first qubit:

$$\frac{\alpha_{000} + \alpha_{100}}{\sqrt{2}}|000\rangle + \frac{\alpha_{001} + \alpha_{101}}{\sqrt{2}}|001\rangle + \frac{\alpha_{010} + \alpha_{110}}{\sqrt{2}}|010\rangle + \frac{\alpha_{011} + \alpha_{111}}{\sqrt{2}}$$
$$+\frac{\alpha_{000} - \alpha_{100}}{\sqrt{2}}|100\rangle + \frac{\alpha_{001} - \alpha_{101}}{\sqrt{2}}|101\rangle + \frac{\alpha_{010} - \alpha_{110}}{\sqrt{2}}|110\rangle + \frac{\alpha_{011} - \alpha_{111}}{\sqrt{2}}|111\rangle$$

Equivalent matrix

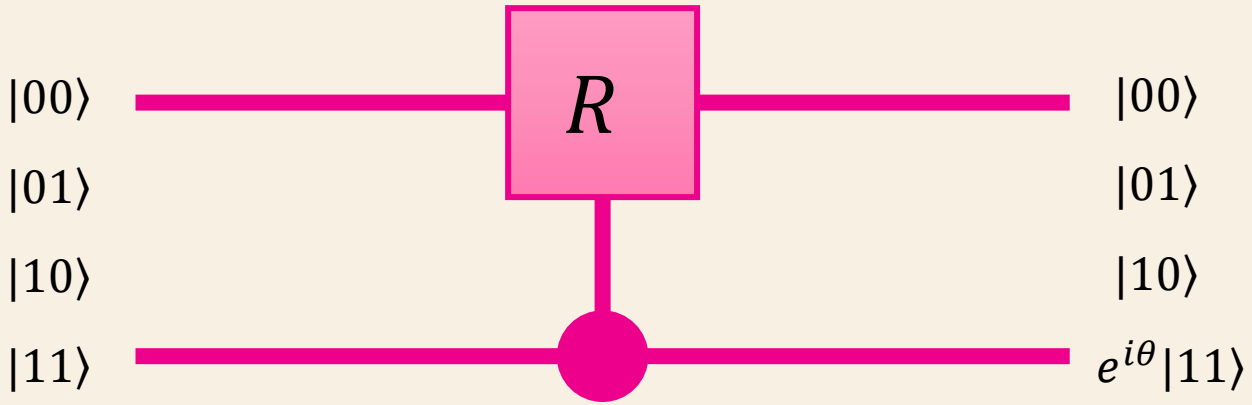
$$\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 & & & & \end{bmatrix}$$

Note

Pair up the states of the form $0x$ and $1x$

ELEMENTARY QUANTUM GATES

- Controlled phase gate:



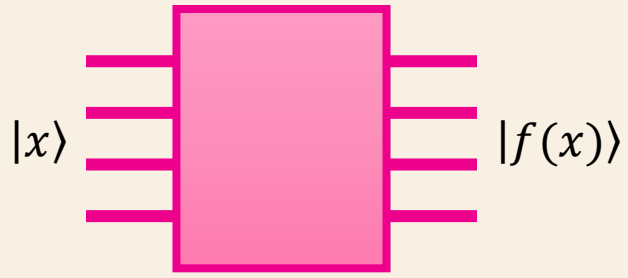
Equivalent matrix

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\theta} \end{bmatrix}$$

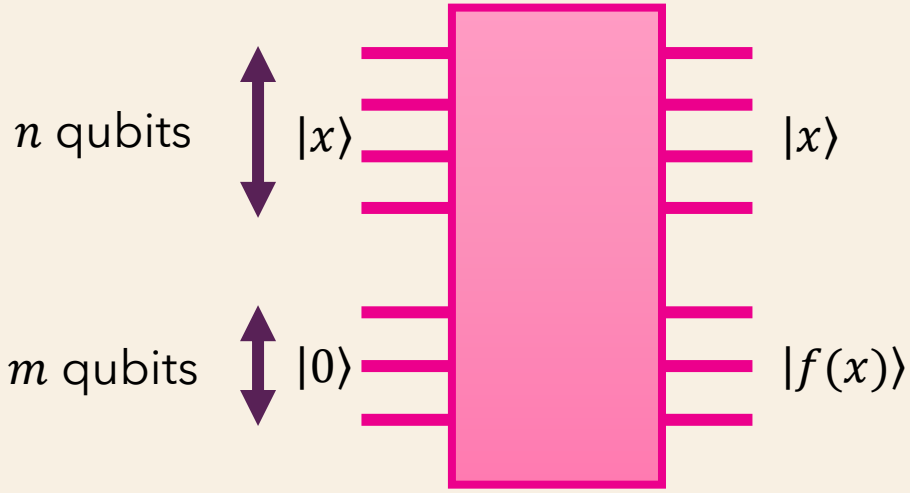
QUANTUM CIRCUITS

- All gates are unitary matrices

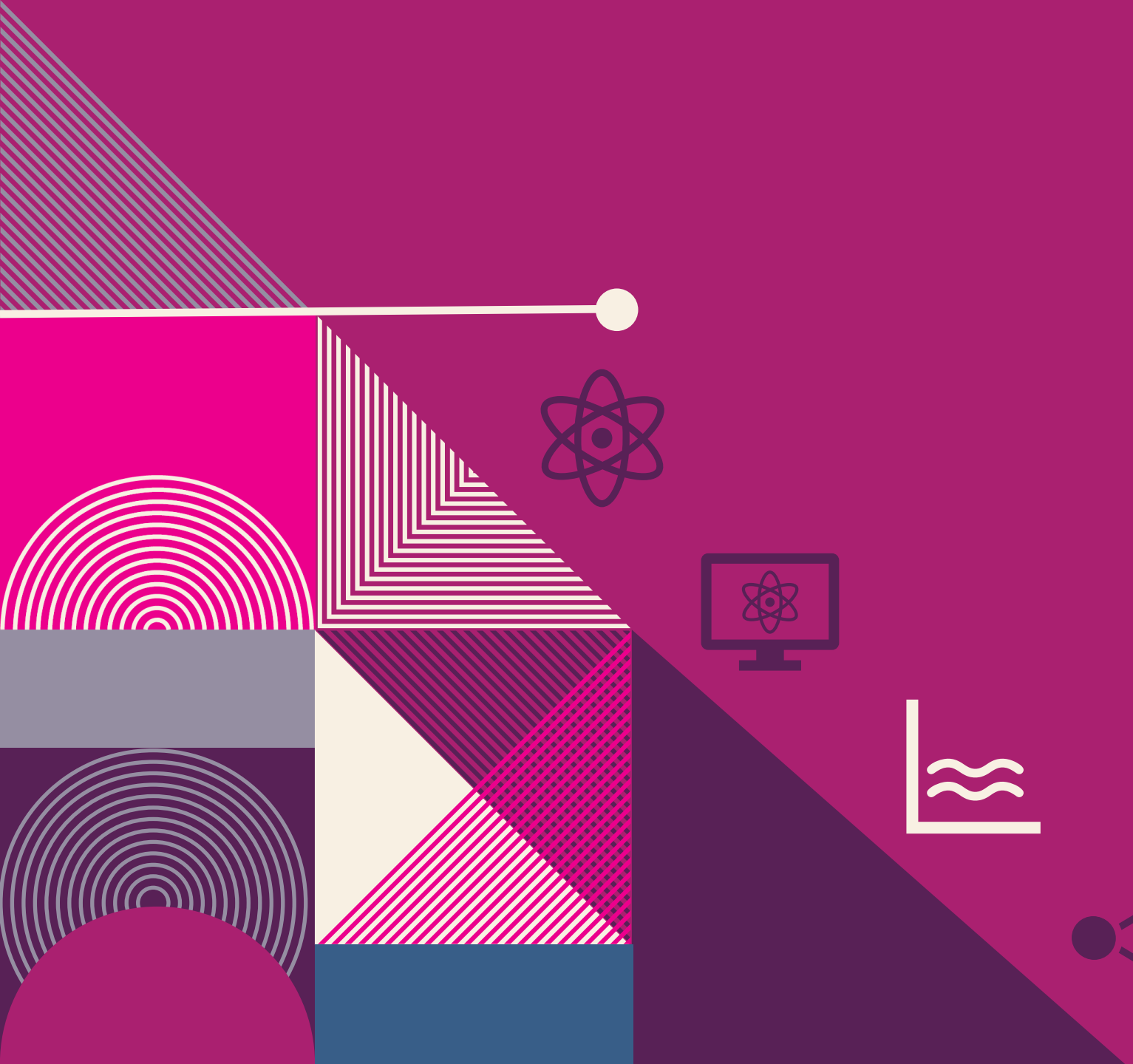
Same number of input and output qubits



Same number of input and output qubits



General approach



QUANTUM FOURIER TRANSFORM

DISCRETE FOURIER TRANSFORM

- Fourier Transform maps a signal from time domain to frequency domain

Discrete Fourier Transform

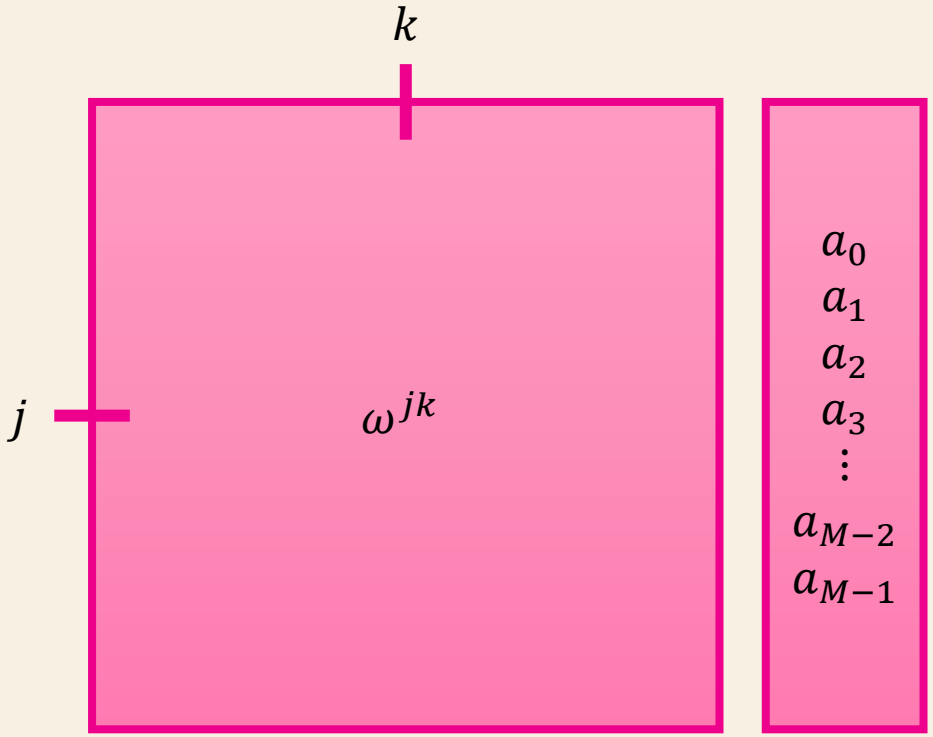
Let $M = 2^m$, the DFT $b \in \mathbb{C}^M$ of a discrete signal $a \in \mathbb{C}^M$ is

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ \vdots \\ b_{M-1} \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \omega & \omega^2 & \dots & \omega^{M-1} \\ 1 & \omega^2 & \omega^4 & \dots & \omega^{2(M-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{M-1} & \omega^{2(M-1)} & \dots & \omega^{(M-1)(M-1)} \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_{M-1} \end{bmatrix}$$

