Intro à Computação Quântica - Parte 5

Aula passada:

- Algoritmo de Grover

Busca em vetor não estruturado de $N \to \sqrt{N}$

Hoje:

- Algoritmo de Shor

Resolve fatoração

$n = \log_2 N$

cl. Fat $N = pq$ $2^{O(\sqrt[3]{n})}$

quântica. $O(n^3 \ldots) \ldots$

Ideia do Algoritmo de Shor

$N = pq$

Problema: Encontrar fator de N $\neq 1, N$

Fácil ① Reduzir fatoração ao problema de encontrar período da função $f_{a,N}(x) = a^x \bmod N$

Difícil ② Usar a transformada quântica de Fourier (QFT) para encontrar período de $f_{a,N}(x)$ eficientemente

$QFT([f(0), f(1), f(2), \ldots N])$

Redução: Achar período ⇒ fatoração (Miller) ?

Fixe a, N inteiros positivos $\operatorname{mdc}(a,N)=1$ e considere

$f : \mathbb{Z}^+ : \mathbb{Z}_{15}$

a função $f_{a,N}(x) = a^x \bmod N$.

Para $\begin{cases} a = 7 \\ N = 15 \end{cases}$, temos

$$\begin{cases} f(0) = a^0 \bmod 15 = 1 \\ f(1) = 7^1 = 1 \\ f(2) = 49 = 3.15 + 4 = 4 \\ f(3) = 13 \end{cases}$$

$(-1)15 + 1$

$f(1)$

x	0	1	2	3	4	5	6	...
$f_{7,15}(x)$	1	7	4	13	1	7	4	...

Pelo teorema de EULER

$$\mathbb{Z}_N^* = \langle a \rangle \mathbb{Z}^* = \mathbb{Z}_N^*$$

$$\left\{ a^{\varphi(N)} \equiv 1 \mod N, \quad \text{mdc}(a,N)=1 \right.$$

onde $\varphi(n) = \#\{ j : \text{mdc}(j,N) = 1 \}$.

$(a^r)^k = 1$

Portanto $\boxed{f_{a,N}}$ é periódica, com período $a^{\varphi(N)} = 1$

no maximo $\varphi(N)$. Período r sempre $r \mid \varphi(n)$ $rk = \varphi(N)$

Note que para a conclusão, usar teo Euler é

não é necessário, só suficiente.

Seja r o período de $f_{a,N}$. Então

$$f_{a,N}(0) = f_{a,N}(r)$$

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

$\boxed{r \text{ par}}$

$$\Rightarrow \quad a^r - 1 \equiv 0 \mod N = (a^{r/2}+1)\cdot(a^{r/2}-1) = kN$$

$a^r \mod N$

$$\underbrace{1, a, a^2 \ldots}_{r} 1, a$$

a^0

$mdc(a, N) = 1$

Se, por sorte r for par, então

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

$$\Rightarrow \left(a^{r/2}-1\right)\left(a^{r/2}+1\right) = kN$$

$$\Rightarrow \begin{cases} \text{mdc}\left(a^{r/2}-1, N\right) \mid N \\ \text{e} \\ \text{mdc}\left(a^{r/2}+1, N\right) \mid N \end{cases}$$

Sup $a^{r/2} \equiv -1 \bmod N$

Se dermos ainda mais sorte e

$a^{r/2} \not\equiv -1 \bmod N$, $\quad 1 \cdot N \quad (a^{r/2}-1)\underbrace{(a^{r/2}+1)}_{0} = kN$

$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad \| \ 0$

(sabemos que $a^{r/2} \not\equiv 1 \bmod N$ pois r é período)

então encontramos fatores de N:

$$\begin{cases} mdc(a^{r/2}-1, N) & \neq 1, N \\ mdc(a^{r/2}+1, N) & \end{cases}$$

Podemos então melhorar um pouco a descrição do algo. Shor.

$\varphi(N) = (p-1)(q-1)$

Dado N $= p\,q\,p_1\,p_2 \ldots$

$mdc(a, N) \neq 1$

1. Escolha um a, $mdc(a,N) = 1$, aleatório
2. Use QFT para achar período r da $f_{a,N}$
3. Se r é par e $a^{r/2} \not\equiv -1 \mod N$,

   Devolva $mdc(a^{r/2} - 1, N)$ como fator de N
4. Se não, volte para 1

Por que precisamos de computação quântica para encontrar o período?

$n = \log N$

Seja $n = \log N$

* Algo trivial usa $O(N) = O(2^n)$ operações para achar período. Compare com GNFS que custa

