Shorov algoritam

Kvantna računala (SI)

siječanj 2023.

Kvantna Fourierova tranformacija: Definicija

Notacija:

- Cijeli broj $0 \leq x \leq 2^n - 1$ zapisujemo korištenjem n klasičnih bitova x_i,

$$x = \sum_{i=0}^{n-1} 2^i x_i = 2^{n-1} x_{n-1} + 2^{n-2} x_{n-2} + \cdots + 2x_1 + x_0.$$

- Vektori računalne baze $\{|x\rangle ; x = 0, \ldots, 2^n - 1\}$ Hilbertovog prostora dimenzije 2^n izraženi kao tenzorski produkt vektora stanja n kvantnih bitova su

$$|x\rangle = \bigotimes_{i=0}^{n-1} |x_i\rangle = |x_{n-1}\rangle \otimes |x_{n-2}\rangle \otimes \cdots \otimes |x_1\rangle \otimes |x_0\rangle$$
$$= |x_{n-1}\ x_{n-2}\ \cdots\ x_1\ x_0\rangle .$$

Analogno $y = \sum_{i=0}^{n-1} 2^i y_i$, $|y\rangle = \bigotimes_{i=0}^{n-1} |y_i\rangle$ itd.

Kvantna Fourierova transformacija

Ako su $|x\rangle$ i $|y\rangle$ stanja računalne baze u Hilbertovom prostoru dimenzije 2^n, kvantna Fourierova transformacija U_{FT} jest unitarna transformacija definirana s

$$\langle y| U_{\mathrm{FT}} |x\rangle = \frac{1}{2^{n/2}} \exp\left[2\pi \mathrm{i} \frac{xy}{2^n}\right].$$

Djelovanje U_{FT} na stanje $|x\rangle$ možemo izraziti kao

$$U_{\mathrm{FT}} |x\rangle = \sum_{y=0}^{2^n-1} |y\rangle \langle y| U_{\mathrm{FT}} |x\rangle = \frac{1}{2^{n/2}} \sum_{y=0}^{2^n-1} \mathrm{e}^{2\pi \mathrm{i}\, xy/2^n} |y\rangle .$$

U gornjem računu korištena je relacija potpunosti $I = \sum_{y=0}^{2^n-1} |y\rangle \langle y|$.

Stanje $|\Phi\rangle$ koje nastaje djelovanjem U_{FT} na općenito stanje

$$|\Psi\rangle = \sum_{x=0}^{2^n-1} f(x)\,|x\rangle\,,$$

gdje je $f(x) = \langle x|\Psi\rangle$, možemo izraziti kao

$$|\Phi\rangle = U_{\mathrm{FT}}\,|\Psi\rangle = \sum_{x=0}^{2^n-1} f(x)\,U_{\mathrm{FT}}\,|x\rangle = \cdots = \sum_{y=0}^{2^n-1} \tilde{f}(y)\,|y\rangle\,,$$

gdje su koeficijenti $\tilde{f}(y)$ dani s

$$\tilde{f}(y) = \langle y|\Phi\rangle = \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} \mathrm{e}^{2\pi \mathrm{i}\, xy/2^n} f(x).$$

Koeficijente $\tilde{f}(y)$, $y = 0, \ldots, 2^n - 1$, prepoznajemo kao diskretnu Fourierovu transformaciju (DFT) koeficijenata $f(x)$, $x = 0, \ldots, 2^n - 1$.

Unitarnost U_{FT} dokazujemo time što pokazujemo da vrijedi $U_{\mathrm{FT}}^{\dagger} U_{\mathrm{FT}} = I$, odn. $\langle y| U_{\mathrm{FT}}^{\dagger} U_{\mathrm{FT}} |x\rangle = \delta_{xy}$:

$$\langle y| U_{\mathrm{FT}}^{\dagger} U_{\mathrm{FT}} |x\rangle = \sum_{z=0}^{2^n-1} \langle y| U_{\mathrm{FT}}^{\dagger} |z\rangle \langle z| U_{\mathrm{FT}} |x\rangle = \sum_{z=0}^{2^n-1} \langle z| U_{\mathrm{FT}}|y\rangle^{*} \langle z| U_{\mathrm{FT}} |x\rangle$$

$$= \frac{1}{2^n} \sum_{z=0}^{2^n-1} \mathrm{e}^{-2\pi \mathrm{i}\, yz/2^n} \mathrm{e}^{2\pi \mathrm{i}\, xz/2^n} = \frac{1}{2^n} \sum_{z=0}^{2^n-1} \left(\mathrm{e}^{2\pi \mathrm{i}(x-y)/2^n}\right)^z$$

