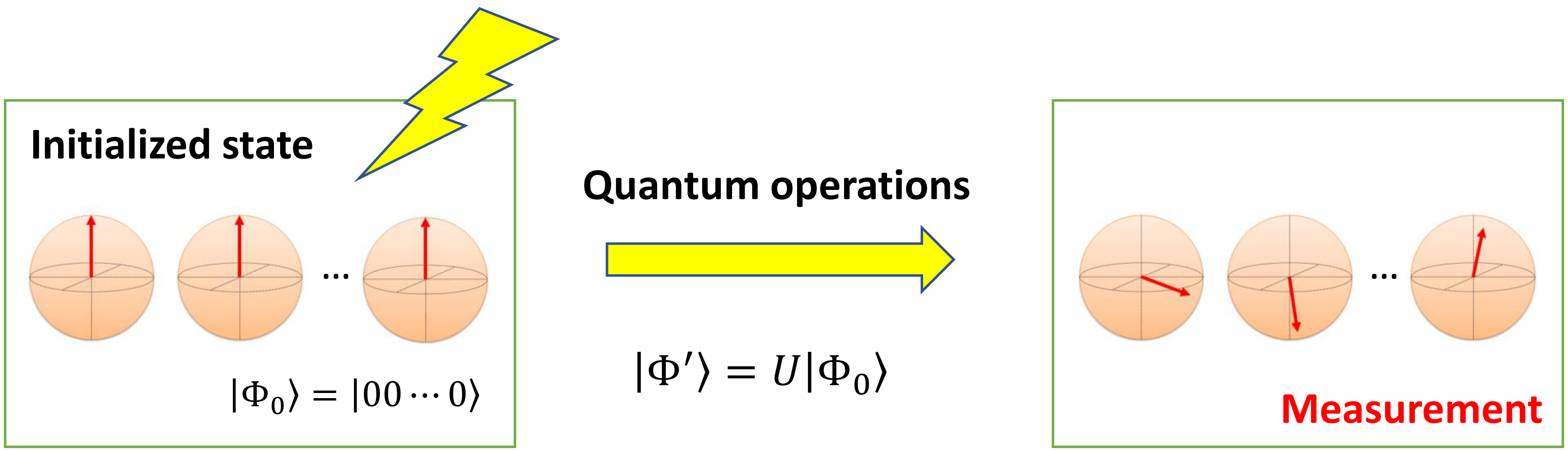
Quantum Chemistry on Quantum Computers

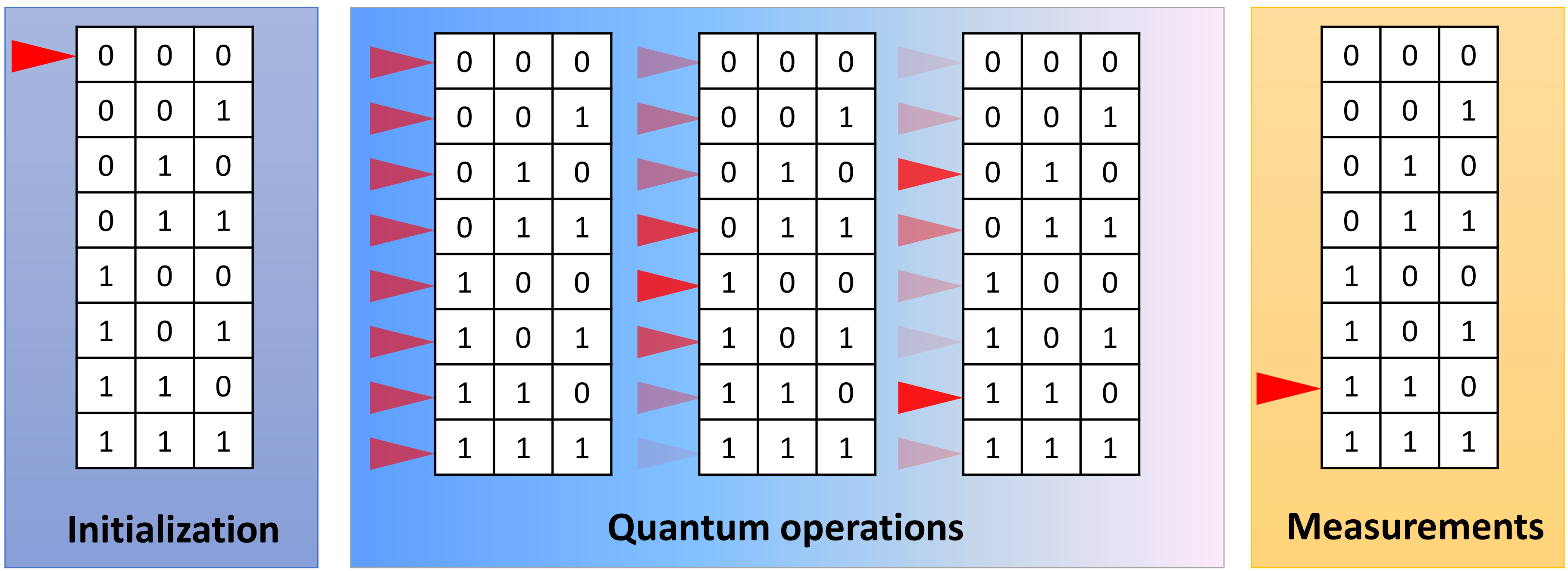
#2 Quantum Algorithms

Kenji Sugisaki[1,2,3]

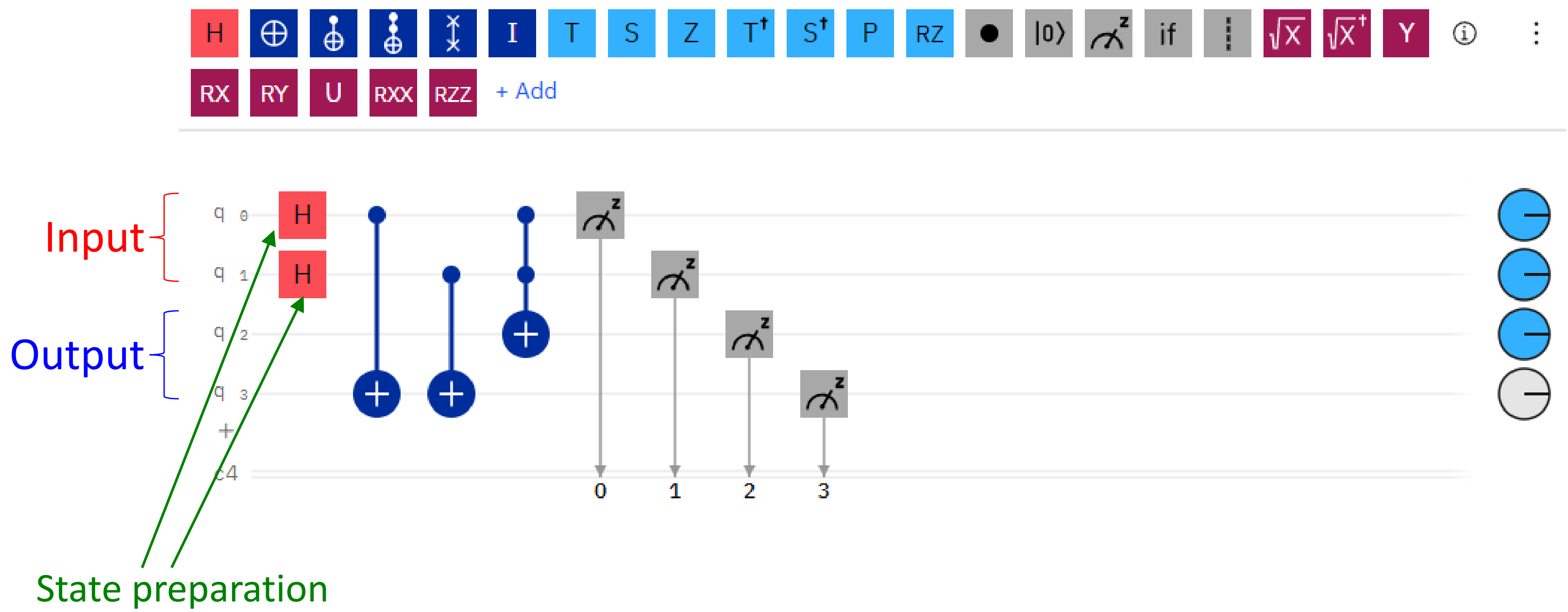
[1]*Department of Chemistry, Graduate School of Science, Osaka City University, Japan*
[2]*JST PRESTO, Japan*
[3]*CQuERE, TCG-CREST, India*

