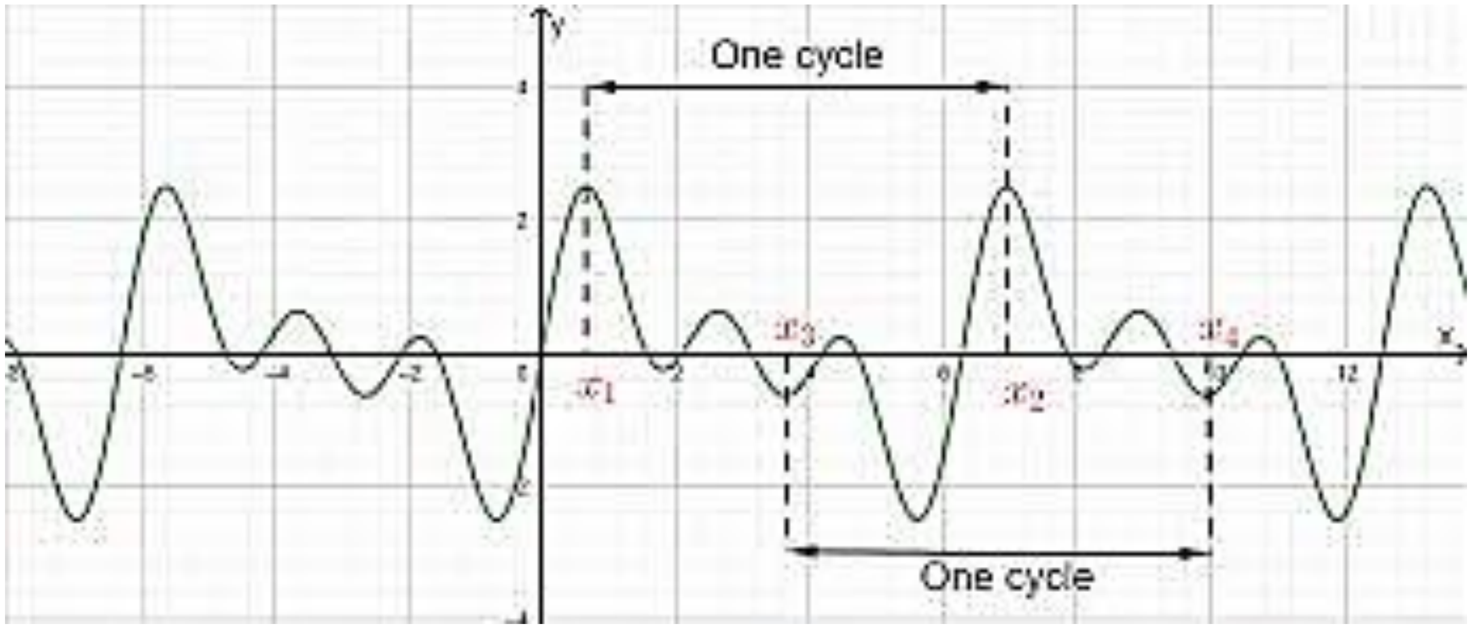
Integer Factorization by Quantum Computers

Wen-Guey Tzeng

Computer Science Department

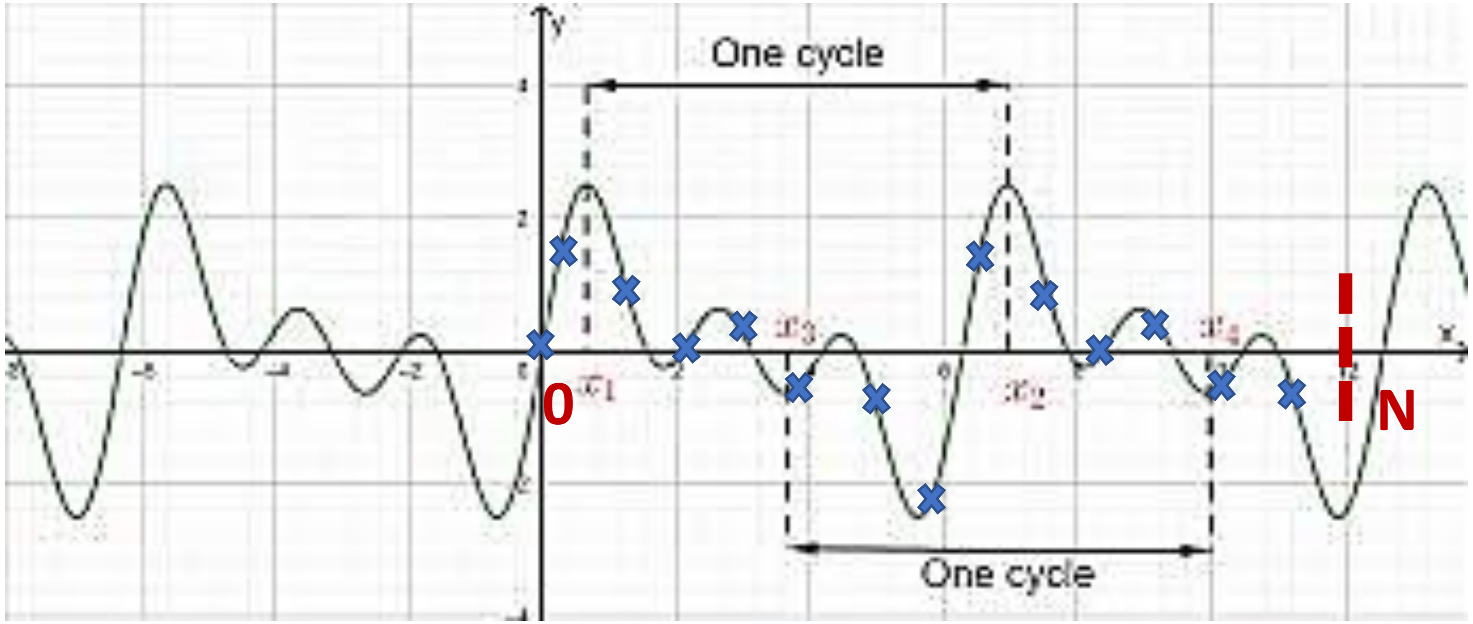
National Chiao Tung University

Periodic function



The <u>period</u> of g(x) is the minimum s that makes g(x)=g(x+s) for all x.

Question: find the period?

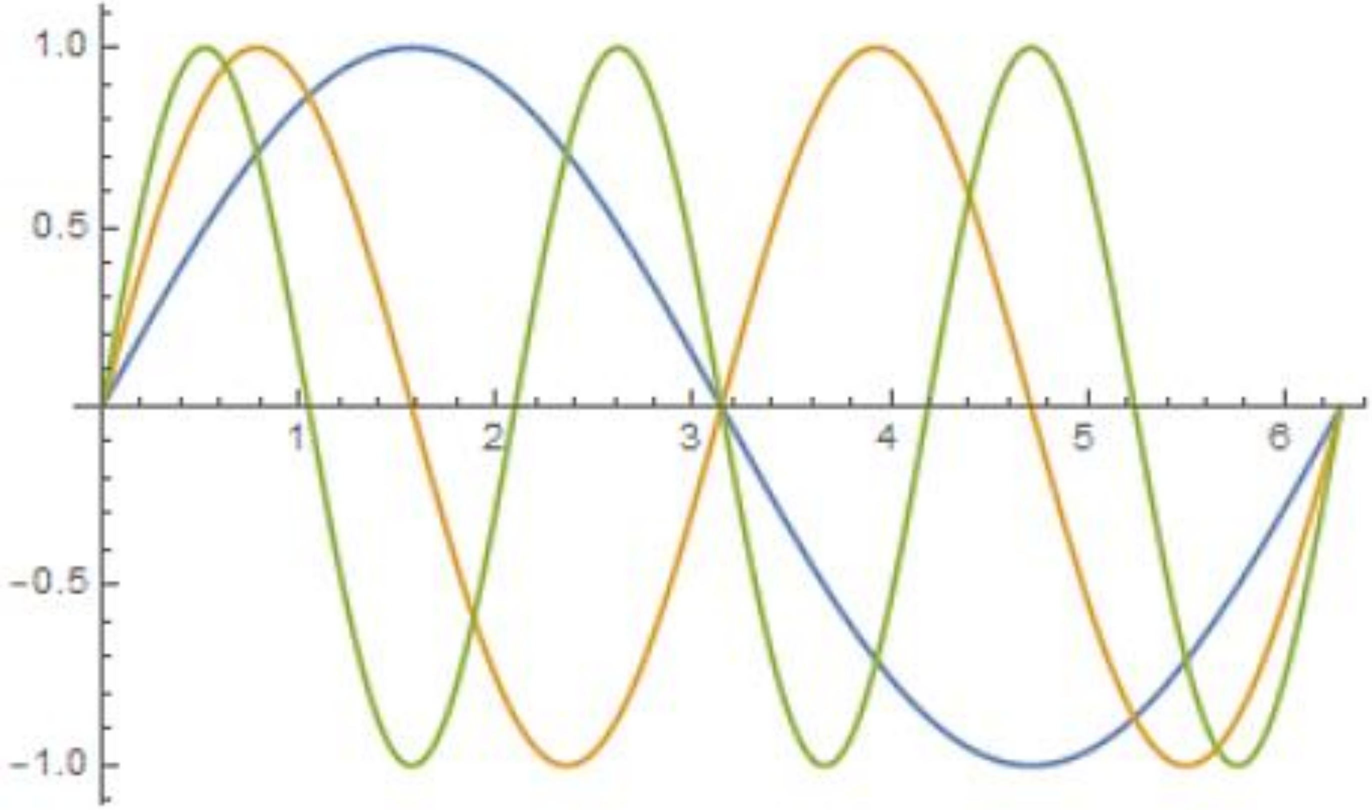


1. Sample N points a_0, a_1, …, a_{N-1} every time unit
2. Find the frequency F in the sampled sequence a_0 a_1 … a_{N-1}.
3. Then, s=1/F.

