Quantum algorithms: Shor's integer factoring quantum part

Yipeng Huang

Rutgers University

February 23, 2024

Prog Assignment 1. :

Problem Sets 1/2/3 :

Project. = Parameters for project

Prog Assignment. 2, 3. near term algo.
{ optimization
chem.

Table of contents

The factoring problem

One way functions for cryptography

1. Multiplying two b-bit numbers: on order of b^2 time.

2. Best known classical algorithm to factor a b-bit number: on order of about $2^{\sqrt[3]{b}}$ time.

   ▶ Makes multiplying large primes a candidate one-way function.
   ▶ It's an open question of mathematics to prove whether one way functions exist.

Public key cryptography

Numberphile YouTube channel explanation of RSA public key cryptography:
`https://www.youtube.com/watch?v=M7kEpw1tn50`

The factoring problem

One way functions for cryptography

1. Multiplying two b-bit numbers: on order of b^2 time.
2. Best known classical algorithm to factor a b-bit number: on order of about $2^{\sqrt[3]{b}}$ time.

Quantum integer factoring algorithm

▶ Quantum algorithm to factor a b-bit number: b^3.

▶ Peter Shor, 1994.

▶ Important example of quantum algorithm offering exponential speedup.

Table of contents

The classical part: converting factoring to order finding / period finding

General strategy for the classical part

1. Factoring
2. Modular square root
3. Discrete logarithm
4. Order finding
5. Period finding

The fact that a quantum algorithm can support all these primitives leads to additional ways that future quantum computing can be useful / threatening to existing cryptography.

Factoring

$$N = pq$$

$$N = 15 = 3 \times 5$$

Modular square root

Finding the modular square root

$$s^2 \mod N = 1$$

$$s = \sqrt{1} \mod N$$

Trivial roots would be $s = \pm 1$.

▶ Are there other (nontrivial) square roots?

▶ For $N = 15$, $s = \pm 4$, $s = \pm 11$, $s = \pm 14$ are all nontrivial square roots. (Show this).

▶ Later in these slides, we will see how nontrivial square roots are useful for factoring.

Discrete log

1. Pick a that is relatively prime with N.
2. Efficient to test if relatively prime by finding GCD using Euclid's algorithm. For example, a=6 and n=15.

Exercise: list the possible a's for $N = 15$.

Discrete log

1. Pick a that is relatively prime with N.
2. Efficient to test if relatively prime by finding GCD using Euclid's algorithm. For example, $a = 6$ and $n = 15$.

So now our factoring problem is:

$$a^r \mod N = 1$$

$$a^r \equiv 1 \mod N$$

In fact, this algorithm for finding discrete log even more directly attacks other crypto primitives such as Diffie-Hellman key exchange.

Order finding

Our discrete log problem is equivalent to order finding.

	$a^1 \mod 15$	$a^2 \mod 15$	$a^3 \mod 15$	$a^4 \mod 15$
a=2	2	4	8	1
a=4	4	1	4	1
a=7	7	4	13	1
a=8	8	4	2	1
a=11	11	1	11	1
a=13	13	4	7	1
a=14	14	1	14	1

Find smallest r such that $a^r \equiv 1 \mod N$

Period finding

In other words, the problem by now can also be phrased as finding the period of a function.

$$f(x) = f(x + r)$$

Where

$$f(x) = a^x = a^{x+r} \mod N$$

Find r.

What to do after quantum algorithm gives you r

▶ If r is odd or if $a^{\frac{r}{2}} + 1 \equiv 0 \mod N$, abandon.

▶ There is separate theorem saying no more than a quarter of trials would have to be tossed.

Exercise: try for $a = 14$.

What to do after quantum algorithm gives you r

▶ If r is odd or if $a^{\frac{r}{2}} + 1 \equiv 0 \mod N$, abandon.

▶ There is separate theorem saying no more than a quarter of trials would have to be tossed.

Exercise: try for $a = 14$.

Otherwise, factors are GCD($a^{\frac{r}{2}} \pm 1$, N)

a=2	r=4	$2^2 \pm 1 = 4 \pm 1$
a=4	r=2	$4^1 \pm 1 = 4 \pm 1$
a=7	r=4	$7^2 \pm 1 = 49 \pm 1$
a=8	r=4	$8^2 \pm 1 = 64 \pm 1$
a=11	r=2	$11^1 \pm 1 = 11 \pm 1$
a=13	r=4	$13^2 \pm 1 = 169 \pm 1$
a=14	r=2	$14^2 \pm 1 = 196 \pm 1$ (bad case)

Notice why we discarded 14.

Proof why this works and why factoring is modular square root

$$a^r \equiv 1 \mod N$$

So now $a^{\frac{r}{2}}$ is a nontrivial square root of 1 mod N.

$$a^r - 1 \equiv 0 \mod N$$

$$(a^{\frac{r}{2}} - 1)(a^{\frac{r}{2}} + 1) \equiv 0 \mod N$$

The above implies that

$$\frac{(a^{\frac{r}{2}} - 1)(a^{\frac{r}{2}} + 1)}{N}$$

is an integer. So now we have to prove that

1. $\frac{a^{\frac{r}{2}} - 1}{N}$ is not an integer, and

2. $\frac{a^{\frac{r}{2}} + 1}{N}$ is not an integer.

$$(a^r - 1) = kN = kpq$$

$$(a^{\frac{r}{2}} - 1)(a^{\frac{r}{2}} + 1) = kpq$$

$$a^{\frac{r}{2}} - 1 = k_0 p$$

$$a^{\frac{r}{2}} + 1 = k_1 q$$

Proof why this works and why factoring is modular square root

Suppose $\frac{a^{\frac{r}{2}}-1}{N}$ is an integer

that would imply

$$a^{\frac{r}{2}} - 1 \equiv 0 \mod N$$

$$a^{\frac{r}{2}} \equiv 1 \mod N$$

but we already defined r is the smallest such that $a^r \equiv 1 \mod N$, so there is a contradiction, so $\frac{a^{\frac{r}{2}}-1}{N}$ is not an integer.

Suppose $\frac{a^{\frac{r}{2}}+1}{N}$ is an integer

that would imply

$$a^{\frac{r}{2}} + 1 \equiv 0 \mod N$$

but we already eliminated such cases because we know this doesn't give us a useful result.