where $\omega = e^{i2\pi/M}$ is a complex M-th root of unity

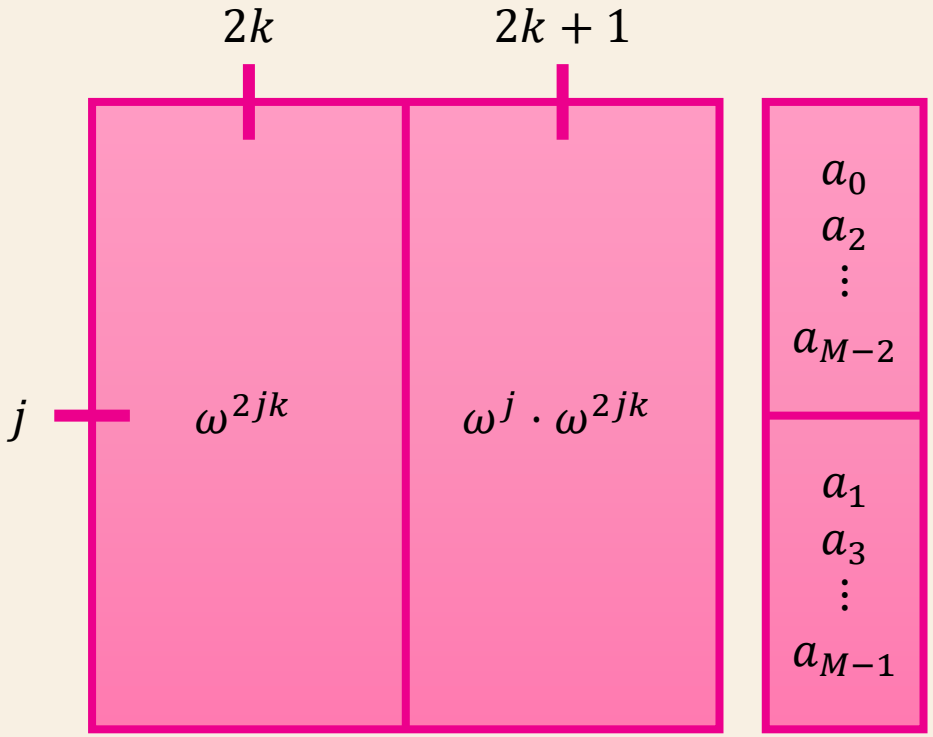
DISCRETE FOURIER TRANSFORM

- Divide-and-conquer strategy on matrix F_M



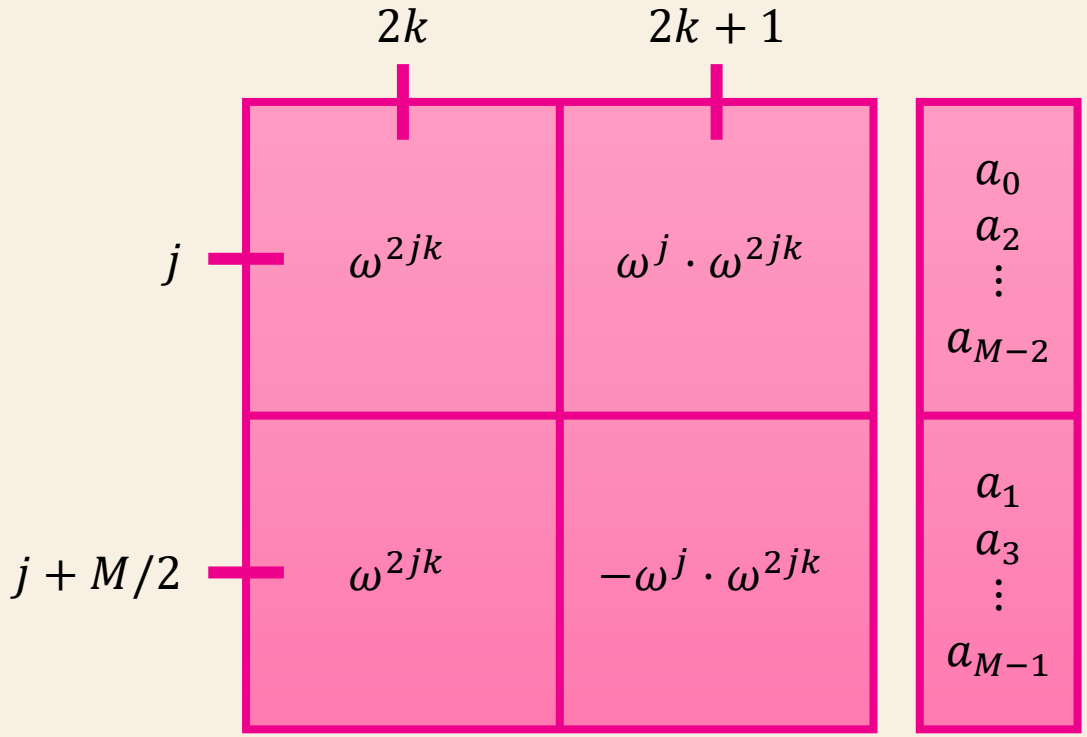
DISCRETE FOURIER TRANSFORM

- Divide-and-conquer strategy on matrix F_M
- Divide columns by evens and odds



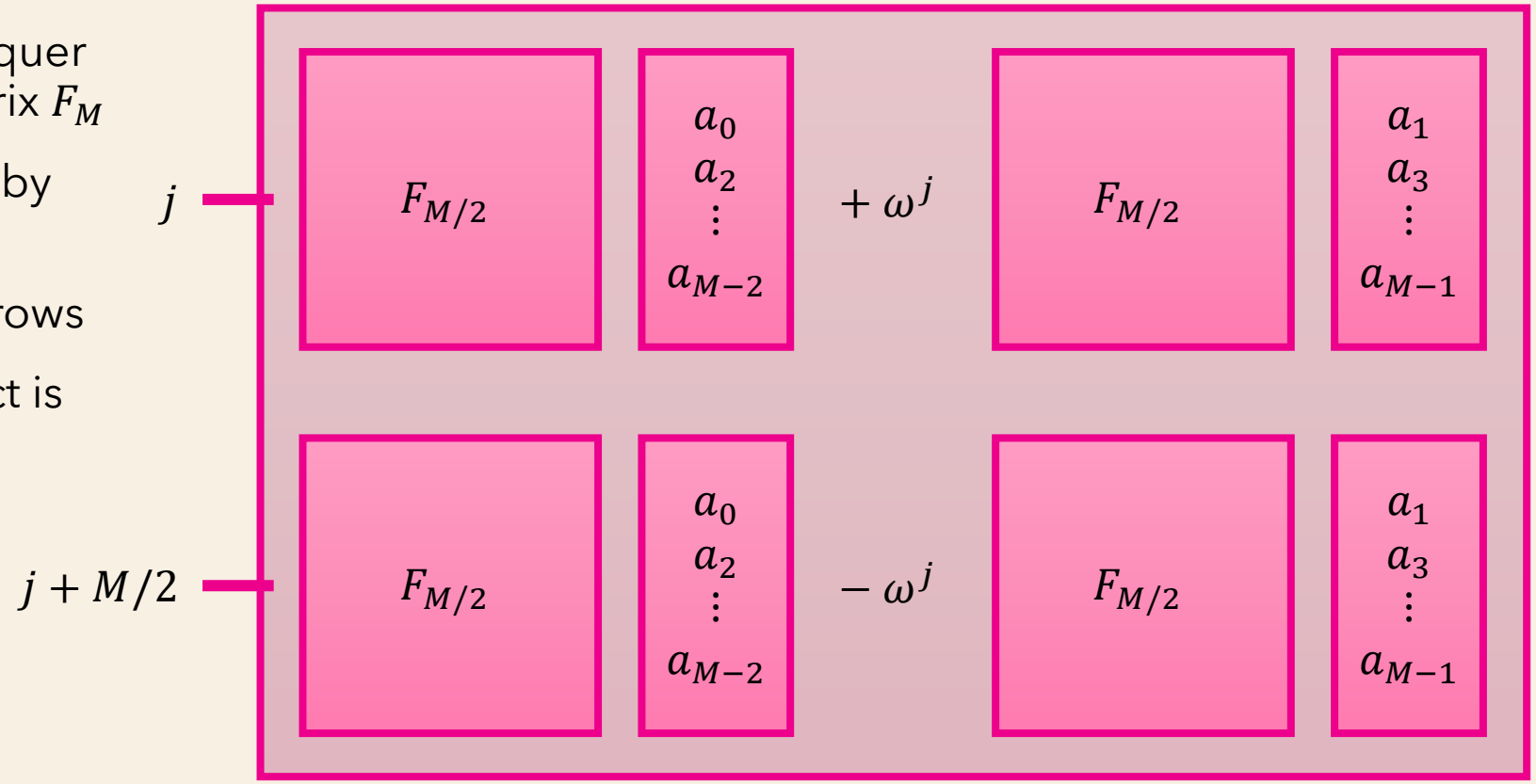
DISCRETE FOURIER TRANSFORM

- Divide-and-conquer strategy on matrix F_M
- Divide columns by evens and odds
- Divide also the rows



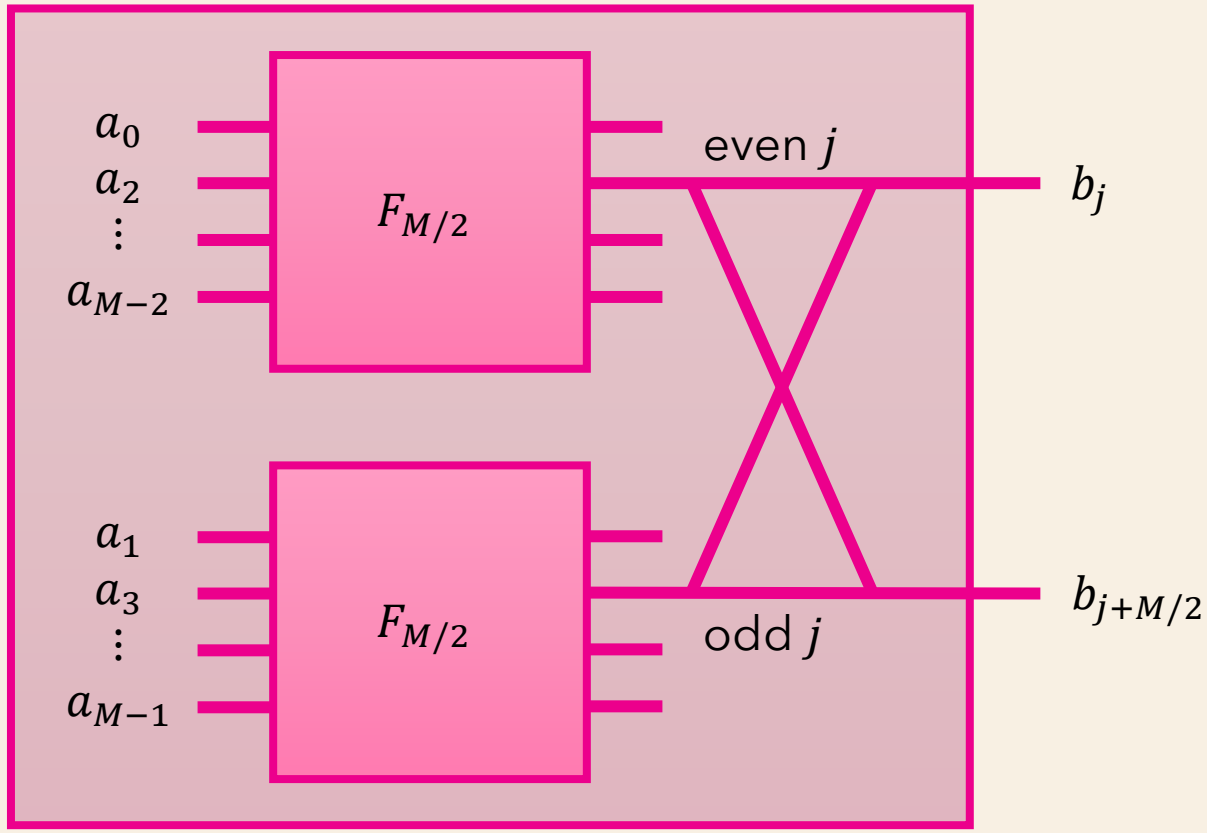
DISCRETE FOURIER TRANSFORM

- Divide-and-conquer strategy on matrix F_M
- Divide columns by evens and odds
- Divide also the rows
- The final product is the vector



DISCRETE FOURIER TRANSFORM

- Divide-and-conquer strategy on matrix F_M
- Divide columns by evens and odds
- Divide also the rows
- The final product is the vector
- The equivalent circuit



QUANTUM FOURIER TRANSFORM

Quantum Fourier Transform

Given a superposition $|\alpha\rangle$ over $m = \log_2 M$ qubits, the QFT $|\beta\rangle$ of $|a\rangle$ is

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

where $\omega = e^{i2\pi/M}$ is a complex M-th root of unity

QUANTUM FOURIER TRANSFORM

Quantum Fourier Transform

Given a superposition $|\alpha\rangle$ over $m = \log_2 M$ qubits, the QFT $|\beta\rangle$ of $|a\rangle$ is

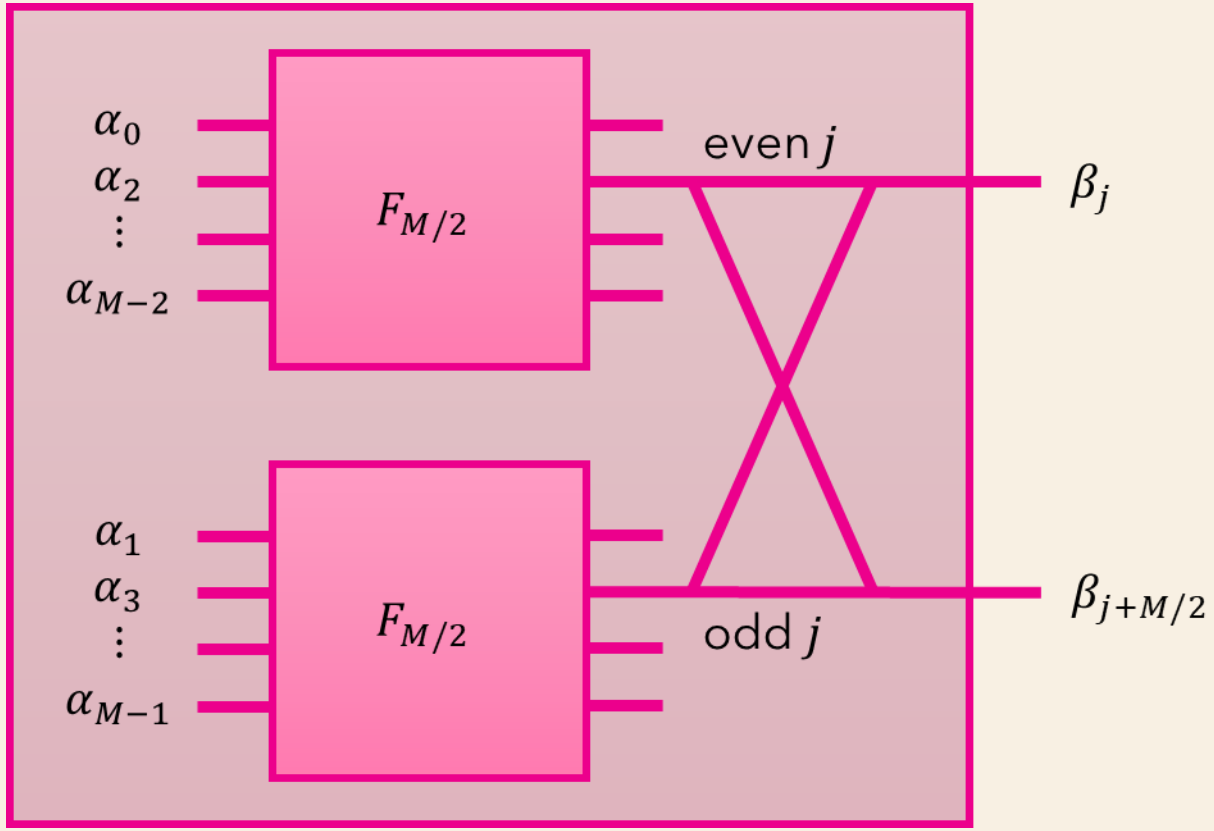
$$\begin{bmatrix} \beta_0 \\ \beta_1 \\ \beta_2 \\ \vdots \\ \beta_{M-1} \end{bmatrix} = \frac{1}{\sqrt{M}} \begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \omega & \omega^2 & \dots & \omega^{M-1} \\ 1 & \omega^2 & \omega^4 & \dots & \omega^{2(M-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{M-1}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

where $\omega = e^{i2\pi/M}$ is a complex M-th ro

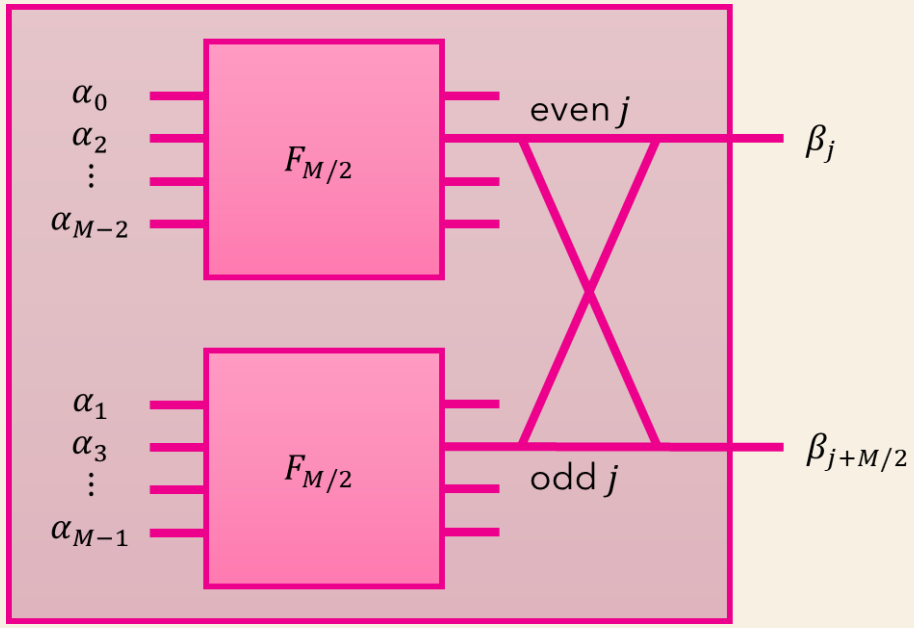
Quantum Fourier Sampling

The output is superposition of $m = \log_2 M$ qubits:
we can only access to the index of one component