Za $y = x$ gornji izraz jednak je jedinici, dok je za $y \neq x$ on jednak nuli. Ovo posljednje pokazujemo korištenjem formule za geometrijski red (?),

$$\sum_{z=0}^{2^n-1} \left(\mathrm{e}^{2\pi \mathrm{i}(x-y)/2^n}\right)^z = \frac{1 - \left(\mathrm{e}^{2\pi \mathrm{i}(x-y)/2^n}\right)^{2^n}}{1 - \mathrm{e}^{2\pi \mathrm{i}(x-y)/2^n}} = \frac{1 - \mathrm{e}^{2\pi \mathrm{i}(x-y)}}{1 - \mathrm{e}^{2\pi \mathrm{i}(x-y)/2^n}} = 0.$$

(Formula za geometrijski red: $\sum_{k=0}^{\infty} r^k = (1-r)^{-1}$ za $|r| < 1$. Ovdje uvjet $|r| < 1$ nije ispunjen—treba provjeriti opravdanost primjene!)

QFT: Implementacija

Uočavamo da cjelobrojni dio kvocijenta $xy/2^n$ ne utječe na vrijednost koeficijenta $\mathrm{e}^{2\pi \mathrm{i}\, xy/2^n}$, a što znači da ga možemo po volji promijeniti.

Sam kvocijent $xy/2^n$ možemo izraziti korištenjem bitova x_i i y_j kao

$$\frac{xy}{2^n} = \frac{1}{2^n} \sum_{j=0}^{n-1} 2^j y_j \sum_{i=0}^{n-1} 2^i x_i = \sum_{j=0}^{n-1} y_j \sum_{i=0}^{n-1} 2^{i+j-n} x_i .$$

Kako bismo odbacili cjelobrojne dijelove članova pod sumom, a zadržali samo njihove necjelobrojne dijelove, zadržavamo samo članove u kojima je potencija broja 2 negativna, a što znači $i = 0, \ldots, n-j-1$. Članove koji preostaju možemo napisati kao

$$\sum_{j=0}^{n-1} y_j \sum_{i=0}^{n-j-1} \frac{x_i}{2^{n-(i+j)}} = \sum_{j=0}^{n-1} y_j \left(\frac{x_{n-j-1}}{2} + \cdots + \frac{x_0}{2^{n-j}} \right).$$

Uvedemo li za zbroj "binarnih razlomaka" u okruglim zagradama u prethodnm izrazu kompaktnu oznaku

$$\frac{x_{n-j-1}}{2} + \cdots + \frac{x_0}{2^{n-j}} = 0.x_{n-j-1} \cdots x_0,$$

odbacivanjem cjelobrojnih dijelova članova u sumi imamo

$$\frac{xy}{2^n} \longrightarrow \sum_{j=0}^{n-1} y_j \, 0.x_{n-j-1} \cdots x_0,$$

a koeficijent $\mathrm{e}^{2\pi \mathrm{i}\, xy/2^n}$ koji ostaje nepromijenjen sada možemo izraziti kao

$$\mathrm{e}^{2\pi \mathrm{i}\, xy/2^n} = \prod_{j=0}^{n-1} \mathrm{e}^{2\pi \mathrm{i}\, y_j \, 0.x_{n-j-1} \cdots x_0} = \mathrm{e}^{2\pi \mathrm{i}\, y_{n-1} \, 0.x_0} \; \mathrm{e}^{2\pi \mathrm{i}\, y_{n-2} \, 0.x_1 x_0} \cdots$$

$$\cdots \mathrm{e}^{2\pi \mathrm{i}\, y_1 \, 0.x_{n-2} \cdots x_0} \; \mathrm{e}^{2\pi \mathrm{i}\, y_0 \, 0.x_{n-1} \cdots x_0}.$$

Djelovanje U_{FT} na stanje $|x\rangle$ računalne baze:

$$U_{\mathrm{FT}}|x\rangle = \frac{1}{2^{n/2}} \sum_{y=0}^{2^n-1} \mathrm{e}^{2\pi \mathrm{i}\, xy/2^n} |y\rangle$$

$$= \frac{1}{2^{n/2}} \sum_{y_{n-1},\cdots,y_0=0}^{1} \mathrm{e}^{2\pi \mathrm{i}\, y_{n-1}\, 0.x_0}\ \mathrm{e}^{2\pi \mathrm{i}\, y_{n-2}\, 0.x_1 x_0} \cdots$$

$$\cdots \mathrm{e}^{2\pi \mathrm{i}\, y_1\, 0.x_{n-2}\cdots x_0}\ \mathrm{e}^{2\pi \mathrm{i}\, y_0\, 0.x_{n-1}\cdots x_0}\ |y_{n-1}\, y_{n-2}\, \cdots y_1\, y_0\rangle$$