Quantum Computations





Summation of two 1-bit integers



$$|0000\rangle \longrightarrow \frac{1}{2}(|0000\rangle + |0101\rangle + |1001\rangle + |1110\rangle)$$

0 + 0 = 00
0 + 1 = 01
1 + 0 = 01
1 + 1 = 10

Quantum algorithms

Quantum Algorithm Zoo

This is a comprehensive catalog of quantum algorithms. If you notice any errors or omissions, please email me at stephen.jordan@microsoft.com. (Alternatively, you may submit a pull request to the repository on github.) Your help is appreciated and will be acknowledged.

Algebraic and Number Theoretic Algorithms

Algorithm: Factoring
Speedup: Superpolynomial
Description: Given an *n*-bit integer, find the prime factorization. The quantum algorithm of Peter Shor solves this in $\widetilde{O}(n^3)$ time [82,125]. The fastest known classical algorithm for integer factorization is the general number field sieve, which is believed to run in time $2^{\widetilde{O}(n^{1/3})}$. The best rigorously proven upper bound on the classical complexity of factoring is $O(2^{n/4+o(1)})$ via the Pollard-Strassen algorithm [252, 362]. Shor's factoring algorithm breaks RSA public-key encryption and the closely related quantum algorithms for discrete logarithms break the DSA and ECDSA digital signature schemes and the Diffie-Hellman key-exchange protocol. A quantum algorithm even faster than Shor's for the special case of factoring "semiprimes", which are widely used in cryptography, is given in [271]. If small factors exist, Shor's algorithm can be beaten by a quantum algorithm using Grover search to speed up the elliptic curve factorization method [366]. Additional optimized versions of Shor's algorithm are given in [384, 386]. There are proposed classical public-key cryptosystems not believed to be broken by quantum algorithms, *cf.* [248]. At the core of Shor's factoring algorithm is order finding, which can be reduced to the Abelian hidden subgroup problem, which is solved using the quantum Fourier transform. A number of other problems are known to reduce to integer factorization including the membership problem for matrix groups over fields of odd order [253], and certain diophantine problems relevant to the synthesis of quantum circuits [254].

Algorithm: Discrete-log
Speedup: Superpolynomial
Description: We are given three *n*-bit numbers *a*, *b*, and *N*, with the promise that $b = a^s \mod N$ for some *s*. The task is to find *s*. As shown by Shor [82], this can be achieved on a quantum computer in poly(*n*) time. The fastest known classical algorithm requires time superpolynomial in *n*. By similar techniques to those in [82], quantum computers can solve the discrete logarithm problem on elliptic curves, thereby breaking elliptic curve cryptography [109, 14]. A further optimization to Shor's algorithm is given in [385]. The superpolynomial quantum speedup has also been extended to the discrete logarithm problem on semigroups [203, 204]. See also Abelian hidden subgroup.

Algorithm: Pell's Equation

Navigation

- Algebraic & Number Theoretic
- Oracular
- Approximation and Simulation
- Optimization, Numerics, & Machine Learning
- Acknowledgments
- References

Translations

This page has been translated into:
Japanese
Chinese

Other Surveys

For overviews of quantum algorithms I recommend:

- Nielsen and Chuang
- Childs
- Preskill
- Mosca
- Childs and van Dam
- van Dam and Sasaki
- Bacon and van Dam
- Montanaro
- Hidary

Terminology

If there exists a positive constant α such that the runtime $C(n)$ of the best known classical algorithm

https://quantumalgorithmzoo.org/

No cloning theorem

Unknown quantum state cannot be cloned by unitary operations.

[Proof] Let us imagine that there is a unitary operator *U* that can clone the quantum state.

$$U|\varphi\rangle \otimes |0\rangle = |\varphi\rangle \otimes |\varphi\rangle$$
$$U|\psi\rangle \otimes |0\rangle = |\psi\rangle \otimes |\psi\rangle$$

Consider the quantum superposition state $|\alpha\rangle = c_\varphi|\varphi\rangle + c_\psi|\psi\rangle$

$$\begin{aligned} U|\alpha\rangle \otimes |0\rangle &= U\left(c_\varphi|\varphi\rangle \otimes |0\rangle + c_\psi|\psi\rangle \otimes |0\rangle\right) \\ &= c_\varphi U|\varphi\rangle \otimes |0\rangle + c_\psi U|\psi\rangle \otimes |0\rangle \\ &= c_\varphi|\varphi\rangle \otimes |\varphi\rangle + c_\psi|\psi\rangle \otimes |\psi\rangle \qquad \text{eq (1)} \end{aligned}$$

From the definition of *U*, we can also derive the following equation:

$$U|\alpha\rangle \otimes |0\rangle = |\alpha\rangle \otimes |\alpha\rangle$$

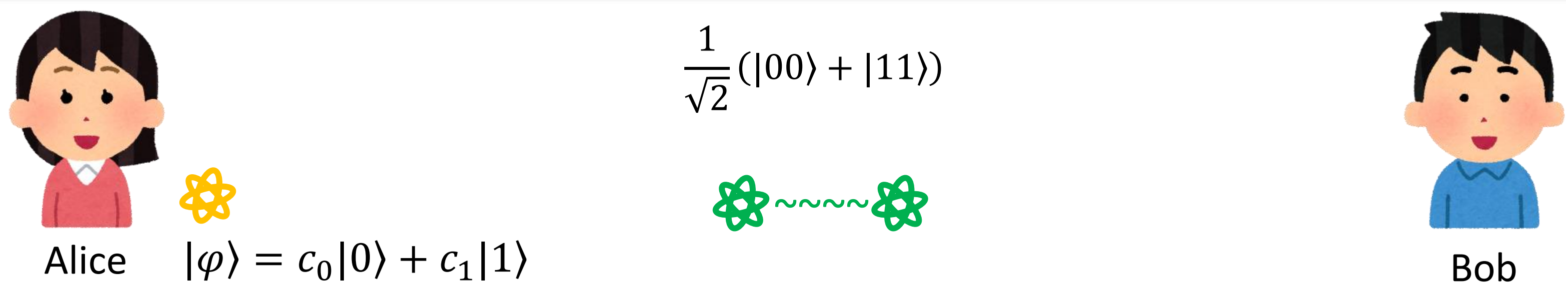
$$= c_\varphi^2|\varphi\rangle \otimes |\varphi\rangle + c_\varphi c_\psi|\varphi\rangle \otimes |\psi\rangle + c_\psi c_\varphi|\psi\rangle \otimes |\varphi\rangle + c_\psi^2|\psi\rangle \otimes |\psi\rangle \qquad \text{eq (2)}$$