Periodic function: sin(Fx)

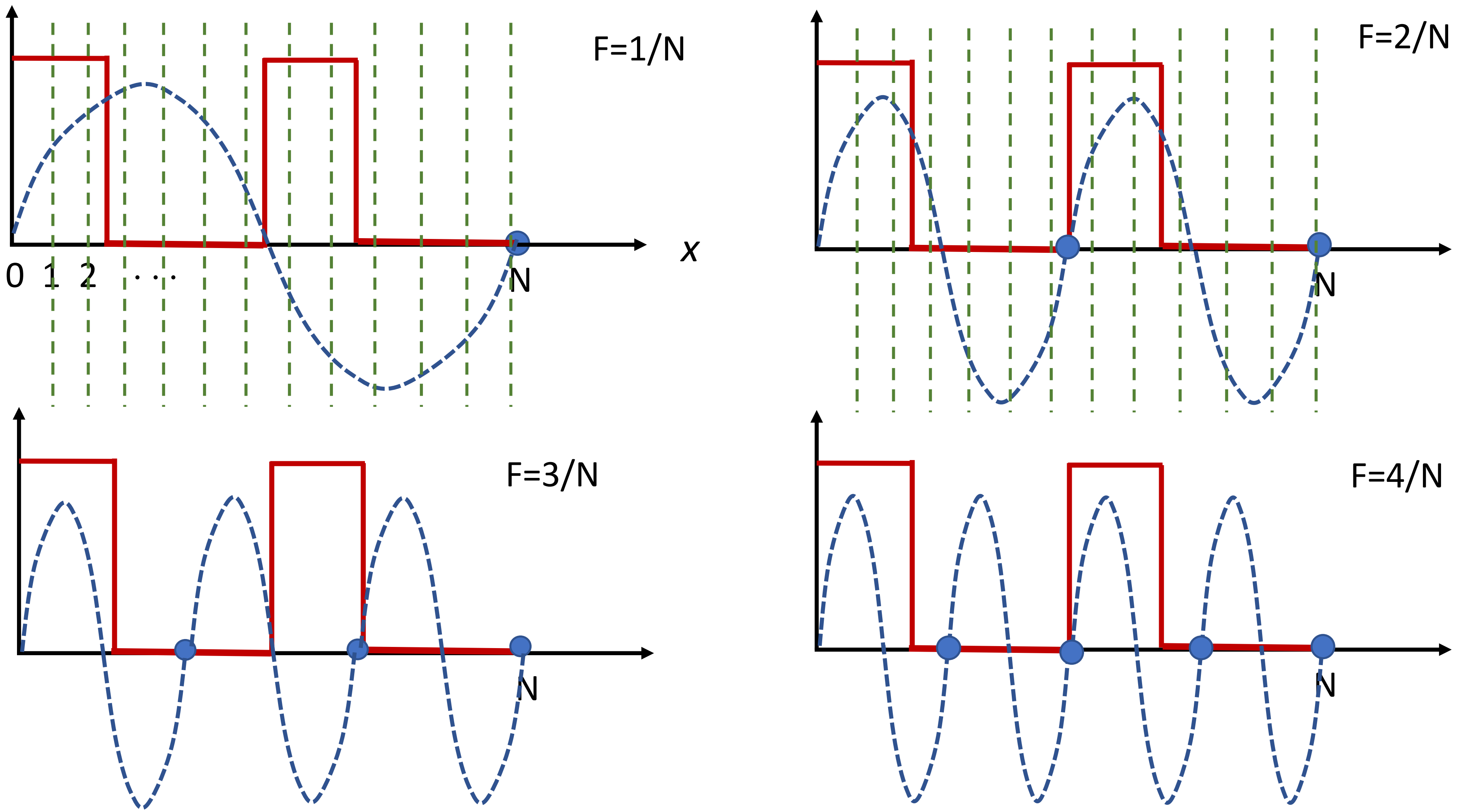
```
In[27]:= Plot[{Sin[x], Sin[2 x], Sin[3 x]}, {x, 0, 2 Pi}]
```

Out[27]=



Convolution with sin(2π(y/N)x)

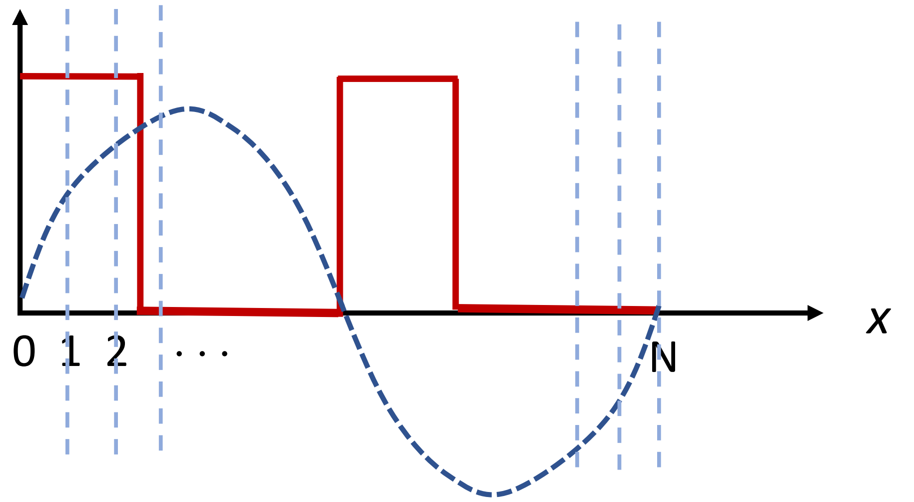
g(x) with period = N/2, frequency =2/N



Convolution with $\sin(2\pi(y/N)x)$: observation

- $F=y/N$ is a multiple of the frequency of $g(x)$, the convoluted result is larger
- $F=y/N$ is not a multiple of the frequency of $g(x)$, the convoluted result is smaller

Discrete Fourier Transform (DFT)

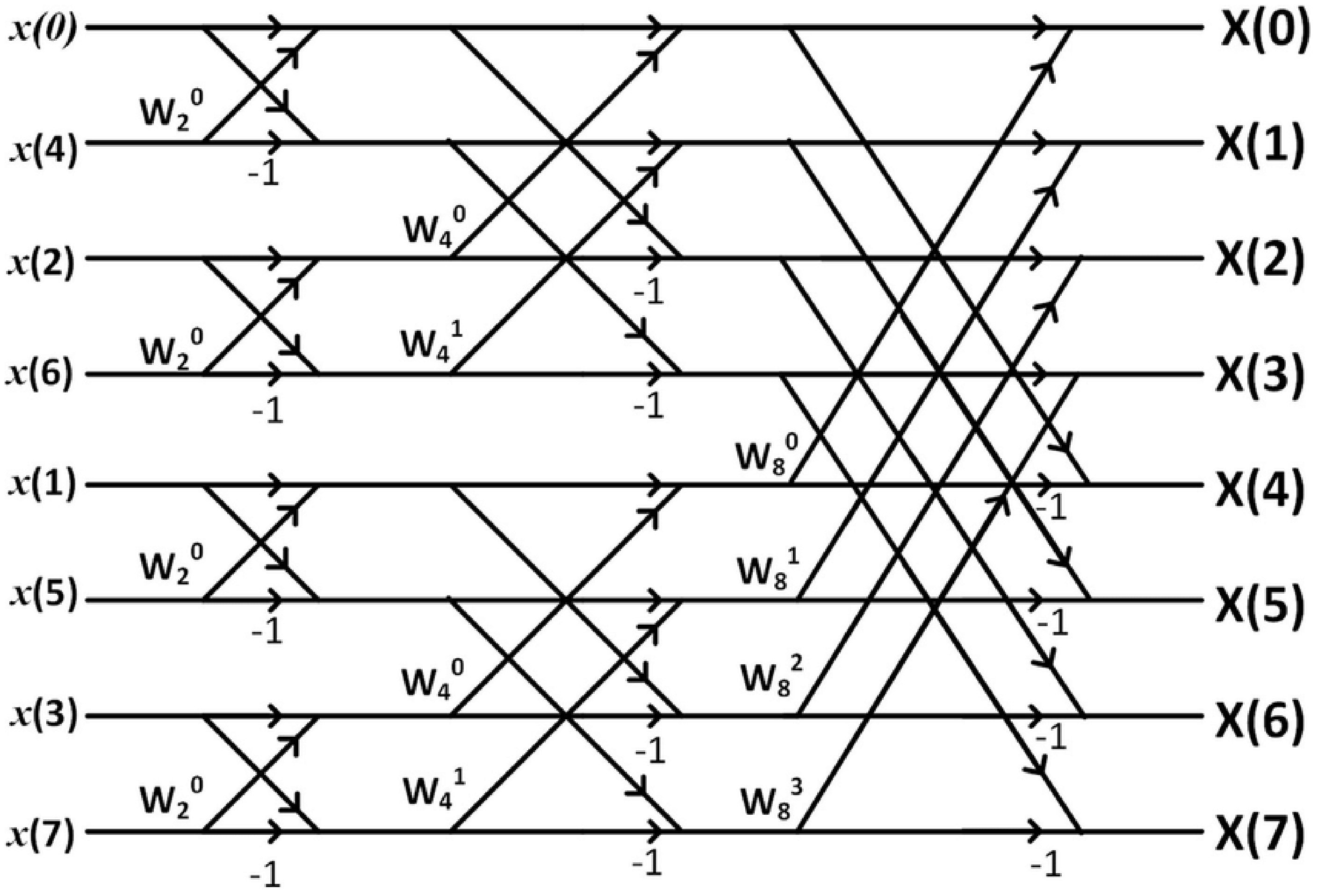


- $\vec{\text{a}} = [\, a_0 \;\; a_1 \;\; \dots a_{N-1} \,]$
- $e^{ix} = \cos x + i \sin x,\;\; i = \sqrt{-1}$
- Let $\omega = e^{2\pi i/N}$
- $\text{DFT}(\vec{a}) = \vec{f} = [f_0 \;\; f_1 \;\; \dots f_{N-1}]$, where

