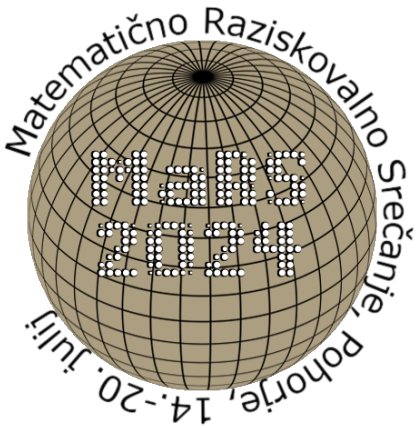
Shorov algoritem

Aleksander Kalacun, Matjaž Meža, Jakob Žorž
Mentor: Tim Milanez



Povzetek

Spoznamo kvantni algoritem za faktorizacijo števil, imenovan Shorov algoritem, ki, vsaj v teoriji, po časovni zahtevnosti premaga še najhitrejši do sedaj znan klasični algoritem. V prvem delu razložimo klasični del algoritma, ki temelji na osnovah teorije števil, v drugem delu pa se spoprimemo še s kvantnim delom algoritma, kjer spoznamo temelje kvantne mehanike in kvantnega računanja, ki so zasnovani okoli linearne algebre.

1 Uvod

Šifriranje večine medmrežnih komunikacijskih poti danes deluje na podlagi RSA algoritma, ki omogoča varen in zaseben prenos informacij med različnimi uporabniki medmrežja. Algoritem sloni na dejstvu, da zmorejo računalniki hitro izračunati produkt dveh praštevil (šifriranje), medtem ko razcep tekšnega števila terja ogromno časa (dešifriranje), zato imamo RSA algoritem za varnega. Ob rodu kvantnega računalništva pa se je varnost te enkripcije postavila pod vprašaj, ko je leta 1995 ameriški matematik Peter Schor pretresel svet kriptografije in predstavil nov algoritem za faktorizacijo števil, zasnovan na konceptih kvantne mehanike. Z njim je, vsaj v teoriji, možno številu N, ki je produkt dveh praštevil, poiskati prafaktorje v

$$O((\log N)^2(\log\log N))$$

časa, kar je znatno hitrejše od najbolšega do sedaj znanega klasičnega algoritma, ki ima časovno zahtevnost [1]

$$O(e^{1.9(\log N)^{\frac{1}{3}}(\log\log N)^{\frac{2}{3}}}).$$

V delu predstavimo omenjeni Shorov algoritem, kjer sledimo [2].

2 Klasični del algoritma

Naj $\mathbb{Z}_n$ označuje množico števil $\{0, 1, 2, \ldots, n-1\}$, v kateri seštevamo in množimo po modulu n. Dva elementa a, b v tej množici sta enaka, kar pišemo kot $a \equiv b \mod n$ in pravimo, da je a **kongruenten** b **po modulu** n, če velja $n|a-b$. To se zgodi natanko tedaj, ko imata števili isti ostanek pri deljenju z n.

Po Bezoutevi lemi ima element $x \in \mathbb{Z}_n$ multiplikativni inverz v $\mathbb{Z}_n$, tj. tak $y \in \mathbb{Z}_n$, da velja $xy \equiv 1 \mod n$, natanko tedaj, ko je y tuj n. Podmnožico elementov, ki imajo multiplikativni inverz v $\mathbb{Z}_n$, označimo z $\mathbb{Z}_n^*$. Množica $\mathbb{Z}_n^*$ vsebuje natanko $\varphi(n)$ elementov, kjer φ označuje Eulerjevo totientsko funkcijo.