$$\approx 2^{O\left((n)^{1/3}(\log n)^{2/3}\right)}$$

$O(n^{1/3})$

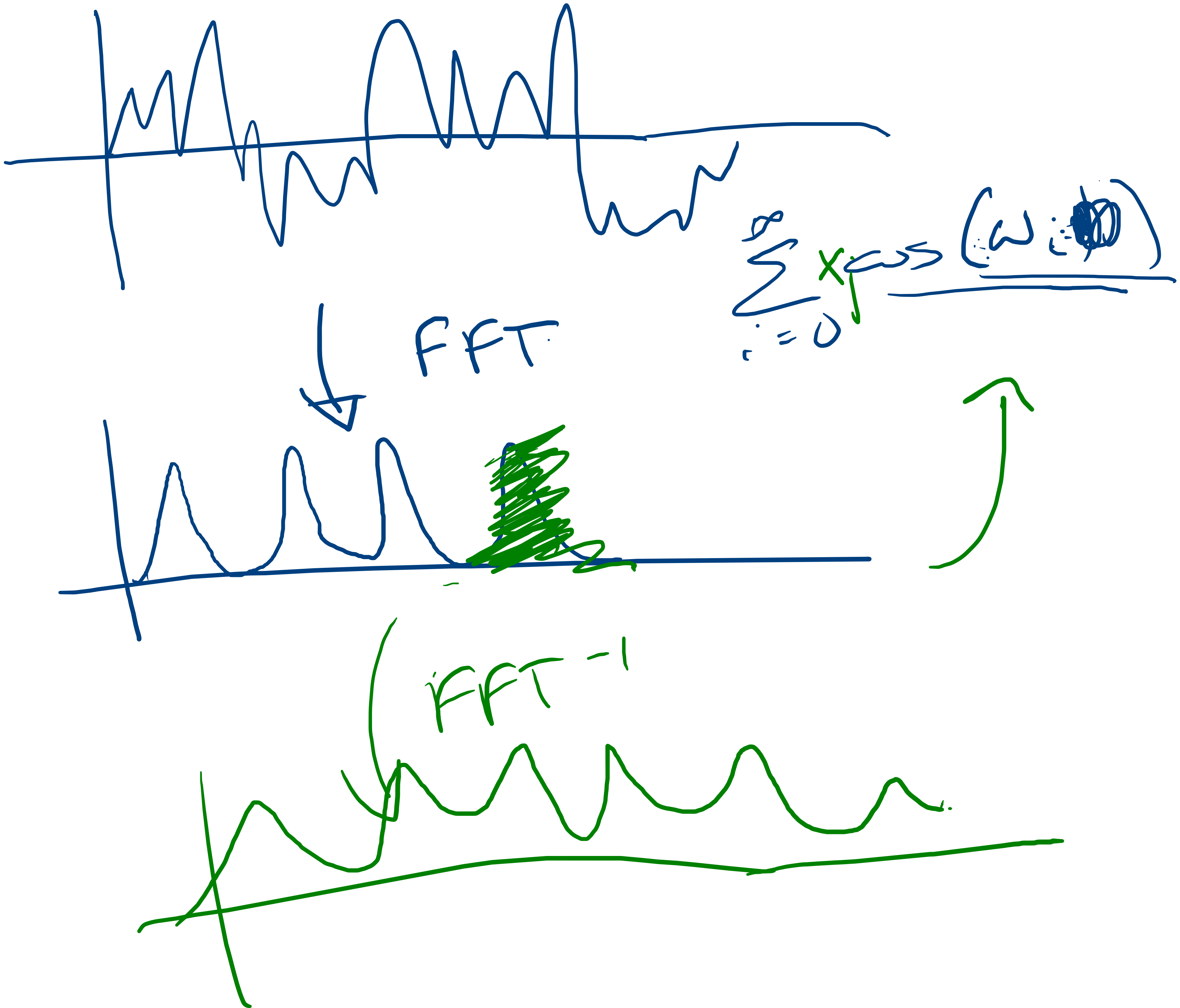
General
Number
Field
Sieve

* E usando FFT em vez de QFT?

O custo seria $O(N \log N) = O(2^n n)$ que é pior ainda.

$2^n n \gg n^2$

$\Rightarrow$ O algoritmo de Shor funciona pois é possível calcular a FT com $\boxed{O(n^2)}$ portas quânticas. Porém os coeficientes de Fourier ficam ocultos e devemos ser espertos ao usar a QFT $\Rightarrow$ QFT não substitui DFT em geral


FFT
$\sum_{i=0}^{\infty} x_j \cos(\omega_i t)$
FFT^{-1}

QUANTUM FOURIER TRANSFORM - QFT

É a variante quântica da DFT (Discrete Fourier Transform)

DFT : Dado um vetor $x = [x_0, x_1, \dots, x_{N-1}] \in \mathbb{C}^N$

$DFT(x) = [y_0, y_1, \dots, y_{N-1}] \in \mathbb{C}^N$ t.q.

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

fator normalização

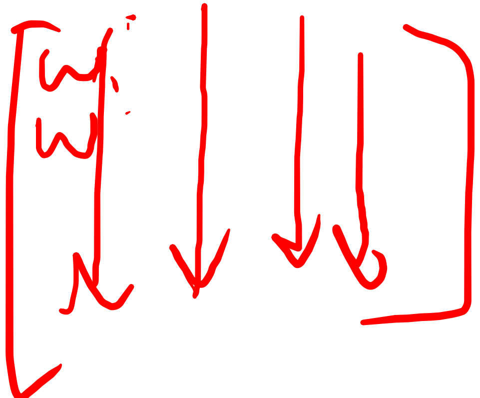
$\frac{1}{N}$

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

$\frac{1}{\sqrt{N}}$ $\frac{1}{\sqrt{N}}$ N N N

$\frac{1}{N}$ ...

DFT



DFT: Dado um vetor $x = [x_0, x_1, \dots, x_{N-1}] \in \mathbb{C}^N$

$DFT(x) = [y_0, y_1, \dots, y_{N-1}] \in \mathbb{C}^N$ t.q.

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{(2\pi i j k/N)}$$

QFT: Dado um estado básico $|j\rangle$, $j \in \{0, \dots, N-1\}$

$$QFT|j\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i k j/N} |k\rangle$$

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

$j = 4$

$$j = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \Big\} \; 2^n = N \xrightarrow{QFT} \frac{1}{\sqrt{N}} \begin{bmatrix} e^{2\pi i 0 4/8} \\ e^{2\pi i 1 4/8} \\ e^{2\pi i 2 4/8} \\ e^{2\pi i 3 4/8} \\ e^{2\pi i 4 4/8} \\ e^{2\pi i 5 4/8} \\ e^{2\pi i 6 4/8} \\ e^{2\pi i 7 4/8} \end{bmatrix} = \begin{bmatrix} 1 \\ i \\ \\ \\ \\ \\ \\ \end{bmatrix}$$