$$f_y = \sum_{x=0}^{N-1} a_x \omega^{-xy}, \qquad 0 \le y \le N-1$$

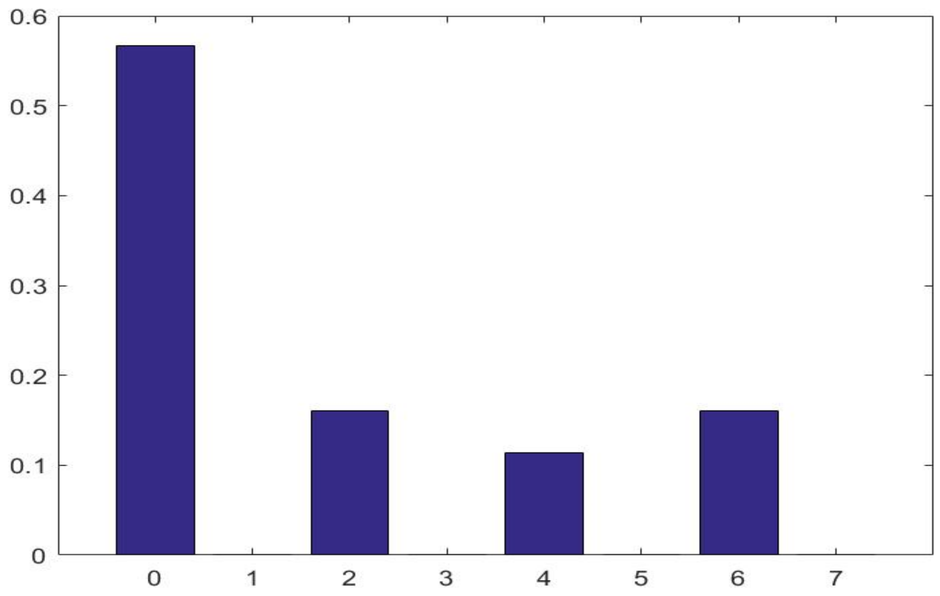
- $f_y = a_0\omega^{-0y} + a_1\omega^{-1y} + \dots + a_{N-1}\omega^{-(N-1)y}$ is the magnitude of frequency y/N
- Convoluted with $\sin(2\pi(y/N)x)$ and $\cos(2\pi(y/N)x)$, $0 \le y \le N-1$

Discrete Fourier Transform (DFT)



DFT: special case (s|N)

- N=8 points, period s=4, $\vec{a} = [\,1\;\;2\;\;3\;\;4\;\;1\;\;2\;\;3\;\;4\,]$
- Matlab (fft, abs, normalized)
  - $\vec{f} = [\mathbf{0.5664}\quad \mathbf{0}\quad \mathbf{0.1602}\quad \mathbf{0}\quad 0.1133\quad 0\quad 0.1602\quad 0]$



- N points, the period=s, s|N
- $\vec{f} = [\boldsymbol{f}_{\mathbf{0}(\frac{N}{s})}\ \mathbf{0}\ \ \mathbf{0}\ \ \ldots \mathbf{0}\ \ \boldsymbol{f}_{\frac{N}{s}}\ \ \mathbf{0}\ \ \mathbf{0}\ \ \ldots \mathbf{0}\ \ \boldsymbol{f}_{\frac{2N}{s}}\ \ \mathbf{0}\ \ \mathbf{0}\ \ldots\ \ \mathbf{0}\ \ \ldots .\ \boldsymbol{f}_{(s-1)\frac{N}{s}}\ \mathbf{0}\ \mathbf{0}\ \ \ldots \mathbf{0}]$
- Random measure on $\vec{f}$
  - Get a frequency y with probability $|f_y|$ (after normalizing $\vec{f}$)
- Compute s
  - Take r random measures and obtain frequencies $i_1(N/s)$, $i_2(N/s)$, …, $i_r(N/s)$
  - Compute $b=\gcd(i_1(N/s), i_2(N/s), \ldots, i_r(N/s))$
  - Compute N/b = s with high probability since b=N/s with high probability

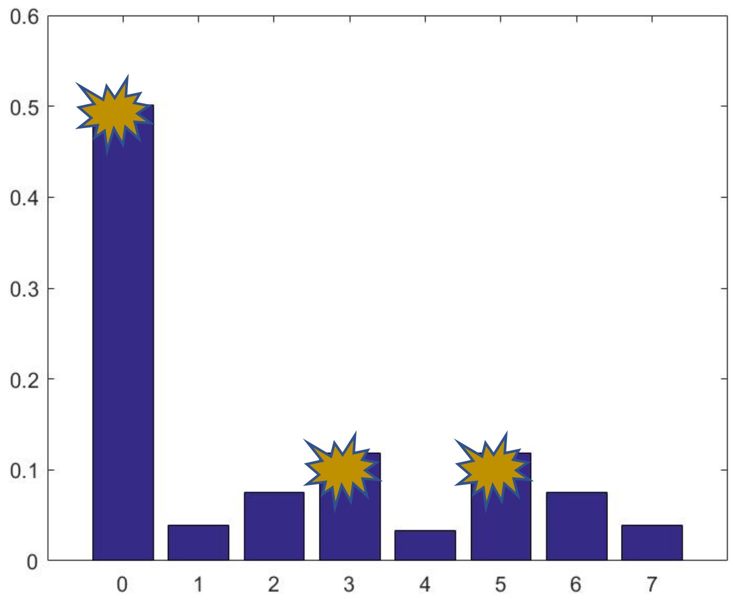
Find the period of g: special case (s|N)

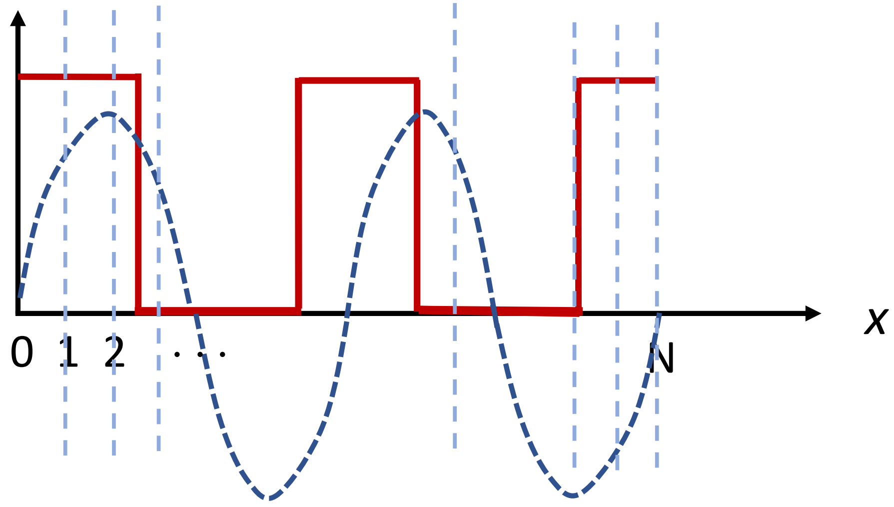
Algorithm I:

1. Prepare a vector $\vec{u} = [0\ 1\ 2\ \ \dots N-1]$
2. Compute $\vec{a} = g(\vec{u}) = [g(0)\ g(1)\ g(2) \dots g(N-1)]$
3. Compute and normalize $\vec{f} = DFT(\vec{a})$
4. Randomly measure $\vec{f}$ r times to obtain frequencies $d_1, d_2, \dots, d_r$
5. Compute $b=\gcd(d_1, d_2, \dots, d_r)$
6. Return (N/b)

DFT: general case (N mod s ≠ 0)

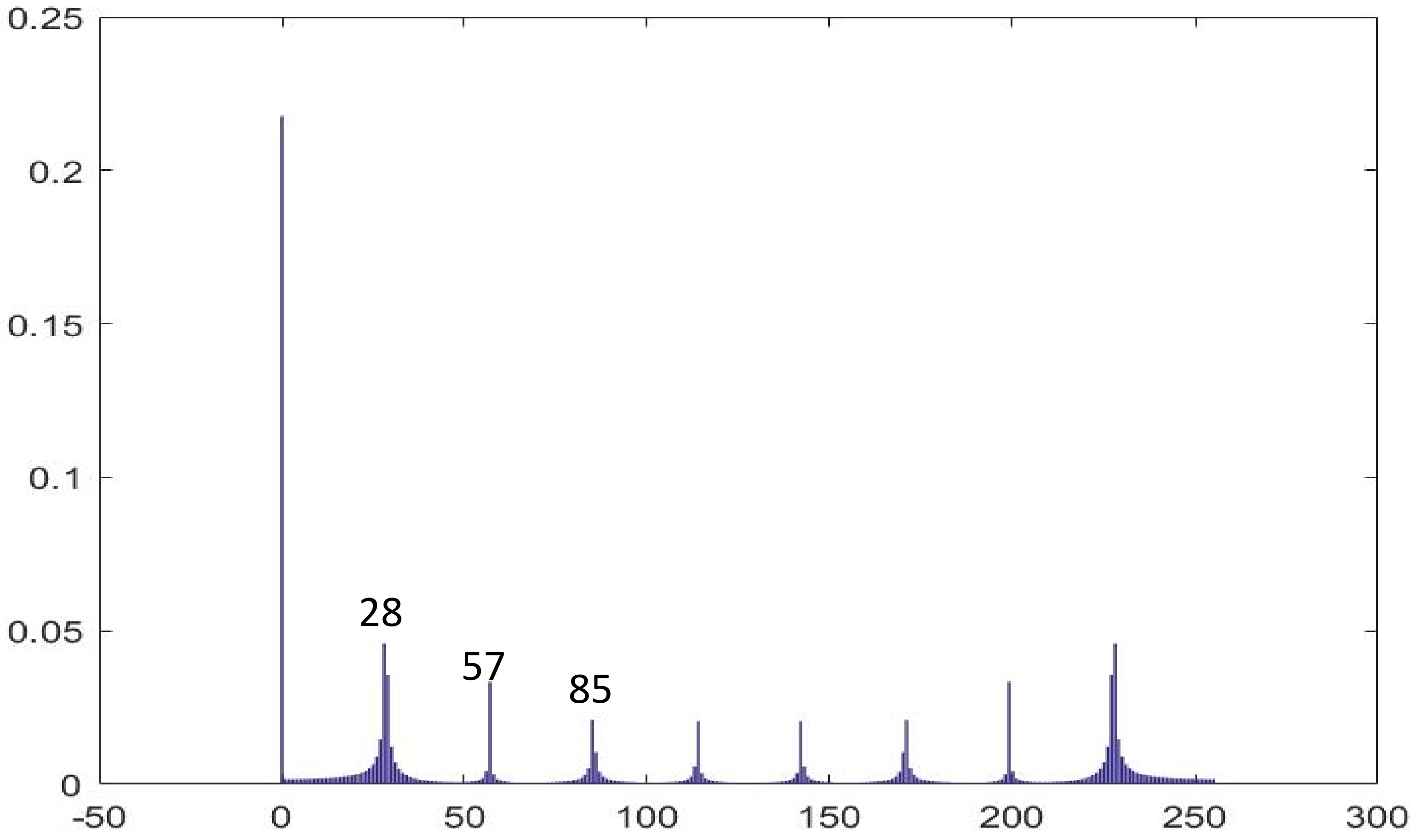
- N=8, s=3, $\vec{a} = [\,1\ \ 2\ \ 3\ \ 1\ \ 2\ \ 3\ \ \mathbf{1}\ \ \mathbf{2}\,]$
- $\vec{f} = [0.5016\quad 0.0388\quad 0.0748\quad 0.1190\quad 0.0334\quad 0.1190\quad 0.0748\quad 0.0388]$





