pe vec identic după ce e compilat – ~~optimiz.~~ timp real)

Curs 10 STLS II

circuite booleene (transf. în circ. cuantic)
calcule nr. complexe

Examen – sp vect peste corp finit : nucleu? ponderi?
def de bază! de aplicat McWilliams pe un spațiu; math.
(superpoz) Th de neclonare, entanglement (calc. cu baze)

Th. $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, $k \geq 2$, $a \in \mathbb{Z}_m^{\times}$ random

$$P(\mathrm{ord}_m(a) \text{ par} \wedge a^{r/2} \not\equiv -1 \bmod m) \geq \frac{9}{16}$$

Algoritm cuantic pentru aflarea lui $\mathrm{ord}_m(a)$

Aleg $\mathbb{Z}_M$, $M > m$ suficient de mare pt. apariția unei perioade

$M = 2^{\ell}$ QFT, ℓ se va fixa mai târziu

$|x\rangle |y\rangle \in \mathbb{Z}_M \times \mathbb{Z}_m$

ℓ qubiți $\leq \ell$ qubiți

Pași:

① $|0\rangle|0\rangle$, Hadamard-Walsh pe primul.

$$\frac{1}{\sqrt{M}} \sum_{k=0}^{M-1} |k\rangle|0\rangle$$

pt. un anumit a

② Se calc. $k \to a^k \bmod m$ (exponențiere rapidă ⇒ circuit boolean mic ⇒ circuit cuantic mic)

$$\frac{1}{\sqrt{M}} \sum_{k=0}^{M-1} |k\rangle|a^k\rangle$$

superpoziție

Funcția $k \to a^k \bmod m$ are perioada $\mathrm{ord}_m(a) = r$

$$= \frac{1}{\sqrt{M}} \sum_{\ell=0}^{r-1} \sum_{q=0}^{s_\ell} |qr+\ell\rangle|a^\ell\rangle$$

unde s_ℓ este cel mai mic întreg a.î. $s_\ell \cdot r + \ell < M$

(i.e. $\frac{M}{r} - 1 - \frac{\ell}{r} \leq s_\ell < \frac{M}{r} - \frac{\ell}{r}$

③ QFT inversă pe $\mathbb{Z}_m$

$$\frac{1}{\sqrt{m}}\sum_{l=0}^{r-1}\sum_{q=0}^{s_l}\frac{1}{\sqrt{m}}\sum_{p=0}^{m-1}\exp\left(\frac{2\pi i p(qr+l)}{m}\right)|p\rangle|a^l\rangle =$$

e la-puterea

$$= \frac{1}{m}\sum_{l=0}^{r-1}\sum_{p=0}^{m-1}\exp\left(\frac{2\pi i pl}{m}\right)\sum_{q=0}^{s_l}\exp\left(\frac{2\pi i prq}{m}\right)|p\rangle|a^l\rangle$$

④ Obs. se citește $p\in\mathbb{Z}_m$

⑤ Se consideră raționalul $\frac{p}{m}$ și se descompune în fracție periodică. Se găsește cel mai mic q_i numitor convergent a.î. $a^{q_i}\equiv 1 \bmod m$ (sau se face altă observație) dacă ∄

Fracții continue

ex. $\frac{263}{189}$ ireductibilă — cu Euclid:

$263 = 1\cdot 189 + 74$
$189 = 2\cdot 74 + 41$
$74 = 1\cdot 41 + 33$
$41 = 1\cdot 33 + 8$
$33 = 4\cdot 8 + \underline{1}$

răsturnare fracție

$$\frac{263}{189} = 1 + \frac{74}{189}$$
$$\frac{189}{74} = 2 + \frac{41}{74}$$
$$\frac{74}{41} = 1 + \frac{33}{41}$$
$$\frac{41}{33} = 1 + \frac{8}{33}$$
$$\frac{33}{8} = 4 + \frac{1}{8}$$

nu se mai răstoarnă fiindcă dă nr. întreg

Notație fracție continuă $[a_1, \ldots, a_n]$

$$\frac{263}{189} = 1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{4 + \cfrac{1}{8}}}}}$$

fracție continuă

$[1, 2, 1, 1, 4, 8]$ ← pt. cea de mai sus

pt. cazul nostru

ex. •

Convergenți: $\frac{p_i}{q_i}$ unde:

pt. cazul nostru

$$\frac{p_0}{q_0} = \frac{a_0}{1}, \quad \frac{p_1}{q_1} = \frac{a_0 a_1 + 1}{a_1}, \quad \frac{p_i}{q_i} = \frac{a_i p_{i-1} + p_{i-2}}{a_i q_{i-1} + q_{i-2}}$$

convergenți: $1, \frac{3}{2}, \frac{4}{3}, \frac{7}{5}, \frac{32}{23}, \frac{263}{189}$

ex • $n = 15$, $a = 7$, $ord_{15}(7) = ?$

alegem $m = 16$

① Hadamard-Walsh pe primul $|0\rangle$ $\rightarrow \frac{1}{4} \sum_{k=0}^{15} |k\rangle|0\rangle$