$e^{2\pi i \frac{1}{\cdot}}$

$$\begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ \vdots \\ x_{N-1} \end{bmatrix} \in \mathbb{C}^N, \quad \|x\|_2 = 1$$

$$|x_0|^2 + |x_1|^2 \ldots = 1$$

Para uma superposição qualquer $\sum_{j=0}^{N-1} x_j |j\rangle$, temos

$$QFT\left(\sum_{j=0}^{N-1} x_j |j\rangle\right) = \sum_{k=0}^{N-1} y_k |k\rangle, \text{ onde}$$

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_k e^{2\pi i jk/N}$$

IMPORTANTE Houve apenas mudança de notação

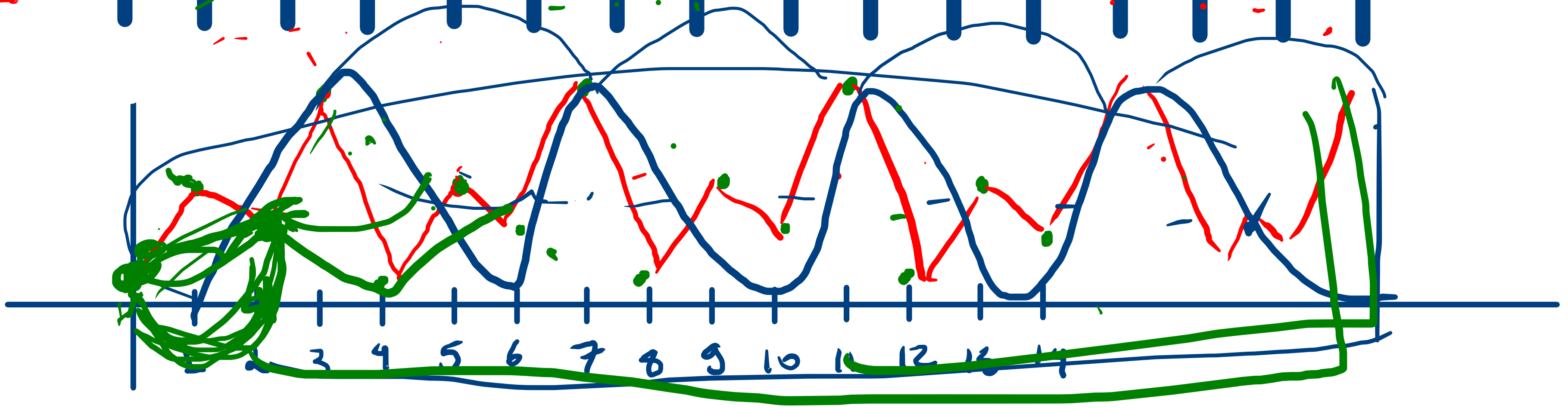
$$\rightarrow QFT\left(\sum x_j |j\rangle\right) = QFT\left(\begin{bmatrix} x_0 \\ x_1 \\ \vdots \\ x_{N-1} \end{bmatrix}\right) = QFT(x)$$

Intuição Clássica

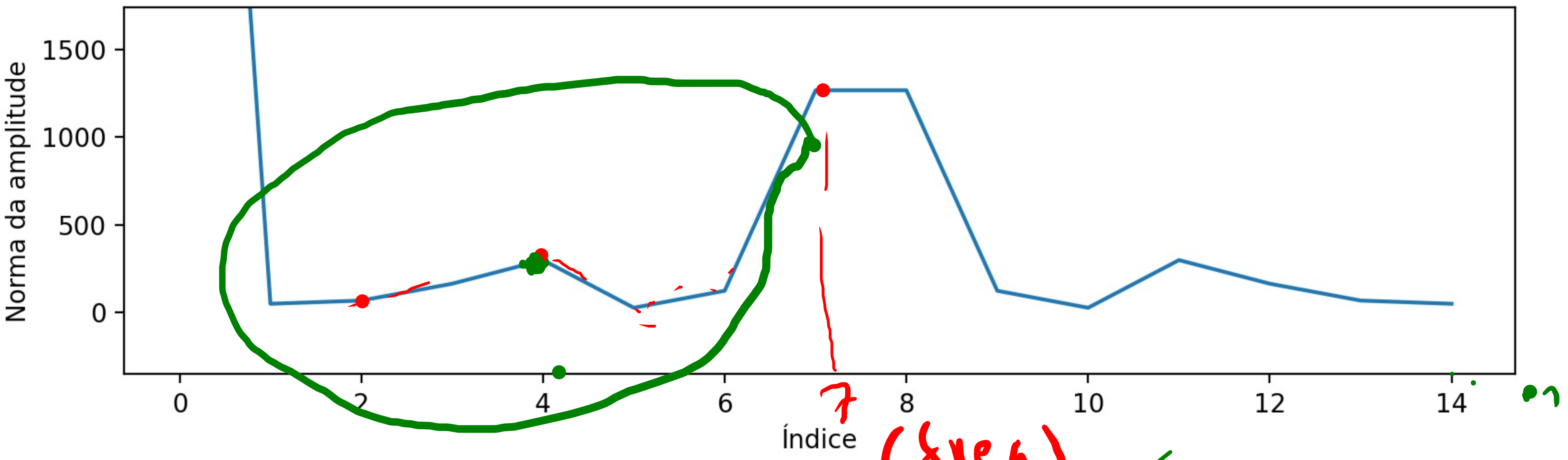
$$f_{7,15}(x) = 7^x \bmod 15$$

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$f_{7,15}(x)$	1	7	4	13	1	7	4	13	1	7	4	13	1	7	4