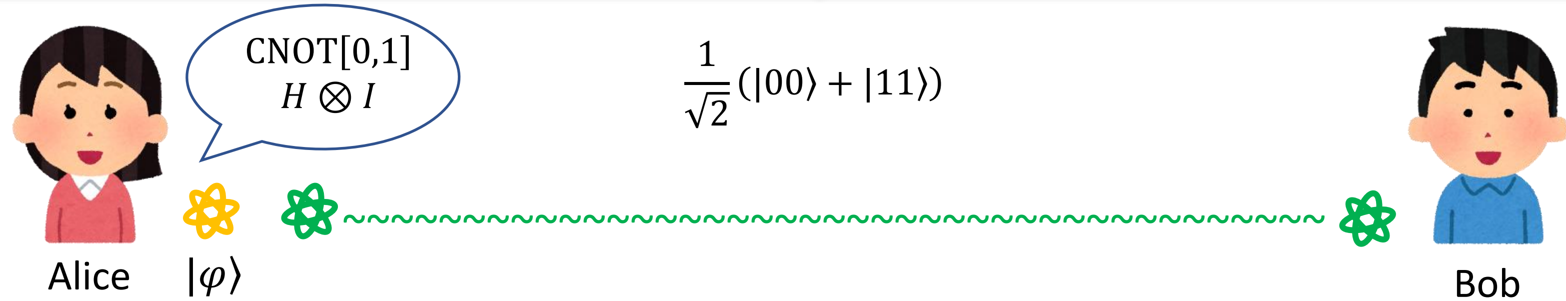
Eq (1) and eq (2) contradicts.

W. K. Wootters, W. H. Zurek, *Nature* **1982**, *299*, 802–803.

Quantum Teleportation

Unknown quantum state cannot be cloned, but it can be teleported.





$$(c_0|0\rangle + c_1|1\rangle) \otimes \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(c_0|000\rangle + c_0|011\rangle + c_1|100\rangle + c_1|111\rangle)$$

$$\xrightarrow{\mathrm{CNOT}[0,1]} \frac{1}{\sqrt{2}}(c_0|000\rangle + c_0|011\rangle + c_1|110\rangle + c_1|101\rangle)$$

$$\xrightarrow{H\otimes I\otimes I} \frac{1}{2}(c_0|000\rangle + c_0|100\rangle + c_0|011\rangle + c_0|111\rangle + c_1|010\rangle - c_1|110\rangle + c_1|001\rangle - c_1|101\rangle)$$

$$= \frac{1}{2}(|00\rangle \otimes \{c_0|0\rangle + c_1|1\rangle\} + |01\rangle \otimes \{c_0|1\rangle + c_1|0\rangle\} + |10\rangle \otimes \{c_0|0\rangle - c_1|1\rangle\} + |11\rangle \otimes \{c_0|1\rangle - c_1|0\rangle\})$$

$|\varphi\rangle = c_0|0\rangle + c_1|1\rangle$

Quantum Teleportation

Alice

CNOT[0,1]
$H \otimes I$
Measure

$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

$|\varphi\rangle$

Bob

Measurement outcome	Quantum state of Bob's qubit
00	$c_0\|0\rangle + c_1\|1\rangle$
01	$c_0\|1\rangle + c_1\|0\rangle$
10	$c_0\|0\rangle - c_1\|1\rangle$
11	$c_0\|1\rangle - c_1\|0\rangle$

Alice

Measurement outcome was
(i) 00
(ii) 01
(iii) 10
(iv) 11

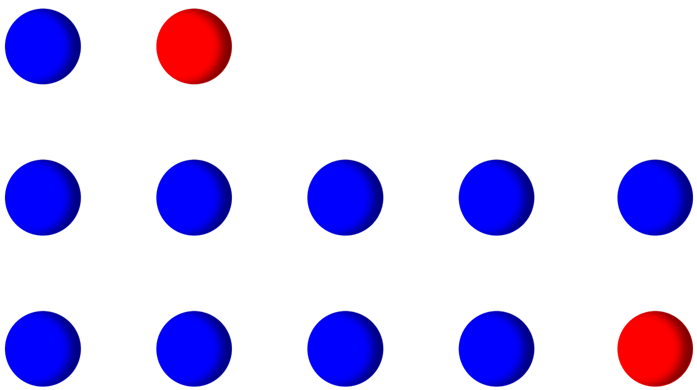
OK, I will apply
(i) nothing
(ii) X gate
(iii) Z gate
(iv) X and Z gates
to recover the original state.

Bob

Deutsch–Jozsa algorithm

- There are *n* balls in the box.
- The balls are either all red or all blue (pure), or half red and half blue (mixed).
- How many trials do you need to identify either pure or mixed?

$n = 8$



Mixed!

Pure!

Mixed!

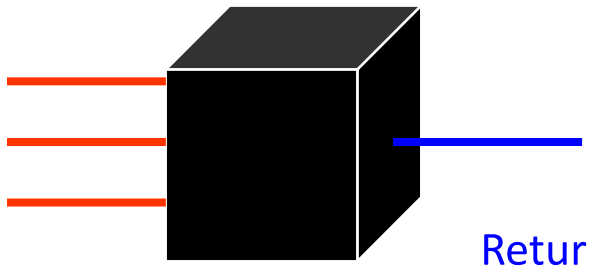
In the worst case we need 5 trials to identify.

Black box

Input	Output
000	0
001	0
010	1
011	0
100	1
101	1
110	0
111	1

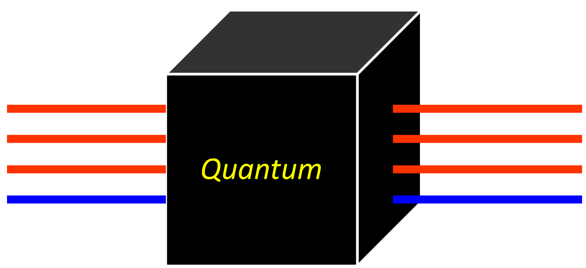
- Assume n = 8 in the previous slide.
- Red = 0, Blue = 1.
- The system can be [00101101], for example.