QUANTUM FOURIER TRANSFORM

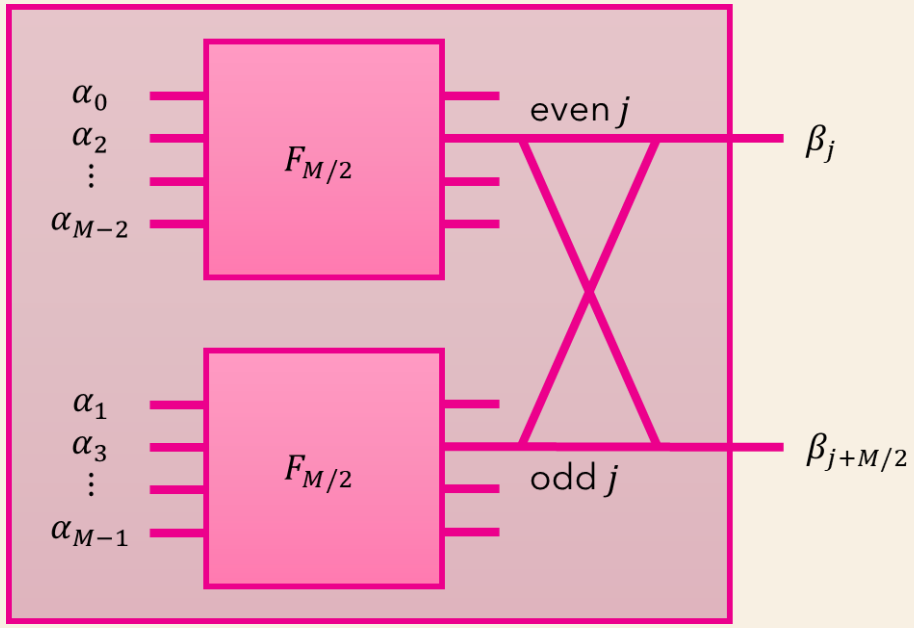


QUANTUM FOURIER TRANSFORM

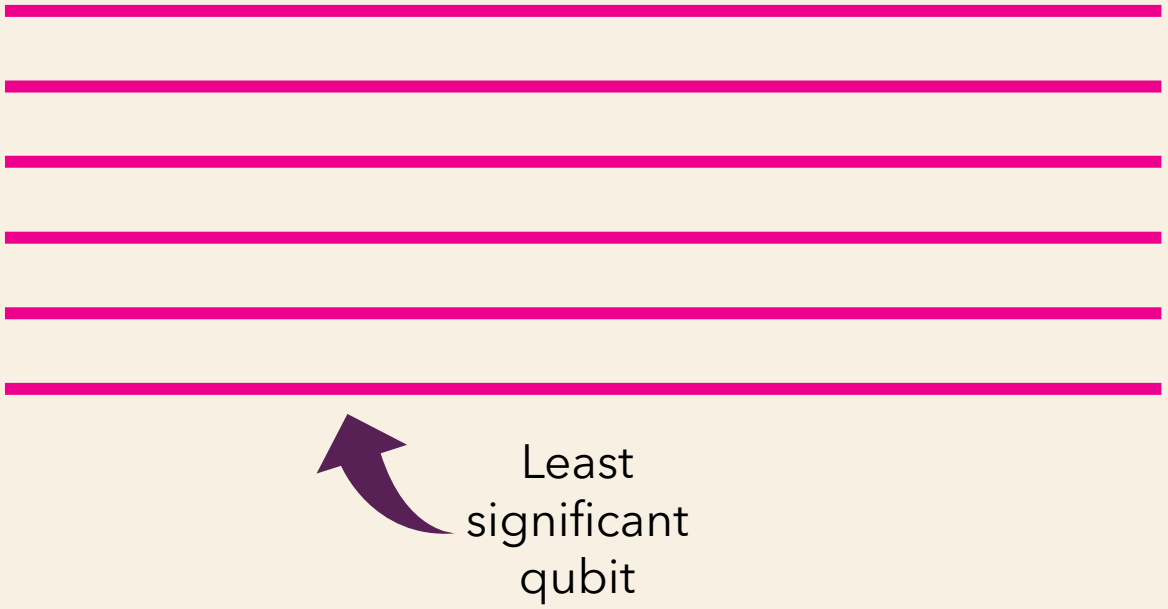


- Same number of input and output qubits

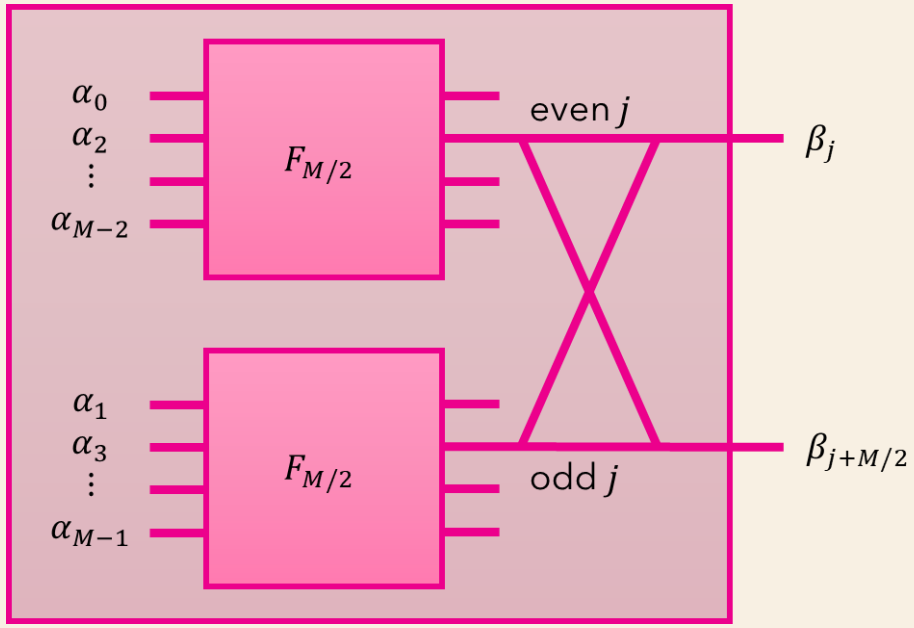
QUANTUM FOURIER TRANSFORM



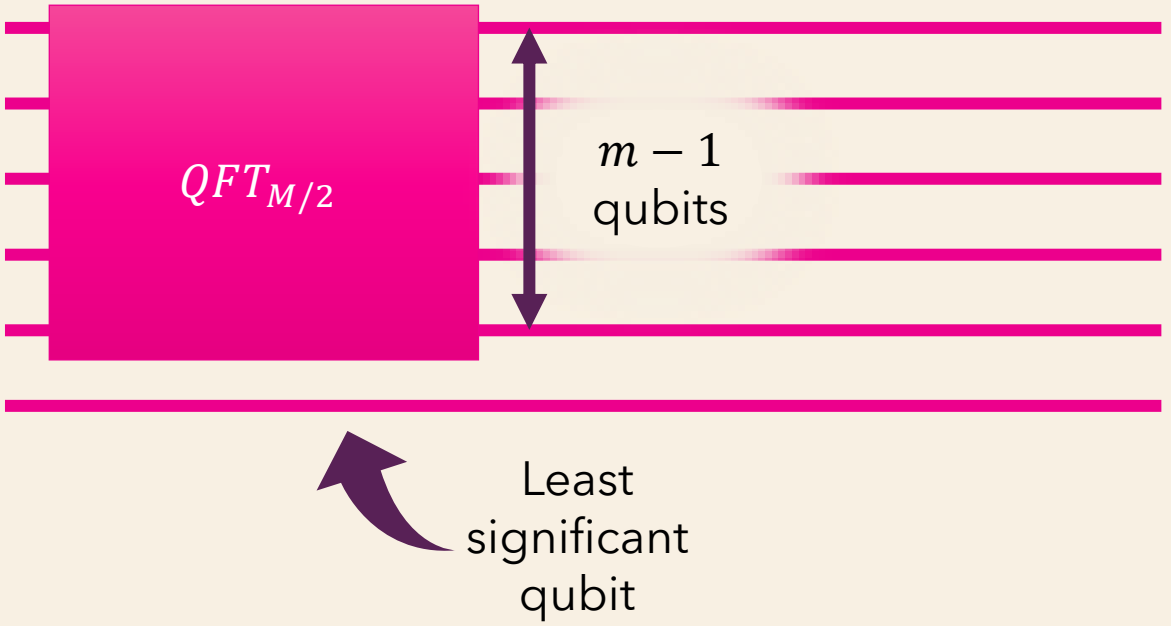
- Decompose the inputs into evens and odds



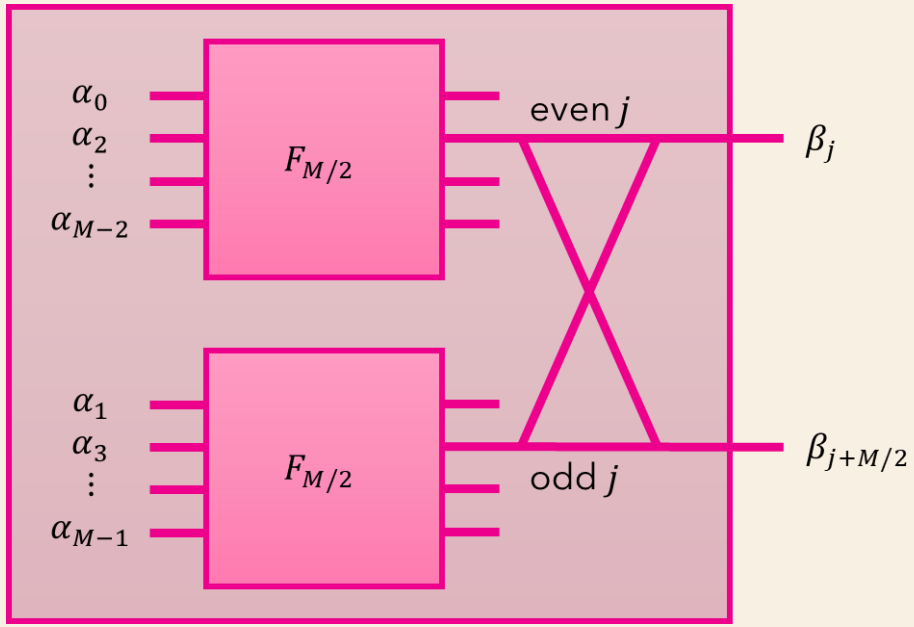
QUANTUM FOURIER TRANSFORM



- Apply the recursive circuits



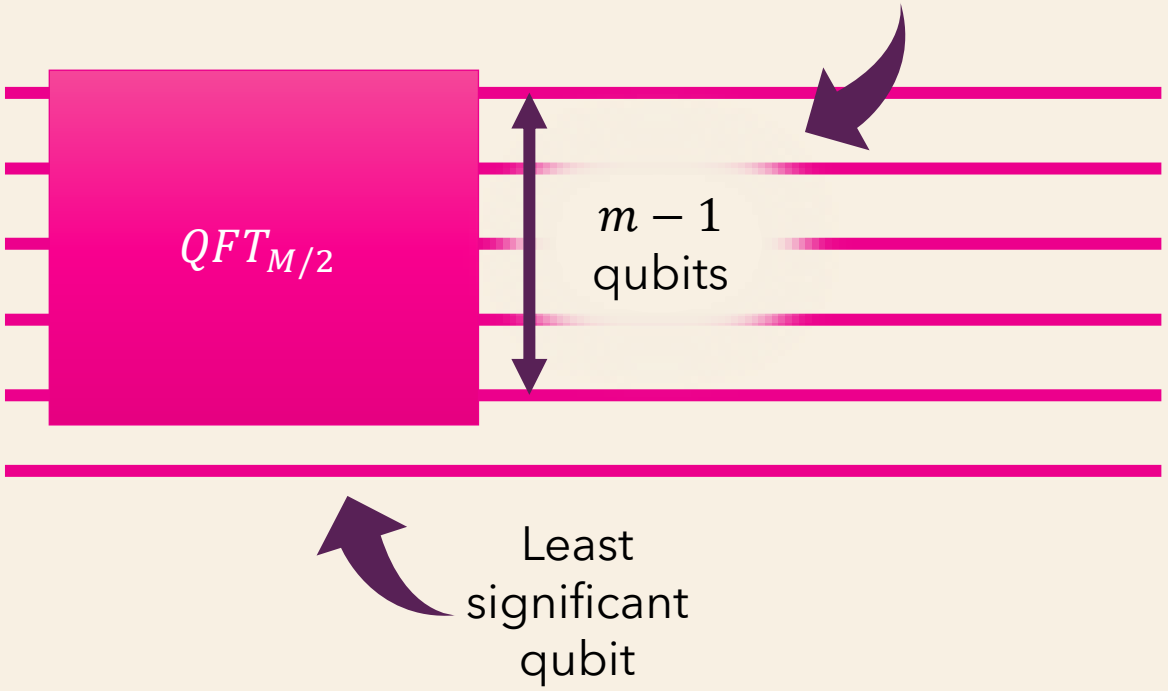
QUANTUM FOURIER TRANSFORM



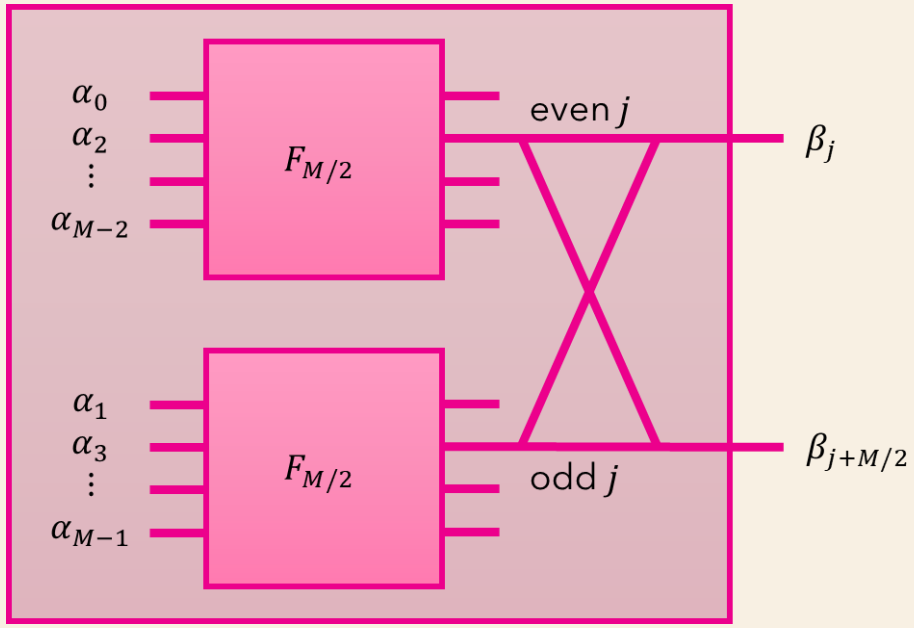
- Apply th

Note

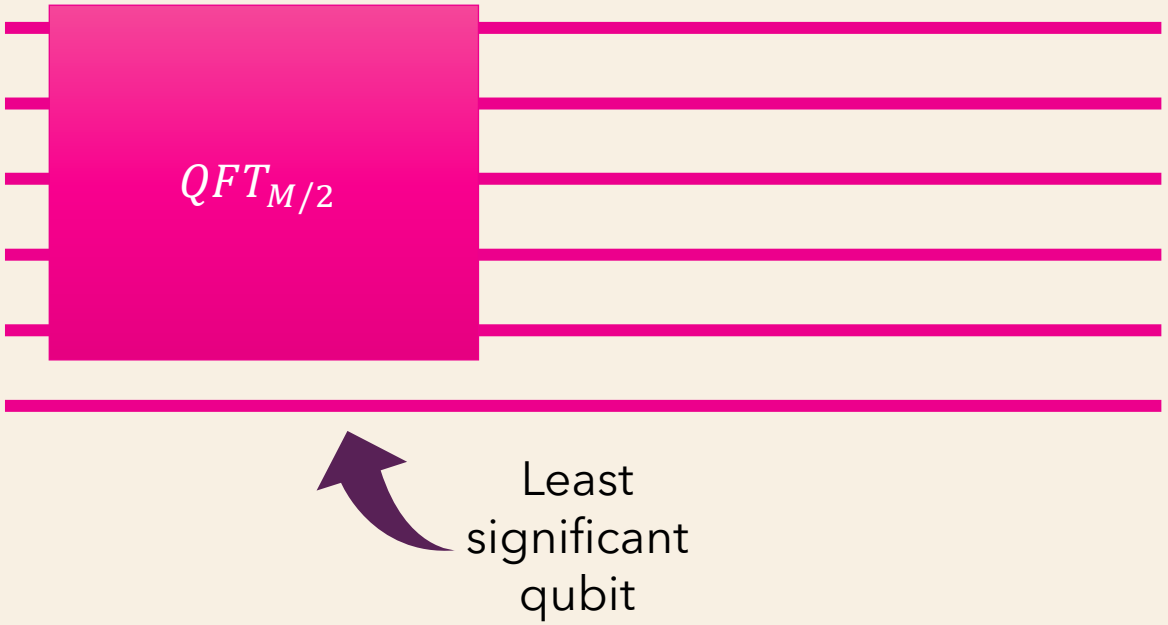
Apply $QFT_{M/2}$ to the superposition of all states of the form $x0$ independently of the superposition of all states of the form $x1$



