Odredivanje reda elementa u $(\mathbb{Z}/N\mathbb{Z})^*$

Ključna procedura za Shorov algoritam

Def. Neka su $(x, N) = 1$. Red od x modulo N je najmanji $r \in \mathbb{N}$ t.d. $x^r \equiv 1 \pmod N$

Problem je za dane x i N odrediti r.

Klasičnr je to težak problem. Nije poznat polinomijalni algoritam koji ga rješava.

Za cijeli broj $0 \leq y < 2^L$ $(L = \lceil \log_2 N \rceil$ broj bitova od $N)$

definiramo operator na prostorom stanja $\langle |0\rangle, |1\rangle \rangle^{\otimes L}$

$$U|y\rangle = \begin{cases} |x y \bmod N\rangle & \text{ako je } y < N \\ |y\rangle & \text{inače} \end{cases}$$

identificiramo $y \in \mathbb{Z}$ s njegovim binarnim zapisom

↑ proširenje da je U unitarni operator

Ideja: Svojstvene vrijednosti od U sadrže informaciju o redu r.

Naime, za sve $0 \leq s \leq r-1$ neka je

$$|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \exp\left(\frac{-2\pi i s k}{r}\right) |x^k \bmod N\rangle.$$

Tada je $U|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \exp\left(\frac{-2\pi i s k}{r}\right) |x^{k+1} \bmod N\rangle$

$$= \exp\left(\frac{2\pi i s}{r}\right) |u_s\rangle, \text{ odnosno}$$

zaključujemo da su vektori $|u_s\rangle$ svojstveni za U sa svojstvenim vrijednostima $e^{\frac{2\pi i s}{r}}$.

Pretp. na trenutak da nam je dan vektor $|u_s\rangle$ za neki nama nepoznati $s \in \{0, \dots, r-1\}$. Primjenom algoritma za određivanje faze možemo izračunati aproksimaciju ϕ razlomka $\frac{s}{r}$.

Možemo li iz ϕ izračunati r^2?

Uz malo sreće možemo. Vrijedi sljedeći teorem

Teorem: Neka je $\phi \in \mathbb{R}$. Pretp. da je $\frac{s}{r}$ racionalan broj takav da je $\left|\phi - \frac{s}{r}\right| \leq \frac{1}{2r^2}$.

Tada je $\frac{s}{r}$ **konvergenta** verižnog razlomka od ϕ.

Malo o diofantskim aproksimacijama – verižni razlomci.

Za $\alpha \in \mathbb{R}$ računamo:

- $a_0 := [\alpha]$

  ako je $\alpha \neq a_0$ onda postoji $\alpha_1 \in \mathbb{R}$, $\alpha_1 > 1$, t.d. $\alpha = a_0 + \frac{1}{\alpha_1}$.

- $a_1 := [\alpha_1]$

  ako je $\alpha_1 \neq a_1$ onda postoji $\alpha_2 \in \mathbb{R}$, $\alpha_2 > 1$, t.d. $\alpha_1 = a_1 + \frac{1}{\alpha_2}$

  odnosno $\alpha = a_0 + \cfrac{1}{a_1 + \frac{1}{\alpha_2}}$ .....

Ponavljanjem ovog postupka dobivamo

verižni razlomak broja α

racionalan broj ima konačan verižni razlomak

$$[a_0, a_1, \ldots, a_n, \ldots] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_n + \cfrac{1}{\ddots}}}}}$$

Racionalni brojevi

$$\frac{p_n}{q_n} = [a_0, a_1, \ldots, a_n]$$ se nazivaju **konvergente** verižnog razlomka

i možemo ih efikasno računati.

Lema: Uz početne uvjete $p_0 = a_0$, $p_1 = a_0 a_1 + 1$, $q_0 = 1$, $q_1 = a_1$ brojevi p_n i q_n zadovoljavaju rekurzivne relacije

$$p_n = a_n p_{n-1} + p_{n-2}, \qquad q_n = a_n q_{n-1} + q_{n-2}.$$

Konvergente su važne jer dobro aproksimiraju α u sljedećem smislu. U diof. aproksimacijama "kvaliteta" aproksimacija se "mjeri" time koliko je $\frac{p}{q}$ blizu broju α u odnosu na veličinu nazivnika q.

Znamo da prema Dirichletovom teoremu $\exists$ ∞ mnogo parova (p,q) t.d. $\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}$

ništa posebno ne možemo reći o ovakvom $\frac{p}{q}$ - aproksimacija nije dovoljno dobra

No 1

Teorem (Legendre) Neka je $\alpha \in \mathbb{R}$. Pretp. da je $\frac{p}{q}$ racionalan broj za koji je

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{2q^2}.$$

Tada je $\frac{p}{q}$ konvergenta vencznog razlomka broja α.