3-bit binary as the input
E.g., x = 011



Return x-th value

Allow quantum superposition as the input

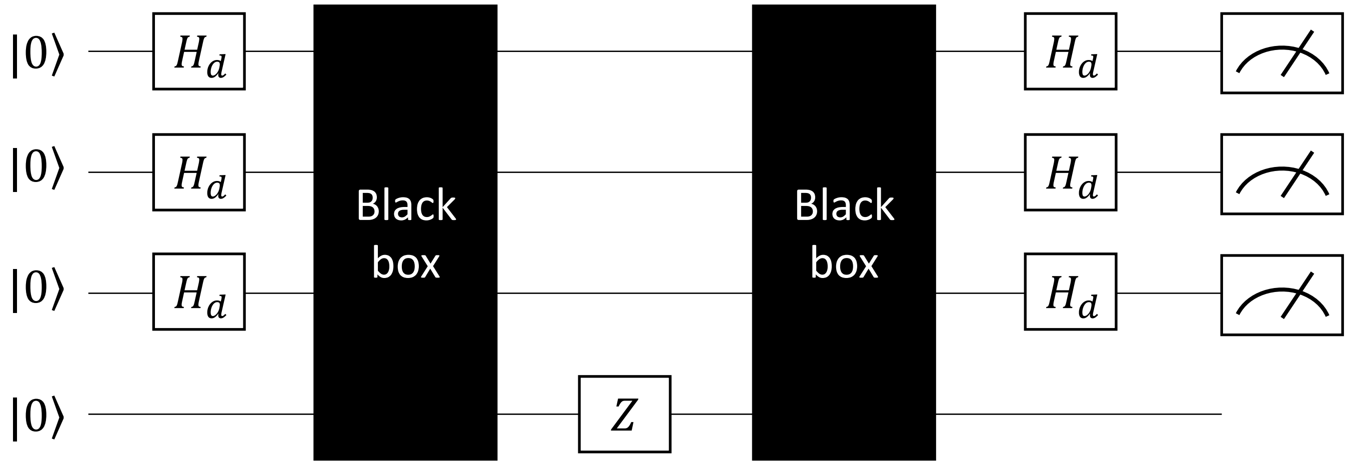


Three qubits in the top are for input, one qubit in the bottom is for output.

$$|0110\rangle \xrightarrow{\text{Black box}} |0110\rangle, \quad |0100\rangle \xrightarrow{\text{Black box}} |0101\rangle, \text{ etc.}$$

Deutsch–Jozsa algorithm

[00101101]



$$|0000\rangle \xrightarrow{H\otimes H\otimes H\otimes I} \frac{1}{2\sqrt{2}}(|0000\rangle + |0010\rangle + |0100\rangle + |0110\rangle + |1000\rangle + |1010\rangle + |1100\rangle + |1110\rangle)$$

$$\xrightarrow{\text{Black box}} \frac{1}{2\sqrt{2}}(|0000\rangle + |0010\rangle + |0101\rangle + |0110\rangle + |1001\rangle + |1011\rangle + |1100\rangle + |1111\rangle)$$

$$\xrightarrow{I\otimes I\otimes I\otimes Z} \frac{1}{2\sqrt{2}}(|0000\rangle + |0010\rangle - |0101\rangle + |0110\rangle - |1001\rangle - |1011\rangle + |1101\rangle - |1110\rangle)$$

$$\xrightarrow{\text{Black box}} \frac{1}{2\sqrt{2}}(|0000\rangle + |0010\rangle - |0101\rangle + |0110\rangle - |1001\rangle - |1011\rangle + |1101\rangle - |1110\rangle)$$

$$\xrightarrow{H\otimes H\otimes H\otimes I} \frac{1}{2}(|0010\rangle + |0110\rangle - |1000\rangle + |1100\rangle)$$

If "mixed", at least one of the qubit measurement outcome should be "1".

Deutsch–Jozsa algorithm

Assume $n = 2^N$.

On the *classical* computer, we need $(2^{N-1} + 1)$ operations in the worst case.
On the *quantum* computer, we need $2N + 3$ operatios.

N	$n = 2^N$	Classical computer	Quantum computer
3	8	5	9
4	16	9	11
5	32	17	13
10	1024	513	23
100	1.267×10^{30}	6.338×10^{29}	203

SWAP test

VOLUME 87, NUMBER 16 PHYSICAL REVIEW LETTERS 15 OCTOBER 2001

Quantum Fingerprinting

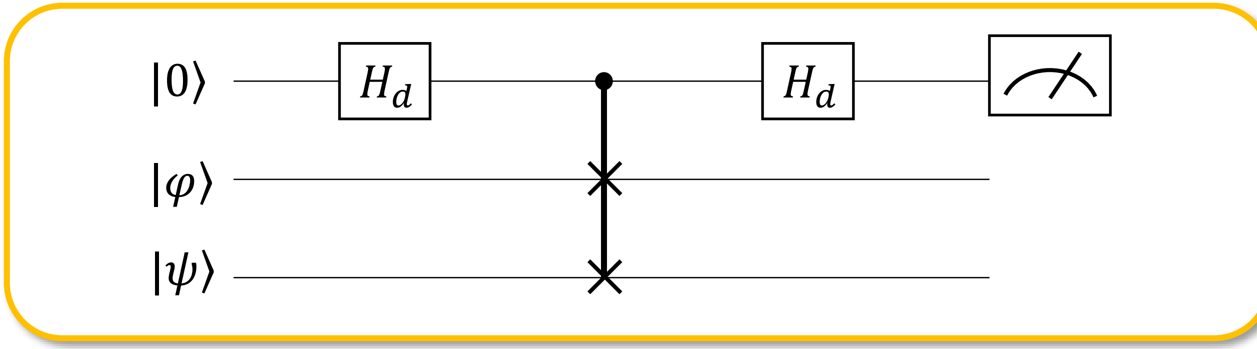
Harry Buhrman,[1,*] Richard Cleve,[2,†] John Watrous,[2,‡] and Ronald de Wolf[1,§]
[1]CWI, P.O. Box 94709, Amsterdam, The Netherlands
and University of Amsterdam, Amsterdam, The Netherlands
[2]Department of Computer Science, University of Calgary, Calgary, Alberta, Canada T2N 1N4
(Received 19 April 2001; published 26 September 2001)

Classical fingerprinting: The fingerprint cannot be made exponentially smaller than the original strings, unless the parties preparing the fingerprints have access to correlated random sources.

Quantum fingerprinting: The fingerprint can be exponentially smaller than the original strings, without any correlations or entanglements between two parties.