$$= \frac{1}{\sqrt{2}} \sum_{y_{n-1}=0}^{1} \mathrm{e}^{2\pi \mathrm{i}\, y_{n-1}\, 0.x_0} |y_{n-1}\rangle \otimes \frac{1}{\sqrt{2}} \sum_{y_{n-2}=0}^{1} \mathrm{e}^{2\pi \mathrm{i}\, y_{n-2}\, 0.x_1 x_0} |y_{n-2}\rangle \otimes \cdots$$

$$\cdots \otimes \frac{1}{\sqrt{2}} \sum_{y_1=0}^{1} \mathrm{e}^{2\pi \mathrm{i}\, y_1\, 0.x_{n-2}\cdots x_0} |y_1\rangle \otimes \frac{1}{\sqrt{2}} \sum_{y_0=0}^{1} \mathrm{e}^{2\pi \mathrm{i}\, y_0\, 0.x_{n-1}\cdots x_0} |y_0\rangle$$

Uvrštavanjem eksplicitnih vrijednosti kvantnih bitova izraz poprima oblik

$$U_{\mathrm{FT}}\left|x\right\rangle = \frac{1}{\sqrt{2}}\left(\left|0\right\rangle + \mathrm{e}^{2\pi \mathrm{i}\, 0.x_0}\left|1\right\rangle\right)_{n-1} \otimes \frac{1}{\sqrt{2}}\left(\left|0\right\rangle + \mathrm{e}^{2\pi \mathrm{i}\, 0.x_1 x_0}\left|1\right\rangle\right)_{n-2} \otimes \cdots$$
$$\cdots \otimes \frac{1}{\sqrt{2}}\left(\left|0\right\rangle + \mathrm{e}^{2\pi \mathrm{i}\, 0.x_{n-2}\cdots x_0}\left|1\right\rangle\right)_{1} \otimes \frac{1}{\sqrt{2}}\left(\left|0\right\rangle + \mathrm{e}^{2\pi \mathrm{i}\, 0.x_{n-1}\cdots x_0}\left|1\right\rangle\right)_{0}$$

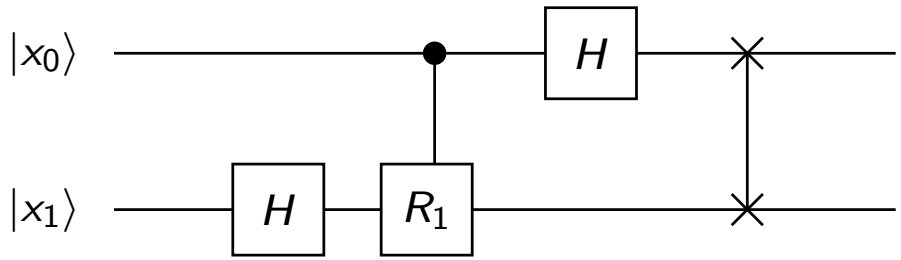
Konačno, uvedemo li oznaku R_j^i za upravljani operator rotacije oko osi z za kut $\pi/2^j$, pri čemu i-ti kvantni bit u sustavu ima ulogu upravljačkog bita, nalazimo

$$U_{\mathrm{FT}}\left|x\right\rangle = \left(H\left|x_0\right\rangle\right)_{n-1} \otimes \left(R_1^0 H\left|x_1\right\rangle\right)_{n-2} \otimes \left(R_2^0 R_1^1 H\left|x_2\right\rangle\right)_{n-3} \otimes \cdots$$
$$\cdots \otimes \left(R_{n-2}^0 \cdots R_1^{n-3} H\left|x_{n-2}\right\rangle\right)_{1} \otimes \left(R_{n-1}^0 \cdots R_1^{n-2} H\left|x_{n-1}\right\rangle\right)_{0}.$$

Primjer: QFT za $n = 2$

$$U_{\mathrm{FT}} |x\rangle = (H |x_0\rangle)_1 \otimes \left(R_1^0 H |x_1\rangle\right)_0$$

