Curs 9

STLS II

superpoziții

QFT : $\sum_{i=1}^{m} \underset{\in \mathbb{C}}{f(g_i)} |g_i\rangle \rightsquigarrow \sum_{i=1}^{m} \hat{f}(g_i) |g_i\rangle$

o particulă se află într-o singură stare

Exemplu:

$\mathbb{F}_2^m \quad |\vec{x}\rangle \longrightarrow \sum_{y \in \mathbb{F}_2^m} (-1)^{\vec{x}\cdot\vec{y}} |y\rangle$

$|\vec{x}\rangle = |x_1\rangle |x_2\rangle \dots |x_m\rangle$ qubiți independenți

$\mathbb{F}_2 \quad |0\rangle \to \frac{1}{\sqrt{2}}\left((-1)^{0\cdot 0}|0\rangle + (-1)^{0\cdot 1}|1\rangle\right)$

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

$W_2 = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ $\quad W_2^{\otimes m}$: elementul $\vec{x}\vec{y}$ este $\left(\frac{1}{\sqrt{2}}\right)^m (-1)^{\vec{x}\cdot\vec{y}}$

Exemplu: $\mathbb{Z}_n$: dacă $n = n_1 \cdot n_2$, $\gcd(n_1, n_2) = 1$ (i.e. dacă nu este p^k cu p prim), atunci:

$\mathbb{Z}_n = \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \qquad (\mathbb{Z}_{p^2} \not\cong \mathbb{Z}_p \times \mathbb{Z}_p)$

$\Rightarrow$ QFT este decompozabilă în factori mai mici.

Suficient QFT pt. $\mathbb{Z}_{p^m}$ (care nu sunt decompozabile)

$\mathbb{Z}_{2^m}$ are o reprezentare de m qubiți.

$x = x_m 2^{m-1} + x_{m-1} 2^{m-2} + \dots + x_2 2^1 + x_1, \; x_i \in \{0,1\}$

$|x\rangle = |x_m\rangle |x_{m-1}\rangle \dots |x_1\rangle$.

QFT inversă: $|x\rangle \to \frac{1}{\sqrt{2^m}} \sum_{y=0}^{2^m-1} e^{\frac{2\pi i x y}{2^m}} |y\rangle$

! Obs. Acțiunea acestei transformări pe un element din bază este decompozabilă.

$$\sum_{y=0}^{2^m-1} e^{\frac{2\pi i x y}{2^m}} |y\rangle = \left(|0\rangle + e^{\frac{\pi i x}{2^0}}|1\rangle\right) \cdot \ldots \cdot \left(|0\rangle + e^{\frac{\pi i x}{2^{m-1}}}|1\rangle\right)$$

• Input: $|\vec{x}\rangle = |x_1\rangle|x_2\rangle \ldots |x_m\rangle$

• Circuit pt. QFT^{-1} (inversul) pe $\mathbb{Z}_{2^m}$:

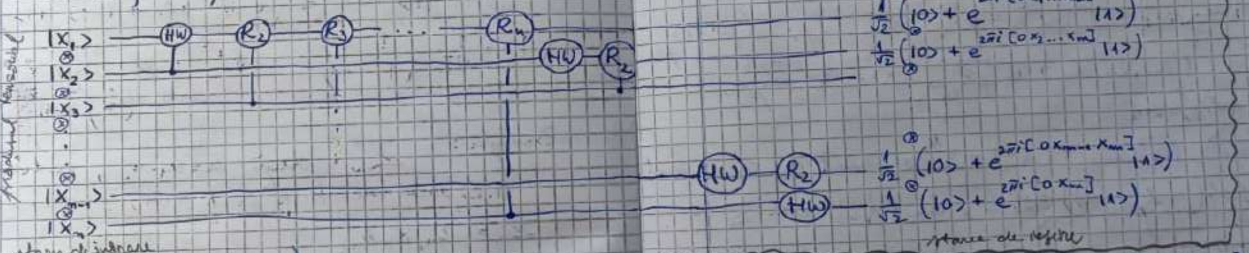
① Hadamard - Walsh pe qubitul m:

$$\frac{1}{\sqrt{2}} |x_1\rangle|x_2\rangle \ldots |x_{m-2}\rangle \left(|0\rangle + (-1)^{x_m}|1\rangle\right)$$