QUANTUM FOURIER TRANSFORM



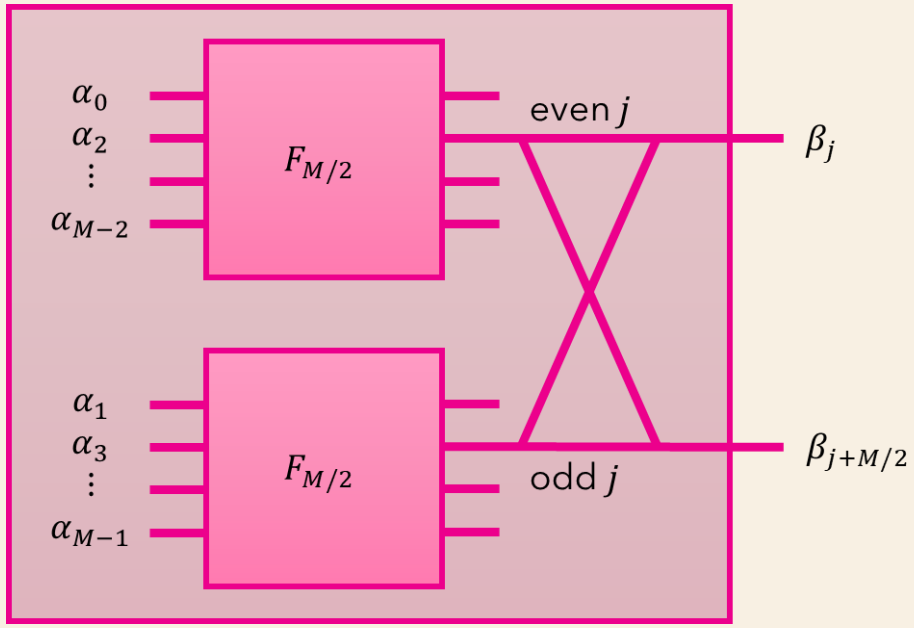
- Apply the phase ω^j to the odd j-th value
- If $j = j_1 \ldots j_{m-1}$, then $\omega^j = \prod_{l=1}^{m-1} \omega^{j_l 2^{m-l}}$



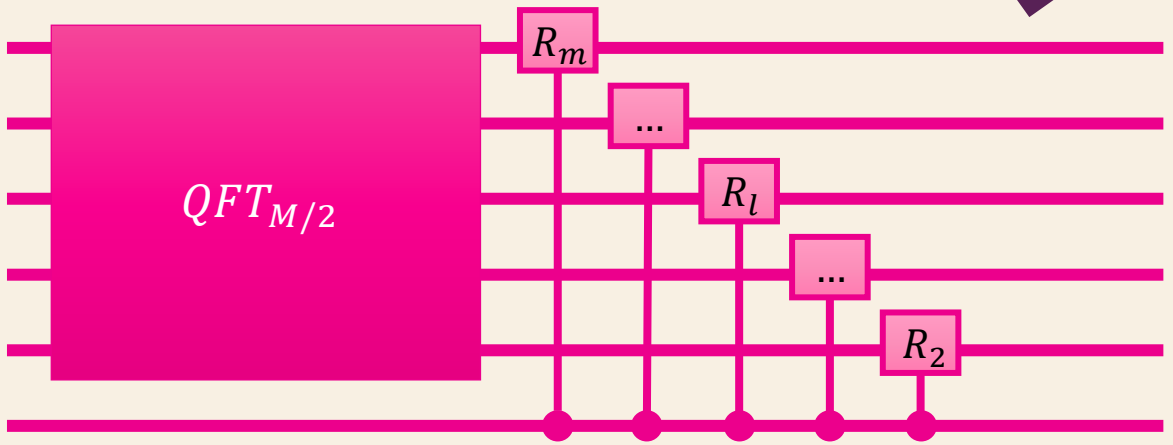
QUANTUM FOURIER

R_p matrix

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{2\pi i/2^p} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \omega^{2^{m-p}} \end{bmatrix}$$

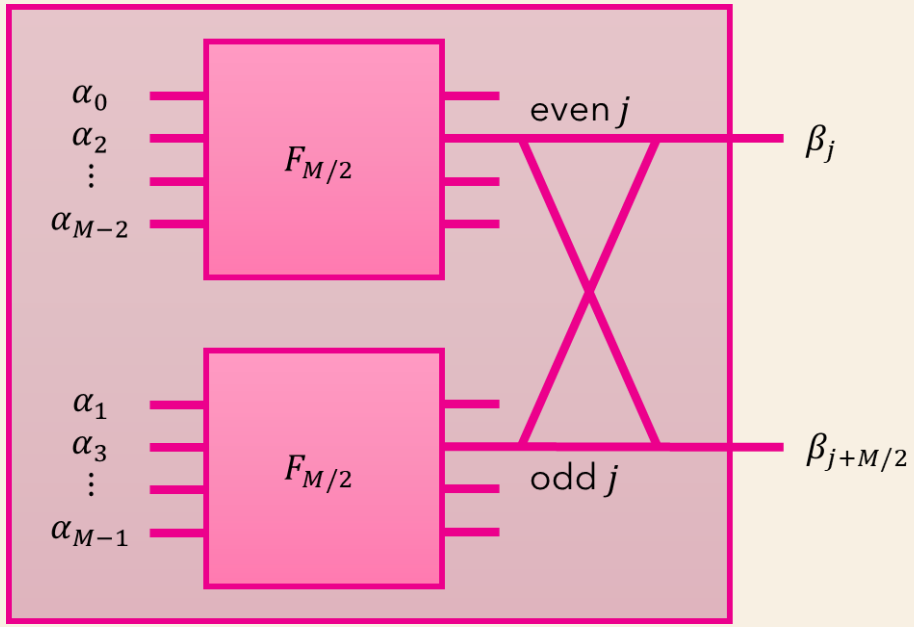


- Apply the phase ω^j to the odd j-th value
- If $j = j_1 \ldots j_{m-1}$, then $\omega^j = \prod_{l=1}^{m-1} \omega^{j_l 2^{m-l}}$

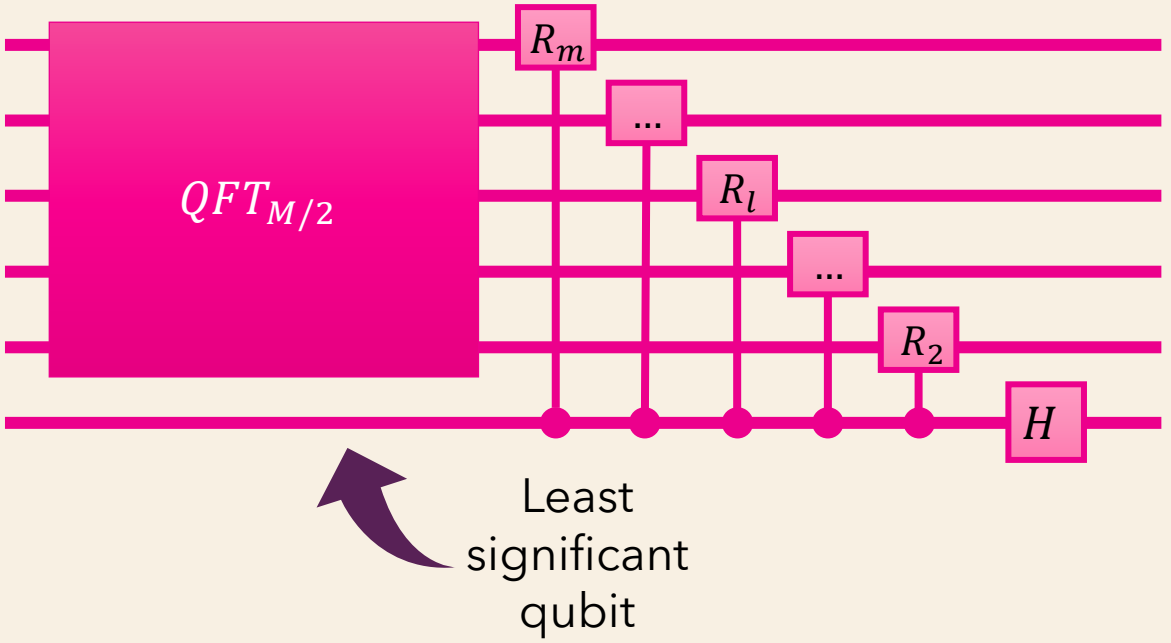


Least significant qubit

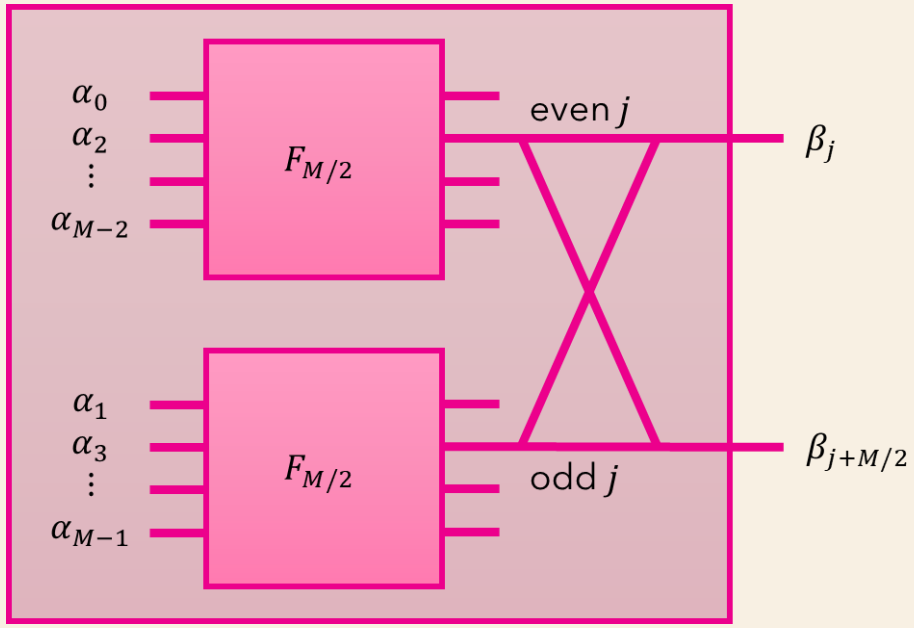
QUANTUM FOURIER TRANSFORM



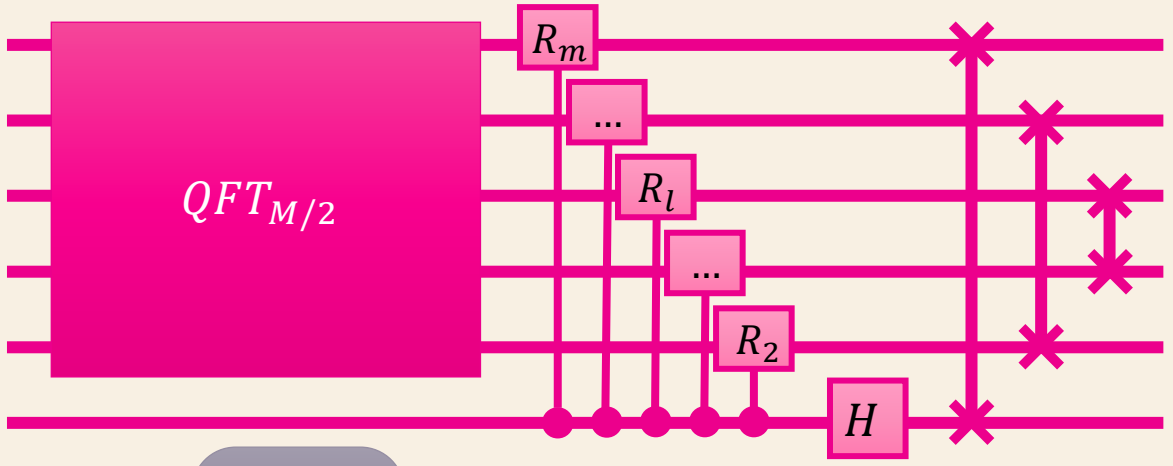
- Add and subtract even j-th and odd j-th values to obtain the j-th and the $(M/2 + j)$-th outputs