Table of contents

I. Simon's problem

hidden string:
period finding:

$$f(x) = f(x \oplus s) \in \{0,1\}^{\otimes m}$$

$$f(x) = f(x+r)$$

$$f(x) \neq f(x \oplus s)$$

$n=1$	$s=0$				$s=1$			
$f(0)$	$f(0)=f(0)$	0	1		$f(0)=f(1)$	0	1	
$f(1)$	$f(1)=f(1)$	1	0		$f(1)=f(0)$	0	1	

$n=2$	$s=00$			$s=01$			$s=11$		
$f(00)$	$f(00)=f(00)$ 11			$f(00)=f(01)$	0	1	$f(00)=f(11)$ 0	1	
$f(01)$	$f(01)=f(01)$ 10			$f(01)=f(00)$			$f(01)=f(10)$ 1	0	
$f(10)$	$f(10)=f(10)$ 01	$\cdots$		$f(10)=f(11)$	1	0	$f(10)=f(01)$ 1	0	
$f(11)$	$f(11)=f(11)$ 00			$f(11)=f(10)$			$f(11)=f(00)$ 0	1	

$$A: \quad \frac{1}{\sqrt{2}^n} \sum_{x=0}^{2^n-1} |x\rangle \otimes |0\rangle^{\otimes m}$$

$$B: \quad \frac{1}{\sqrt{2}^n} \sum_{x=0}^{2^n-1} |x\rangle \otimes |f(x)\rangle$$

$$= \frac{1}{\sqrt{2}^n} \sum_{x=0}^{2^n-1} \frac{1}{\sqrt{2}} \left(|x\rangle + |x \oplus s\rangle \right) \otimes |f(x)\rangle$$
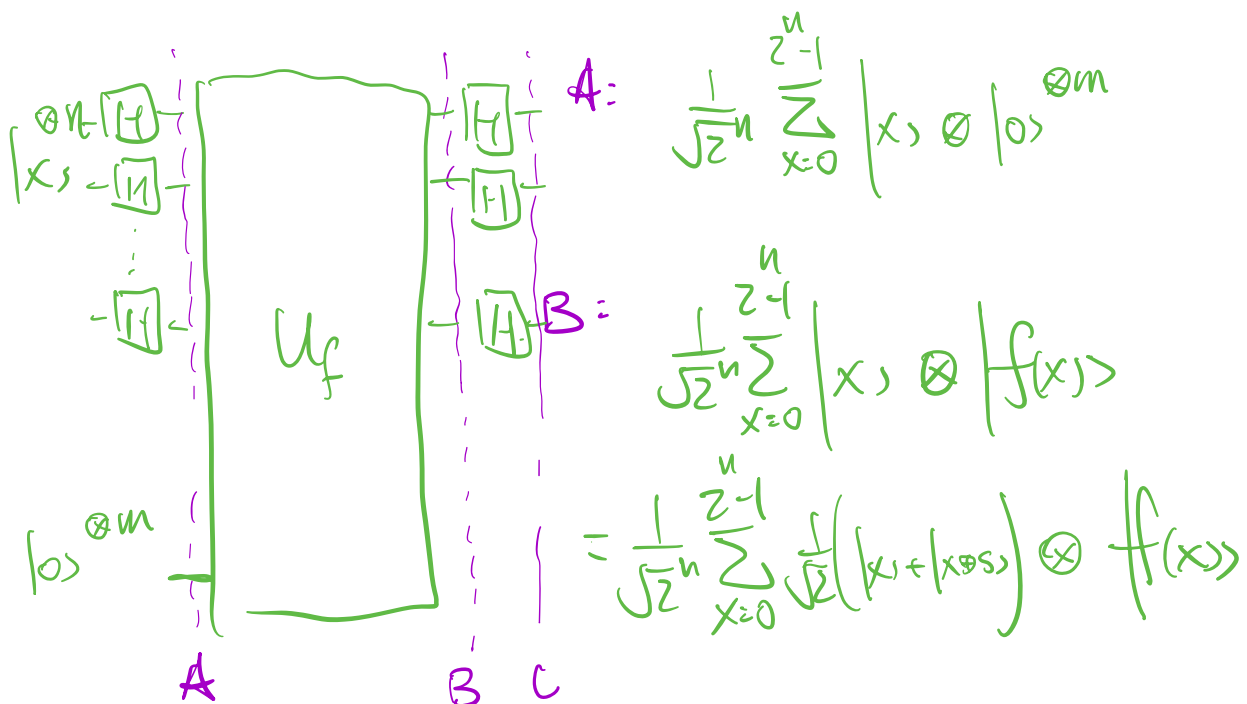
$$H^{\otimes n}\bigg|x\rangle = \frac{1}{\sqrt{2}^n}\sum_{y=0}^{2^n-1}(-1)^{x\cdot y}\bigg|y\rangle \quad C: \quad \frac{1}{\sqrt{2}^n}\sum_{y=0}^{2^n-1}\frac{1}{\sqrt{2}}\frac{1}{\sqrt{2}^n}\sum_{x=0}^{2^n-1}\left((-1)^{x\cdot y}+(-1)^{(S\oplus x)\cdot y}\right)\bigg|y\rangle\otimes\bigg|f(x)\rangle$$

$$= C_{norm}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1}\left((-1)^{x\cdot y}\left(1+(-1)^{S\cdot y}\right)\right)|y\rangle\otimes|f(x)\rangle$$

$$S\cdot y = 0$$

$S = 010$

$$y = \begin{cases}000? & S\cdot y = 010\cdot000 = 0\oplus0\oplus0 = 0 & \checkmark\\001? & S\cdot y = 010\cdot001 = 0\oplus0\oplus0 = 0 & \checkmark\\010? & S\cdot y = 010\cdot010 = 0\oplus1\oplus0 = 1 & \times\\011? & S\cdot y = 010\cdot011 = 0\oplus1\oplus0 = 1 & \times\\100? & S\cdot y = 010\cdot100 = 0\oplus0\oplus0 = 0 & \checkmark\\101? & S\cdot y = 010\cdot101 = 0\oplus0\oplus0 = 0 & \checkmark\\110? & S\cdot y = 010\cdot110 = 0\oplus1\oplus0 = 1 & \times\\111? & S\cdot y = 010\cdot111 = 0\oplus1\oplus0 = 1 & \times\end{cases}$$

$$y = \begin{cases}000\\001\\100\\101\end{cases}$$

$$\Downarrow H\otimes I$$

$$\frac{1}{\sqrt{2}^n}\sum_{y=0}^{2^n-1}\frac{1}{\sqrt{2}}\frac{1}{\sqrt{2}^n}\left[(-1)^{x\cdot y}+(-1)^{(x\oplus a)\cdot y}\right]|y\rangle|f(x)\rangle$$

$$= (-1)^{x\cdot y}\boxed{\left[1+(-1)^{a\cdot y}\right]}|y\rangle$$

any y you measure, $a\cdot y = 0$

Table of contents

The quantum part: period finding using quantum Fourier transform

▶ After picking a value for a, use quantum parallelism to calculate modular exponentiation: $a^x \mod N$ for all $0 \leq x \leq 2^n - 1$ simultaneously.