Želeli bi rešiti naslednji problem. Dano je število

$$N = pq,$$

za katerega vemo, da je produkt dveh praštevil p in q. Ob znani vrednosti N bi želeli hitro izračunati faktorja p in q. Če je N sod, potem je zagotovo eden od prašteviliskih faktorjev enak 2, torej lahko predpostavimo, da je N lih. Če sta p in q enaka in je torej N kvadrat praštevila, se lahko hitro in z visoko natančnostjo izračuna koren od števila N in s tem p, torej lahko nadalje še predpostavimo, da sta p in q različna.

Vzemimo naključno število

$$1 < y < N.$$

Če imata N in y skupen faktor, smo končali, saj je $\gcd(N, y)$ v tem primeru enak enemu izmed faktorjev p, q in najmanjši skupni večkratnik dveh števil se s pomočjo Evklidovega algoritma da hitro izračunati. V nasprotnem primeru sta si N in y tuji in je $y \in \mathbb{Z}_N^*$, torej ima multiplikativni inverz v $\mathbb{Z}_N$. Ker je množica $\mathbb{Z}_N$ končna, se členi v zaporedju $1, y, y^2, \ldots$ elementov v $\mathbb{Z}_N$ ponavljajo, zato obstajata neki potenci $0 \leq l < k$, da velja

$$y^k \equiv y^l \mod N \qquad \text{oziroma} \qquad y^{k-l} \equiv 1 \mod N.$$

Naj bo $r \geq 1$ najmanjše takšno število, da velja

$$y^r \equiv 1 \mod N.$$

Recimo, da smo imeli „srečo“ in da je r sodo število. Potem lahko razcepimo

$$y^r - 1 \equiv (y^{\frac{r}{2}} + 1)(y^{\frac{r}{2}} - 1) \equiv 0 \mod N.$$

Po minimalnosti r število N ne deli $y^{\frac{r}{2}} - 1$, zato si $y^{\frac{r}{2}} + 1$ in N zagotovo nista tuja. Recimo, da smo imeli „izredno srečo“ in da poleg sodosti r tudi N ne deli $y^{\frac{r}{2}} + 1$. Potem velja

$$1 < \gcd(y^{\frac{r}{2}} + 1, N) < N,$$

torej je $\gcd(y^{\frac{r}{2}} + 1, N)$ enak enemu izmed prafaktorjev in smo končali.

Da zgornji algoritem uspe, smo potrebovali dve predpostavki: r je sod in $N \nmid y^{\frac{r}{2}} + 1$. Verjetnost, da naključno izbrano število y, ki je tuje N, zadošča tema predpostavkama, nam podaja naslednji izrek.

Izrek 1. *Recimo, da je N lih in da ima k praštevilskih faktorjev. Potem vsebuje množica*

$$\{y \in \mathbb{Z}_N^* \mid \textit{red } r \textit{ števila } y \textit{ je sod in } y^{r/2} + 1 \not\equiv 0 \mod N\}$$

vsaj

$$\varphi(N)\left(1 - \frac{1}{2^{k-1}}\right)$$

elementov.

V našem primeru je $k = 2$, od koder sledi, da imamo „izredno srečo“ v vsaj polovici primerov. Edini časovno zahtevni korak v zgornjem algoritmu je izračun r, ki ga klasični računalnik ne more hitro izračunati. Tukaj pa nam pa na pomoč lahko priskočijo kvantni računalniki.

3 Uvod v linearno algebro

3.1 Vektorski prostori

V tem razdelku bomo razširili pojme vektorja, skalarja in baze, ki jih že poznamo iz srednje šole.