QUANTUM FOURIER TRANSFORM



- Swap exchanges to restore the required state order



Note

Amplitudes associated with states in bit reversal

QUANTUM FOURIER TRANSFORM

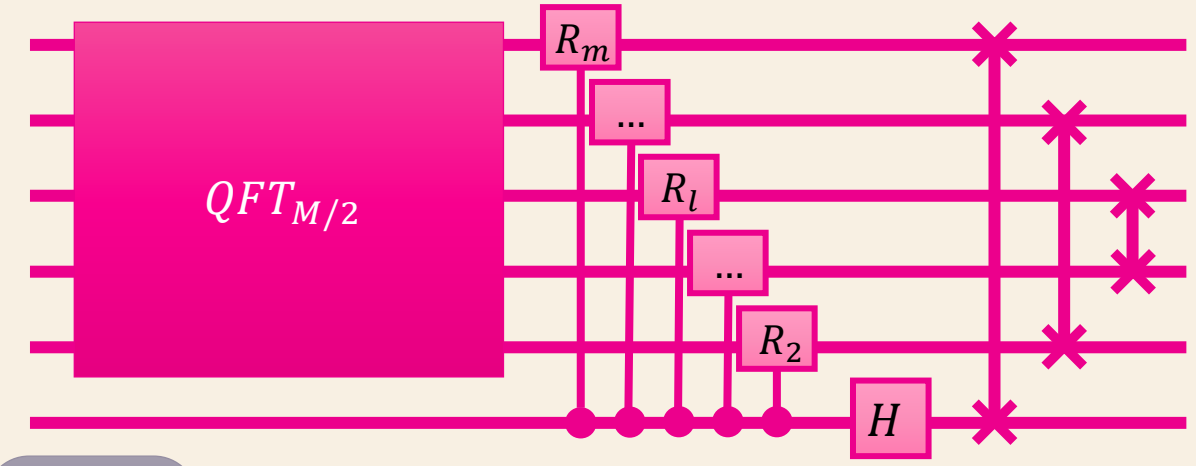
- Time complexity:

$$T_r(m) = \begin{cases} T_r(m-1) + m & \text{if } m > 1 \\ 1 & \text{if } m = 1 \end{cases}$$

$$T_r(m) = O(m^2)$$

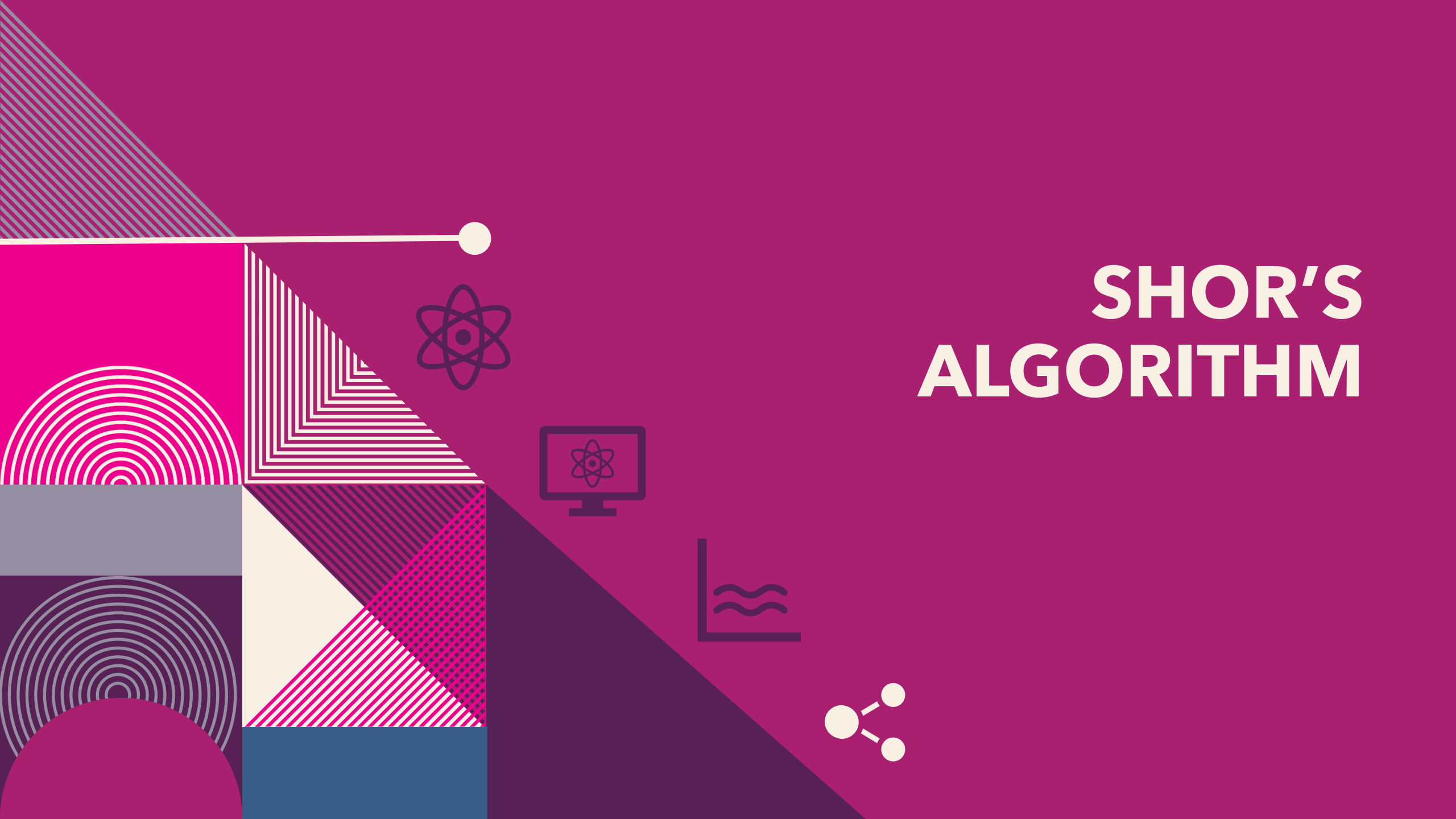
$$T_s(m) = m/2$$

$$T(m) = T_r(m) + T_s(m) = O(m^2)$$



Note

Exponential speed up: $O(M \log M) = O(m\, 2^m)$



SHOR'S ALGORITHM

REDUCTIONS FOR SHOR'S ALGORITHM

Problem

Factoring a large integer N

Finding a nontrivial square root of 1 modulo N

Computing the order of a random integer modulo N

The order of an integer is the period of a particular periodic superposition

Periods of superpositions can be found by the QFT

FACTORING AS ROOT FINDING

- Factoring a large integer N is reduced to finding a nontrivial square root of $1\ mod\ N$

Nontrivial square root of $1\ mod\ N$

Any integer $x \not\equiv \pm 1\ mod\ N$ such that $x^2 \equiv 1\ mod\ N$

Lemma

If x is a nontrivial square root of $1\ mod\ N$, then $\gcd(x+1, N)$ is a nontrivial factor of N

ROOT FINDING AS ORDER FINDING

- Finding such a root is reduced to computing the order of a random integer modulo N

Order of $x \ mod \ N$

The smallest positive integer r such that $x^r \equiv 1 \ mod \ N$

Lemma

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

ORDER FINDING AS PERIODICITY

- The order of an integer is the period of a particular periodic superposition

Order of $x \ mod \ N$

The smallest positive integer r such that $x^r \equiv 1 \ mod \ N$

- r is the period of function $f(a) = x^a \ mod \ N$

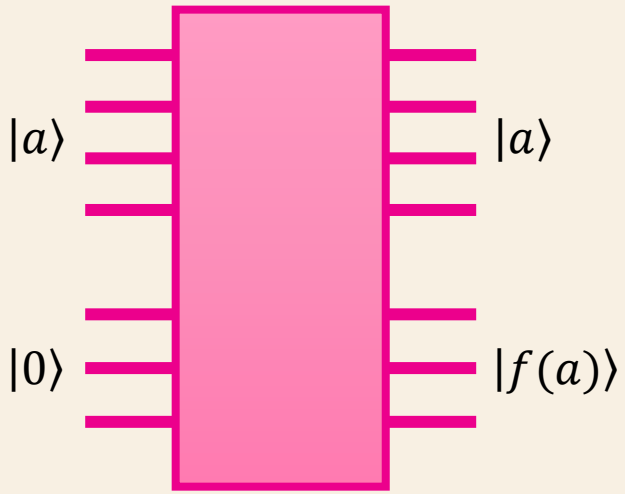
Periodic superposition

Given the superposition $\sum_{a=0}^{M-1} \frac{1}{\sqrt{M}} |a, f(a)\rangle$, the measurement of the second register makes the first register being in a periodic superposition with period r

ORDER FINDING AS PERIODICITY

Periodic superposition

Given the superposition $\sum_{a=0}^{M-1} \frac{1}{\sqrt{M}} |a, f(a)\rangle$, the measurement of the second register makes the first register being in a periodic superposition with period r



- Initial superposition (ignoring the coefficient)

$$|0, f(0)\rangle + |1, f(1)\rangle + \ ... + |M-1, f(M-1)\rangle$$

since r is the period of function $f(a)$

$$|0, f(0)\rangle + |1, f(1)\rangle + \ ... + |r-1, f(r-1)\rangle$$
$$+ |r, f(0)\rangle + |r+1, f(1)\rangle + \ ... + |2r-1, f(r-1)\rangle + \ ...$$

- Superposition after reading the second register

$$|k, f(k)\rangle + |k+r, f(k)\rangle + |k+2r, f(k)\rangle + \ ...$$

FIND THE PERIOD OF A PERIODIC SUPERPOSITION

- Periods of superpositions can be found by the QFT

Periodic superposition

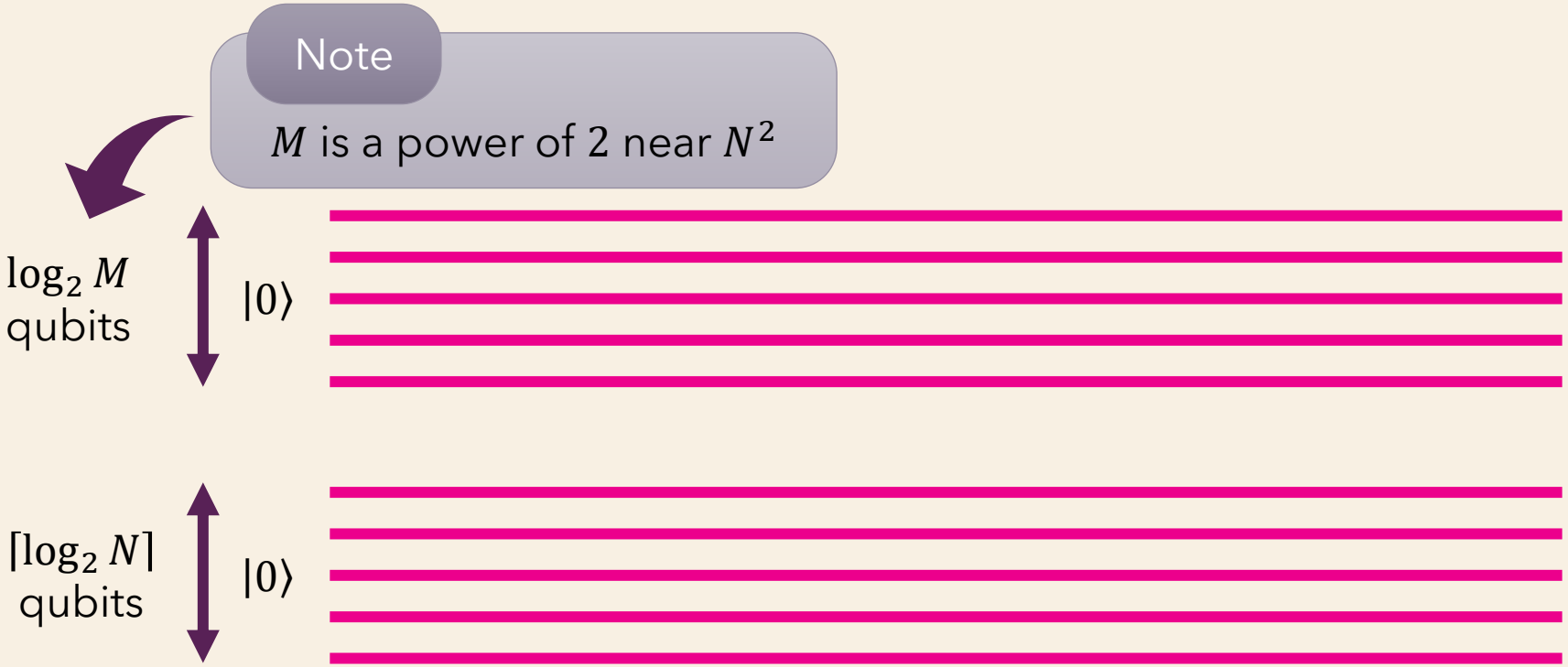
A superposition $|\alpha\rangle = (\alpha_0, \alpha_1, \dots, \alpha_{M-1})$ is periodic (with period r) if $\alpha_i = \alpha_j$ for each $i \equiv j \; mod \; r$

QFT of a periodic superposition

Given a periodic superposition $|\alpha\rangle$ with period r, $|\alpha\rangle = \sqrt{\frac{r}{M}} \sum_{j=0}^{M/r-1} |k + jr\rangle$, $k \in [0, r-1]$

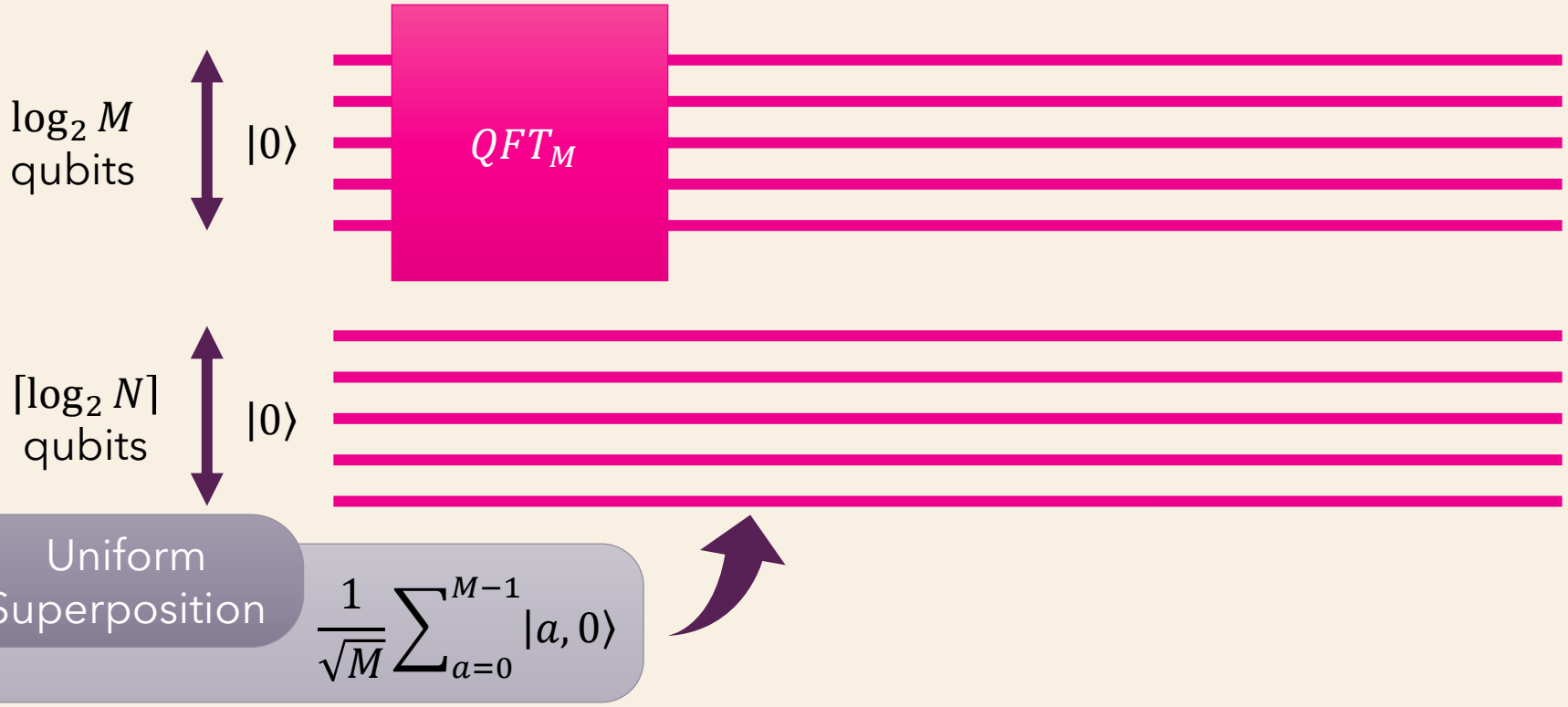
Its Fourier transform $|\beta\rangle$ is periodic with period M/r, $|\beta\rangle = \frac{1}{\sqrt{r}} \sum_{j=0}^{r-1} \omega^{kjM/r} \left|\frac{jM}{r}\right\rangle$