▶ Use interference to find a global property, such as the period r.

Calculate modular exponentiation
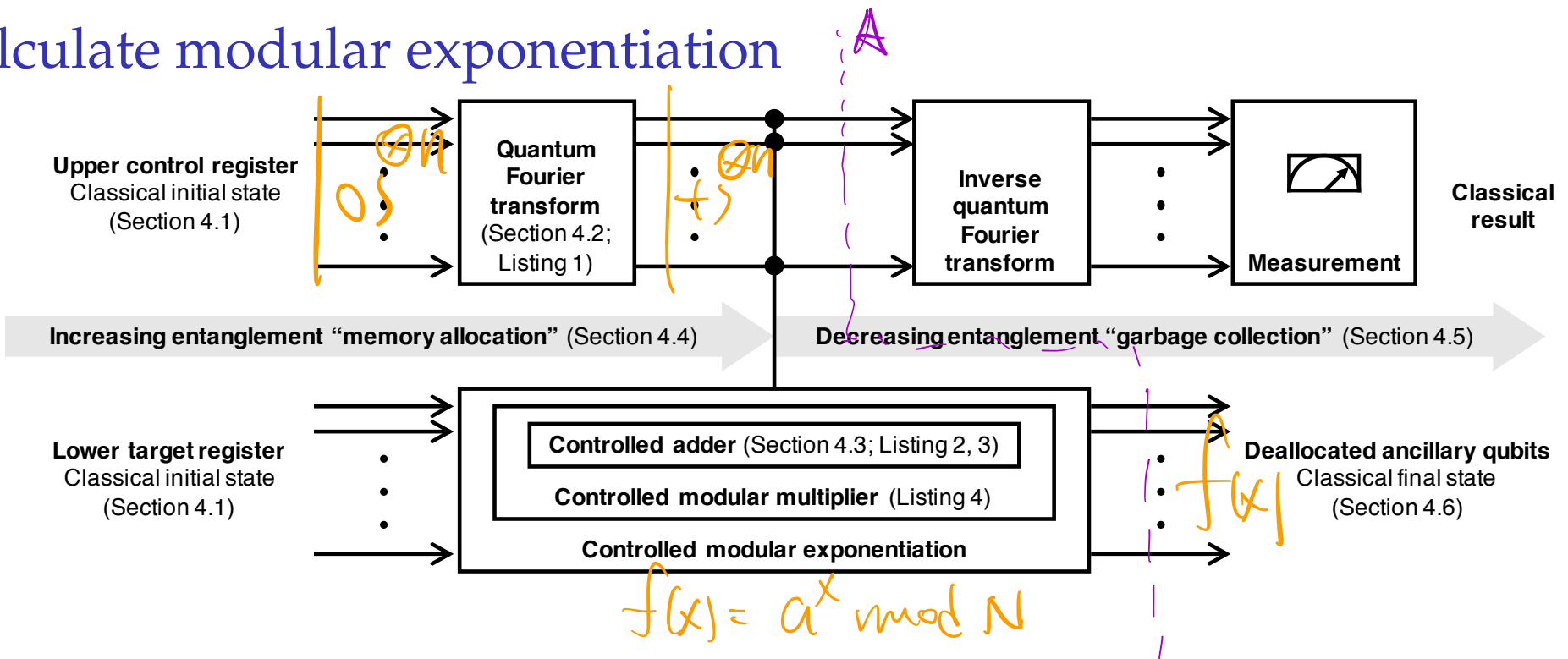
- ▶ Image source: Huang and Martonosi, Statistical assertions for validating patterns and finding bugs in quantum programs, 2019.
- ▶ A good source on how to build the controlled adder, controlled multiplier, and controlled exponentiation is in Beauregard, Circuit for Shor's algorithm using 2n+3 qubits, 2002.

Calculate modular exponentiation

► State after applying modular exponentiation circuit is

$$A: \qquad \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle |f(x)\rangle$$

► Concretely, using our running example of $N = 15$, need $n = 4$ qubits to encode, and suppose we picked $a = 2$, the state would be

$$\frac{1}{4} \sum_{x=0}^{15} |x\rangle |2^x \mod 15\rangle$$

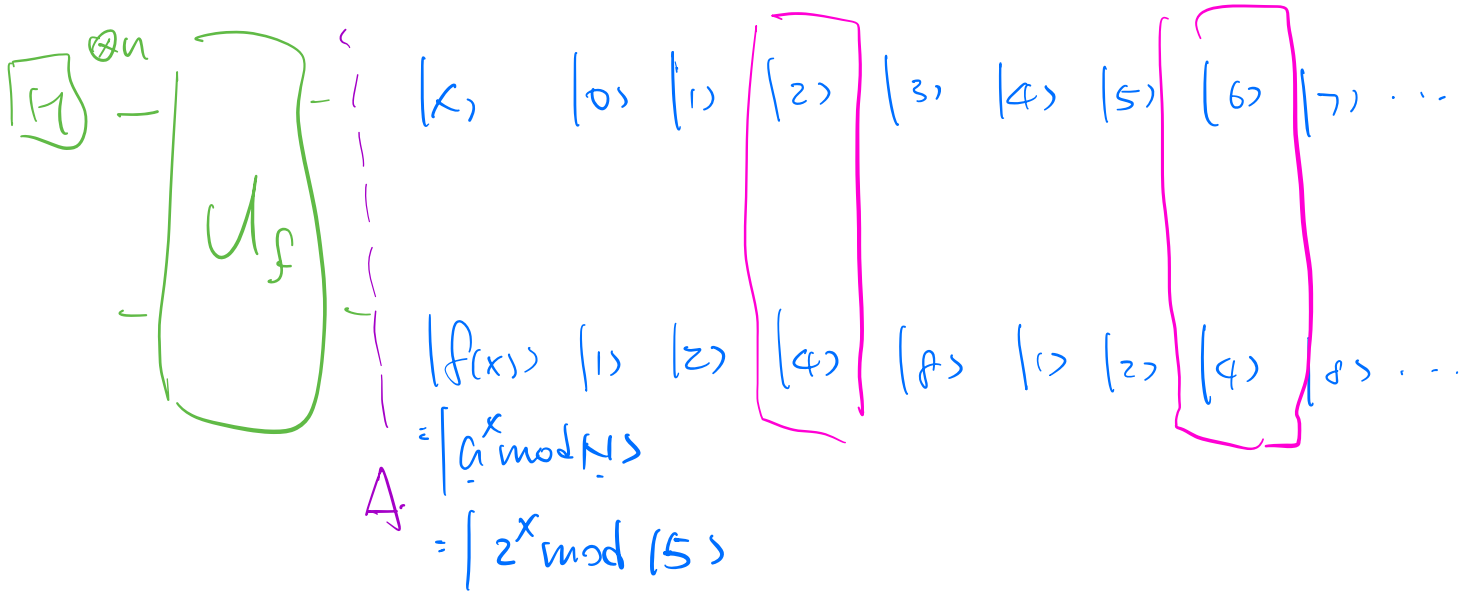# Measurement of target (bottom, ancillary) qubit register