② Se completează faza $(-1)^{x_m}$ la faza

$$(-1)^{x_m} \underbrace{\exp\left(\frac{2\pi i\, x_{m-1}}{2^2}\right) \ldots \exp\left(\frac{2\pi i\, x_1}{2^m}\right)}_{\text{rotație}}$$

O rotație se aplică $\Leftrightarrow x_m = x_i = 1$



starea de intrare

$$R_k: \begin{pmatrix} 1 & 0 \\ 0 & \exp\left(\frac{2\pi i}{2^k}\right) \end{pmatrix}$$

Aplicația condiționată este prin compunere cu matrice M_{CNOT}, Toffoli.

$n = p_1^{e_1} \cdots p_m^{e_m}$ impar, factorizarea e necunoscută

• există algoritm care decide dacă $n = k^m$ cu $m \geq 2$ (timp polinomial):

- dacă da, atunci output: k.
- dacă găsim divizor d al lui n, $1 < d < n$, atunci output: d (d, n/d)

• alege la întâmplare $a \in \mathbb{Z}_m$, $a \notin \{0, 1\}$

- dacă $d = \gcd(a, n) > 1$, atunci output $= d$ ($\approx \|n\|^3$ polinomial)
- dacă nu, atunci $\gcd(a, n) = 1$, adică $a \in \mathbb{Z}_n^{\times}$ (a este unitate în inelul $\mathbb{Z}_n$ – element inversabil)
- pp. că putem afla ordinul multiplicativ $r = ord_n(a)$

$\Leftrightarrow$ cel mai mic r a.î. $a^r = 1$ în $\mathbb{Z}_m \Leftrightarrow n \mid a^r - 1 \Leftrightarrow$

$\Leftrightarrow a^r \equiv 1 \mod n$

→ dacă r par: $n \mid (a^{r/2}-1)(a^{r/2}+1)$, deci ar avea factor comun cu unul dintre ele și acela s-ar putea afla cu Euclid (în timp polinomial)

problemă ▲ $n \mid (a^{r/2}+1)$ sau $n \mid (a^{r/2}-1)$?

se arată că e improbabil:

$n \mid (a^{r/2}-1) \Rightarrow a^{r/2} \equiv 1 \mod n$ ↯ def. $ord_n(a)$

$n \mid (a^{r/2}+1) \rightarrow a^{r/2} \equiv -1 \mod n$

$\gcd(n, a^{r/2}-1) = 1$ și

se va arăta că probabilitatea ca $ord(a)$ să fie par și ca $a^{r/2} \not\equiv 1 \mod n$ este $\geq \frac{9}{16} > \frac{1}{2}$

$\Rightarrow$ QC (quantum comp.) ar trebui să rezolve problema $ord_n(a)$ dacă a este inversabil mod n.

Ex. $\mathbb{Z}_{15}^{\times} = \{1, 2, 4, 7, 8, 11, 13, 14\}$

ord(a): 0, 4, 2, 4, 4, 2, 4, 2

$\{a \mid a^{r/2} \equiv -1 \bmod 15\} = \{14\}$ „evenimentul neplăcut"

$a = 7$, $7^2 - 1 = 48 \equiv 3 \bmod 15$ | factori ai lui 15
$7^2 + 1 = 50 \equiv 5 \bmod 15$

$n = p_1^{e_1} \cdots p_k^{e_k}$ impar, $k \geq 2$; $a \in \mathbb{Z}_n^{\times}$

Th Chineză a resturilor: $\mathbb{Z}_n^{\times} = \mathbb{Z}_{p_1^{e_1}}^{\times} \times \dots \times \mathbb{Z}_{p_k^{e_k}}^{\times}$ produs direct de grupuri ciclice

$|\mathbb{Z}_{p_i^{e_i}}^{\times}| = \varphi(p_i^{e_i}) = p_i^{e_i} - p_i^{e_i - 1} = p_i^{e_i - 1}(p_i - 1)$ par

$a = (a_1, \dots, a_k) \in \mathbb{Z}_{p_1^{e_1}}^{\times} \times \dots \times \mathbb{Z}_{p_k^{e_k}}^{\times}$

$\mathrm{ord}_{p_1^{e_1}}(a_1)$

Lema Dacă $\varphi(p^e) = 2^u v$, $2 \nmid v$, $s \geq 0$ fixat

$\mathrm{prob}(\mathrm{ord}_{p^e}(a)) = 2^s t$, cu $2 \nmid t$ este $\leq \frac{1}{2}$.