$$4 \approx \frac{15}{4}$$

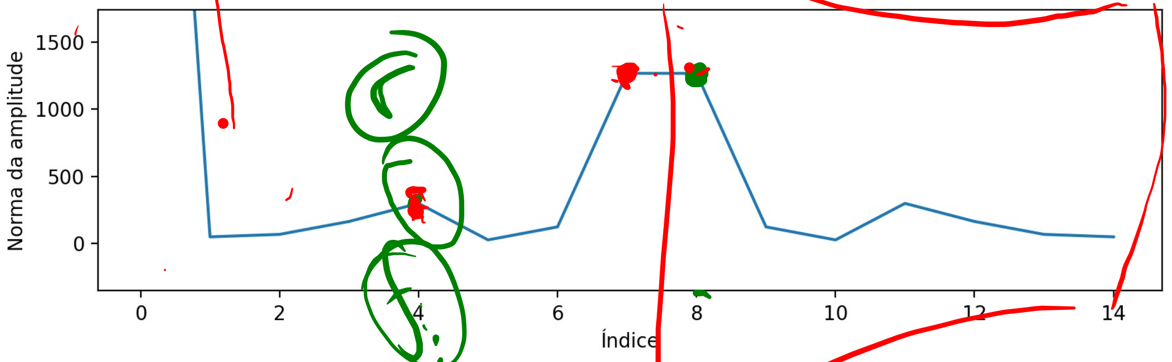


DFT

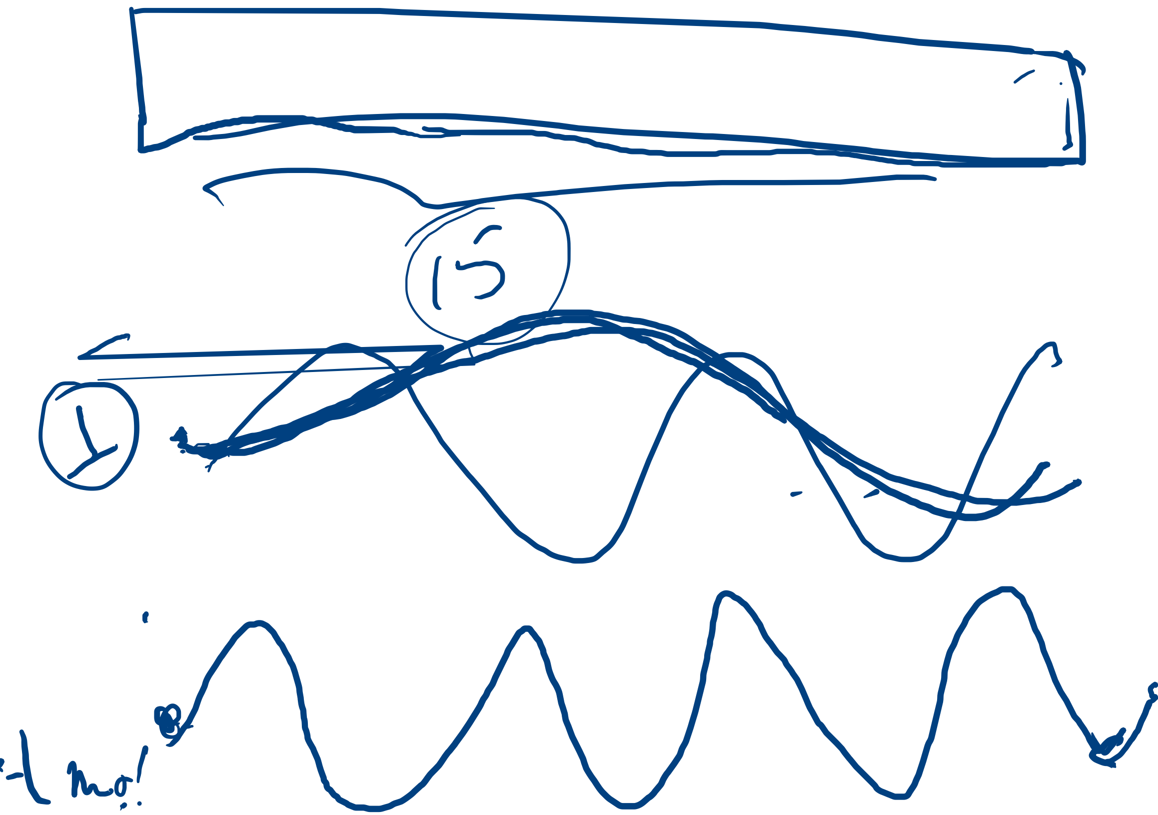


f

$$\boxed{\frac{15}{\text{pico}} = r}$$



$\left(\frac{15}{4}\right)$

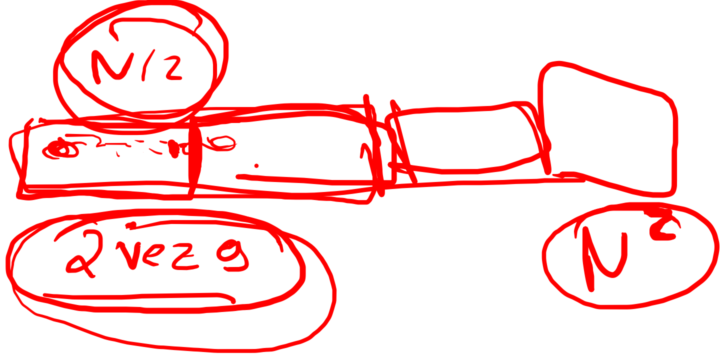


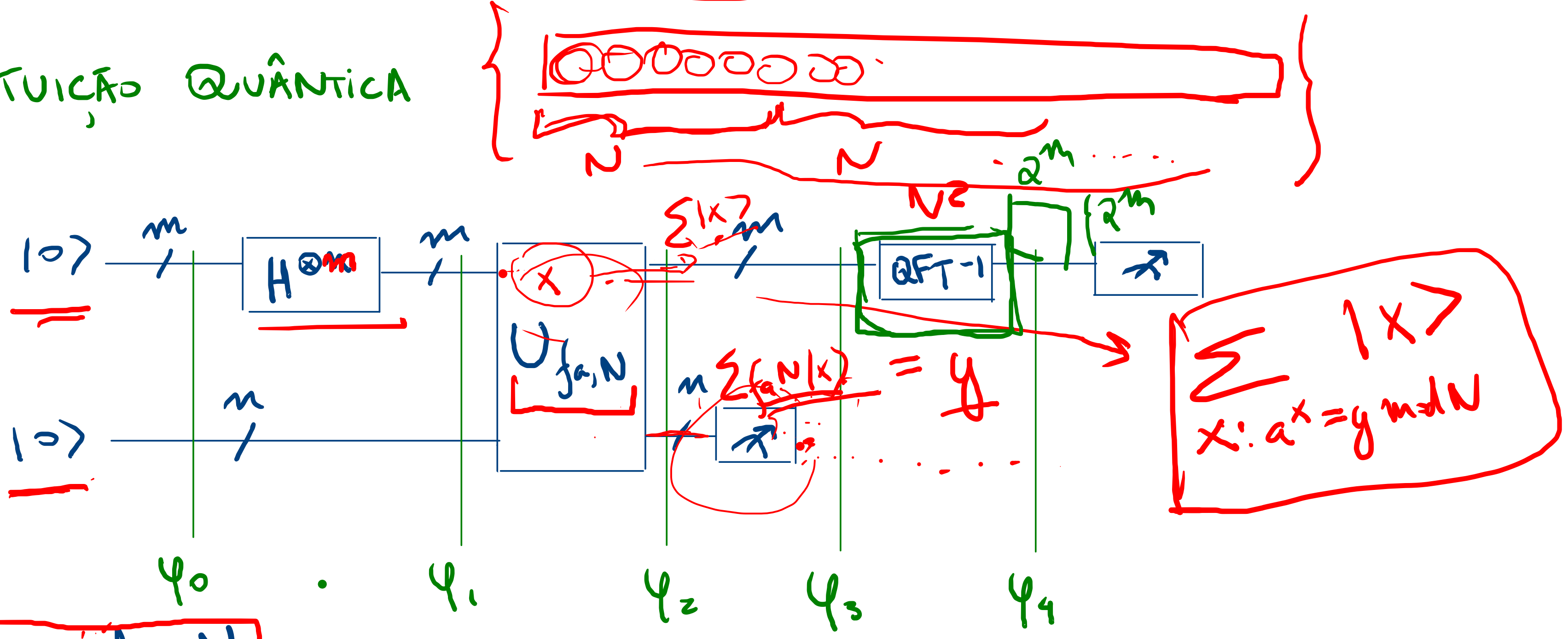
$f=4$ é a freq de maior amplitude

$\Rightarrow r \approx 15/4 \approx 4$ provavelmente $\quad r/2$