Definicija 1. ***Kompleksni vektorski prostor z bazo*** $e_1, \ldots, e_n$ *je množica*

$$V = \{\lambda_1 e_1 + \cdots + \lambda_n e_n \mid \lambda_1, \ldots, \lambda_n \in \mathbb{C}\},$$

ki je opremljena z operacijama

(1) seštevanja:

$$\begin{aligned}&(\lambda_1 e_1 + \cdots + \lambda_n e_n) + (\mu_1 e_1 + \cdots + \mu_n e_n)\\ &= (\lambda_1 + \mu_1)e_1 + \cdots + (\lambda_n + \mu_n)e_n \quad \text{za } \lambda_1, \ldots, \lambda_n, \mu_1, \ldots, \mu_n \in \mathbb{C}, \text{ in}\end{aligned}$$

(2) množenja s skalarjem:

$$\lambda \cdot \left(\sum_{i=1}^{n} \mu_i e_i\right) = \sum_{i=1}^{n} (\lambda \mu_i) e_i \quad \text{za } \lambda, \mu_1, \ldots, \mu_n \in \mathbb{C}.$$

Številu n, tj. številu elementov v bazi, pravimo ***dimenzija*** *vektorskega prostora V.*

Kompleksni vektorski prostor z bazo $\{e_1, \ldots, e_n\}$ bomo označevali tudi kot $\mathbb{C}[\{e_1, \ldots, e_n\}]$.

Definicija 2. *Naj bosta V in W kompleksna vektorska prostora s končno bazo. Preslikava $L \colon V \to W$ je* ***linearna****, če velja*

(1) $L(x + y) = L(x) + L(y)$ za vsaka $x, y \in V$ in

(2) $L(\lambda x) = \lambda L(x)$ za vsak $x \in V$ in $\lambda \in \mathbb{C}$.

Enako se lahko definira tudi **realen vektorski prostor z bazo** in linearno preslikavo med realnima vektorskima prostoroma, kjer v definiciji zamenjamo vsako ponovitev množice $\mathbb{C}$ z množico $\mathbb{R}$.

Poljuben vektor $x \in V = \mathbb{C}[\{e_1, \ldots, e_n\}]$ lahko razpišemo po bazi

$$x = \sum_{i=1}^{n} \lambda_i e_i.$$

Linearna preslikava L slika x v

$$L(x) = L(\lambda_1 e_1) + \cdots + L(\lambda_n e_n) = \sum_{i=1}^{n} \lambda_i L(e_i).$$

Torej je L določena že s tem, kam slika bazne vektorje $e_1, \ldots, e_n$. Razpišimo $L(e_i)$ po bazi

$$L(e_i) = \sum_{j=1}^{n} a_{ij} e_j,$$

kjer so $a_{ij} \in \mathbb{C}$. Po prejšnjem razmisleku je L natanko določena z izbiro skalarjev $(a_{ij})_{i,j\in\{1,\ldots,n\}}$, ki jih zapišemo v tabelo, kot je prikazano spodaj

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix}.$$

Takšnemu zapisu pravimo **matrika**. Po zgornjem postopku lahko vsaki linearni preslikavi priredimo matriko. Izkaže se, da je takšen zapis linearnih preslikav zelo priročen. Na primer, če želimo izračunati, kam linearna preslikava L slika nek vektor $x \in V$, moramo ta vektor najprej razviti po bazi $x = \sum_{i=1}^{n} \lambda_i e_i$, kar zapišemo kot

$$x = \begin{bmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_n \end{bmatrix},$$

nato pa poračunati vsote $\mu_i = \sum_{j=1}^{n} a_{ij}\lambda_j$ in jih zapisati v rezultat

$$L(x) = \begin{bmatrix} \mu_1 \\ \mu_2 \\ \vdots \\ \mu_n \end{bmatrix}.$$

Zgled. *Naj bo $L\colon \mathbb{R}^2 \to \mathbb{R}^2$ preslikava, ki zamenja koordinati*

$$L(x, y) = (y, x).$$

Po definiciji se da preveriti, da je L linearna preslikava med realnima vektorskima prostoroma $\mathbb{R}^2$ s standardno bazo $e_1 = (1, 0),\ e_2 = (0, 1)$. Pripadajoča matrika je

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

3.2 Vektorski prostori s skalarnim produktom

Standardni skalarni produkt vektorjev v prostoru $\mathbb{R}^3$, ki ga poznamo že iz srednje šole, je definiran kot

$$(x_1, x_2, x_3) \cdot (y_1, y_2, y_3) = x_1y_1 + x_2y_2 + x_3y_3.$$

Njegova uporabnost se je pokazala pri izračunu kotov med vektorji. Ta koncept bi radi definirali tudi na bolj splošnih vektorskih prostorih, kar naredimo na sledeči način.