$$d = \left[\frac{kN}{s}\right] : closest\ integer\ to\ kN/s$$

- N=256, s=9, $\vec{a} = [\,1\;2\;3\;4\;5\;7\;8\;9\;\; \ldots\; 1\;2\;3\;4\;5\;6\;7\;8\;9\;\mathbf{1\;2\;3\;4}\,]$
- $\vec{f} = DFT(\vec{a})$



Find period s from measured frequency d=[kN/s]

- F $= \frac{256}{9} = 28.44$
- From $\vec{f}$, we sample frequencies: d = 28, 57, which are of form [kN/s]
- **Question**: to find s from d=[kN/s]
- Observation:

$$\frac{kN}{s} - 0.5 < \left[\frac{\mathrm{kN}}{\mathrm{s}}\right] \leq \frac{\mathrm{kN}}{\mathrm{s}} + 0.5 \quad \Rightarrow \quad \frac{\mathrm{k}}{\mathrm{s}} - \frac{1}{2\mathrm{N}} < \frac{\mathrm{d}}{\mathrm{N}} \leq \frac{k}{s} + \frac{1}{2N}$$

- Find the rational k/s that is close to d/N within the range 1/2N
- Thus, s is the denominator of k/s

- Consider
  - $d_1/N = 28/256 = 0.109375$
  - $d_2/N = 57/256 = 0.22265625$
  - $d_3/N = 85/256 = 0.33203125$
- Rational numbers to approximate d/N
  - 1/9 - 0.109375 = 0.001736…
  - 2/9 - 0.22265625 = 0.0004340…
  - 3/9 – 0.33203125 = 0.001302…

Continued fraction

- Use a rational number to approximate an irrational number or another rational number
- Example: π=3.14159265368…
  - 22/7 = 3.1428…
  - 333/106 = 3.1415094…
  - 355/113 = 3.14159292035…
  - …
- How to compute
  - 3.14159265368 = $3 + \cfrac{1}{7 + \cfrac{1}{15 + \cfrac{1}{1 + 0.00341\ldots}}} \approx 3 \approx \frac{7}{22} \approx \frac{333}{106} \approx \frac{355}{113} \approx$

- Use Matlab to compute
  - rats(pi, 5) = 22/7
  - rats(pi, 10)=355/113
  - rat(pi) = 3 + 1/(7 + 1/(16))
  - rat(pi, 0.00000001) = 3 + 1/(7 + 1/(16 + 1/(-294)))
  - …

Theorem: For d=[kN/s], gcd(k,s)=1, **s is n-bit long**, and N is 2n-bit long, **k/s is the unique rational** that approximates d/N such that $\left|\frac{k}{s} - \frac{d}{N}\right| \leq \frac{1}{2N}$.

Proof.

- $\left|\frac{d}{N} - \frac{k}{s}\right| = \left|\frac{\left[\frac{kN}{s}\right]}{N} - \frac{k}{s}\right| = \left|\frac{\frac{kN \pm b}{s}}{N} - \frac{k}{s}\right| = \left|\frac{b}{sN}\right| \leq \frac{1}{2N}$ for some $0 \leq \mathrm{b} \leq \lfloor \mathrm{s}/2 \rfloor$

- For another $\frac{k'}{s'} \neq \frac{k}{s}$, s' is n-bit long, $\left|\frac{k}{s} - \frac{k'}{s'}\right| = \left|\frac{\mathrm{ks'} - \mathrm{k's}}{ss'}\right| > \frac{1}{2^{2n}} = \frac{1}{N}$
- Thus, k/s is unique. ♦

Note

- Even though d is [kN/s]+i, for small i, it is still ok to find k/s. This increases the success probability up to 90%.

- $\vec{a} = [\,1\ 2\ 3\ 4\ 5\ 7\ 8\ 9\ \ \ldots\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ \mathbf{1\ 2\ 3\ 4}\,]$
- N=256, s=9, F=256/9=28.4
- Apply DFT on $\vec{a}$ to get $\vec{f} = [\ldots]$
- Randomly measure and get d_1=28, d_2=57, d_3=85.
- s is 4-bit long at most
- $\frac{d_1}{256} = \frac{28}{256} \approx \frac{1}{9} \approx \frac{7}{64}$
  - 64 is over 4 bits (X)
  - 9 is within 4-bit long.
  - 9 is a candidate for s since $|1/9\text{-}28/256| = 0.001736 \le 1/2N = 0.00195$
  - Note: if d_1=27, 29 or 30, 27/256 ≈ 1/9, 29/256 ≈ 1/9, 30/256 ≈ 1/9

- $\frac{d_2}{256} = \frac{57}{256} \approx \frac{1}{4} \approx \frac{2}{9} \approx \frac{57}{256}$.
  - 4 and 9 are within 4-bit long.
  - 9 is a candidate for s since $|1/4 - 57/256| = 0.0273 > 1/2N$ and $|2/9 - 57/256| = 0.000434 < 1/2N$
- $\frac{d_3}{256} = \frac{85}{256} \approx \frac{1}{3} \approx \frac{85}{256}$
  - 3 is within 4-bit and |1/3-85/256| = 0.001302 < 1/2N.
  - 3 is a candidate for s.
  - However, it is wrong since the correct one 3/9 has gcd(3,9)≠1.

Some facts

Theorem: s is n-bit long. For a random k, prob(gcd(k, s)=1) is almost 1.

Proof:

- s has n prime factors at most.
- There are at least s/n primes less than s.
- The probability that a random prime can divide s is at most n^2/s.
- k has at most log k ($\approx$ n) prime factors.
- Thus, the probability that k has a prime factor that is also a prime factor for s is $n \cdot n^2/s = n^3/s$.
- n^3/s is almost 1 if s is large enough.

Theorem: For each d of form $\left[\frac{kN}{s}\right], 1 \leq k < s$, the probability that a random measure gets this d is at least 0.4/s. Thus, the probability of getting a frequency of form $\left[\frac{kN}{s}\right]$ is at least 0.4

Proof. Omit.

Find the period of g: general case

Algorithm II: (assume that s is n-bit long at most)

1. Prepare a vector $\vec{u} = [0\ 1\ 2\ \ldots N-1]$, where $N \geq 2^{2n}$
2. Compute $\vec{a} = g(\vec{u}) = [g(0)\ \ g(1)\ \ g(2) \ldots\ g(N-1)]$
3. Compute and normalize $\vec{f} = DFT(\vec{a})$
4. Randomly measure $\vec{f}$ r times to obtain frequencies **$d_1, d_2, \ldots, d_r$**
5. Use "**continued fraction**" method to compute rationals **$z_1, z_2, \ldots,$** z_r of denominators at most n-bit long for approximating d_1/N , d_2/N, ..., d_r/N within $1/2N$
6. A denominator of z_i's is very likely to be the period s

Factoring M $\equiv$ Finding the period of $g_{a,M}(x)$

- Let M=pq and $a \in Z_M^*$, $\mathrm{g}_{\mathrm{a,M}}(\mathrm{x}) = \mathrm{a}^{\mathrm{x}} \bmod \mathrm{M}$, $0 \le x \le M-1$
- $\mathrm{g}_{\mathrm{a,M}}(\mathrm{x})$ has period s. That is, $a^s \bmod M = 1$.
  - Eluer's theorem: $a^{\phi(M)}\ mod\ M = 1$
  - Thus, $s \le \phi(M)$
- If s is even and $a^{s/2} \bmod M \neq \pm 1$, then $\gcd\left(a^{s/2} \pm 1, M\right) = p\ or\ q$
  - $a^{s/2}$ is a nontrivial solution for $x^2 = 1 \bmod M$
- Example
  - M=35=5x7, a=2, $g_{a,M}(x)$ has period s=12, $2^{12} \bmod 35 = 1$.
  - $2^6 \bmod 35 = 29$, 29+1 = 30, 29-1 = 28. gcd(30, 35) = 5 = p, gcd(28, 35)=7=q.

Theorem: M=pq. For random $a \in Z_M^*$, the probability that $g_{a,M}(x)$ has an even period s and $a^{s/2}$ mod M $\neq \pm 1$ is at least ½.

Proof. Omit.