é a freq de $f_{7,15}$ $\rightarrow a \neq 1$ mod!

INTUIÇÃO QUÂNTICA





$$\boxed{n = \log N}$$

$$m = \log N^2 = 2n \quad \leftarrow \text{motivo técnico}$$

$$U_{hash}|x\rangle|0\rangle = |x\rangle|hash(x)\rangle$$

$$\downarrow$$

$$y$$

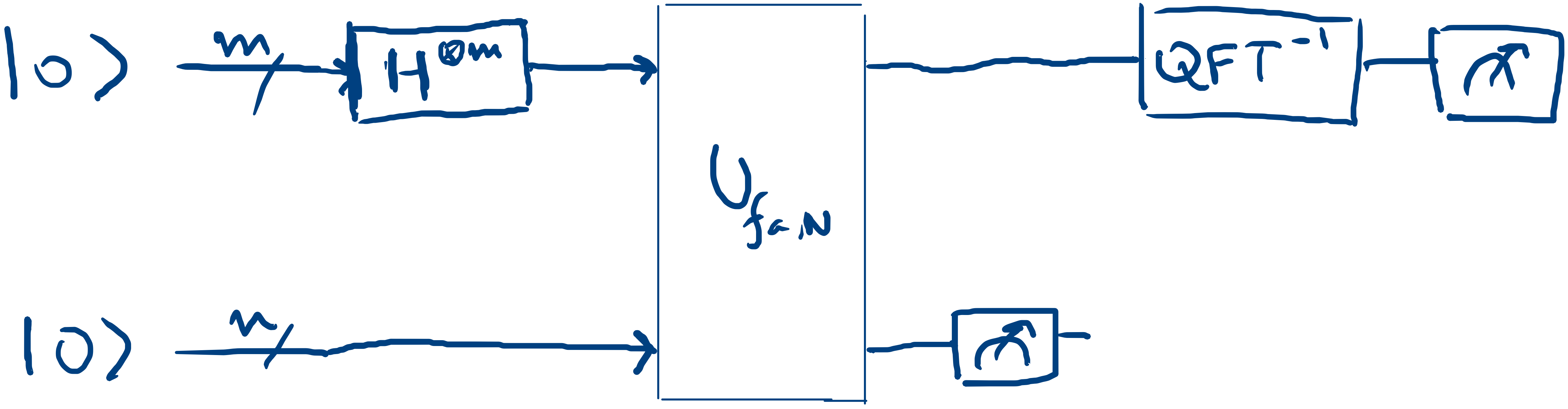
$$U_{hash}\sum|x\rangle|0\rangle = \sum|x\rangle|hash(x)\rangle$$