Calculate the overlap between two quantum states $|\varphi\rangle$ and $|\psi\rangle$

SWAP test



$$|0\rangle \otimes |\varphi\rangle \otimes |\psi\rangle \xrightarrow{H\otimes I\otimes I} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |\varphi\psi\rangle$$

$$\xrightarrow{\text{c−SWAP[0,1,2]}} \frac{1}{\sqrt{2}}(|0\rangle \otimes |\varphi\psi\rangle + |1\rangle \otimes |\psi\varphi\rangle)$$

$$\xrightarrow{H\otimes I\otimes I} \frac{1}{2}(|0\rangle \otimes |\varphi\psi\rangle + |1\rangle \otimes |\varphi\psi\rangle + |0\rangle \otimes |\psi\varphi\rangle - |1\rangle \otimes |\psi\varphi\rangle)$$

$$= \frac{1}{2}|0\rangle(|\varphi\psi\rangle + |\psi\varphi\rangle) + \frac{1}{2}|1\rangle(|\varphi\psi\rangle - |\psi\varphi\rangle)$$

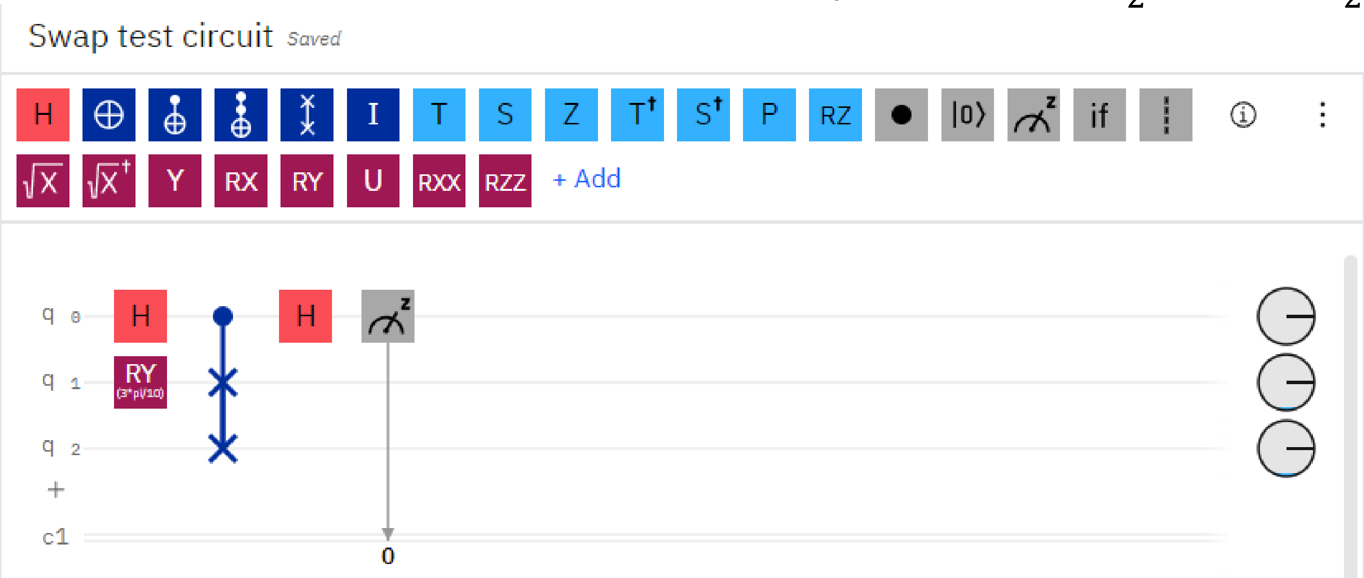
Probability to obtain 0 in the measurement

$$P(0) = \frac{1}{4}(\langle\varphi\psi|\varphi\psi\rangle + \underline{\langle\varphi\psi|\psi\varphi\rangle} + \langle\psi\varphi|\varphi\psi\rangle + \langle\psi\varphi|\psi\varphi\rangle) = \frac{1}{2}(1 + |\langle\varphi|\psi\rangle|^2)$$

$$\langle\varphi\psi|\psi\varphi\rangle = \langle\varphi|\psi\rangle\langle\psi|\varphi\rangle = |\langle\varphi|\psi\rangle|^2$$

SWAP test on IBM-Q

Apply the SWAP test with $|\varphi\rangle = R_y(\theta)|0\rangle = \cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}|1\rangle$ and $|\psi\rangle = |0\rangle$




```
OPENQASM 2.0;
include "qelib1.inc";

qreg q[3];
creg c[1];

h q[0];
ry(3*pi/10) q[1];
cswap q[0],q[1],q[2];
h q[0];
measure q[0] -> c[0];
```

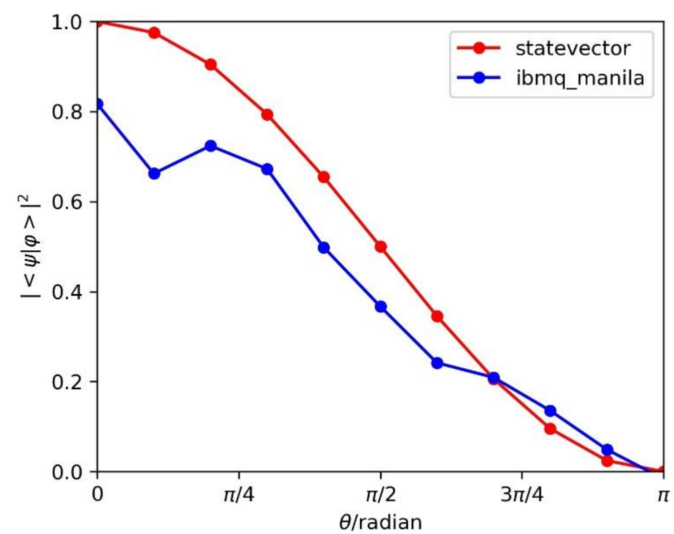
$$P(0) = \frac{1}{2}\left(1 + \cos^2\frac{\theta}{2}\right)$$

$P(0) = 1$ if $\theta = 0$

$P(0) = 0.5$ if $\theta = \pi$

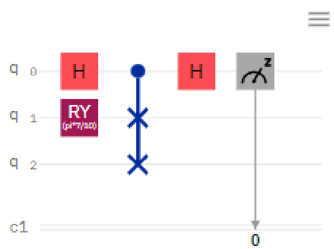
$|\langle\varphi|\psi\rangle|^2 = 1$ if $\theta = 0$

$|\langle\varphi|\psi\rangle|^2 = 0$ if $\theta = \pi$



SWAP test on IBM-Q

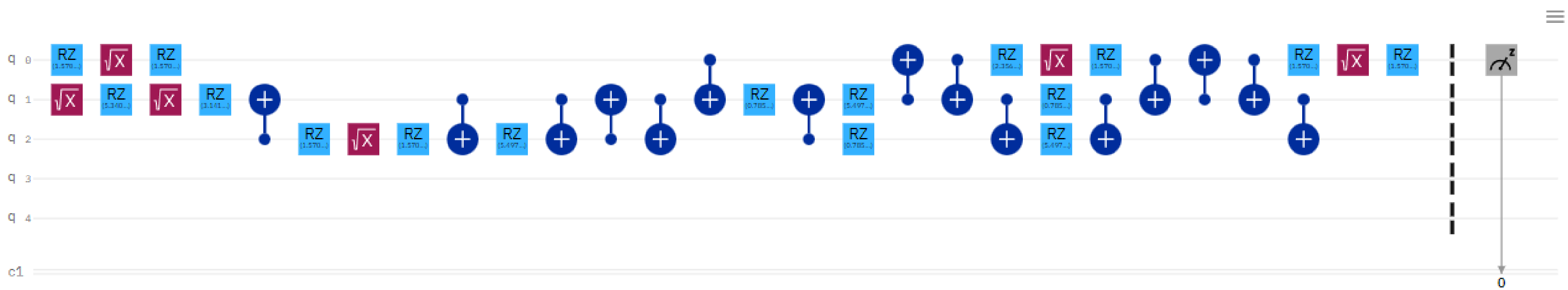
Original circuit



Original circuit: 3 one-qubit gates and 1 CSWAP (Fredkin) gate

Transpiled one: 22 one-qubit gates and 15 CNOT gates

Transpiled circuit



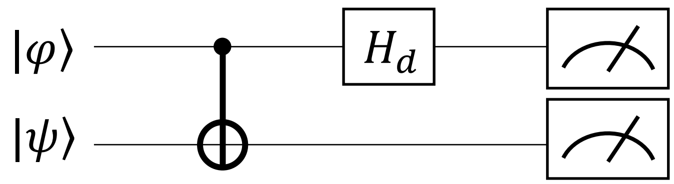
Implementation of CSWAP (Fredkin) gate requires many quantum gates