Definicija 3. ***Skalarni produkt*** *na kompleksnem vektorskem prostoru V je preslikava*

$$\langle \cdot, \cdot \rangle \colon V \times V \to \mathbb{C},$$

ki zadošča naslednjim lastnostim.

(i) $\langle v_1 + v_2, w \rangle = \langle v_1, w \rangle + \langle v_2, w \rangle$ *za vsak* $v_1, v_2, w \in V$.

(ii) $\langle \lambda v, w \rangle = \lambda \langle v, w \rangle$ *za vsak* $v, w \in V$ *in* $\lambda \in \mathbb{C}$.

(iii) $\langle w, v \rangle = \overline{\langle v, w \rangle}$ *za vsak* $v, w \in V$.

(iv) $\langle v, v \rangle \geq 0$ *za vsak* $v \in V$ *in* $\langle v, v \rangle = 0$ *natanko tedaj, ko je* $v = 0$.

Število $\sqrt{\langle x, x \rangle}$ *bomo označevali z* $\|x\|$ *in mu pravili* ***norma*** *vektorja* x.

Iz zgornjih lastnosti sledi, da je skalarni produkt linearen v prvem faktorju in „poševno linearen“ v drugem faktorju, tj. velja

$$\langle v, \lambda_1 w_1 + \lambda_2 w_2 \rangle = \overline{\lambda_1} \langle v, w_1 \rangle + \overline{\lambda_1} \langle v, w_1 \rangle \text{ za vsak } v, w_1, w_2 \in V \text{ in } \lambda \in \mathbb{C}.$$

Zgled. *Na kompleksnem vektorskem prostoru $\mathbb{C}^n$ lahko skalarni produkt definiramo z naslednjo formulo*

$$\langle (z_1, \ldots, z_n), (w_1, \ldots, w_n) \rangle = z_1 \overline{w_1} + \cdots + z_n \overline{w_n}.$$

Enostavno se da preveriti, da zgornji predpis res zadošča vsem lastnostim od (i) do (iv).

Kvantna mehanika dovoljuje le zelo specifične linearne preslikave, ki ohranjajo normo.

Definicija 4. *Linearna preslikava $U \colon V \to W$ med vektorskima prostoroma je* ***unitarna****, če velja*

$$\|Ux\| = \|x\| \text{ za vsak } x \in V.$$

Zgled. *Premislimo, kako izgledajo unitarne preslikave $U \colon \mathbb{R}^2 \to \mathbb{R}^2$ v realnem vektorskem prostorom $\mathbb{R}^2$ s standardno bazo $e_1 = (1, 0)$, $e_2 = (0, 1)$. Linearno preslikavo U lahko predstavimo z matriko*

$$U = \begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$

Po unitarnosti imata vektorja e_1 in

$$Ue_1 = \begin{bmatrix} a \\ c \end{bmatrix}$$

enako normo, torej mora veljati

$$1 = a^2 + c^2.$$

Podobno imata tudi vektorja e_2 in Ue_2 enako normo, od koder sledi

$$1 = b^2 + d^2.$$

Potem obstajata takšni števili $\varphi \in [0, 2\pi)$ in $\theta \in [0, 2\pi)$, da velja $a = \cos\varphi$, $c = \sin\varphi$ in $b = \cos\theta$, $d = \sin\theta$. Enako normo pa morata imeti tudi vektorja

$$\begin{bmatrix} 1 \\ 1 \end{bmatrix} \quad \textit{in} \quad \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 1 \\ 1 \end{bmatrix},$$