Problems of the above method

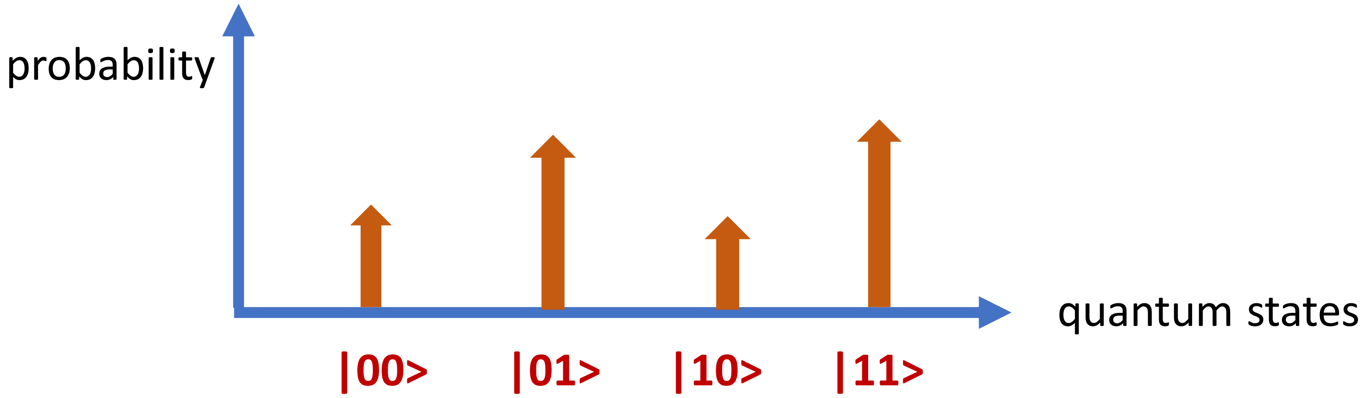
- For n-bit M, the period could be as long as s=O(2^n)
- We need to choose N: 2n-bit long
- It takes O(N) time to compute the vector

$$\vec{a} = g(\vec{u}) = [g(0)\ \ g(1)\ \ g(2) \dots\ g(N-1)]$$

- It takes O(N) space to store $\vec{a}$
- Also, it takes O(N log N) time to do DFT

Quantum bits

- 1 qbit: $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$, where $\alpha, \beta\ are\ complex\ and\ \ \alpha^2 + \beta^2 = 1$
  - Bra-ket notation, Dirac notation
  - Vector notation: $\begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \alpha \begin{bmatrix} \mathbf{1} \\ \mathbf{0} \end{bmatrix} + \beta \begin{bmatrix} \mathbf{0} \\ \mathbf{1} \end{bmatrix} = \alpha|\mathbf{0}\rangle + \beta|\mathbf{1}\rangle,\ \ \alpha^2 = \alpha\alpha^*,\ \beta^2 = \beta\beta^*$
  - **Bits 0 and 1 co-exist in superposition (simultaneous existence)**
- 2 qbits : $|\Psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle,\ \ \alpha^2 + \beta^2 + \gamma^2 + \delta^2 = 1$
  - Vector notation: $\begin{bmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{bmatrix} = \alpha \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} + \beta \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} + \gamma \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} + \delta \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$



- n qbits: let $N=2^n$

$$|\Psi\rangle = \sum_{b_1 \mathrm{b}_2 \dots b_n \in Z_2^n} \alpha_{\mathrm{b}_1 b_2 \dots b_n} |b_1 b_2 \dots b_n\rangle = \sum_{x=0}^{N-1} \alpha_x |x\rangle$$

Unknown vs superposition

- An unknow x with some distribution
- A quantum state y with some distribution for sampling
- **Exact copy**
    - x→ x’
    - y→y’
- Measure (open)
    - x must be equal to x’
    - y may not be equal to y’
- x: only one value exists (unknown)
    - x+1 → another value
- **y: all values co-exist (superposition)**
    - **y+1 → all values**

Measurement

1 qbit $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$

- Measure: get bit 0 with prob. α^2 and bit 1 with prob. β^2 -- no longer qbits

2 qbits $|\Psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$

- Measure: get bits 00 with prob. α^2, etc.
- Partial measure the last qbit: $\aleph(|\Psi\rangle)$
  - With prob. $\alpha^2 + \gamma^2$, we see bit 0 and $\aleph(|\Psi\rangle)$ becomes 1 qbit
$$\frac{\alpha}{\sqrt{\alpha^2 + \gamma^2}}|0\rangle[0] + \frac{\gamma}{\sqrt{\alpha^2 + \gamma^2}}|1\rangle[0]$$
  - With prob. $\beta^2 + \delta^2$, we see bit 1 and $\aleph(|\Psi\rangle)$ becomes 1 qbit
$$\frac{\beta}{\sqrt{\beta^2 + \delta^2}}|0\rangle[1] + \frac{\delta}{\sqrt{\beta^2 + \delta^2}}|1\rangle[1]$$

n qbits: let N=2^n

$$|\Psi\rangle = \sum_{b_1 \mathrm{b}_2 \ldots b_n \in Z_2^n} \alpha_{\mathrm{b}_1 b_2 \ldots b_n} |b_1 b_2 \ldots b_n\rangle = \sum_{x=0}^{N-1} \alpha_x |x\rangle$$

- Full measure and partial measures
- Example: measure the last bit.
  - The first n-1 qbits are left in superposition and the last one collapses to either 0 or 1

$$\sum_{b_1 \mathrm{b}_2 \ldots b_{n-1} \in Z_2^n} \alpha'_{\mathrm{b}_1 b_2 \ldots b_{n-1}} |b_1 b_2 \ldots b_{n-1}\rangle [0]$$

$$\sum_{b_1 \mathrm{b}_2 \ldots b_{n-1} \in Z_2^n} \alpha''_{\mathrm{b}_1 b_2 \ldots b_{n-1}} |b_1 b_2 \ldots b_{n-1}\rangle [1]$$

Entanglement

Two quantum states

$$|\Psi\rangle = \sum_{b_1 \mathrm{b}_2 \ldots b_n \in Z_2^n} \alpha_{\mathrm{b}_1 b_2 \ldots b_n} |b_1 b_2 \ldots b_n\rangle$$

$$|\Omega\rangle = \sum_{c_1 c_2 \ldots c_m \in Z_2^m} \beta_{c_1 c_2 \ldots c_m} |c_1 c_2 \ldots c_m\rangle$$

- Entanglement

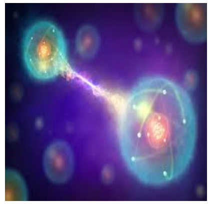
$$|\Psi\rangle \otimes |\Omega\rangle = \sum_{x=0}^{2^{n+m}-1} \gamma_x |x\rangle$$

- Example

$$(\alpha_1|0\rangle + \beta_1|1\rangle) \otimes (\alpha_2|0\rangle + \beta_2|1\rangle)$$

$$= \alpha_1\alpha_2|00\rangle + \alpha_1\beta_2|01\rangle + \beta_1\alpha_2|10\rangle + \beta_1\beta_2|11\rangle$$

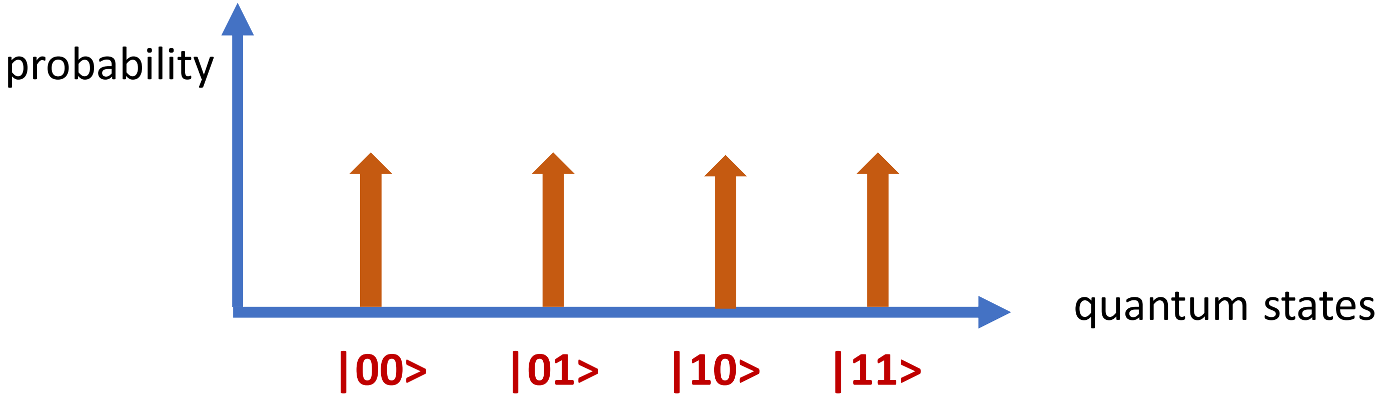
Entanglement for teleportation

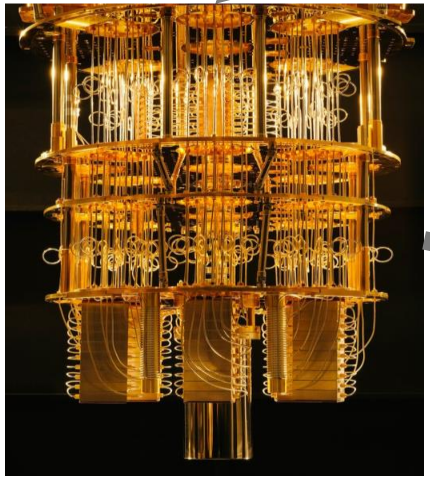


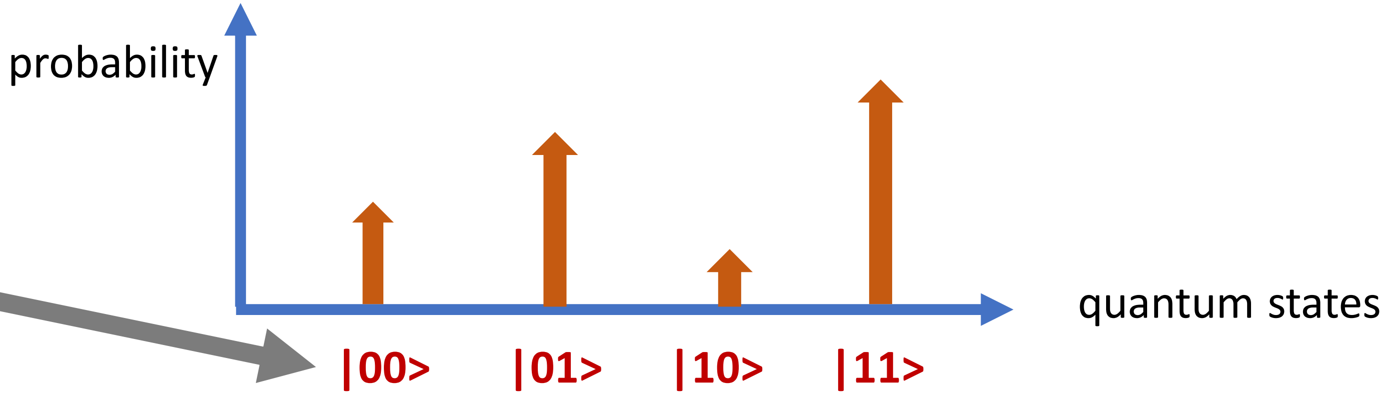
$$|\Psi\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

Information transmission exceeds the speed of light !!!