▶ We then measure the target qubit register, collapsing it to a definite value. The state of the upper register would then be limited to:

$$\frac{1}{\sqrt{A}} \sum_{a=0}^{A-1} |x_0 + ar\rangle$$

▶ Concretely, using our running example of $N = 15$, and suppose we picked $a = 2$, and suppose measurement results in 2, the upper register would be a uniform superposition of all $|x\rangle$ such that $2^x \equiv 2 \mod 15$:

$$\frac{|1\rangle}{2} + \frac{|5\rangle}{2} + \frac{|9\rangle}{2} + \frac{|13\rangle}{2}$$

▶ The key trick now is can we extract the period $r = 4$ from such a quantum state. We do this using the quantum Fourier transform.

$$|H\rangle^{\otimes n} \quad U_f$$

$$|x\rangle \qquad |0\rangle \ |1\rangle \ |2\rangle \ |3\rangle \ |4\rangle \ |5\rangle \ |6\rangle \ |7\rangle \ \cdots$$

$$|f(x)\rangle \ |1\rangle \ |2\rangle \ |4\rangle \ |8\rangle \ |1\rangle \ |2\rangle \ |4\rangle \ |8\rangle \ \cdots$$

$$= |a^x \bmod N\rangle$$

$$A: \quad = |2^x \bmod 15\rangle$$

convert a series w/ large periodicity r
into a series w/ small periodicity P.

Quantum Fourier transform to obtain period

The task now is to use Fourier transform to obtain the period.

$$QFT\left(\,|x\rangle\,\right) = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{\frac{2\pi i}{2^n}xy} \,|y\rangle$$

$$QFT = \frac{1}{\sqrt{2^n}} \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \cdots & \omega^{2^n-1} \\ 1 & \omega^2 & \omega^4 & \cdots & \omega^{2(2^n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{2^n-1} & \omega^{2(2^n-1)} & \cdots & \omega^{(2^n-1)(2^n-1)} \end{bmatrix}$$
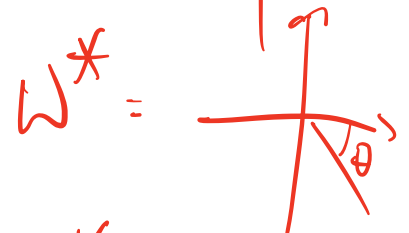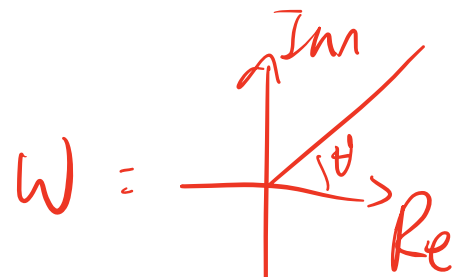
Where

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

And recall that

$$e^{ix} = \cos x + i \sin x$$

Q3.6)

$$QFT = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 \\ 1 & \omega^2 & \omega^9 & \omega^6 \\ 1 & \omega^3 & \omega^6 & \omega^9 \end{bmatrix}$$

$$W = $$

$$W^* = $$

$$W^* = \omega^{-1}$$

$$QFT \cdot QFT^\dagger = I$$

$$QFT^\dagger = (QFT)^{T*} = QFT^* = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & \omega^{-1} & \omega^{-2} & \omega^{-3} \\ 1 & \omega^{-2} & \omega^{-4} & \omega^{-6} \\ 1 & \omega^{-3} & \omega^{-6} & \omega^{-9} \end{bmatrix}$$
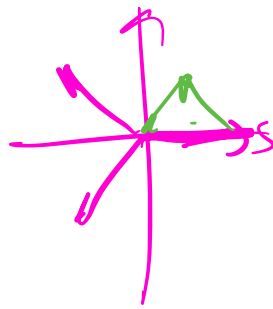
$$= QFT^{-1}$$

$$QFT \cdot QFT^\dagger = QFT \cdot QFT^{-1} = I.$$

Properties of W_N^j

① $\displaystyle\sum_{j=0}^{N-1} W_N^j = \emptyset$

$N = 2^n$

② $\displaystyle\sum_{j=0}^{N-1} W_N^{j \cdot k}$

if $k = mN$: $\displaystyle\sum_{j=0}^{N-1} e^{\frac{2\pi i j m N}{N}} = \sum_{j=0}^{N-1} 1 = N$

else $\displaystyle\sum_{j=0}^{N-1} e^{\frac{2\pi i j k}{N}} = \emptyset$

$$H|x\rangle \Rightarrow H^{\otimes n}|x\rangle = \frac{1}{\sqrt{2}^n}\sum_{y=0}^{N-1} (-1)^{x\cdot y}|y\rangle$$

$$\Downarrow$$

$$QFT|x\rangle = \frac{1}{\sqrt{2}^n}\sum_{y=0}^{N-1} W_N^{xy}|y\rangle$$

$$= \frac{1}{\sqrt{2}^n}\sum_{y=0}^{N-1} e^{\frac{2\pi i}{2^n}\cdot xy}|y\rangle$$

$$x = x_0 x_1 \cdots x_{n-2} x_{n-1} = x_0 \cdot 2^{n-1} + x_1 2^{n-2} \cdots x_{n-2} 2^1 + x_{n-1} 2^0$$

$$y = y_0 y_1 \cdots y_{n-2} y_{n-1} = y_0 2^{n-1} + y_1 2^{n-2} \cdots y_{n-2} 2^1 + y_{n-1} 2^0$$