zato velja

$$2 = (a+b)^2 + (c+d)^2.$$

Desna stran zgornje enačbe pa je enaka $2 + 2(ab+cd)$*, zato dobimo*

$$ab + cd = 0,$$

oziroma

$$\cos(\varphi - \theta) = \cos\varphi\cos\theta + \sin\varphi\sin\theta = 0.$$

Torej je $\varphi - \theta \in \{\frac{\pi}{2}, \frac{3\pi}{2}\}$*. Če je* $\theta = \varphi - \frac{\pi}{2}$*, dobimo matriko*

$$U = \begin{bmatrix} \cos\varphi & \sin\varphi \\ \sin\varphi & -\cos\varphi \end{bmatrix}, \tag{1}$$

če pa je $\theta = \varphi - \frac{3\pi}{2}$*, dobimo matriko*

$$U = \begin{bmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{bmatrix}. \tag{2}$$

Pokazali smo torej, da so vse unitarne matrike ene izmed zgornjih dveh matrik. Matrike oblike 2 predstavljajo ravno rotacije okoli izhodišča za kot φ*.*

Definicija 5. *Naj bo* V *vektorski prostor s skalarnim produktom. Sistem vektorjev* $v_1, \ldots, v_n$ *je* ***ortonormiran****, če velja* $\langle v_i, v_j \rangle = 0$ *za vsak* $i \neq j$ *in* $\|v_i\| = 1$ *za vsak* i*.*

3.3 Tenzorski produkt

Naslednja definicija nam omogoča iz dveh vektorskih prostorov V dimenzije n in W dimenzije m konstruirati vektorski prostor dimenzije $n \cdot m$.

Definicija 6. ***Tenzorski produkt*** *vektorskih prostorov* V *z bazo* $e_1, \ldots, e_n$ *in* W *z bazo* $f_1, \ldots, f_m$ *je vektorski prostor* $V \otimes W$ *z bazo* $e_i \otimes f_j$*,* $i \in \{1, \ldots n\}$*,* $j \in \{1, \ldots m\}$*, da za vsaka* $v, v' \in V$ *in* $w, w' \in W$ *ter vse skalarje* λ *velja*

(i) $(v + v') \otimes w = v \otimes w + v' \otimes w$*,*

(ii) $v \otimes (w + w') = v \otimes w + v \otimes w'$*,*

(iii) $\lambda v \otimes w = (\lambda v) \otimes w = v \otimes (\lambda w)$*.*

Naj bosta $A\colon V_1 \to W_1$ in $B\colon V_2 \to W_2$ linearni preslikavi. Ti nam inducirata linearno preslikavo na tenzorskem produktu $A \otimes B\colon V_1 \otimes V_2 \to W_1 \otimes W_2$, ki je na baznih vektorjih definirana kot

$$(A \otimes B)(x \otimes y) = Ax \otimes By.$$

Zgled (Walsh-Hadamardova preslikava)**.** *Naj bo* $V_1 = \mathbb{C}[\mathbb{Z}_2]$ *in* $W_1\colon V_1 \to V_1$ *linearna preslikava s pridruženo matriko*

$$W_1 = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix}.$$

To je ravno matrika oblike 1 pri vrednosti $\varphi = \frac{\pi}{4}$*, torej je* W_1 *unitarna. Za* $n \in \mathbb{N}$ *označimo*

$$V_n = \underbrace{V_1 \otimes \ldots \otimes V_1}_{n\text{-krat}}.$$

Preslikavo

$$W_n = \underbrace{W_1 \otimes \ldots \otimes W_1}_{n\text{-krat}} \colon V_n \otimes V_n \to V_n \otimes V_n$$

imenujemo ***n-ta Walsh-Hadamardova preslikava****. Njen matrični zapis dobimo induktivno na sledeči način. Matrični zapis W_n dobimo s pomočjo matričnega zapisa W_{n-1}, tako da koeficient a_{ij} v matričnem zapisu W_{n-1} zamenjamo z matriko $a_{ij} \cdot W_1$. Tako je na primer*

$$W_2 = \begin{bmatrix} \frac{1}{\sqrt{2}}W_1 & \frac{1}{\sqrt{2}}W_1 \\ \frac{1}{\sqrt{2}}W_1 & -\frac{1}{\sqrt{2}}W_1 \end{bmatrix} = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \end{bmatrix}.$$