$$\downarrow$$

$$y$$

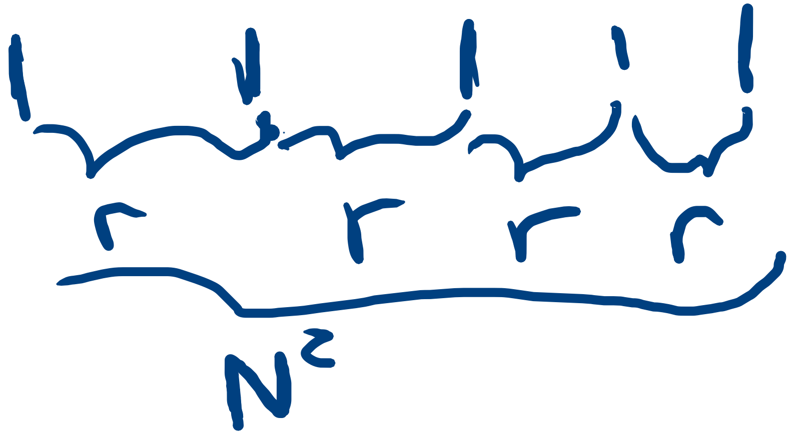
$$= \sum_{hash(\bar{x})=y}|\bar{x}\rangle|y\rangle$$

$$f_{a,N}(x) = a^x \bmod N$$



$$n = \log N \qquad (N = pq)$$

$$\boxed{m} = \underset{2n}{2\log N} = \log N^2$$



$$f_{a,N}: \mathbb{Z} \to \mathbb{Z}_N^*$$

$$f_{a,N}(x) = a^x \bmod N \qquad \mathrm{mdc}(a, N) = 1$$

$\Rightarrow$ periódica $\quad a \longrightarrow \underline{r}$

Se período $\underline{r \text{ for par}}$,

$$a^r - 1 = \underbrace{(a^{r/2}+1)}_{\neq 0 \iff a^{r/2} \not\equiv -1 \bmod N}(a^{r/2}-1) = kN \Rightarrow \begin{cases} \mathrm{mdc}(a^{r/2}+1, N) \\ \mathrm{mdc}(a^{r/2}-1, N) \end{cases}$$

$$|\varphi_0\rangle = |0_m\rangle|0_n\rangle$$

$$|\varphi_1\rangle = \left(H^{\otimes m}|0_m\rangle\right)|0_n\rangle$$

$$= \underbrace{\left(\frac{1}{\sqrt{2^m}}\sum_{i=0}^{m-1}|i\rangle\right)}|0_n\rangle$$

$$\overbrace{}^{m}$$

$$|00000\rangle = |0\rangle$$

$$|0001\rangle = |1\rangle$$

$$|00\ 10\rangle = |2\rangle$$

$$|3\rangle$$

$$|\varphi_1\rangle = \left(\frac{1}{\sqrt{2^m}} \sum_{i=0}^{m-1} |i\rangle\right) |0_{\underline{n}}\rangle$$

$$f_{a,N} \rightarrow \mathbb{Z}_N$$

$$n = \lg N$$

$$|\varphi_2\rangle = U_{f_{a,N}} |\varphi_1\rangle |0_n\rangle$$

$$= \frac{1}{\sqrt{2^m}} \sum_{i=0}^{m-1} U_{\underline{f_{a,N}}} \left(|i\rangle |0_{\underline{n}}\rangle\right) = \frac{\sum_{i=0}^{m-1} |i\rangle |f_{a,N}(i)\rangle}{\sqrt{2^m}}$$

$$|\varphi_2\rangle = \frac{1}{\sqrt{2^m}} \sum_{i=0}^{m-1} \underbrace{|i\rangle|f_{a,N}(i)\rangle}_{\text{entrelaçados}}$$

Se eu medir os m qubits de entrada $\to x$

$\Rightarrow$ os n bits de saída colapsam para $f(x)$

$|x\rangle|f(x)\rangle$

$$\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$$

$\downarrow$

$|1\rangle$

$|0\rangle$

$|1\rangle$

$$\frac{|01\rangle+|10\rangle}{\sqrt{2}}$$

0 1

$$\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)$$

50%: $\boxed{|0\rangle}$

50%: $|1\rangle$

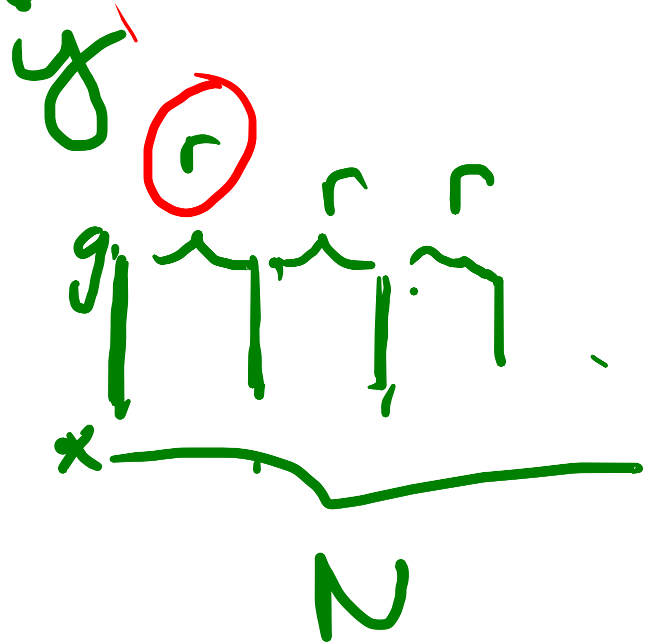
$$|\varphi_2\rangle = \frac{1}{\sqrt{2^m}} \sum_{i=0}^{m-1} |i\rangle \underbrace{|f_{a,N}(i)\rangle}$$

nos n qubits de saída

r período de a

$a^x = y$

$$|\varphi_3\rangle = \frac{1}{\sqrt{\left\lceil \frac{N}{r} \right\rceil}} \sum_{\underbrace{x:\, f_{a,N}(x)=y}} |x\rangle|y\rangle$$



x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$f_{7,15}(x)$	1	7	4	13	1	7	4	13	1	7	4	13	1	7	4