Quantum computation: concept







Operations on qbits

- Operator on n qbits: H is 2^nx2^n unitary matrix
  - Unitary matrix: HH*=I.
- Example: $H = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{bmatrix}$
  - apply H on qbit $\alpha|0\rangle + \beta|1\rangle$ and obtain $\frac{1}{\sqrt{2}}(\alpha+\beta)|0\rangle + \frac{1}{\sqrt{2}}(\alpha-\beta)|1\rangle$
  - $H\begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \alpha \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} + \beta \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{-1}{\sqrt{2}} \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}}(\alpha+\beta) \\ \frac{1}{\sqrt{2}}(\alpha-\beta) \end{bmatrix}$

Concept

- **Each quantum state is mapped to all quantum states**

<u>Example</u>

- $|\Psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle,\ H = [h_{i,j}]$
  - $|00\rangle$ ➔ $h_{1,1}|00\rangle + h_{2,1}|01\rangle + h_{3,1}|10\rangle + h_{4,1}|11\rangle$
  - $|01\rangle$ ➔ $h_{1,2}|00\rangle + h_{2,2}|01\rangle + h_{3,2}|10\rangle + h_{4,2}|11\rangle$
  - $|10\rangle$ ➔ $h_{1,3}|00\rangle + h_{2,3}|01\rangle + h_{3,3}|10\rangle + h_{4,3}|11\rangle$
  - $|00\rangle$ ➔ $h_{1,4}|00\rangle + h_{2,4}|01\rangle + h_{3,4}|10\rangle + h_{4,4}|11\rangle$
- $\mathrm{H}|\Psi\rangle = \alpha(h_{1,1} + h_{1,2} + h_{1,3} + h_{1,4})|00\rangle + \ldots$

Operations on 1 qbit

X Gate
Bit–flip, Not

$$-\boxed{X}- \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \beta|0\rangle + \alpha|1\rangle$$

Z Gate
Phase–flip

$$-\boxed{Z}- \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \alpha|0\rangle - \beta|1\rangle$$

H Gate
Hadamard

$$-\boxed{H}- \equiv \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \frac{\alpha+\beta|0\rangle + \alpha-\beta|1\rangle}{\sqrt{2}}$$

T Gate

$$-\boxed{T}- \equiv \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \alpha|0\rangle + e^{i\pi/4}\beta|1\rangle$$

Operations on 1 qbit

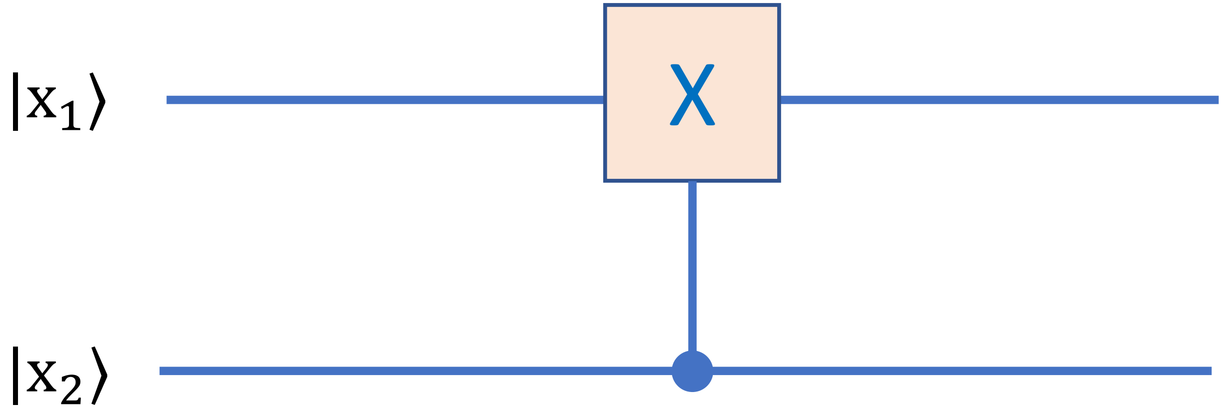
$$Rotation: \ R_k = \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{-2\pi i}{2^k}} \end{bmatrix}, \quad R_k \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \alpha \\ e^{\frac{-2\pi i}{2^k}} \cdot \beta \end{bmatrix}$$

<u>Note:</u>

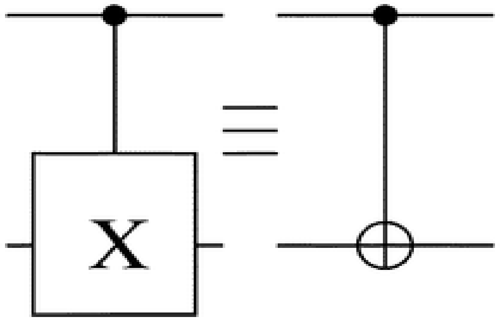
- $e^{i\theta} = \cos\theta + i \sin\theta$
- Euler's identity: $e^{i\pi} = -1$
- $e^{\frac{-2\pi i}{2^k}} \times e^{-2\pi 0.b_1 b_2 \ldots b_{k-1}} = e^{-2\pi 0.b_1 b_2 \ldots b_{k-1} 1}$

Operations on 2 qbits

- Control circuit: x_2=1 if and only if apply gate X on x_1

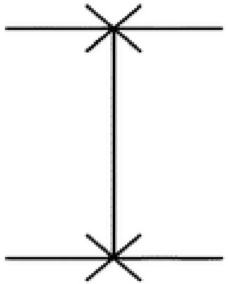


Controlled Not
Controlled X
CNot



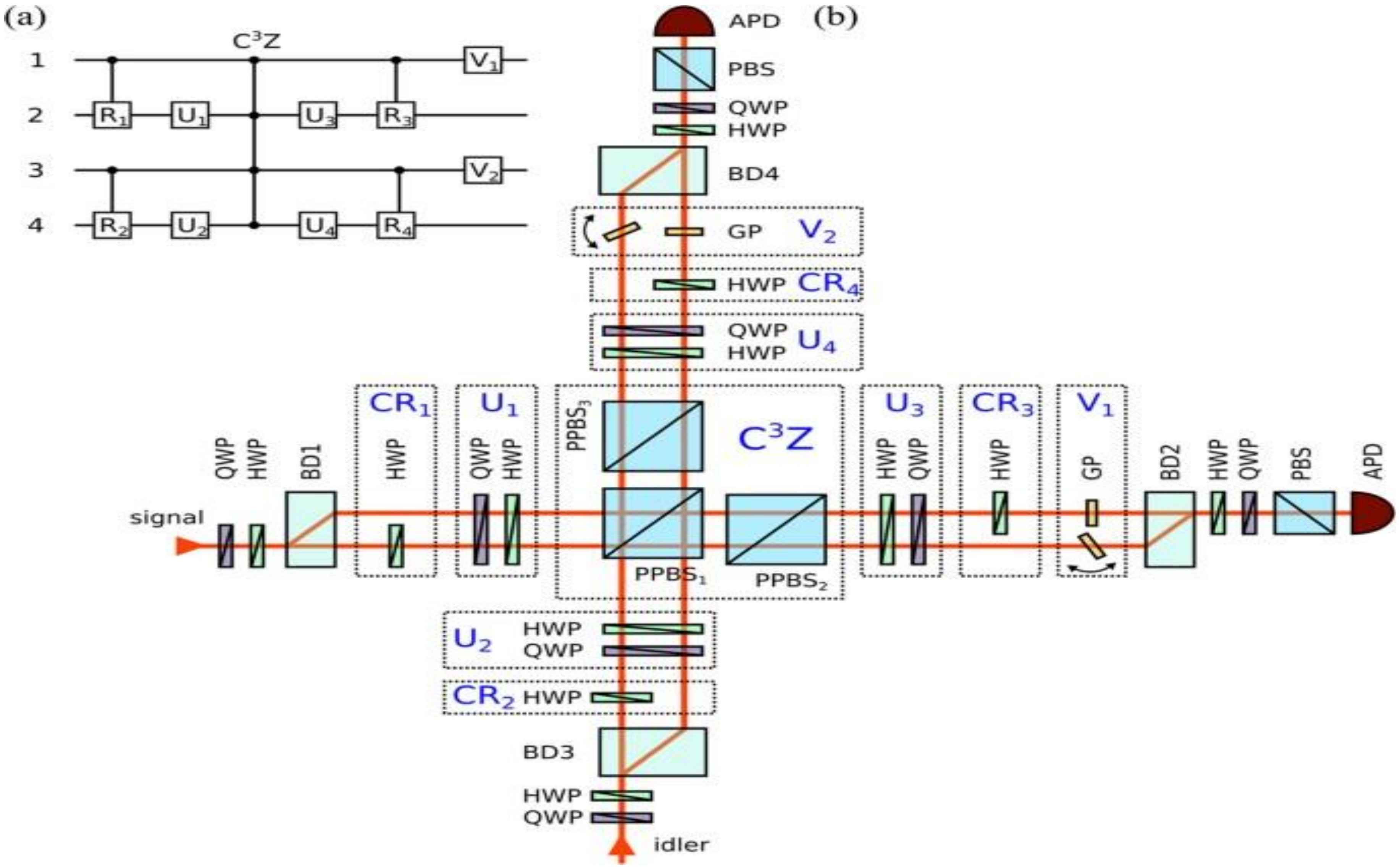
$$\equiv \begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{bmatrix}\begin{bmatrix}a\\b\\c\\d\end{bmatrix} = \begin{matrix}a|00\rangle + b|01\rangle + \\ d|10\rangle + c|11\rangle\end{matrix}$$