4 Kvantno računalništvo

4.1 Temelji kvantne fizike

Preden lahko začnemo naštevati postulate, moramo ustaliti notacijo, ki se jo v kvantni fiziki uporablja. Kot zahteva **Diracov zapis**, bomo vektorje ψ pisali kot $|\psi\rangle$. Uporabili bomo tudi t.i. **bra-ket** notacijo, ki skalarni produkt dveh vektorjev $|\psi\rangle$, $|\varphi\rangle$ označi kot $\langle\psi|\varphi\rangle$.

Postulat 1. ***Kvantni sistem*** *je podan s kompleksnim vektorskim prostorom $\mathcal{H}$ z ortonormirano bazo $|\psi_1\rangle, \ldots, |\psi_n\rangle$ in začetnim enotskim vektorjem $|\psi\rangle \in \mathcal{H}$. Enotskim vekotorjem v $\mathcal{H}$ pravimo* ***stanja****. Baznim vektorjem $|\psi_1\rangle, \ldots, |\psi_n\rangle$ pravimo* ***osnovna stanja****.*

Vsako stanje x lahko zapišemo kot **superpozicijo** osnovnih stanj

$$x = \lambda_1|\psi_1\rangle + \cdots + \lambda_n|\psi_n\rangle,$$

kjer velja

$$\begin{aligned} 1 &= \|x\|^2 \\ &= \left\langle \sum_{i=1}^{n} \lambda_i|\psi_i\rangle, \sum_{j=1}^{n} \lambda_j|\psi_j\rangle \right\rangle \\ &= \sum_{i=1}^{n}\sum_{j=1}^{n} \lambda_i\overline{\lambda_j}\langle\psi_i|\psi_j\rangle \\ &= \sum_{i=1}^{n} |\lambda_i|^2. \end{aligned}$$

Na primer, za kvantni sistem lahko vzamemo spin elektrona, ki je lahko v osnovnih stanjih $|\uparrow\rangle$ (gor) ali $|\downarrow\rangle$ (dol), za začetno stanje pa superpozicijo teh dveh osnovnih stanj

$$|\psi\rangle = \frac{1}{\sqrt{2}}\,|\uparrow\rangle + \frac{1}{\sqrt{2}}\,|\downarrow\rangle. \tag{3}$$

Postulat 2. *Pri razvoju kvantnega sistema lahko stanja spreminjajo zgolj unitarne preslikave.*

Ker je Walsh-Hadamardova preslikava W_1 unitarna, jo lahko uporabimo na stanju 3, ki nam ga slika v stanje

$$|\uparrow\rangle.$$

Opazimo, da se je superpozicija osnovnih stanj preslikala v osnovno stanje. Temu pojavu pravimo *interferenca.*

Postulat 3. *Če je sistem v stanju* $\sum_{i=1}^{n} \lambda_i |\psi_i\rangle$*, bomo ob meritvi izmerili bazno stanje* ψ_i *z verjetnostjo* $|\lambda_i|^2$*, stanje sistema pa se bo kolabiralo (kolapsiralo) v izmerjeno stanje.*

Če merimo stanje 3, bomo v polovici primerov izmerili, da ima elektron spin gor, v drugi polovici primerov pa, da ima elektron spin dol.