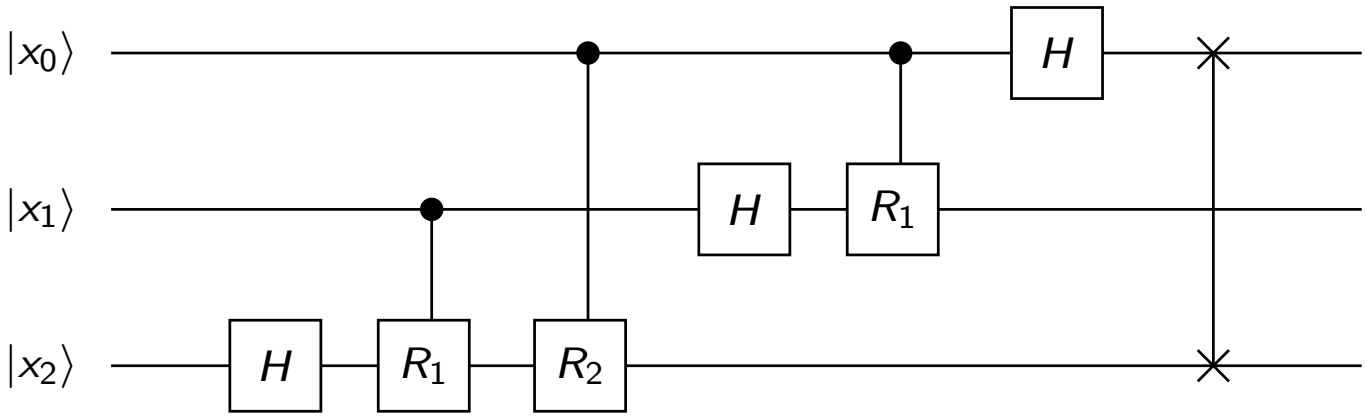
Kvantni logički krug:



Primjer: QFT za $n = 3$

$$U_{\mathrm{FT}} |x\rangle = (H |x_0\rangle)_2 \otimes \left(R_1^0 H |x_1\rangle\right)_1 \otimes \left(R_2^0 R_1^1 H |x_2\rangle\right)_0$$

Kvantni logički krug:



QFT: Nalaženje perioda funkcije

Primjenom QFT-a moguće je odrediti period funkcije.

U ak.g. 2022./2023. ne radimo ovo poglavlje jer u prvom ciklusu nastave nije napravljeno poglavlje o operatoru stanja (matrica gustoće).

Shorov algoritam

Cilj Shorovog algoritma je faktorizirati zadani cijeli broj N.

Zbog jednostavnosti pretpostavljamo da je zadani (poznati) broj N moguće prikazati kao umnožak dvaju nepoznatih prostih brojeva p i q,

$$N = pq.$$

U grubim crtama prikazujemo najvažnije korake algoritma:

- Odabiremo cijeli broj y koji ne posjeduje zajednički dijelitelj s brojem N veći od 1. (Dogodi li se da y i N imaju zajednički djelitelj veći od 1, problem je samim time riješen. Zajednički djelitelj dvaju brojeva nalazimo primjenom Euklidovog algoritma koji smatramo brzim.)

- Tvorimo funkciju (tzv. modularna eksponencijacija)

$$f(a) = y^a \bmod N$$

te primjenom QFT nalazimo njen period. S obzirom da je $f(0) = 1$, ako je r period funkcije, vrijedi

$$f(r) = y^r \bmod N = 1.$$

- Jednakost iz prethodnog koraka možemo napisati u obliku

$$(y^r - 1) \bmod N = 0,$$

što znači da je $y^r - 1 = \lambda N$ gdje je λ cijeli broj. Primjenom formule za razliku kvadrata to još možemo napisati u obliku

$$(y^{r/2} + 1)(y^{r/2} - 1) = \lambda N.$$

- Ako $y^{r/2}+1$ i $y^{r/2}-1$ nisu cijeli brojevi, ili ako je neki od njih višekratnik broja N, vraćamo se na početak i odabiremo drugačiji broj y (vjerojatnost ovakvog ishoda manja je od $1/2$).
- Ako cijeli brojevi $y^{r/2}+1$ i $y^{r/2}-1$ nisu višekratnici N, Euklidovim algoritmom nalazimo zajedničke djelitelje svakoga od njih s brojem N.

U našem slučaju gdje smo pretpostavili $N = pq$ imamo

$$y^{r/2}+1 = \lambda_p p, \tag{1}$$

$$y^{r/2}-1 = \lambda_q q, \tag{2}$$

što znači da će potraga za zajedničkim djeliteljem u jednom slučaju dati p, a u drugom će dati q.

Primjer: Za $N = 15$ uz $y = 2$ nalazimo period $r = 4$,

$$y^{r/2} + 1 = 5, \qquad y^{r/2} - 1 = 3, \qquad 5 \times 3 = 15.$$

Primjer: Za $N = 15$ uz $y = 11$ nalazimo period $r = 2$,

$$y^{r/2} + 1 = 12, \qquad y^{r/2} - 1 = 10,$$

$$\gcd(12, 15) = 3, \qquad \gcd(10, 15) = 5, \qquad 5 \times 3 = 15.$$