Square overlap estimation using Hong–Ou–Mandel effect

$$|\varphi\rangle = c_{0\varphi}|0\rangle + c_{1\varphi}|1\rangle$$

$$|\psi\rangle = c_{0\psi}|0\rangle + c_{1\psi}|1\rangle$$

$$|\langle\varphi|\psi\rangle|^2 = \left(c_{0\varphi}c_{0\psi} + c_{1\varphi}c_{1\psi}\right)^2$$
$$= c_{00}^2 + 2c_{00}c_{11} + c_{11}^2$$



$$|\varphi \otimes \psi\rangle = c_{0\varphi}c_{0\psi}|00\rangle + c_{0\varphi}c_{1\psi}|01\rangle + c_{1\varphi}c_{0\psi}|10\rangle + c_{1\varphi}c_{1\psi}|11\rangle$$
$$= c_{00}|00\rangle + c_{01}|01\rangle + c_{10}|10\rangle + c_{11}|11\rangle$$
$$\xrightarrow{\text{CNOT}[0,1]} c_{00}|00\rangle + c_{01}|01\rangle + c_{10}|11\rangle + c_{11}|10\rangle$$

$$\xrightarrow{H\otimes I} \frac{c_{00}}{\sqrt{2}}(|00\rangle + |10\rangle) + \frac{c_{01}}{\sqrt{2}}(|01\rangle + |11\rangle)$$
$$+ \frac{c_{10}}{\sqrt{2}}(|01\rangle - |11\rangle) + \frac{c_{11}}{\sqrt{2}}(|00\rangle - |10\rangle)$$

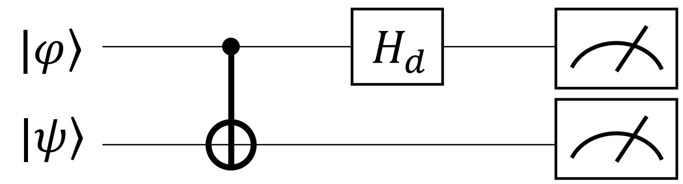
$$= \frac{c_{00} + c_{11}}{\sqrt{2}}|00\rangle + \frac{c_{01} + c_{10}}{\sqrt{2}}|01\rangle + \frac{c_{00} - c_{11}}{\sqrt{2}}|10\rangle + \frac{c_{01} - c_{10}}{\sqrt{2}}|11\rangle$$

J. C. Garcia-Escartin, P. Chamorro-Posada, *Phys. Rev. A* **2013**, *87*, 052330.

Square overlap estimation using Hong–Ou–Mandel effect

$$|\varphi\rangle = c_{0\varphi}|0\rangle + c_{1\varphi}|1\rangle$$

$$|\psi\rangle = c_{0\psi}|0\rangle + c_{1\psi}|1\rangle$$



$$|\langle\varphi|\psi\rangle|^2 = \left(c_{0\varphi}c_{0\psi} + c_{1\varphi}c_{1\psi}\right)^2$$
$$= c_{00}^2 + 2c_{00}c_{11} + c_{11}^2$$

$$|\varphi \otimes \psi\rangle \longrightarrow \frac{c_{00}+c_{11}}{\sqrt{2}}|00\rangle + \frac{c_{01}+c_{10}}{\sqrt{2}}|01\rangle + \frac{c_{00}-c_{11}}{\sqrt{2}}|10\rangle + \frac{c_{01}-c_{10}}{\sqrt{2}}|11\rangle$$

$$P(00) = \frac{c_{00}^2 + 2c_{00}c_{11} + c_{11}^2}{2}$$

$$P(01) = \frac{c_{01}^2 + 2c_{01}c_{10} + c_{10}^2}{2}$$

$$P(10) = \frac{c_{00}^2 - 2c_{00}c_{11} + c_{11}^2}{2}$$

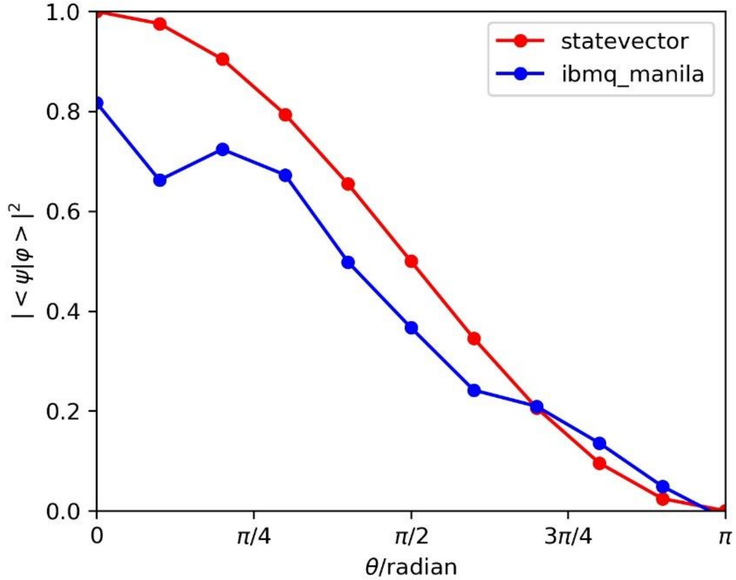
$$P(11) = \frac{c_{01}^2 - 2c_{01}c_{10} + c_{10}^2}{2}$$

$$|\langle\varphi|\psi\rangle|^2 = [P(00) + P(01) + P(10) - P(11)]$$

J. C. Garcia-Escartin, P. Chamorro-Posada, *Phys. Rev. A* **2013**, *87*, 052330.

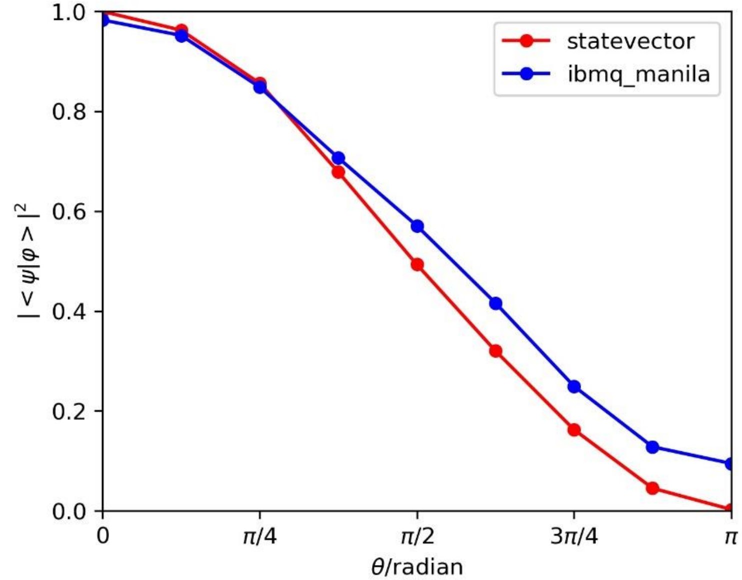
Square overlap estimation using Hong–Ou–Mandel effect