Postulat 4. *Kvantni sistem, ki ga dobimo z združitvijo kvantnih sistemov s prostorom stanj* $\mathcal{H}_1$ *in* $\mathcal{H}_2$ *ter začetnima stanjema* $|\psi\rangle$ *in* $|\varphi\rangle$*, je podan s prostorom stanj* $\mathcal{H}_1 \otimes \mathcal{H}_2$ *in začetnim stanjem* $\psi \otimes \varphi$*. Če je združen sistem v stanju*

$$\sum_{i=1}^{n} \lambda_i |e_i\rangle \otimes |\psi_i\rangle,$$

kjer so e_i *osnovna stanja sistema* $\mathcal{H}_1$ *in* $\psi_i \in \mathcal{H}_2$ *enotski vektorji, potem ob meritvi prvega sistema z verjetnostjo* $|\lambda_i|^2$ *izmerimo stanje* e_i*, sistem pa se kolabira v stanje*

$$|e_i\rangle \otimes |\psi_i\rangle.$$

4.2 Primerjava klasičnega računalnika s kvantnim

Klasični računalnik računa z **biti**, ki so lahko ali v stanju 0 ali v stanju 1, torej elementi $\mathbb{Z}_2$. Kvantni računalnik računa s **kubiti**, ki tvorijo kvantni sistem z osnovnimi stanji $|0\rangle$ in $|1\rangle$, tj. $\mathbb{C}[\mathbb{Z}_2]$. Poljubno stanje kubita je potem superpozicija teh dveh osnovnih stanj

$$\lambda_1 |0\rangle + \lambda_2 |1\rangle,$$

kjer $|\lambda_1|^2 + |\lambda_2|^2 = 1$. Če klasični računalnik deluje na n bitih, je njegov **register** (**spomin**) enak $\mathbb{Z}_2^n$, torej velikosti 2^n. Ko imamo kvantni računalnik z n kubiti, je njegov register enak n-ternemu tenzorskemu produktu

$$V_n = \underbrace{\mathbb{C}[\mathbb{Z}_2] \otimes \cdots \otimes \mathbb{C}[\mathbb{Z}_2]}_{n\text{-krat}} = \mathbb{C}[\underbrace{\mathbb{Z}_2 \otimes \cdots \otimes \mathbb{Z}_2}_{n\text{-krat}}].$$

Poleg 2^n osnovnih stanj vsebuje kvantni register še torej vse linearne kombinacije teh osnovnih stanj.

Račun na klasičnem računalniku je preslikava

$$f \colon \mathbb{Z}_n \to \mathbb{Z}_m$$

med dvema registroma. **Kvantni račun** na kvantnem računalniku je unitarna preslikava

$$U \colon V_n \to V_n$$

med dvema registroma z *enakim* številom kubitov.

Zgled (NOT vrata)**.** *Klasična NOT vrata so predstavljena z računom* $f \colon \mathbb{Z}_2 \to \mathbb{Z}_2$*, ki ima predpis*

$$f(k) = 1 - k.$$

Kvantna NOT vrata pa predstavlja matrika

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$

ki zamenja osnovni stanji $|0\rangle$ *in* $|1\rangle$*.*

V splošnem lahko vsak klasični račun $f\colon \mathbb{Z}_n \to \mathbb{Z}_m$ simuliramo na kvantnem računalniku, in sicer z linearno preslikavo

$$U_f\colon V_n \otimes V_m \to V_n \otimes V_m,$$

ki ima na baznih stanjih predpis

$$U_f(x \otimes y) = x \otimes (y + f(x)).$$

Izkaže se, da je ta preslikava unitarna, zato tvori kvantni račun. Račun f lahko iz nje povrnemo preko razvoja

$$U_f(x \otimes |\underbrace{0\cdots 0}_{n\text{-krat}}\rangle) = x \otimes f(x)$$

in projiciranjem na drugi register.