Swap



$$\equiv \begin{bmatrix}1&0&0&0\\0&0&1&0\\0&1&0&0\\0&0&0&1\end{bmatrix}\begin{bmatrix}a\\b\\c\\d\end{bmatrix} = \begin{matrix}a|00\rangle + c|01\rangle + \\ b|10\rangle + d|11\rangle\end{matrix}$$

Quantum circuit



DFT on N=2^n bits

- $\vec{a} = [\, a_0 \;\; a_1 \;\; \dots a_{N-1} \,], \omega = e^{2\pi i/N}, \;\; i = \sqrt{-1}$

$$\mathrm{DFT}(\vec{a}) = \vec{f} = \begin{bmatrix} f_0 \\ f_1 \\ \vdots \\ f_{N-1} \end{bmatrix} = \sum_{x=0}^{N-1} a_x \begin{bmatrix} \omega^{-x\cdot 0} \\ \omega^{-x\cdot 1} \\ \vdots \\ \omega^{-x\cdot(N-1)} \end{bmatrix} = \sum_{x=0}^{N-1} a_x V_x$$

where $V_x = \begin{bmatrix} \omega^{-x\cdot 0} \\ \omega^{-x\cdot 1} \\ \vdots \\ \omega^{-x\cdot(N-1)} \end{bmatrix}$

- Example: n=2, N=4, $\vec{a}$ = [a_0 a_1 a_2 a_3], $\omega = e^{2\pi i/4}, \omega^4 = 1$

$$DFT(\vec{a}) = \vec{f} = \begin{bmatrix} f_0 \\ f_1 \\ f_2 \\ f_3 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & \omega^{-1} & \omega^{-2} & \omega^{-3} \\ 1 & \omega^{-2} & \omega^{-4} & \omega^{-6} \\ 1 & \omega^{-3} & \omega^{-6} & \omega^{-9} \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix}$$

$$= a_0 \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} + a_1 \begin{bmatrix} 1 \\ \omega^{-1} \\ \omega^{-2} \\ \omega^{-3} \end{bmatrix} + a_2 \begin{bmatrix} 1 \\ \omega^{-2} \\ \omega^{-4} \\ \omega^{-6} \end{bmatrix} + a_3 \begin{bmatrix} 1 \\ \omega^{-3} \\ \omega^{-6} \\ \omega^{-9} \end{bmatrix} = \begin{bmatrix} a_0 + a_1 + a_2 + a_3 \\ a_0 + a_1\omega^{-1} + a_2\omega^{-2} + a_3\omega^{-3} \\ a_0 + a_1\omega^{-2} + a_2\omega^{-4} + a_3\omega^{-6} \\ a_0 + a_1\omega^{-3} + a_2\omega^{-6} + a_3\omega^{-9} \end{bmatrix}$$

QFT on coefficients of 1 qbit

- $\vec{\mathrm{a}} = [a_0 \; a_1]$,

  $$DFT(\vec{a}) = \begin{bmatrix} 1 & 1 \\ 1 & e^{\frac{-2\pi i}{2}} \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \end{bmatrix} = \begin{bmatrix} a_0 + a_1 \\ a_0 - a_1 \end{bmatrix}$$

- $H = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{bmatrix}$, $\quad |\Psi\rangle = a_0|0\rangle + a_1|1\rangle$

  $$\mathrm{QFT}(|\Psi\rangle) = H|\Psi\rangle = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} a_0 + a_1 \\ a_0 - a_1 \end{bmatrix}$$

QFT on coefficients of n qbits

- DFT: $\vec{a} = [a_0\ a_1\ \ldots a_{N-1}],\ \ N = 2^n,$

$$\vec{f} = \begin{bmatrix} f_0 \\ f_1 \\ \vdots \\ f_{N-1} \end{bmatrix} = \sum_{x=0}^{N-1} a_x V_x,\ \text{where } V_x = \begin{bmatrix} \omega^{-x\cdot 0} \\ \omega^{-x\cdot 1} \\ \vdots \\ \omega^{-x\cdot(N-1)} \end{bmatrix}$$

- **QFT**: $|x\rangle = \begin{bmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{bmatrix} \rightarrow \begin{bmatrix} \omega^{-x\cdot 00\ldots0} \\ \omega^{-x\cdot 00\ldots1} \\ \vdots \\ \omega^{-x\cdot 11\ldots1} \end{bmatrix} = \boldsymbol{V_x = \sum_{y=0}^{N-1} \omega^{-xy}|y\rangle}$

- **Put $\vec{a}$ into n-qbit quantum state: $|\boldsymbol{\Psi}\rangle = \sum_{x=0}^{N-1} \boldsymbol{a_x}|\boldsymbol{x}\rangle$**

$$\mathrm{QFT}(|\Psi\rangle) = \mathrm{QFT}\left(\sum_{x=0}^{N-1} a_x|x\rangle\right) = \sum_{x=0}^{N-1} a_x \mathrm{QFT}(|x\rangle)$$

$$= \sum_{x=0}^{N-1} a_x V_x = \sum_{x=0}^{N-1} a_x \sum_{y=0}^{N-1} \omega^{-xy}|y\rangle$$

$$= \sum_{y=0}^{N-1}\left(\sum_{x=0}^{N-1} a_x \omega^{-xy}\right)|y\rangle = \sum_{y=0}^{N-1} f_y|y\rangle = \begin{bmatrix} f_0 \\ f_1 \\ \vdots \\ f_{N-1} \end{bmatrix}$$

- **Frequency magnitudes are in the coefficients of quantum states**

- $\vec{a} = [a_0\ a_1\ a_2\ \ a_3]$

$\mathrm{QFT}(a_0|00\rangle + a_1|01\rangle + a_2|10\rangle + a_3|11\rangle)$

$$= a_0 \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} + a_1 \begin{bmatrix} 1 \\ \omega^{-1} \\ \omega^{-2} \\ \omega^{-3} \end{bmatrix} + a_2 \begin{bmatrix} 1 \\ \omega^{-2} \\ \omega^{-4} \\ \omega^{-6} \end{bmatrix} + a_3 \begin{bmatrix} 1 \\ \omega^{-3} \\ \omega^{-6} \\ \omega^{-9} \end{bmatrix}$$

$$= \begin{bmatrix} a_0 + a_1 + a_2 + a_3 \\ a_0 + a_1\omega^{-1} + a_2\omega^{-2} + \mathrm{a}_3\omega^{-3} \\ a_0 + a_1\omega^{-2} + a_2\omega^{-4} + \mathrm{a}_3\omega^{-6} \\ a_0 + a_1\omega^{-3} + a_2\omega^{-6} + \mathrm{a}_3\omega^{-9} \end{bmatrix}$$

$$= (f_0|00\rangle + f_1|01\rangle + f_2|10\rangle + f_3|11\rangle)$$

QFT for $|x\rangle$

- $\omega = e^{2\pi i/2^n}$
- $x = x_1 x_2 \dots x_n = \sum_{i=1}^{\mathrm{n}} 2^{n-i} x_i$
- $y = y_1 y_2 \dots y_n = \sum_{i=1}^{\mathrm{n}} 2^{n-i} y_i$

$$\mathrm{QFT}(|x\rangle) = \sum_{y=0}^{N-1} \omega^{-xy} \, |y\rangle$$

$$= \sum_{y_1 \in Z_2} \omega^{-x y_1 2^{n-1}} |y_1\rangle \otimes \sum_{y_2 \in Z_2} \omega^{-x y_2 2^{n-2}} |y_2\rangle \otimes \cdots \otimes \sum_{y_n \in Z_2} \omega^{-x y_n 2^{n-n}} |y_n\rangle$$

$$= (|0\rangle + \omega^{-x \cdot 2^{n-1}} |1\rangle) \otimes (|0\rangle + \omega^{-x \cdot 2^{n-2}} |1\rangle) \otimes \cdots \otimes (|0\rangle + \omega^{-x \cdot 2^{0}} |1\rangle)$$

$$= (|0\rangle + e^{-2\pi i \, 0.x_n} |1\rangle) \otimes (|0\rangle + e^{-2\pi i \, 0.x_{n-1} x_n} |1\rangle) \otimes \cdots \otimes (|0\rangle + e^{-2\pi i \, 0.x_1 x_2 \dots x_n} |1\rangle)$$

$$\mathrm{QFT}(|x_1x_2\rangle)$$

$$= (|0\rangle + e^{-2\pi i\ 0.x_2}|1\rangle) \otimes (|0\rangle + e^{-2\pi i\ 0.x_1x_2}|1\rangle)$$

$$= 1 \cdot |00\rangle + e^{-2\pi i 0.x_1x_2}|01\rangle + \mathrm{e}^{-2\pi i 0.x_2}|10\rangle + e^{-2\pi i(0.x_2+0.x_1x_2)}|11\rangle$$

$$\begin{array}{cc} & \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & \omega^{-1} & \omega^{-2} & \omega^{-3} \\ 1 & \omega^{-2} & \omega^{-4} & \omega^{-6} \\ 1 & \omega^{-3} & \omega^{-6} & \omega^{-9} \end{bmatrix} \\ x_1x_2 & \begin{matrix} 00 & \quad 01 & \quad 10 & \quad 11 \end{matrix} \end{array}$$