SWAP test



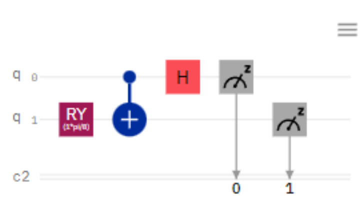
37 quantum gates after transpilation

Hong–Ou–Mandel effect

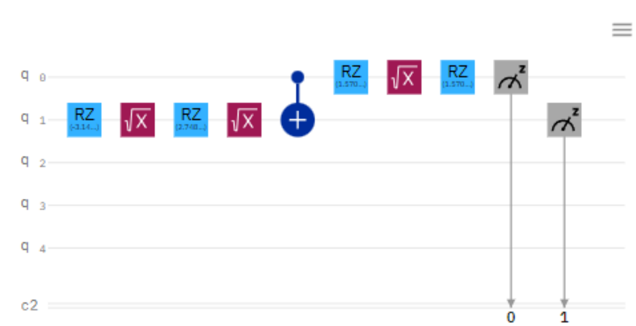


8 quantum gates after transpilation

Original circuit

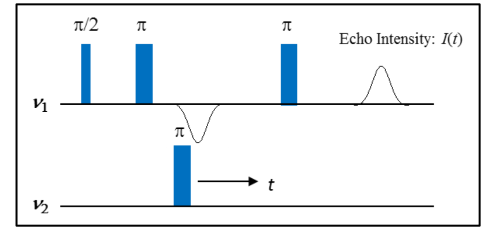


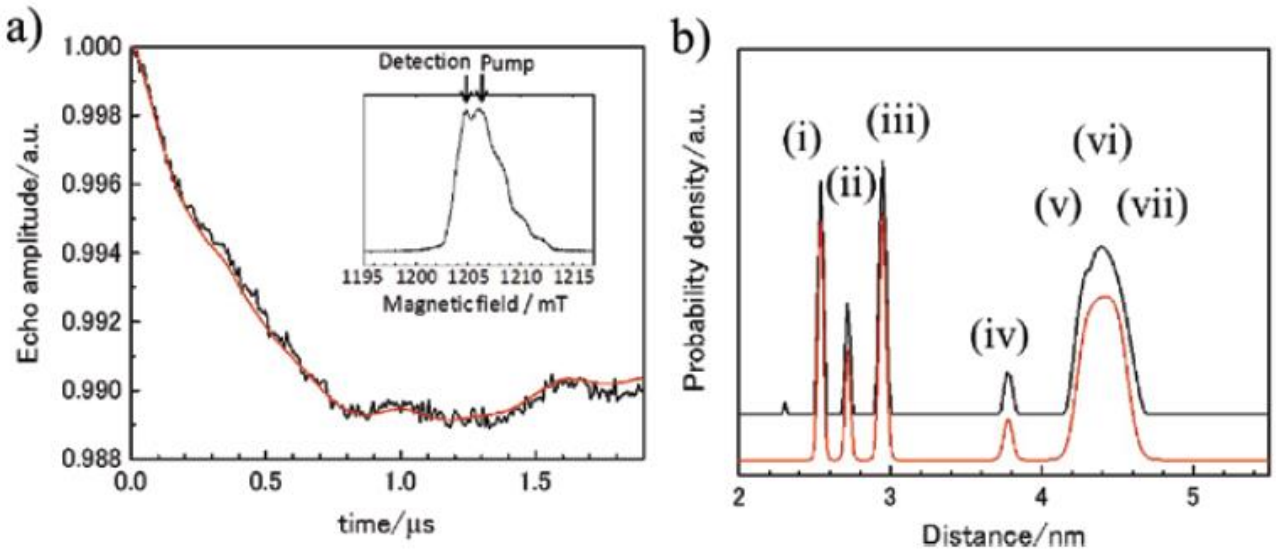
Transpiled circuit



Fourier transformation

Discrete Fourier transformation: $y_k \equiv \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{2\pi i jk/N}$





Dipolar interactions between unpaired electrons → Spin–spin distance measurement

S. Yamamoto, S. Nakazawa, K. Sugisaki, et al, *Z. Phys. Chem.* **2017**, *231*, 439–458.

Quantum Fourier transformation

Discrete Fourier transformation: $y_k \equiv \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{2\pi ijk/N}$

Quantum Fourier transformation: $U|j\rangle = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi ijk/2^n} |k\rangle$

We write the state $|j\rangle$ using the binary representation: $j = 2^{n-1}j_1 + 2^{n-2}j_2 + \cdots + 2^0 j_n$

Also, we use the binary fraction: $0.j_l j_{l+1} \cdots j_m = j_l/2^1 + j_{l+1}/2^2 + \cdots + j_m/2^{m-l+1}$

$$U|j\rangle = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi ijk/2^n} |k\rangle$$

$$= \frac{1}{\sqrt{2^n}} \left(|0\rangle + e^{2\pi i0.j_n}|1\rangle\right)\left(|0\rangle + e^{2\pi i0.j_{n-1}j_n}|1\rangle\right) \cdots \left(|0\rangle + e^{2\pi i0.j_1 j_2 \cdots j_n}|1\rangle\right)$$

Quantum Fourier transformation

$\boxed{n = 1}$

$$U|j\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i 0.j_1}|1\rangle\right)$$

$$j_1 = 0 \longrightarrow e^{2\pi i \times 0} = e^0 = 1 \longrightarrow U|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$j_1 = 1 \longrightarrow e^{2\pi i \times 1/2} = e^{\pi i} = -1 \longrightarrow U|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Schedule of this lecture series

$\boxed{n = 2}$

$$U|j\rangle = \frac{1}{2}\left(|0\rangle + e^{2\pi i 0.j_2}|1\rangle\right)\left(|0\rangle + e^{2\pi i 0.j_1 j_2}|1\rangle\right)$$

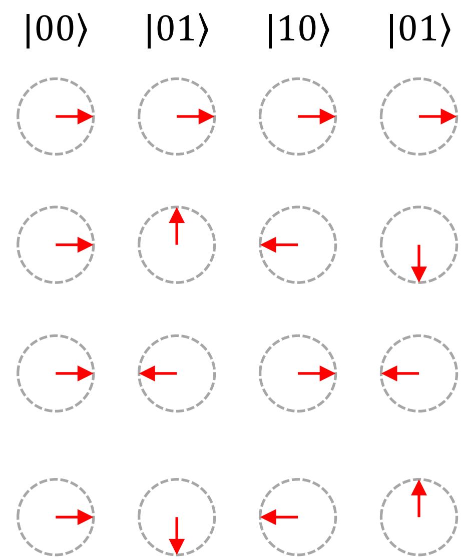
$$= \frac{1}{2}\left\{|00\rangle + e^{2\pi i 0.j_1 j_2}|01\rangle + e^{2\pi i 0.j_2}|10\rangle + e^{2\pi i(0.j_2 + 0.j_1 j_2)}|11\rangle\right\}$$

$$U|00\rangle = \frac{1}{2}\left(|00\rangle + |01\rangle + |10\rangle + |11\rangle\right)$$