$xy =$

	x_0 $x_0 2^{n-1}$	x_1 $x_1 2^{n-2}$	$\cdots$	x_{n-2} $x_{n-2} 2^1$	x_{n-1} $x_{n-1} \cdot 1$
$y_0 \cdot 2^{n-1}$	$x_0 y_0 = 2^{2n-2}$	$x_1 y_0 \cdot 2^{2n-3}$		$x_{n-2} y_0 2^n$	$x_{n-1} y_0 \cdot 2^{n-1}$
$y_1 2^{n-2}$	$x_0 y_1 2^{2n-3}$				
$\vdots$					
$y_{n-2} \cdot 2^1$	$x_0 y_{n-2} 2^n$				
$y_{n-1} \cdot 2^0$	$x_0 y_{n-1} 2^{n-1}$				

$$\frac{xy}{2^n} = \left(\frac{y_0 \cdot 2^{n-1} \cdot x_{n-1}}{2^n}\right) + \left(\frac{y_1 2^{n-2}\left(x_{n-2} \cdot 2^1 + x_{n-1}\right)}{2^n}\right)$$
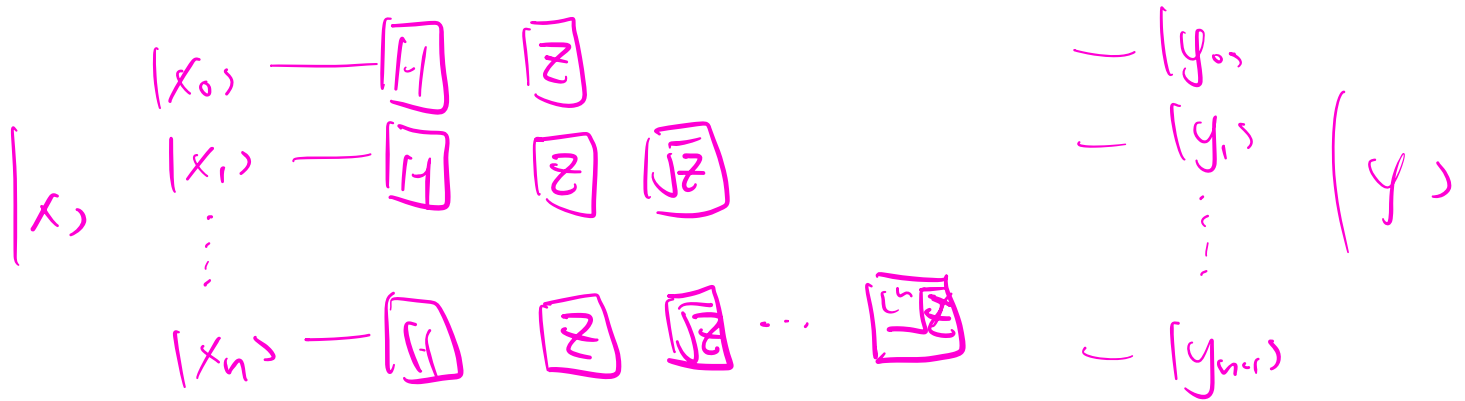
$$\cdots \quad \frac{y_{n-1}\left(x_0 \cdot 2^{n-1} + x_1 \cdot 2^{n-2} \cdots x_{n-1}\right)}{2^n}$$

$$\frac{xy}{2^n} = y_0\left(.x_{n-1}\right) + y_1\left(.x_{n-2}x_{n-1}\right) + \cdots +$$
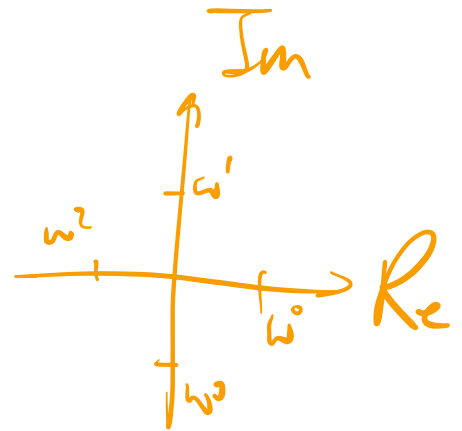$$y_{n-1}\left(.x_0x_1\cdots x_{n-1}\right)$$

$$QFT\,|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{2\pi i\,\frac{xy}{2^n}}\,|y\rangle$$

$$= \quad y_0 \otimes y_1 \otimes \cdots \otimes y_{n-1}$$

$$= \frac{|0\rangle + e^{2\pi i(.x_{n-1})}|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + e^{2\pi i(.x_{n-2}x_{n-1})}|1\rangle}{\sqrt{2}} \otimes \cdots \otimes \frac{|0\rangle + e^{2\pi i(.x_0x_1\cdots x_{n-1})}|1\rangle}{\sqrt{2}}$$

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & \omega_4 & \omega_9^2 & \omega^7 \\ 1 & \omega^2 & \omega^4 & \omega^6 \\ 1 & \omega^7 & \omega^6 & \omega^9 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 \\ \omega^3 \\ \omega^2 \\ \omega^1 \end{bmatrix} = \begin{bmatrix} 1 \\ -i \\ -1 \\ i \end{bmatrix}$$

$$= \quad |\psi\rangle \otimes |\phi\rangle$$

$$= \left(\alpha|0\rangle + \beta|1\rangle\right) \otimes \left(\gamma|0\rangle + \delta|1\rangle\right) = \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|0\rangle - i|1\rangle}{\sqrt{2}}\right)$$

$$= |-\rangle \otimes |-i\rangle$$

$$\begin{aligned} \alpha\gamma &= 1 \\ \alpha\delta &= -i \\ \beta\gamma &= -1 \\ \beta\delta &= i \end{aligned} \qquad \begin{aligned} \alpha &= 1 \\ \delta &= -i \\ \beta &= -1 \\ \gamma &= 1 \end{aligned}$$