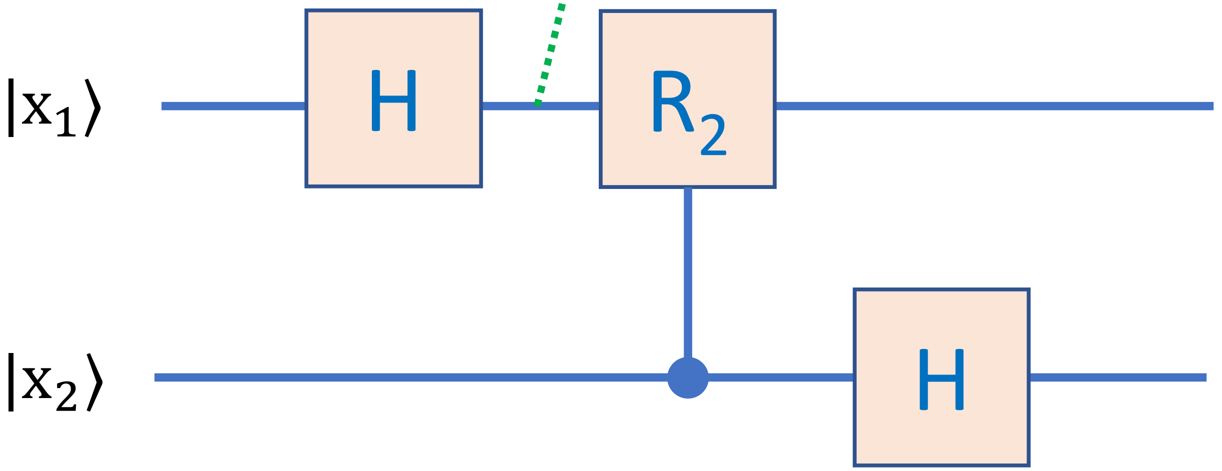
Quantum gates for $\mathrm{QFT}(|x\rangle)$

- $n = 2, \quad R_k = \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{-2\pi i}{2^k}} \end{bmatrix}, \; H = \begin{bmatrix} 1 & 1 \\ 1 & e^{-2\pi i/2} \end{bmatrix}$
- $\mathrm{QFT}(|x_1x_2\rangle) = (|0\rangle + e^{-2\pi i\, 0.x_2}|1\rangle) \otimes (|0\rangle + e^{-2\pi i\, 0.x_1x_2}|1\rangle)$

$|0\rangle + e^{-2\pi i\, 0.x_1}|1\rangle$

$x_2=0$: $e^{-2\pi i\, 0.x_1} \otimes \mathrm{e}^{-2\pi i\, 0.00} = e^{-2\pi i\, 0.x_1x_2}$

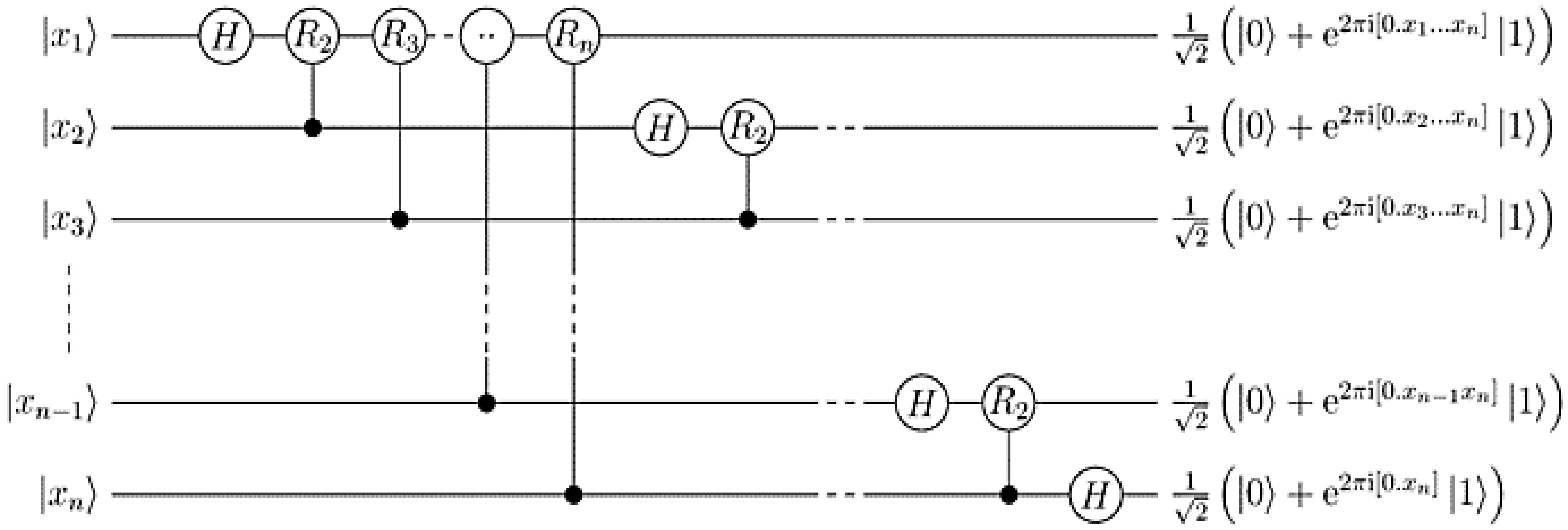
$x_2=1$: $e^{-2\pi i\, 0.x_1} \otimes \mathrm{e}^{-2\pi i\, 0.01} = e^{-2\pi i\, 0.x_1x_2}$



$\frac{1}{\sqrt{2}}(|0\rangle + e^{-2\pi i\, 0.x_1x_2}|1\rangle)$

$\frac{1}{\sqrt{2}}(|0\rangle + e^{-2\pi i\, 0.x_2}|1\rangle)$

- n qbits



$|x_1\rangle$
$|x_2\rangle$
$|x_3\rangle$
$|x_{n-1}\rangle$
$|x_n\rangle$
H
R_2
R_3
R_n
$\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i[0.x_1 \ldots x_n]}|1\rangle\right)$
$\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i[0.x_2 \ldots x_n]}|1\rangle\right)$
$\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i[0.x_3 \ldots x_n]}|1\rangle\right)$
$\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i[0.x_{n-1} x_n]}|1\rangle\right)$
$\frac{1}{\sqrt{2}}\left(|0\rangle + e^{2\pi i[0.x_n]}|1\rangle\right)$

Algorithm for factoring M=pq

- Assume $g_{a,M}(x)=g(x)$ and M is m-bit long. Thus, s is at most m-bit.
- Example
  - $M=35$, $a=4$, $g(x) = 4^x \bmod 35$
  - $m=6$, $n=10$

Algorithm III (M):

1. Randomly pick $a \in Z_M^*$
2. Prepare n+m qbits $|\Psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{b_1 b_2 \ldots b_n \in Z_2^n} |b_1 b_2 \cdots b_n\rangle |00 \ldots 0\rangle$, where n=3m.

-- Prepare $|\Psi\rangle = \frac{1}{\sqrt{1024}} \sum_{b_1 b_2 \ldots b_{10} \in Z_2^{10}} |b_1 b_2 \ldots b_{10}\rangle |000000\rangle$

3. Apply g(x) on the first n qbits and put the result in the last m qbits

$$\mathrm{g}(|\Psi\rangle) = \frac{1}{\sqrt{2^n}} \sum_{b_1 b_2 \ldots b_n \in Z_2^n} |b_1 b_2 \ldots b_n\rangle |g(b_1 b_2 \ldots b_n)\rangle =$$

-- $\mathrm{g}(|\Psi\rangle) = \frac{1}{\sqrt{1024}} (|0\rangle|1\rangle + |1\rangle|4\rangle + |2\rangle|16\rangle + |3\rangle|29\rangle$

$+|4\rangle|11\rangle + |5\rangle|9\rangle + |6\rangle|1\rangle + |7\rangle|4\rangle + \cdots + |1023\rangle|29\rangle)$

4. Measure the last m bits and we get the result θ

$$\aleph\big(\mathrm{g}(|\Psi\rangle)\big) = \sum_{\substack{b_1 b_2 \ldots b_n \in Z_2^n \\ \wedge\, g(b_1 b_2 \ldots b_n) = \theta}} \alpha |b_1 b_2 \ldots b_n\rangle[\theta]$$

-- Assume that we get θ=4:

$$\aleph\big(\mathrm{g}(|\Psi\rangle)\big)$$

$$= \frac{1}{\sqrt{171}}|1\rangle\mathbf{[4]} + \frac{1}{\sqrt{171}}|7\rangle\mathbf{[4]} + \cdots + \frac{1}{\sqrt{171}}|1021\rangle\mathbf{[4]}$$

Note: $\vec{a} = [0\ \ \frac{1}{\sqrt{171}}\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\ \ \frac{1}{\sqrt{171}}\ \ 0 \ldots 0\ \ \frac{1}{\sqrt{171}}\ \ 0\ \ 0\,]$

5. Apply QFT on the coefficients of $\aleph\left(g(|\Psi\rangle)\right)$ and obtain

$$\mathbf{QFT}\left(\aleph\left(g(|\Psi\rangle)\right)\right) = \sum_{y=0}^{N-1} f_y|y\rangle$$

-- $\mathrm{QFT}(\aleph\left(g(|\Psi\rangle)\right))$

$= 0.0562|0\rangle + 0.0001|1\rangle + \cdots$

$+0.0231|171\rangle + 0.0465|172\rangle + \cdots$

$+0.0465|342\rangle + 0.0231|343\rangle + \cdots$

$+\cdots$

6. Measure the first n bits of $\mathbf{QFT}(\aleph(g(|\Psi\rangle)))$ and obtain a frequency **d**.
7. Apply the continued fraction method on d/N to obtain a rational z of an m-bit denominator s.
8. If s is even and $a^{s/2} \pm 1$ mod $M \neq 0$,
   then compute and return $p = \gcd(a^{s/2} \pm 1, M)$ and $q = M/p$.
   else repeat steps 1-7 until M's prime factors are found.

-- Assume $\aleph\left(\mathbf{QFT}\left(\aleph(g(|\Psi\rangle))\right)\right)$ outputs f=172.

- Rational approximation: d/N=172/1024 ≈ 1/5 ≈ 1/6 ≈ 21/125. Since 125 is longer than 6 bits, we use s=6.
- Since the denominator s=6 is even, we have 4^6 mod 35=1.
- $35 | (4^3-1)(4^3+1)$. $\gcd(35, 4^3-1)=7$ and $\gcd(35, 4^3+1)=5$.