$r = 4$

n Saide

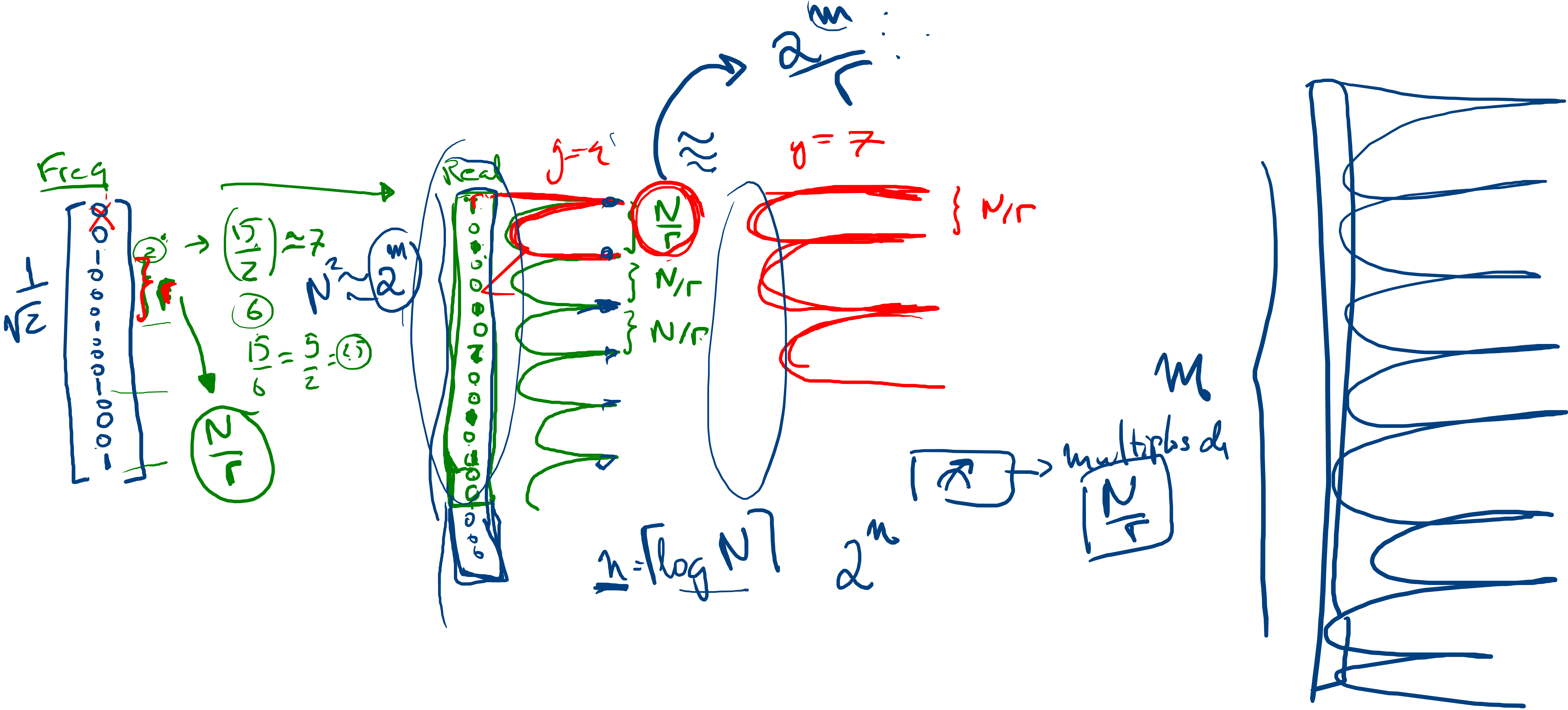
$\rightarrow \boxed{\nearrow} \rightarrow 4 = y$

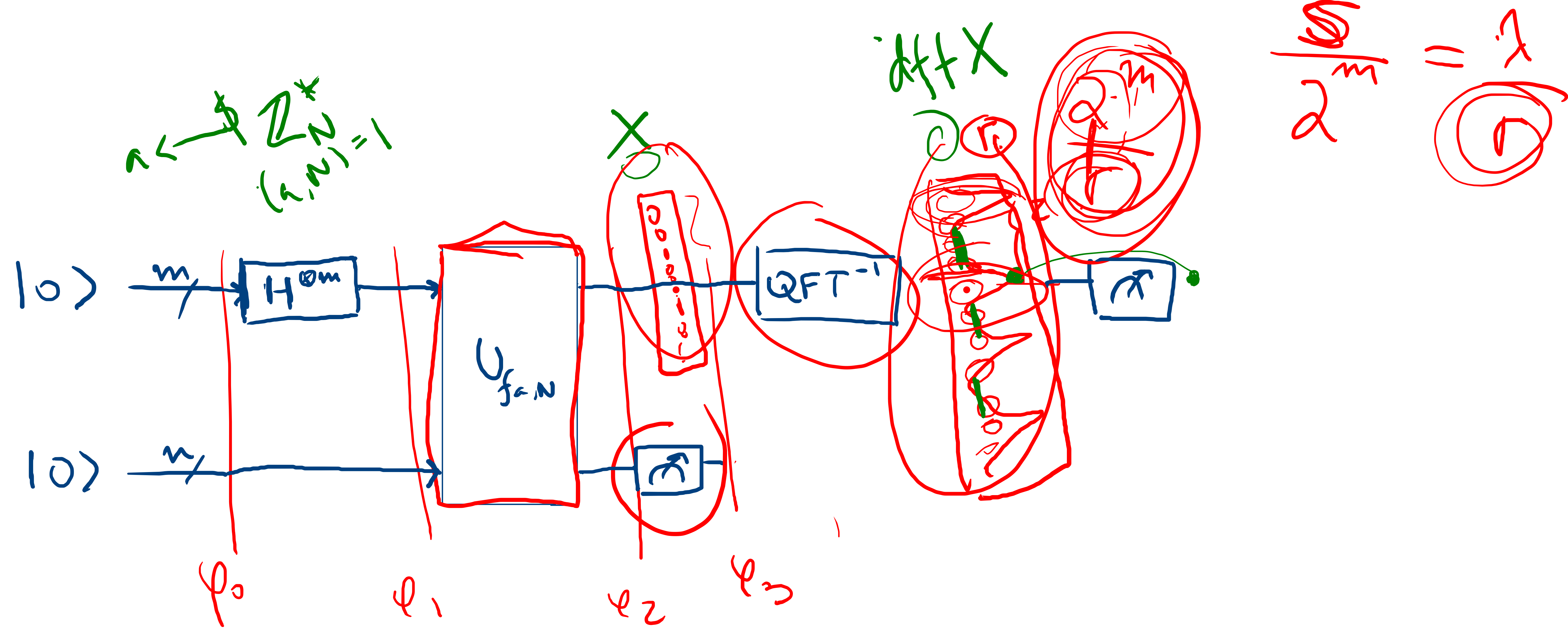
$$\Rightarrow |\varphi_3\rangle = \frac{|2\rangle|4\rangle + |6\rangle|4\rangle + |10\rangle|4\rangle + |14\rangle|4\rangle}{\sqrt{4}}$$