QUANTUM ALGORITHM FOR FACTORING A LARGE INTEGER N



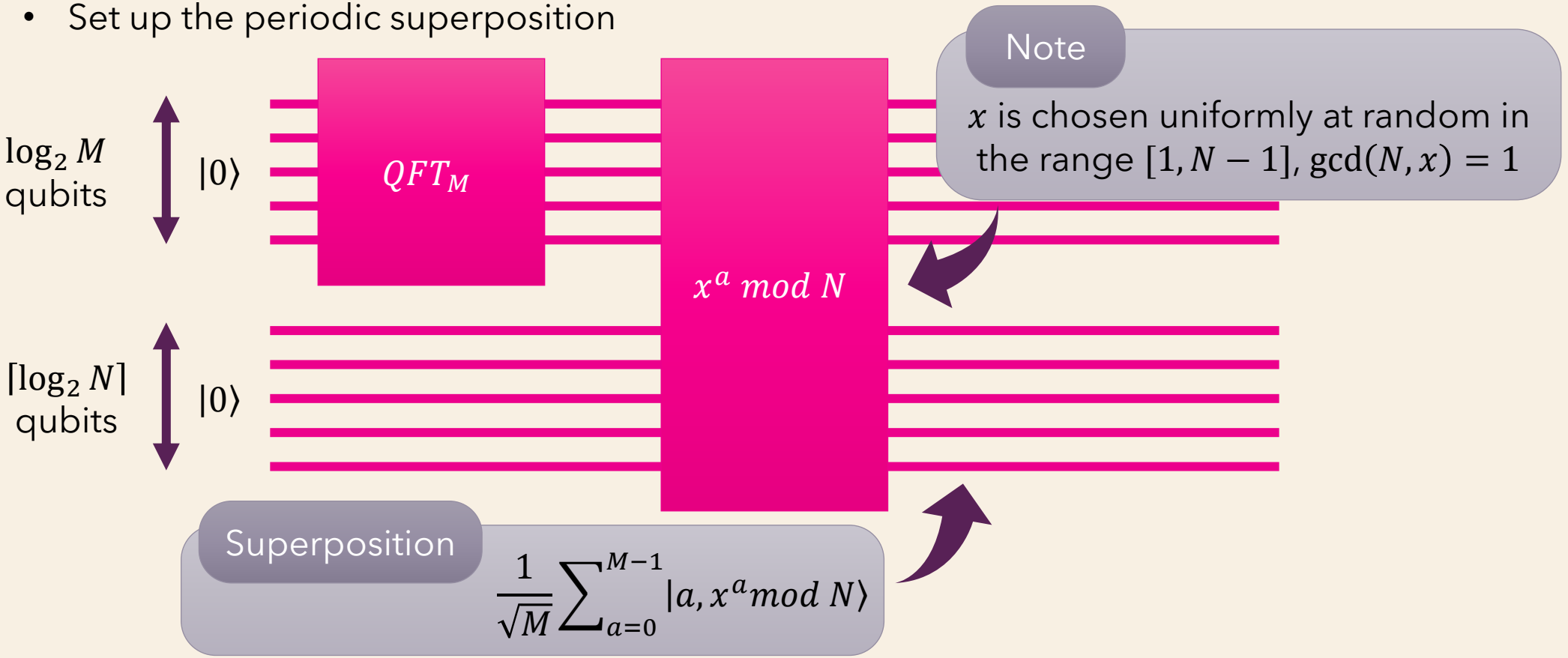
QUANTUM ALGORITHM FOR FACTORING A LARGE INTEGER N

- Set up the periodic superposition



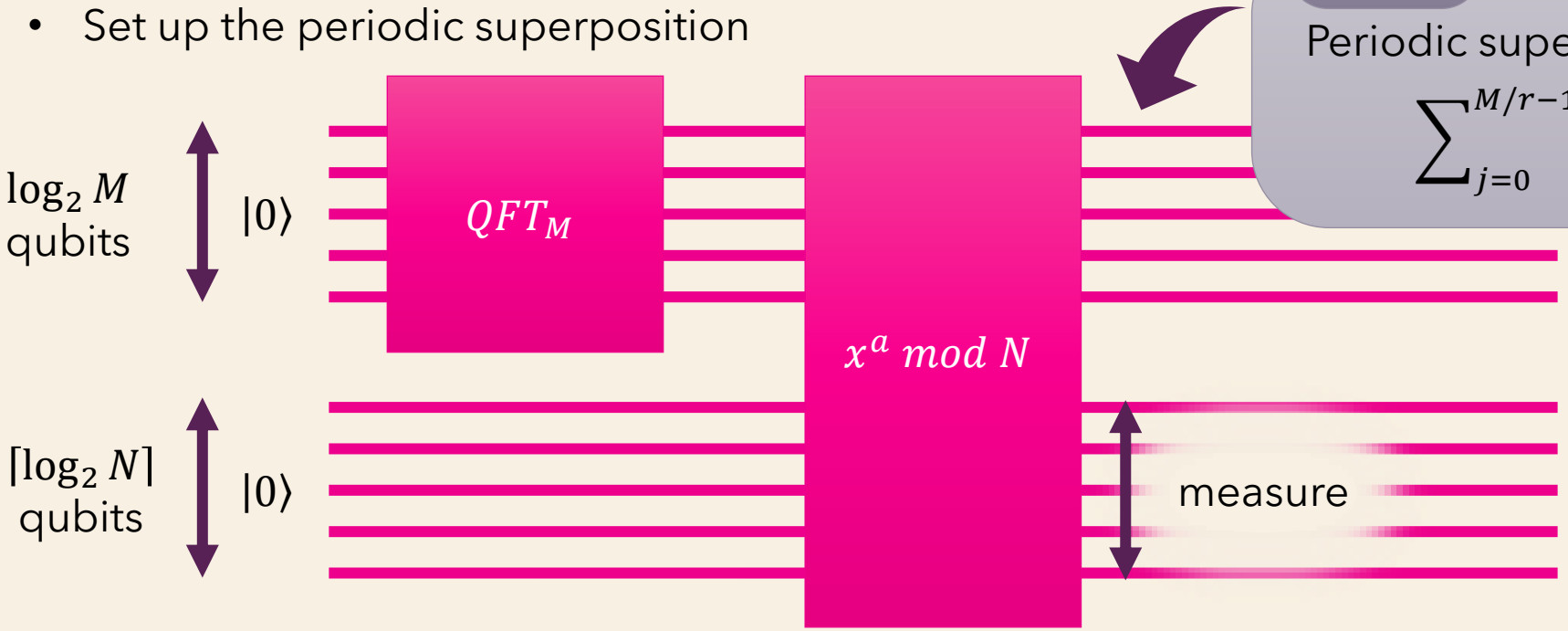
QUANTUM ALGORITHM FOR FACTORING A LARGE INTEGER N

- Set up the periodic superposition



QUANTUM ALGORITHM FOR FACTORING A LARGE INTEGER N

- Set up the periodic superposition

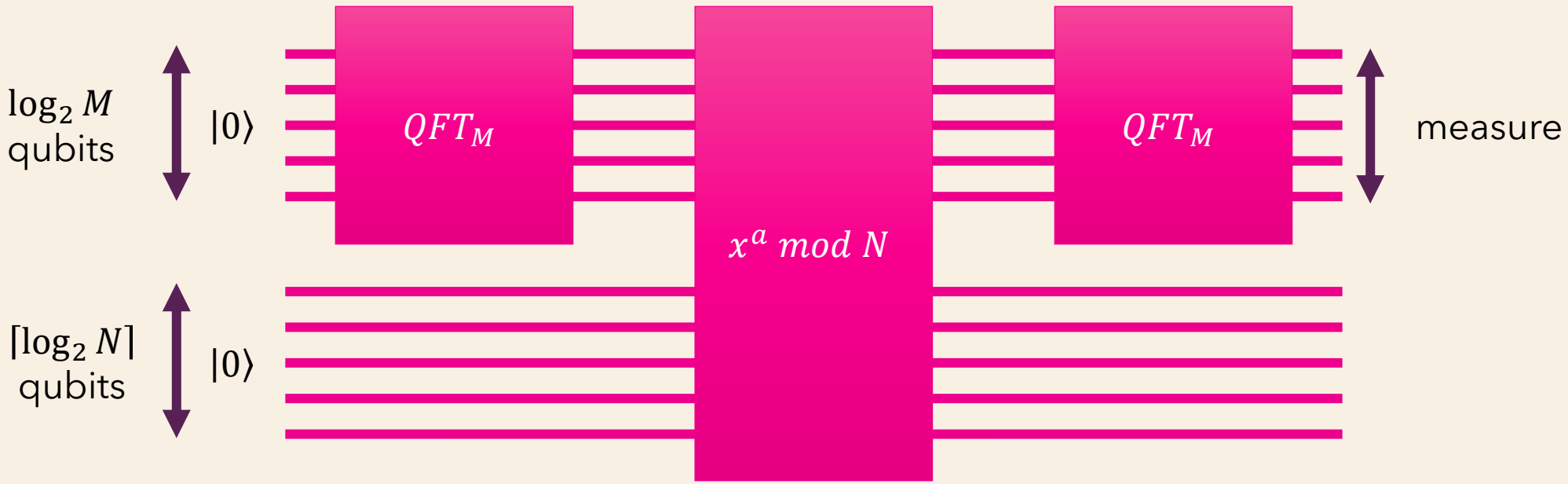


Note

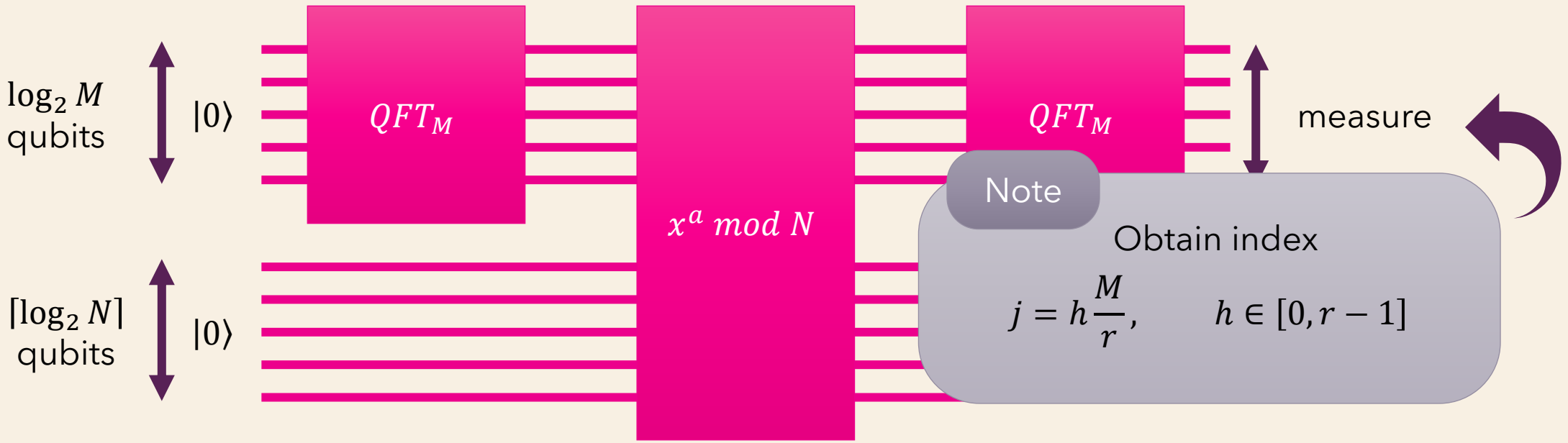
Periodic superposition with period r

$$\sum_{j=0}^{M/r-1} |k + jr\rangle, k \in [0, r]$$

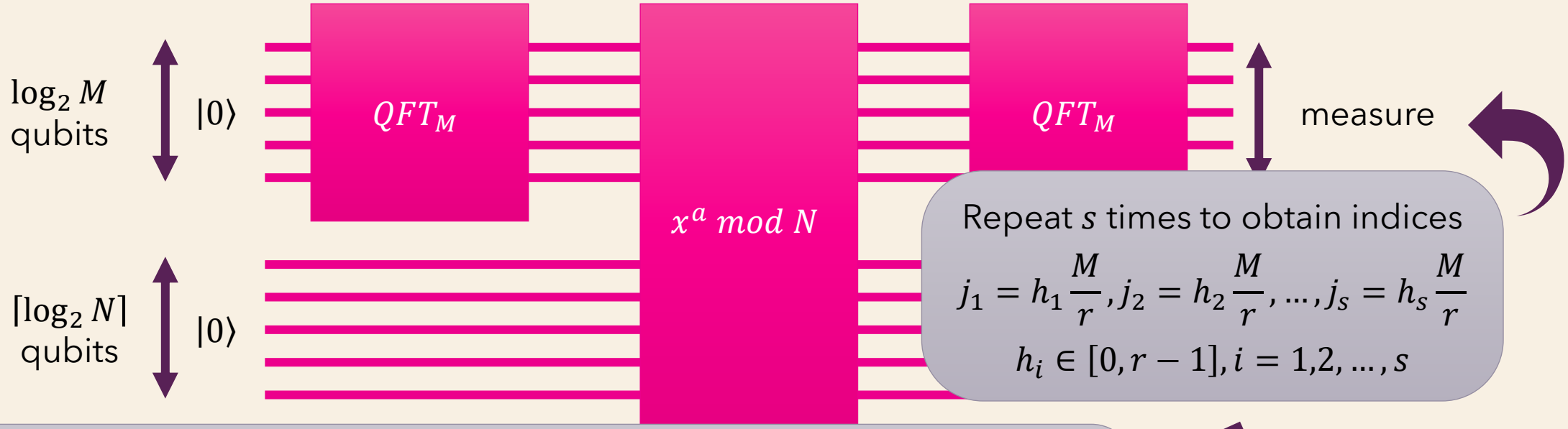
QUANTUM ALGORITHM FOR FACTORING A LARGE INTEGER N



QUANTUM ALGORITHM FOR FACTORING A LARGE INTEGER N



QUANTUM ALGORITHM FOR FACTORING A LARGE INTEGER N



Repeat s times to obtain indices

$$j_1 = h_1 \frac{M}{r}, j_2 = h_2 \frac{M}{r}, \dots, j_s = h_s \frac{M}{r}$$

$$h_i \in [0, r-1], i = 1,2, \dots, s$$

Compute $g = \gcd(j_1, \dots, j_s)$. If M/g is even, then compute $\gcd(N, x^{M/2g} + 1)$ and output it if it is a nontrivial factor of N; otherwise repeat the process

QUANTUM ALGORITHM FOR FACTORING A LARGE INTEGER N

- Time complexity:

  Let $n = \lceil \log_2 N \rceil$, and $s = 2n$

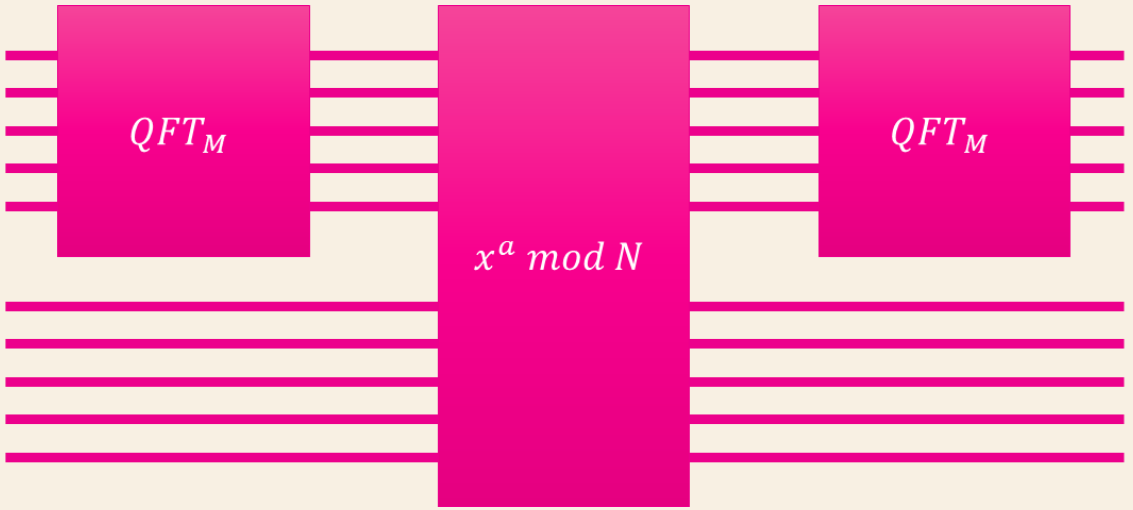
  Modular exponentiation:

  $$T_e(n) = O(n^3)$$

  QFT:

  $$T_{QFT}(2n) = O(n^2)$$

  $$T(n) = s\left(T_e(n) + 2T_{QFT}(2n)\right) = O(n^4)$$



QUANTUM ALGORITHM FOR FACTORING A LARGE INTEGER N

- Time complexity:

  Let $n = \lceil \log_2 N \rceil$, and $s = 2n$

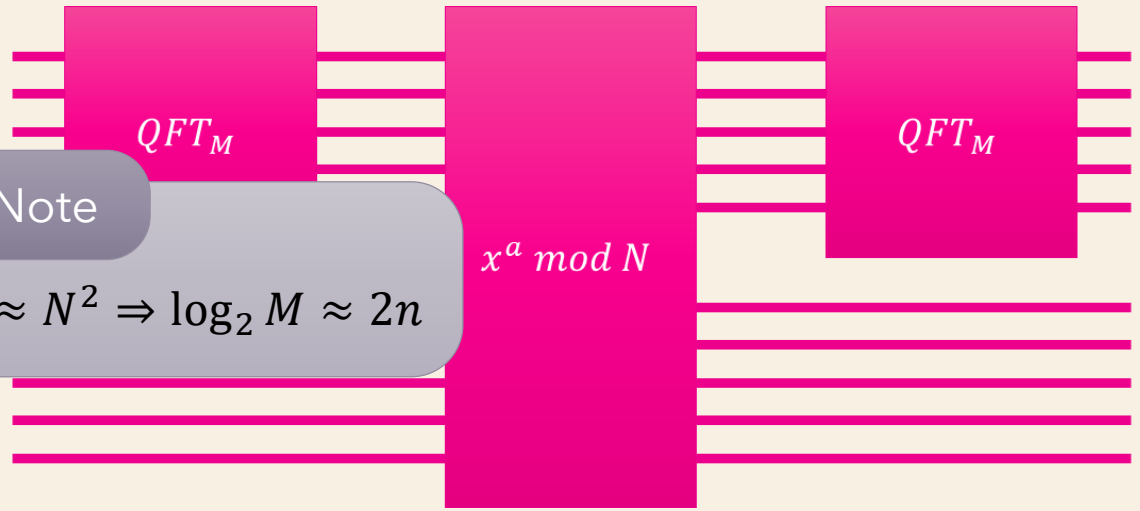
  Modular exponentiation:

  $$T_e(n) = O(n^3)$$

  QFT:

  $$T_{QFT}(2n) = O(n^2)$$

  $$T(n) = s\left(T_e(n) + 2T_{QFT}(2n)\right) = O(n^4)$$



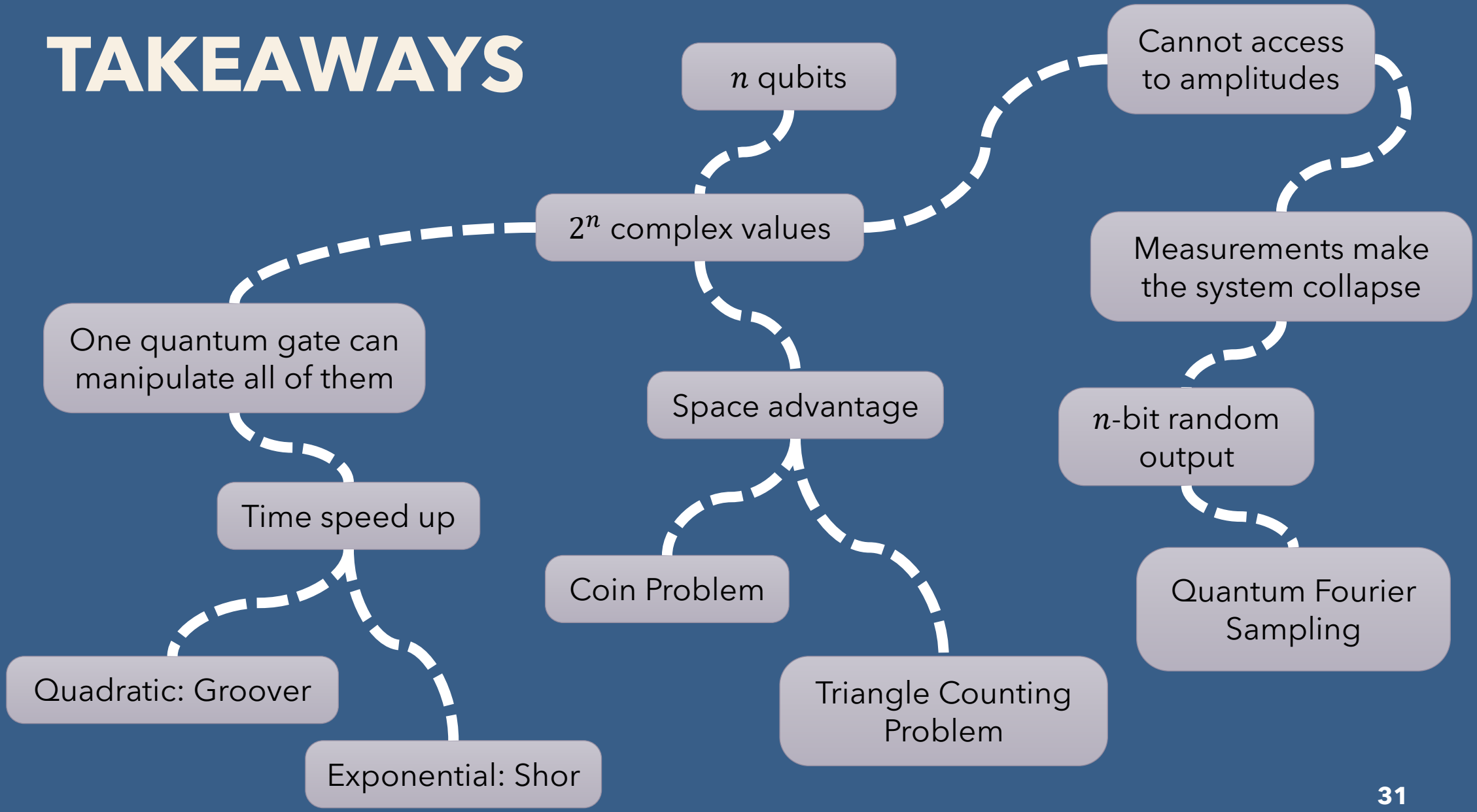
Note

$M \approx N^2 \Rightarrow \log_2 M \approx 2n$

Note

Exponential speed up: $O\left(\exp\left(cn^{1/3}\log^{2/3} n\right)\right)$

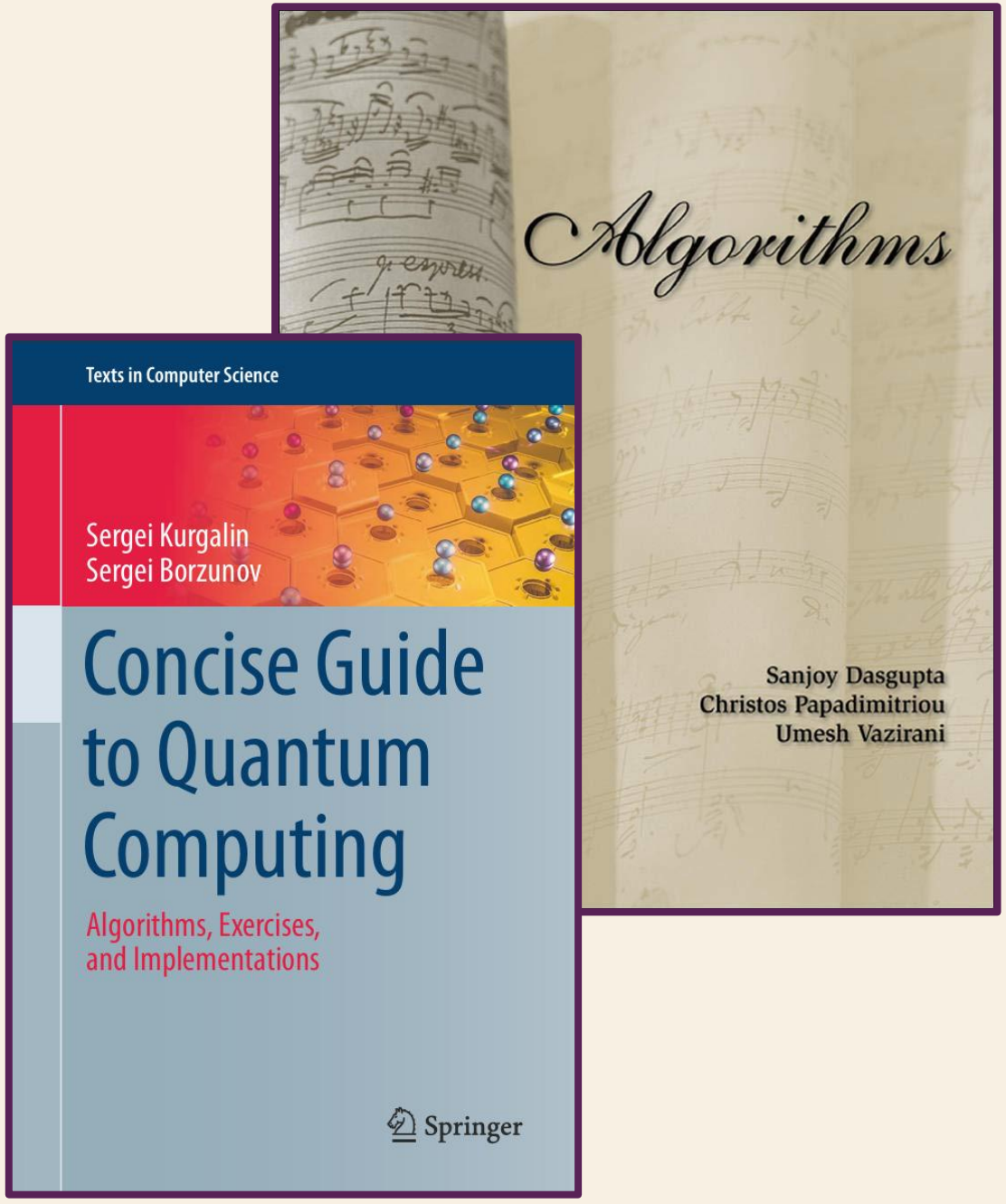
TAKEAWAYS


n qubits
Cannot access to amplitudes
2^n complex values
Measurements make the system collapse
One quantum gate can manipulate all of them
Space advantage
n-bit random output
Time speed up
Coin Problem
Quantum Fourier Sampling
Quadratic: Groover
Triangle Counting Problem
Exponential: Shor

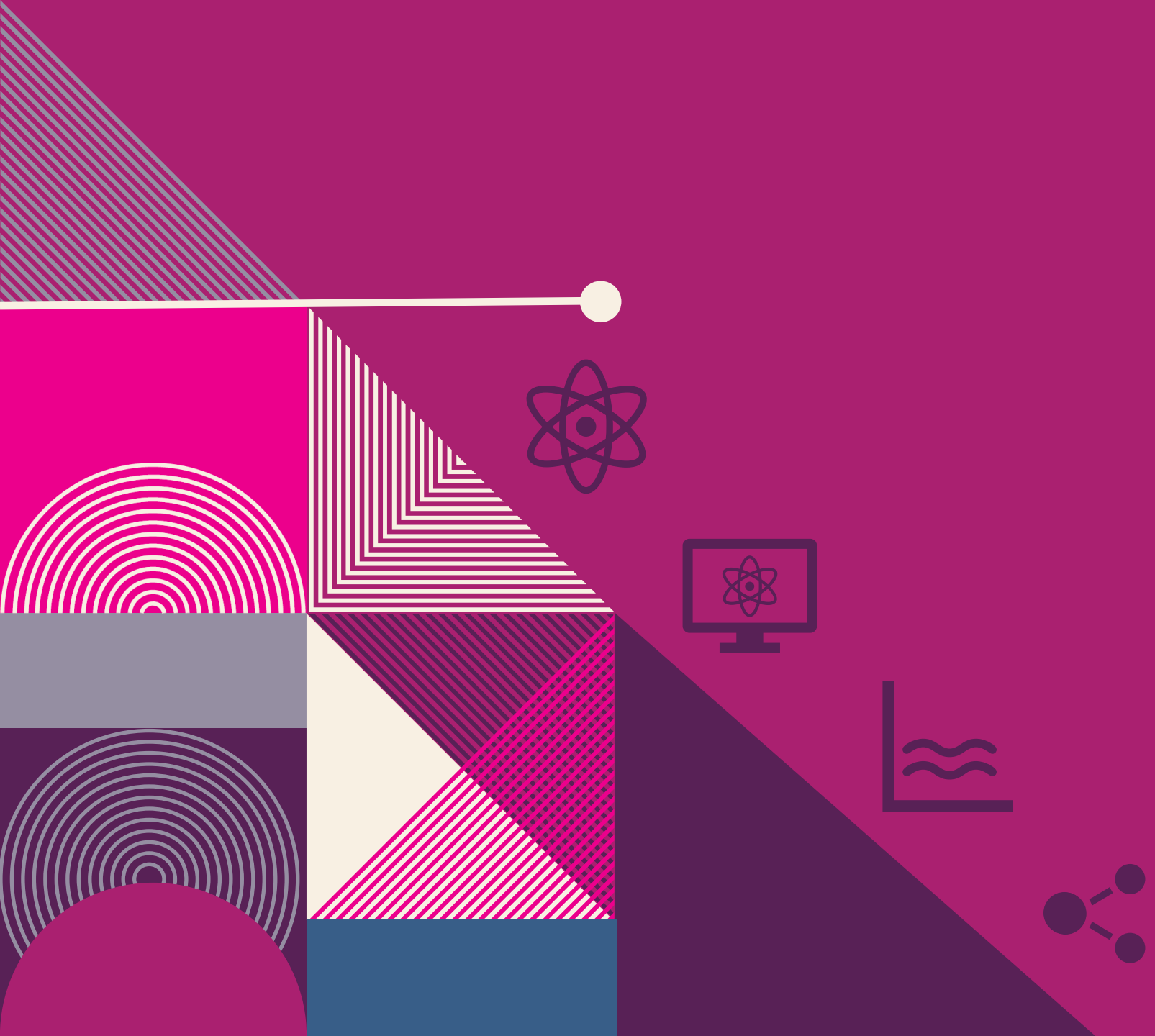
REFERENCES

- Dasgupta, Sanjoy, Papadimitriou Christos, and Vazirani Umesh "**Algorithms**." (2006).