$$|0\rangle - \boxed{H} - \boxed{Z} - |-\rangle$$

$$|0\rangle - \boxed{H} - \boxed{Z} - \boxed{S} $$

$$\begin{bmatrix} 1 \\ -i \end{bmatrix}$$
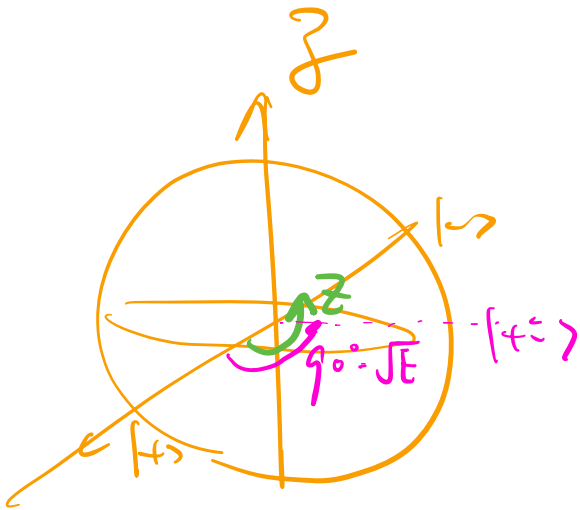
$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

$$P = S = \sqrt{Z} = \begin{bmatrix} 1 & \\ & i \end{bmatrix}$$

$$Z = \sqrt{Z} : \begin{bmatrix} 1 & \\ & -i \end{bmatrix} = (\sqrt{Z})^{\dagger}$$

$$(\sqrt{Z})^{\dagger} = (\sqrt{Z})^{-1}$$

$$U^{\dagger} U = I$$

$$U^{\dagger} = U^{-1}$$

$$S|+\rangle = \begin{bmatrix} 1 & \\ & i \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix}$$

$$= \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{i}{\sqrt{2}} \end{bmatrix} = |+i\rangle$$

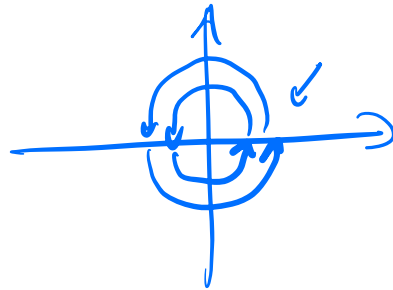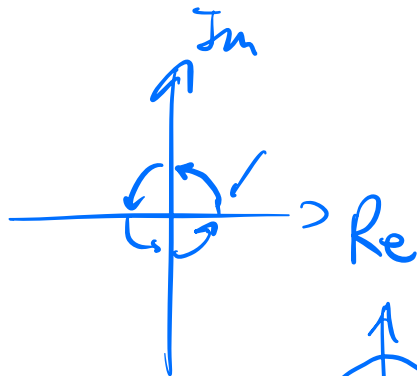$$QFT_4 \, q = \begin{bmatrix} w^0 & w^0 & w^0 & w^0 \\ w^0 & w^1 & w^2 & w^3 \\ w^0 & w^2 & w^4 & w^6 \\ w^0 & w^3 & w^6 & w^9 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & w^1 & w^2 & w^3 \\ 1 & w^2 & 1 & w^2 \\ 1 & w^3 & w^2 & w^1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix}$$

$$= \begin{bmatrix} w^0 + w^0 \\ w^0 + w^2 \\ w^0 + w^4 \\ w^0 + w^6 \end{bmatrix} = \begin{bmatrix} 2 \\ w^0 + w^2 \\ w^0 + w^0 \\ w^0 + w^2 \end{bmatrix} = \begin{bmatrix} 2 \\ w^0 + w^2 \\ 2 \\ w^0 + w^2 \end{bmatrix} = \begin{bmatrix} 2 \\ 0 \\ 2 \\ 0 \end{bmatrix}$$

$$W_4^1 = e^{2\pi i / 2^n} = e^{\frac{2\pi i}{4}} = e^{\frac{1}{2}\pi i} = \cos\frac{\pi}{2} + i\sin\frac{\pi}{2}$$
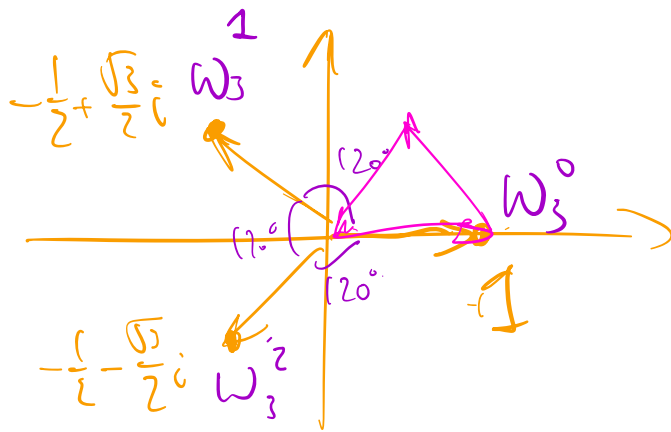$$= i$$

$(W_4^1)^4$

$(W_4^2)^4$

$$W = e^{\frac{2\pi i}{2^n}}$$

Sum property

product property

Roots of unity –

$$W_2 = \sqrt{1} = \pm 1$$

$$\sum_{k=0}^{d-1} W_d^k = \phi$$

$$W_3 = \sqrt[3]{1} = 1,$$

$-\frac{1}{2} + \frac{\sqrt{3}}{2}i$ W_3^1

$120°$

W_3^0

$120°$

$120°$

-1

$-\frac{1}{2} - \frac{\sqrt{3}}{2}i$ W_3^2

Quantum Fourier transform to obtain period

The task now is to use Fourier transform to obtain the period.

$$QFT\Big(\ket{x} \Big) = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{\frac{2\pi i}{2^n} xy} \ket{y}$$

$$QFT\left(\frac{1}{\sqrt{A}} \sum_{a=0}^{A-1} \ket{x_0 + ar} \right)$$

$$= \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} \left(\frac{1}{\sqrt{A}} \sum_{a=0}^{A-1} e^{\frac{2\pi i}{2^n}(x_0+ar)y} \right) \ket{y}$$

$$= \sum_{y=0}^{2^n-1} \left(\frac{1}{\sqrt{2^n A}} e^{\frac{2\pi i}{2^n} x_0 y} \sum_{a=0}^{A-1} e^{\frac{2\pi i}{2^n} ary} \right) \ket{y}$$

Quantum Fourier transform to obtain period

$$\text{Prob}(y) = \frac{A}{2^n} \left| \frac{1}{A} e^{\frac{2\pi i}{2^n} x_0 y} \sum_{a=0}^{A-1} e^{\frac{2\pi i}{2^n} ary} \right|^2$$

$$= \frac{A}{2^n} \left| \frac{1}{A} \sum_{a=0}^{A-1} e^{\frac{2\pi i}{2^n} ary} \right|^2$$

► Here, values of y such that $\frac{ry}{2^n}$ is close to an integer will have maximal measurement probability.