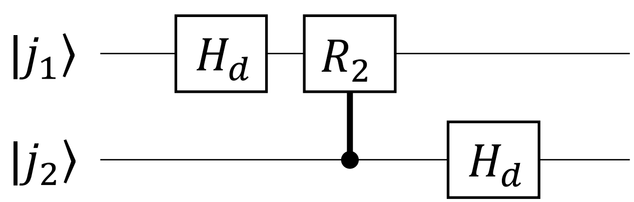
$$U|01\rangle = \frac{1}{2}\left(|00\rangle + e^{2\pi i \times 1/4}\,|01\rangle + e^{2\pi i \times 1/2}\,|10\rangle + e^{2\pi i \times 3/4}\,|11\rangle\right)$$

$$U|10\rangle = \frac{1}{2}\left(|00\rangle + e^{2\pi i \times 1/2}\,|01\rangle + e^{0}\,|10\rangle + e^{2\pi i \times 1/2}\,|11\rangle\right)$$

$$U|11\rangle = \frac{1}{2}\left(|00\rangle + e^{2\pi i \times 3/4}\,|01\rangle + e^{2\pi i \times 1/2}\,|10\rangle + e^{2\pi i \times 5/4}\,|11\rangle\right)$$



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



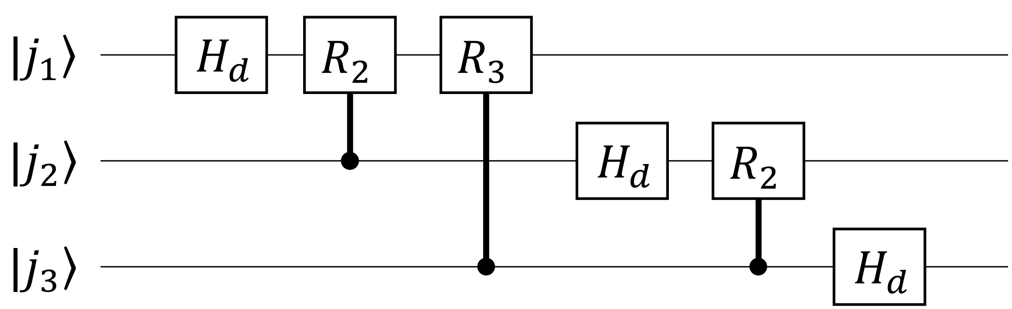
Quantum Fourier transformation

$\boxed{n = 3}$

$$U|j\rangle = \frac{1}{\sqrt{2^3}}\left(|0\rangle + e^{2\pi i 0.j_3}|1\rangle\right)\left(|0\rangle + e^{2\pi i 0.j_2 j_3}|1\rangle\right)\left(|0\rangle + e^{2\pi i 0.j_1 j_2 j_3}|1\rangle\right)$$

$\|j\rangle$	$\|000\rangle$	$\|001\rangle$	$\|010\rangle$	$\|011\rangle$	$\|100\rangle$	$\|101\rangle$	$\|110\rangle$	$\|111\rangle$	Rotational angle
000	→	→	→	→	→	→	→	→	2π × 0/8
001	→	↗	↑	↖	←	↙	↓	↘	2π × 1/8
010	→	↑	←	↓	→	↑	←	↓	2π × 2/8
011	→	↖	↓	↗	←	↘	↑	↙	2π × 3/8
100	→	←	→	←	→	←	→	←	2π × 4/8
101	→	↙	↑	↘	←	↗	↓	↖	2π × 5/8
110	→	↓	←	↑	→	↓	←	↑	2π × 6/8
111	→	↘	↓	↙	←	↖	↑	↗	2π × 7/8

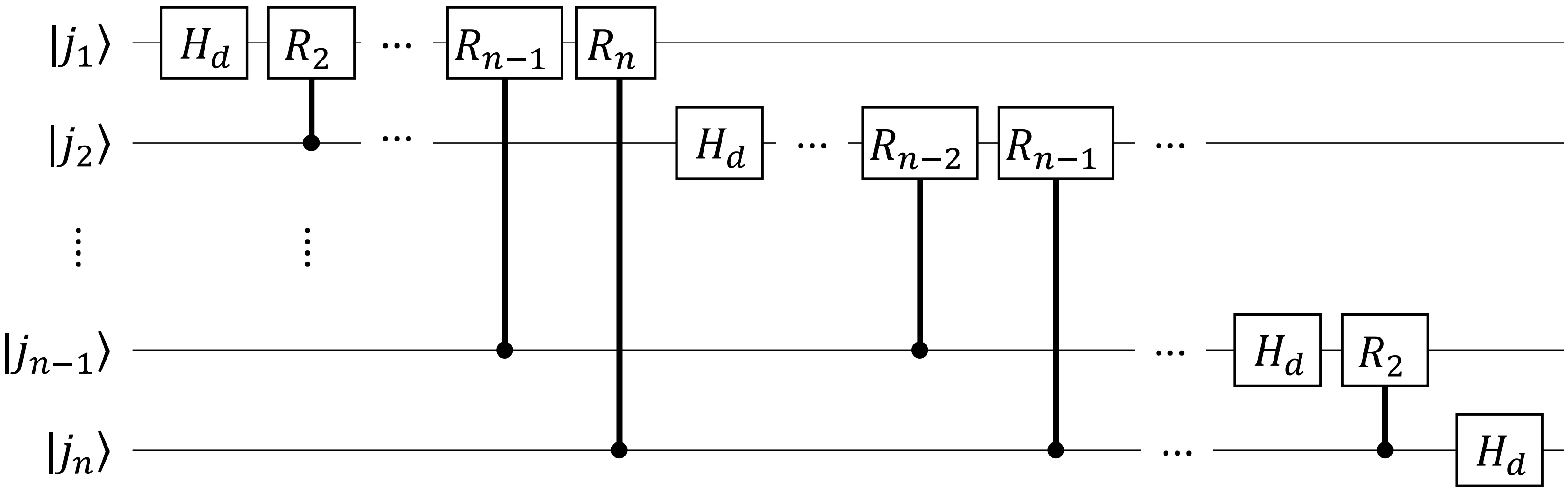
$$R_k \equiv \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{pmatrix}$$



Quantum Fourier transformation

$$U|j\rangle = \frac{1}{\sqrt{2^n}}\left(|0\rangle + e^{2\pi i 0.j_n}|1\rangle\right)\left(|0\rangle + e^{2\pi i 0.j_{n-1}j_n}|1\rangle\right)\cdots\left(|0\rangle + e^{2\pi i 0.j_1 j_2\cdots j_n}|1\rangle\right)$$

For general *n*



Applications of QFT

- Shor's algorithm for prime factorization
- Quantum phase estimation for the eigenproblems of unitary operators
- Hidden subgroup problems
- Linear systems of equations by Harrow, Hassidim, and Lloyd (HHL algorithm)