② $k \rightsquigarrow 7^k \bmod 15$

1, 7, 4, 13 - periodicitate

$$\frac{1}{4}\Big(|0\rangle|1\rangle + |1\rangle|7\rangle + |2\rangle|4\rangle + |3\rangle|13\rangle + |4\rangle|1\rangle + \dots + |15\rangle|13\rangle\Big) =$$

$$= \frac{1}{4}\big(|0\rangle + |4\rangle + |8\rangle + |12\rangle\big)|1\rangle +$$

$$+ \frac{1}{4}\big(|1\rangle + |5\rangle + |9\rangle + |13\rangle\big)|7\rangle +$$

$$+ \frac{1}{4}\big(|2\rangle + |6\rangle + |10\rangle + |14\rangle\big)|4\rangle +$$

$$+ \frac{1}{4}\big(|3\rangle + |7\rangle + |11\rangle + |15\rangle\big)|13\rangle \rightsquigarrow$$

③ QFT inversă pe $\mathbb{Z}_{16}$:

$$\rightsquigarrow \frac{1}{4}\big(|0\rangle + |4\rangle + |8\rangle + |12\rangle\big)|1\rangle +$$

$$+ \frac{1}{4}\big(|0\rangle + i|4\rangle - |8\rangle - i|12\rangle\big)|7\rangle +$$

$$+ \frac{1}{4}\big(|0\rangle - |4\rangle + |8\rangle - |12\rangle\big)|4\rangle +$$

$$+ \frac{1}{4}\big(|0\rangle - i|4\rangle - |8\rangle + i|12\rangle\big)|13\rangle$$

4 **Obs.** $|0\rangle, |4\rangle, |8\rangle, |12\rangle$ cu probabilitate $\frac{1}{4}$ fiecare

$0/0$ nu dă nimic ; $4/16$ cu convergenți : $\frac{0}{1}, \frac{1}{4}$ perioadă

$8/16$ cu convergenți : $\frac{0}{1}, \frac{1}{2}$ nu dă nimic ; $12/16$ cu convergenți : $\frac{0}{1}, \frac{1}{1}, \frac{3}{4}$ perioadă

$ord_{15}(7) = 4$

Probabilitatea observării unui $p \in \mathbb{Z}_m$ este

$$P(p) = \sum_{l=0}^{r-1} \frac{1}{m^2} \left| \exp\left(\frac{2\pi i p l}{m}\right) \sum_{q=0}^{s_l} \exp\left(\frac{2\pi i p q r}{m}\right) \right|^2 =$$

$$= \frac{1}{m^2} \sum_{l=0}^{r-1} \left| \sum_{q=0}^{s_l} \exp\left(\frac{2\pi i p q r}{m}\right) \right|^2 = \frac{1}{m^2} \left| \sum_{q=0}^{\frac{m}{r}-1} \exp\left(\frac{2\pi i p q}{m/r}\right) \right|^2$$

s_l : cel mai mare întreg a.î. $s_l \cdot r + l < m$, unde $0 \le l < r$ $\forall l$ rest mod r

- Cazul ușor: $r \mid m$

$s_l = \frac{m}{r} - 1$ (se alege așa)

Din propr. de ortogonalitate : $\sum_{q=0}^{\frac{m}{r}-1} \exp\left(\frac{2\pi i p q}{m/r}\right) =$

$$= \begin{cases} \frac{m}{r}, & p = 0 \text{ în } \mathbb{Z}_{\frac{m}{r}} \\ 0, & \text{altfel} \end{cases} \qquad \frac{m}{r} \in \mathbb{N}$$

$$P(p) = \begin{cases} \frac{1}{r}, & \text{dacă } p = 0 \text{ în } \mathbb{Z}_{\frac{m}{r}} \\ 0, & \text{altfel} \end{cases}$$

expl.