- Kurgalin, Sergei, and Sergei Borzunov. "**Concise guide to quantum computing**." *Cham: Springer* (2021).



THANK YOU FOR YOUR ATTENTION!



APPENDIX

ENTANGLEMENT

- Given the quantum state

$$|\alpha\rangle = \alpha_{00}\,|00\rangle + \alpha_{01}\,|01\rangle + \alpha_{10}\,|10\rangle + \alpha_{11}\,|11\rangle$$

- Are there 2 qubits

$$\beta_0|0\rangle + \beta_1|1\rangle$$

$$\gamma_0|0\rangle + \gamma_1|1\rangle$$

such that their joint state of is

$$|\alpha\rangle = \beta_0\gamma_0|00\rangle + \beta_0\gamma_1|01\rangle + \beta_1\gamma_0|10\rangle + \beta_1\gamma_1|11\rangle$$

?

ENTANGLEMENT

Entangled states

Are those states of quantum systems in which qubits interact with each other
Entangled qubits cannot be decomposed into the states of the individual qubits

- **Example:** Bell states

$$|\psi\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

PARTIAL MEASUREMENTS

- Given the quantum state

$$|\alpha\rangle = \alpha_{00}\,|00\rangle + \alpha_{01}\,|01\rangle + \alpha_{10}\,|10\rangle + \alpha_{11}\,|11\rangle$$

- What if we measure the first qubit?
  - What is the probability that the outcome is 0?

$$\Pr[1\text{st bit} = 0] = \Pr[00] + \Pr[01] = |\alpha_{00}|^2 + |\alpha_{01}|^2$$

  - What is the new superposition if the outcome is 0?

$$|\alpha_{\text{new}}\rangle = \frac{\alpha_{00}}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}|00\rangle + \frac{\alpha_{01}}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}|01\rangle$$

Note: Eliminate inconsistent states

Note: Normalize again

FACTORING AS ROOT FINDING

Lemma

If x is a nontrivial square root of $1\ mod\ N$, then $\gcd(x+1, N)$ is a nontrivial factor of N

- Proof:
  - $x^2 \equiv 1\ mod\ N$ implies that N divides $(x^2 - 1) = (x+1)(x-1)$
  - But N does not divide either of these individual terms, since $x \not\equiv \pm 1\ mod\ N$
  - Therefore, N must have a nontrivial factor in common with each of $(x+1)$ and $(x-1)$
  - In particular $\gcd(N, x+1)$ is a nontrivial factor of N

SHOR'S TOY EXAMPLE

- Factor $N = 15$ using $x = 2$:

  The powers of $2\ mod\ 15$ are:

$$2^1\ mod\ 15 = 2, \qquad 2^2\ mod\ 15 = 4,$$
$$2^3\ mod\ 15 = 8, \qquad 2^4\ mod\ 15 = 1,$$
$$2^1\ mod\ 15 = 2, \qquad \ldots$$

  The order of $2\ mod\ 15$ is $r = 4$, that is even and $2^{r/2} = 2^2 = 4 \not\equiv \pm 1\ mod\ 15$

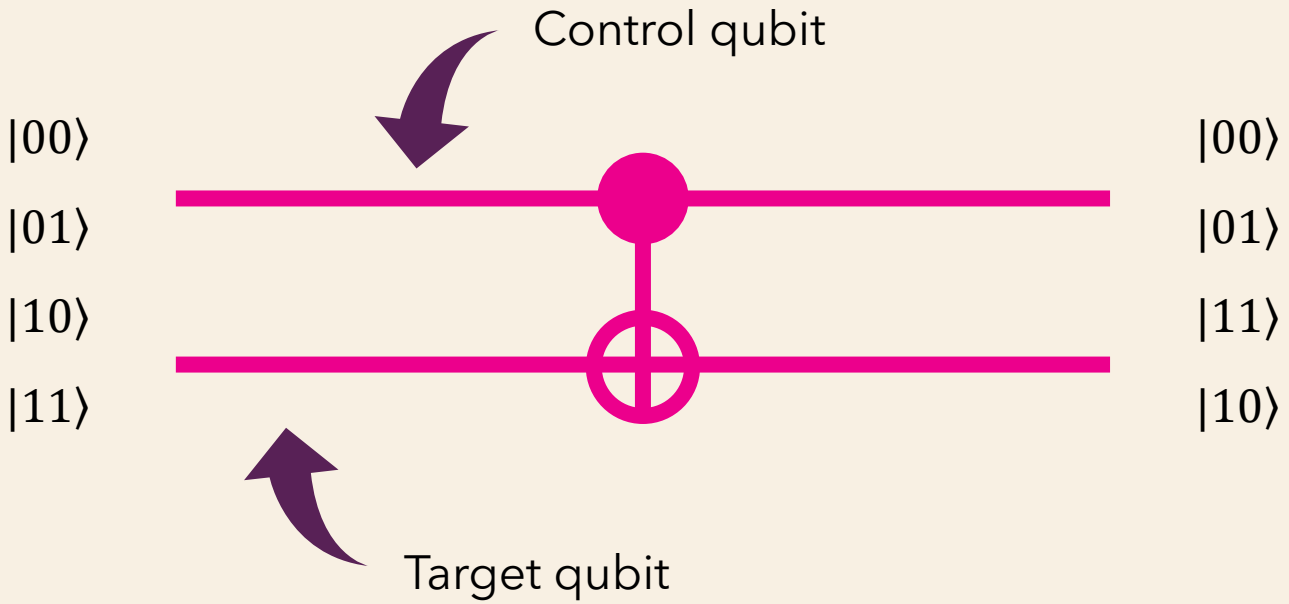
  Then

$$\gcd\left(N, x^{r/2} + 1\right) = \gcd(15, 2^2 + 1) = 5$$

  that is a nontrivial factor of 15

ELEMENTARY QUANTUM GATES

- Controlled-NOT:

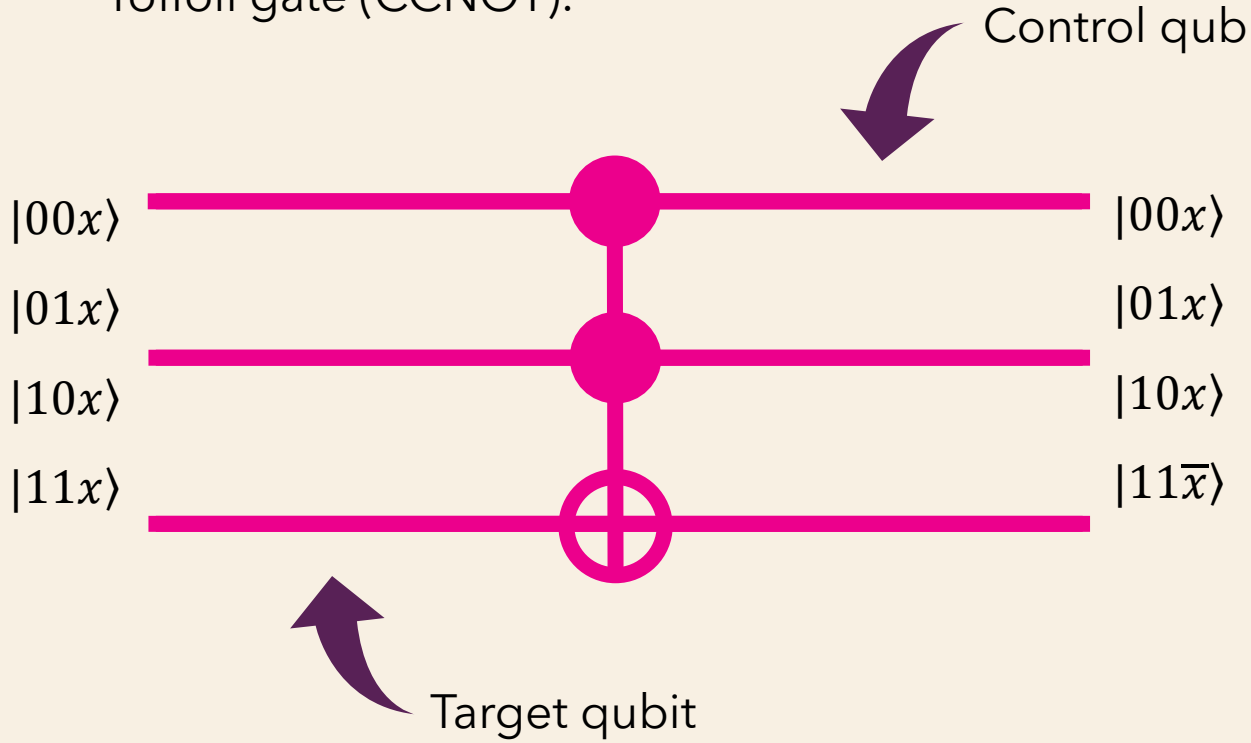


Equivalent matrix

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

ELEMENTARY QUANTUM GATES

- Toffoli gate (CCNOT):

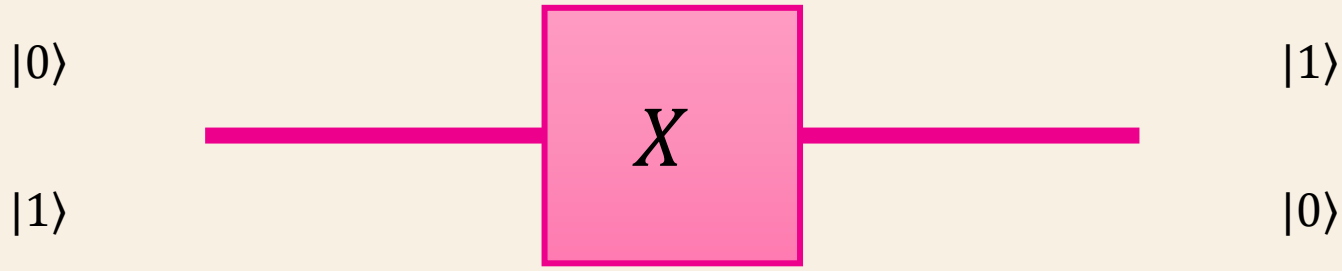


Equivalent matrix

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

ELEMENTARY QUANTUM GATES

- Pauli gate X:

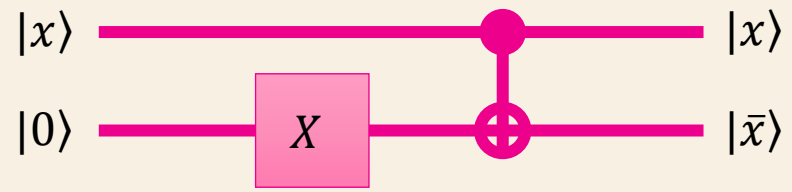


Equivalent matrix

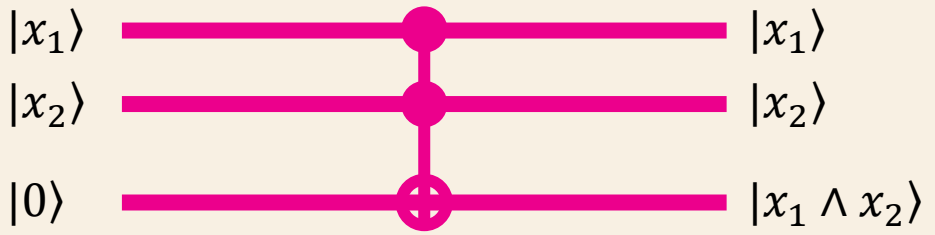
$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

IMPLEMENTATION OF LOGIC GATES

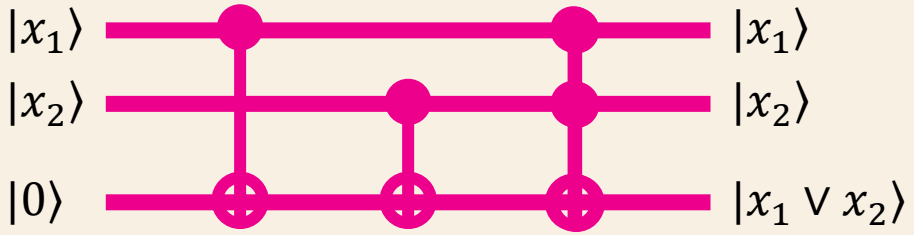
- NOT:



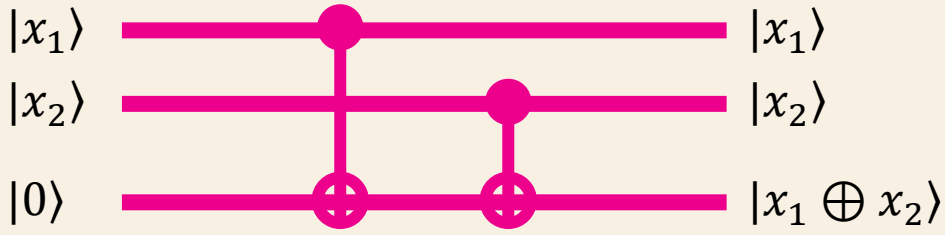
- AND:



- OR:



- XOR:



OTHER INTERESTING PAPERS

- Grover, Lov K. "**A fast quantum mechanical algorithm for database search**." *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*. 1996.
- Shor, Peter W. "**Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer**." *SIAM review* 41.2 (1999): 303-332.
- Gavinsky, Dmitry, et al. "**Exponential separations for one-way quantum communication complexity, with applications to cryptography**." *Proceedings of the thirty-ninth annual ACM symposium on Theory of computing*. 2007.

OTHER INTERESTING PAPERS

- Aaronson, Scott, and Andrew Drucker. "**Advice coins for classical and quantum computation**." *International Colloquium on Automata, Languages, and Programming*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011.
- Kallaugher, John, Ojas Parekh, and Nadezhda Voronova. "**How to design a quantum streaming algorithm without knowing anything about quantum computing**." *2025 Symposium on Simplicity in Algorithms (SOSA)*. Society for Industrial and Applied Mathematics, 2025.
- Cain, Madelyn, et al. "**Shor's algorithm is possible with as few as 10,000 reconfigurable atomic qubits**." *arXiv preprint arXiv:2603.28627* (2026).