► In our case, only $\frac{ry}{2^n} = \frac{4 \cdot 4}{16}$, $|y\rangle = |4\rangle$ will have high measurement probability.

► To get a beautiful explanation of principle of least action, read Feynman, QED.

How to construct the Quantum Fourier transform
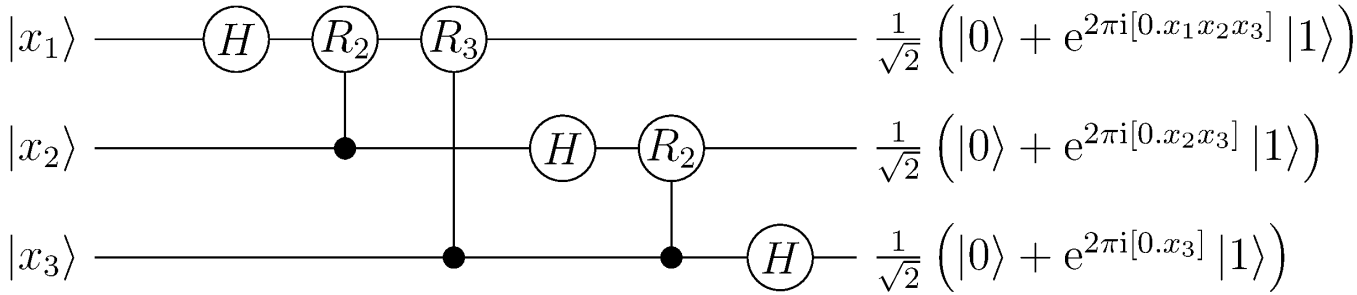

$$|x_1\rangle \quad H \quad R_2 \quad R_3 \qquad \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i[0.x_1 x_2 x_3]}|1\rangle\right)$$

$$|x_2\rangle \qquad\qquad\quad H \quad R_2 \qquad \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i[0.x_2 x_3]}|1\rangle\right)$$

$$|x_3\rangle \qquad\qquad\qquad\qquad H \qquad \frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i[0.x_3]}|1\rangle\right)$$

Figure: Credit: Wikimedia

How to construct the Quantum Fourier transform

$$N = 2^n$$

$$R_k = \begin{bmatrix} 1 & 0 \\ 0 & \exp \frac{2\pi i}{2^k} \end{bmatrix}$$

1.

▶ Cost of computing the FFT for functions encoded in n bits: $O(2^n n) = O\left(N \log N\right)$

$$R_0 = \begin{bmatrix} 1 & 0 \\ 0 & \exp \frac{2\pi i}{2^0} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$$

$$R_1 = \begin{bmatrix} 1 & 0 \\ 0 & \exp \frac{2\pi i}{2^1} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = Z$$

▶ Cost of quantum Fourier transform for functions encoded in n qubits: $O(n^2)$ gates.

$$\| = O(\log^2 N)$$

3.

$$R_2 = \begin{bmatrix} 1 & 0 \\ 0 & \exp \frac{2\pi i}{2^2} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} = S$$

4.

$$R_3 = \begin{bmatrix} 1 & 0 \\ 0 & \exp \frac{2\pi i}{2^3} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & \frac{\sqrt{2}}{2} + \frac{\sqrt{2}i}{2} \end{bmatrix} = T$$

Time cost and implementation

Factoring underpins cryptosystems.

For number represented as b bits:

- ▶ Classical algorithm: needs $O(2^{\sqrt[3]{b}})$ operations. Factoring 512-bit integer: 8400 years. 1024-bit integer: $13 \times 10^{1}2$ years.
- ▶ Quantum algorithm: needs $O(b^2 log(b))$ operations. Factoring 512-bit integer: 3.5 hours. 1024-bit integer: 31 hours.