$p = \{0, \frac{m}{r}, \frac{2m}{r}, \dots, (r-1)\frac{m}{r}\}$ $\quad \underbrace{r}_{\text{de } r \text{ ori}} \cdot \frac{1}{r^2} = \frac{1}{r}$

Se obține rezolventul bun numai dacă $\gcd(d, r) = 1$.

* Cazul general: $m = 2^\ell$, deci $r \nmid m$ în general.

Vrem p aproape de un multiplu al lui $\frac{m}{r}$.

dacă $m \cdot \left|\frac{p}{m} - \frac{d}{r}\right| = \left|p - d \cdot \frac{m}{r}\right|$ suficient de mică și dacă $\gcd(r, d) = 1$, atunci $\frac{d}{r}$ este convergent al lui $\frac{p}{m}$.

Pt. orice $d \in \{0, 1, \dots, r-1\}$ $\exists!\, p$ a.î.

$-\frac{1}{2} < p - d\frac{m}{r} \le \frac{1}{2}$. Alegem m cu $n^2 \le m$.

$\left|\frac{p}{m} - \frac{d}{r}\right| \le \frac{1}{2m} \le \frac{1}{2n^2} < \frac{1}{2r^2}$. Se aplică:

Th. fundamentală a fracțiilor continue.

Dacă $0 < \left|\frac{p}{q} - \alpha\right| \le \frac{1}{2q^2}$ *, atunci $\frac{p}{q}$ convergent al lui α în fracție continuă.

$\gcd(d, r) = 1 \Rightarrow \frac{d}{r}$ este convergent al lui $\frac{p}{m}$.

Există r numere întregi $p \in \mathbb{Z}_m$ care satisfac inegalitatea * (pt. fiecare $d \in \{0, 1, \dots, r-1\}$ există un asemenea p).

$P(p \mid p \in \mathbb{Z}_m$ și $\exists d \in \{0, 1, \dots, r-1\}$ cu $|pr - dm| \le \frac{r}{2})$.

Lemă. Dacă $n \ge 100$, $P(\dots) \ge \frac{2}{5}$ ~~[illegible]~~

(probabilitatea de a observa unul dintre cei r astfel de p este $\frac{2}{5r}$).

Pt. $\forall d$ corespunzător unui asemenea p, prob. de a observa p este $\ge \frac{2}{5r}$. ☆

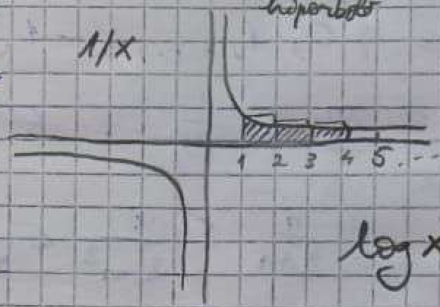
Se estimează prob. ca pt. un asemenea d, $\gcd(d, r) = 1$.

$d \in \{0, 1, \dots, r-1\} \to \frac{\varphi(r)}{r}$.

Th (teoria numerelor) $r \geq 3$, $\frac{r}{\varphi(r)} < e^{\gamma} \log\log r + \frac{2{,}50673}{\log\log r}$

nu i se cunoaște natura algebrică $\gamma = 0{,}577\dots = \lim_{n \to \infty} \left(1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{n} - \log n\right)$

constanta lui Euler



$\log x = \int \frac{dx}{x}$

Lemă $r \geq 19$, prob. ca pt. $d \in \{0, \dots, r-1\}$ să fie $\gcd(r, d) = 1$ este $\geq \frac{1}{4 \log\log n}$ ✡✡

✡ și ✡✡ → probabilitatea de succes $\geq \frac{9}{160} \cdot \frac{1}{\log\log n}$

Algoritm:

① alege $a \in \{1, 2, \dots, n-1\}$ random

② $d = \gcd(a, n)$. Dacă $d > 1$, stop. output d

③ Calc. $r = ord_n(a)$ cu alg. cuantic, $m = 2^{\ell}$ ales a.î. $n^2 < m$.

(dacă $a^r \equiv 1 \bmod n$ sau r impar sau $a^{r/2} \equiv -1 \bmod n$, alege alt a).

④ $d = \gcd(n, a^{r/2} \pm 1)$. output d, stop.

$\Omega\left(\frac{1}{\log \ell(n)}\right)$ $\ell(n)$ = lungimea binară a lui n.

repetare: $O(\log \ell(n))$