Natrag na problem odvrtivanja reda elementa...

ako imamo sreću s aproksimacijom $\varnothing$, tj. ako vrijedi

$$\left|\varnothing - \frac{s}{r}\right| \leq \frac{1}{2r^2}$$

onda ćemo nama nepoznati razlomak $\frac{s}{r}$ pronaći među konačno mnogo konvergenti broja $\varnothing$. Sve što treba je provjeriti je li neki od nazivnika konvergenti red od x modulo N (što je vrlo jednostavno).

Dakle, kad bi mogli generirati neke od svojstvenih vektora $|u_s\rangle$ efikasno bi riješili problem odredivanja perioda.

No, to neznamo. Ali, znamo (provjerite!)

$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |u_s\rangle = |\eta\rangle.$$

Ako u drugi registar algoritma za odredivanje faze umjesto jednog svojstvenog vektora kao ulaz postavimo njihovu linearnu kombinaciju – vektor $|\eta\rangle$

na izlazu ćemo dobiti vektor

$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |\tilde{\psi}_s\rangle |u_s\rangle \quad \text{gdje je}$$

$\tilde{\psi}_s$ aproksimacija broja $\frac{s}{r}$ (= faza vektora $|u_s\rangle$). Mjerenjem prvog registra dobivamo $\tilde{\psi}_s$ za neki nasumični s.

Uz malo sreće, primjenom Legendreovog teorema možemo odrediti period r.

Shorov algoritam

Neka je dan $N = p \cdot q$ (p, q prosti brojevi). Problem je odrediti p i q.

Opišimo klasičnu algoritam koji koristi kvantnu proceduru za određivanje reda elementa.

1. slučajno odaberimo $x \in \mathbb{N}$, $x \leq N$. Ako je $(x, N) > 1$ onda je $(x, N) = p$ ili q pa smo gotovi.

mjeri efikasno računamo Euklidovim algoritmom

2. Izvršimo kvantnu proceduru koja računa red r od x modulo N.

3. Ako je r paran i $x^{\frac{r}{2}} \not\equiv 1 \pmod{N}$ onda je $(x^{\frac{r}{2}} - 1, N)$ jedan od faktora. Inače se vraćamo na prvi korak.

faktore tražimo Euklidovim algoritmom

Zašto? Ako je r paran i $x^{\frac{r}{2}} \not\equiv -1 \pmod N$ onda

greška u skripti

$$N \mid x^r - 1 = (x^{\frac{r}{2}} - 1)(x^{\frac{r}{2}} + 1)$$ ali

ne dijeli niti jedan od faktora $x^{\frac{r}{2}} + 1$, $x^{\frac{r}{2}} - 1$.

zbog prethp. — jer je r najmanji broj za koji je $x^r \equiv 1 (N)$

Primjer u skripti. Varijacija na temu.

Kvantna kriptografija:

← ova tehnologija već postoji

← dokaziv "sigurna" (uz pretp. kvantne mehanike)

BB84 protokol za razmjenu ključeva

Alice i Bob komuniciraju javnim (klasičnim i kvantnim) kanalima dok ih Eva pokušava prisluškivati.

1. Alice za početak slučajno generira dva stringa nula i jedinica duljine n

$$x = x_1 x_2 \dots x_n$$

$$y = y_1 y_2 \dots y_n$$

i konstruira stanj

$$|\psi\rangle = \bigotimes_{i=1}^{n} |\psi_{x_i y_i}\rangle \quad \text{(sustav od } n \text{ qubita)} \qquad \text{gdje je}$$

$$|\psi_{00}\rangle = |0\rangle \qquad |\psi_{01}\rangle = |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$|\psi_{10}\rangle = |1\rangle \qquad |\psi_{11}\rangle = |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

2. Alice pošalje tih n qubita Bobu

3. Bob generira slučajan string $y' \in \{0,1\}^n$ koji određuje bazu u kojoj mjeri Alicin qubitove

a) ako je $y_i' = 0$ onda i-ti qubit mjeri u bazi $\{|0\rangle, |1\rangle\}$.

b) ako je $y_i' = 1$ onda i-ti qubit mjeri u bazi $\{|+\rangle, |-\rangle\}$

Neka je $x' \in \{0,1\}^n$ string rezultata Bobovih mjerenja

(ishod $|0\rangle$ i $|+\rangle$ bilježi se 0 dok ishod $|1\rangle$ i $|-\rangle$ se 1).

4. Alice i Bob javno objave stringove y i y' te iz stringova x i x' izbace sve one bitove x_i i x_i' za koje je $y_i \neq y_i'$. Ono što preostane od stringova x i x' je njihov "polu-privatni ključ".

U idealnom slučaju, ako nije došlo do greške u komunikaciji (ako Eve nije prisluškivala), iz konstrukcije stanja $|\psi\rangle$

vidimo da $y_i = y_i'$ implicira $x_i = x_i'$ (zašto?)

što znači da su Alica i Bob uspjeli razmijeniti ključ.