Dem.

- $s > u \Rightarrow$ prob $= 0$
- $s \leq u$, $\mathbb{Z}_n^{\times}$ ciclic $\Leftrightarrow n \in \{2, 4, p^e, 2p^e\}$ p prim impar

Fie g generator al lui $\mathbb{Z}_{p^e}^{\times}$.

$\mathbb{Z}_{p^e}^{\times} = \{g^0, g^1, \dots, g^{2^u v - 1}\}$

$\mathrm{ord}(g^j) = \dfrac{2^u v}{\gcd(j, 2^u v)}$; $2^s t$ apare ca ordin $\Leftrightarrow j = 2^{u-s} w$, cu $2 \nmid w$

$\{0, 1, 2, \dots, 2^u v - 1\} \ni$ exact $2^s v$ multipli de 2^{u-s}, numai $\frac{1}{2}$ dintre ei au coeficient impar.

Probabilitatea este $\frac{\frac{1}{2}\cdot 2^{s}\cdot v}{2^{u}\cdot v} = \frac{2^{s}}{2^{u+1}} \le \frac{1}{2}$. □

Lemă Dacă $a \in \mathbb{Z}_n^*$, atunci probabilitatea ca $ord_n(a)$ impar este $\le 2^{-k}$.

Dem. $a \xrightarrow{\text{Th. Ch. Rest}} (a_1, \ldots, a_k)$, $r_i = ord_{p_i^{e_i}}(a_i)$

$r = lcm(r_1, \ldots, r_k)$ impar $\Leftrightarrow$ ~~toți~~ r_i impari.

cu lema anterioară: $prob(\ldots) \le \frac{1}{2}\cdot\frac{1}{2}\cdot\ldots\cdot\frac{1}{2} = \left(\frac{1}{2}\right)^k$ □

Lemă $n = p_1^{e_1}\cdots p_k^{e_k}$, $k \ge 2$, dacă $r = ord_n(a)$ par, atunci $prob(a^{r/2} \equiv -1 \bmod n) \le 2^{-k}$.

Dem. $a^{r/2} \equiv -1 \bmod n \Rightarrow a^{r/2} \equiv -1 \bmod p_i^{e_i}$ pt. $\forall i = \overline{1,k}$.

$r = ord_n(a)$, $r_i = ord_{p_i^{e_i}}(a_i)$.

$r = 2^s t$ $\quad r_i = 2^{s_i} t_i$ $\quad t, t_i$ impari

$r_i \mid r \Rightarrow s_i \le s$ $\quad$ congruențele au loc dacă $s_i = s$ $\forall i$

dacă $s < s_i \Rightarrow r_i \mid \frac{r}{2} \Rightarrow a^{r/2} \equiv 1 \bmod p_i^{e_i}$

$\Rightarrow 1 \equiv -1 \bmod p_i^{e_i} \Rightarrow p_i = 2$ dar n impar

deci $prob(\ldots) \le prob(s_i = s \text{ pt. } \forall i) \le \underbrace{\frac{1}{2}\cdot\ldots\cdot\frac{1}{2}}_{k} = 2^{-k}$ □

Th $n = p_1^{e_1}\cdots p_k^{e_k}$, $k \ge 2$; impar, $a \in \mathbb{Z}_n^*$ aleator

Atunci $Prob(ord_n(a) \text{ par} \wedge a^{r/2} \not\equiv -1 \bmod n) \ge$

$\ge (1 - 2^{-k})^2 \ge \left(\frac{3}{4}\right)^2 = \frac{9}{16} > \frac{1}{2}$.

eveniment exploatat cuantic