Source: Oskin et al. A Practical Architecture for Reliable Quantum Computers.
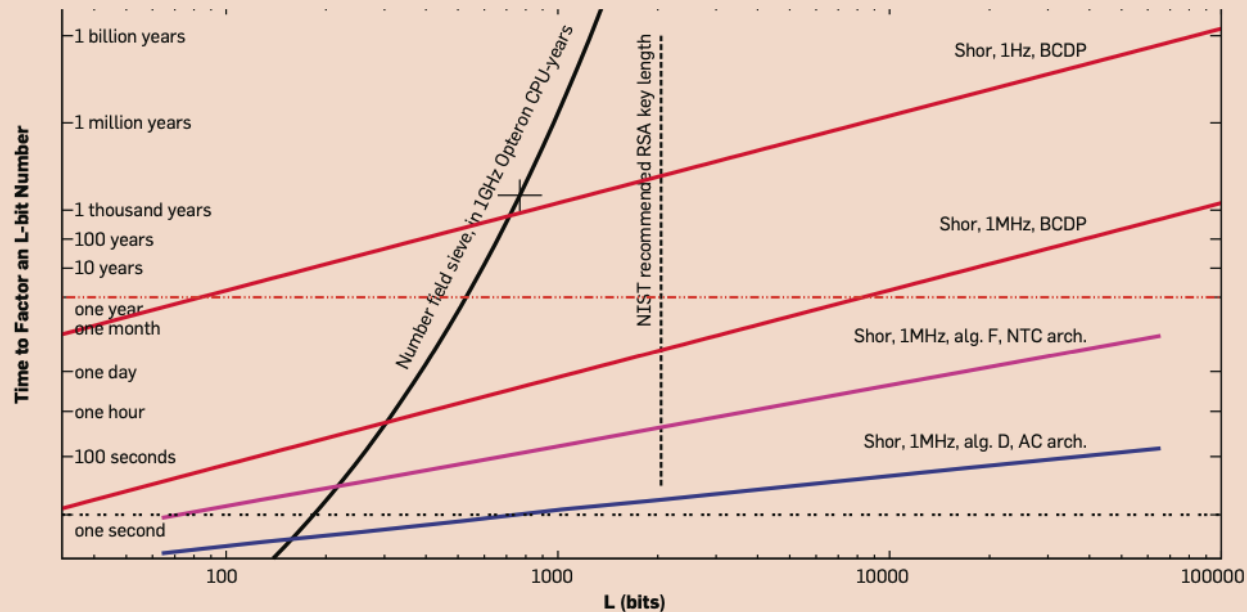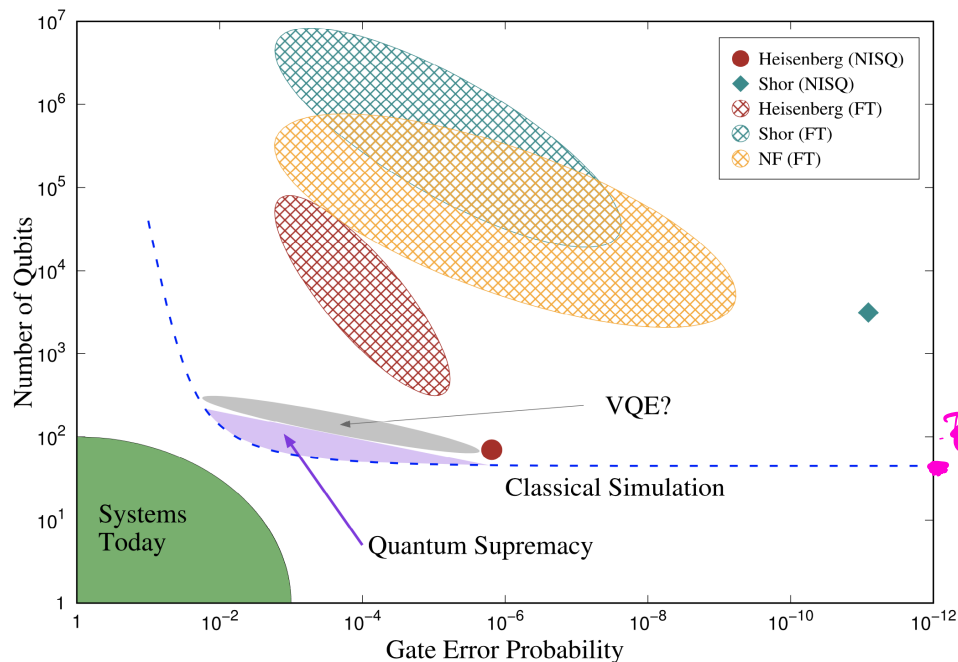
Time cost and implementation

Figure: Credit: Van Meter and Horsman. A Blueprint for Building a Quantum Computer. Communications of the ACM. 2013.

Near-term and far-future quantum computing

Fig. 2. *Performance space of quantum computers, measured by the error probability of each entangling gate in the horizontal axis (roughly inversely proportional to the total number of gates that can be executed on a NISQ machine), and the number of qubits in the system in the vertical axis. Blue dotted line approximately demarcates quantum systems that can be simulated using best classical computers, while the green colored region shows where the existing quantum computing systems with verified performance numbers lie (as of September 2018). Purple shaded region indicates computational tasks that accomplish the so-called "quantum supremacy," where the computation carried out by the quantum computer defies classical simulation regardless of its usefulness. The different shapes illustrate resource counts for solving various problems, with solid symbols corresponding to the exact entangling gate counts and number of qubits in NISQ machines, and shaded regions showing approximate gate error requirements and number of qubits for an FT implementation (not pictured are the regions where the error gets too close to the known fault-tolerance thresholds): cyan diamond and shaded region correspond to factoring a 1024-bit number using Shor's algorithm [14], magenta circle and shaded region represent simulation of a 72-spin Heisenberg model [20], and orange shaded region illustrates NF simulation [21].*

Figure: Credit: Maslov, Nam, and Kim. An Outlook for Quantum Computing. Proceedings of the IEEE. 2019.

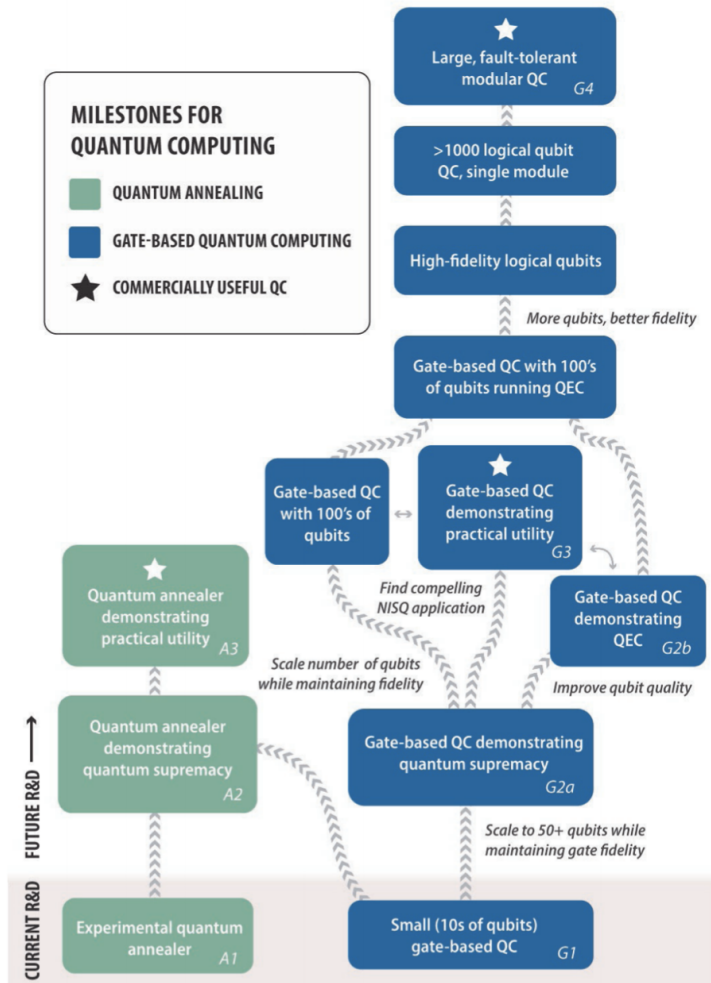# Steps toward useful quantum computing

Figure: Credit: National Academies of Sciences, Engineering, and Medicine. Quantum Computing: Progress and Prospects. 2019.

An illustration of potential milestones of progress in quan-