$$= \left(\frac{\overbrace{|2\rangle + |6\rangle + |10\rangle}^{r} + |14\rangle}{\sqrt{2}}\right)\frac{|4\rangle}{\sqrt{2}}$$

$$|\psi_3\rangle = \underbrace{\left(\frac{|2\rangle + |6\rangle + |10\rangle + |14\rangle}{\sqrt{2}}\right)}\frac{|4\rangle}{\sqrt{2}\rangle}$$

$$\frac{1}{\sqrt{2}}\begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} \qquad \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} \; (y = 7)$$


Freq
1/√2
15/2 ≈ 7
6
15/6 = 5/2 = 2.5
N/r
N² ≈ 2^m
Real
y=4
y=7
N/r
2^m/r
n = ⌈log N⌉
2^n
multiples of N/r
m



$a \xleftarrow{\$} \mathbb{Z}_N^*$
$(a,N)=1$
$|0\rangle$
m
$H^{\otimes m}$
$|0\rangle$
n
$U_{f_{a,N}}$
QFT^{-1}
X
diff X
r
φ_0
φ_1
φ_2
φ_3
$\frac{S}{2^m} = \frac{?}{r}$

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$f_{7,15}(x)$	1	7	4	13	1	7	4	13	1	7	4	13	1	7	4

$$|\varphi_1\rangle = \left(\frac{|0\rangle + |1\rangle + |2\rangle + |3\rangle + \dots + |14\rangle}{\sqrt{N}}\right)|0\rangle$$

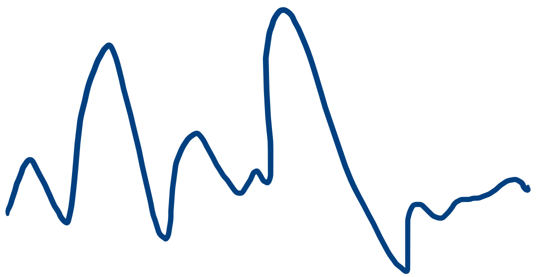
$$|\varphi_2\rangle = |0\rangle|1\rangle + |1\rangle|7\rangle + |2\rangle|4\rangle + |3\rangle|13\rangle + |4\rangle|1\rangle$$

$\boxed{*}$ 2° 7

$$\varphi_3 = \frac{|1\rangle|7\rangle + |5\rangle|7\rangle + |9\rangle|7\rangle + |13\rangle|7\rangle}{\sqrt{4}}$$

$$= \big(|1\rangle + |5\rangle + |9\rangle + |13\rangle\big)\frac{\cancel{|7\rangle}}{\sqrt{4}} = \frac{1}{\sqrt{4}}\begin{bmatrix}0\\1\\0\\0\\0\\1\\0\\0\\0\\1\\0\\0\\0\\1\\0\end{bmatrix}$$

4



$$\boxed{QFT^{-1}} \longrightarrow \boxed{\nearrow} \longrightarrow s$$

$\lambda \in \mathbb{Z}^+$

s é multiplo do periodo da ~~transform.~~ da fourier inversa

$$\boxed{s = \lambda \cdot \frac{2^m}{r}}$$

$$\boxed{\frac{2^m}{r}}$$

$$s = \frac{\lambda 2^m}{r}$$

$$\frac{s}{2^m} = \boxed{\frac{\lambda}{r}}$$

Pela fração irredutível que mais se aprox. da $\frac{s}{2^m}$

Ideia é encontrar λ, r achando um convergente da fração contínua de $(s/2^m)$

$s = 96$

$$\frac{s}{2^m} = \frac{96}{256} = \frac{48}{128} = \frac{24}{64} = \frac{12}{32} = \frac{3}{8} =$$

$$= \frac{1}{p}$$

Continued fractions

$$\frac{31}{13} = 2 + \frac{5}{13}$$

$$= 2 + \frac{1}{\frac{13}{5}} = 2 + \frac{1}{2 + \frac{3}{5}}$$

$$= \boxed{2 + \frac{1}{2 + \frac{1}{\frac{5}{3}}}}$$

$[3, 4, 2, 6]$

$$4 \approx 3 + \cfrac{1}{4 + \cfrac{1}{2 + \cfrac{1}{6}}}$$