5 Iskanje periode funkcije

5.1 Kvantna Fourierova transformacija

Orodje, ki nam bo prišlo prav pri kvantnem delu algoritma, je t.i. kvantna Fourierova transformacija. Fiksirajmo neko naravno število n. Za vsako celo število k definiramo funkcijo $\chi^k\colon \mathbb{Z} \to \mathbb{C}$ s predpisom

$$\chi^k(x) = e^{\frac{2\pi i k x}{n}}.$$

Definicija 7. *Naj bo V vektorski prostor z ortonormirano bazo $|0\rangle, |1\rangle, \ldots, |n-1\rangle$.* ***Kvantna Fourierova transformacija*** *na V je linearna preslikava $\mathcal{F}\colon V \to V$, ki bazni vektor $|x\rangle$ slika v*

$$\mathcal{F}|x\rangle = \frac{1}{\sqrt{n}} \sum_{k=0}^{n-1} \chi^k(x)|k\rangle.$$

Če želimo v prihodnje kvantno Fourierjevo transformacijo uporabiti na kakšnem kvantnem sistemu, se moramo najprej prepričati, da je ta preslikava unitarna.

Trditev 2. *Preslikava $\mathcal{F}$ je unitarna.*

Dokaz. Za bazni vektor $|x\rangle$ velja

$$\begin{aligned}
\|\mathcal{F}|x\rangle\|^2 &= \langle \mathcal{F}|x\rangle, \mathcal{F}|x\rangle\rangle \\
&= \left\langle \frac{1}{\sqrt{n}} \sum_{k=0}^{n-1} \chi^k(x)|k\rangle, \frac{1}{\sqrt{n}} \sum_{l=0}^{n-1} \chi^l(x)|l\rangle \right\rangle \\
&= \frac{1}{n} \left\langle \sum_{k=0}^{n-1} \chi^k(x)|k\rangle, \sum_{l=0}^{n-1} \chi^l(x)|l\rangle \right\rangle.
\end{aligned}$$

Po lastnostih skalarnega produkta je to enako

$$\frac{1}{n} \sum_{k=0}^{n-1} \sum_{l=0}^{n-1} \chi^k(x)\overline{\chi^l(x)}\langle k|l\rangle.$$

Nadalje se po ortonormiranosti baze zgornja vsota poenostavi do

$$\frac{1}{n} \sum_{k=0}^{n-1} \chi^k(x)\overline{\chi^k(x)} = \frac{1}{n} \sum_{k=0}^{n-1} 1 = 1 = \||x\rangle\|^2.$$

Ker $\mathcal{F}$ slika ortonormirano bazo $\{|0\rangle, |1\rangle, \ldots, |n-1\rangle\}$ v ortonormiran sistem, dokazana enakost velja tudi za splošen vektor. □

Pri kvantnem delu algoritma bomo potrebovali še naslednji rezultat.

Lema 3. *Naj bo V vektorski prostor z bazo $\mathbb{Z}_n$. Naj bo $f \in V$, ki jo gledamo kot funkcijo $f\colon \mathbb{Z}_n \to \mathbb{C}$, ki slika i v koeficient pred baznim vektorjem $|i\rangle$ v razvoju f po bazi. Recimo, da je f periodična funkcija s periodo r in da $r \mid n$. Potem velja*

$$\mathcal{F}(f)(k) = \begin{cases} \frac{\sqrt{n}}{r} \sum_{s=0}^{r-1} f(s)\chi^k(s), & \text{če } k \equiv 0 \mod \frac{n}{r} \\ 0, & \text{sicer.} \end{cases}$$

Dokaz. Velja

$$\begin{aligned} \mathcal{F}(f)(k) &= \frac{1}{\sqrt{n}} \sum_{x=0}^{n-1} f(x)\chi^x(k) \\ &= \frac{1}{\sqrt{n}} \sum_{q=0}^{\frac{n}{r}-1} \sum_{s=0}^{r-1} f(qr+s)\chi^k(qr+s). \end{aligned}$$

Po periodičnosti funkcije f in multiplikativnosti funkcije χ^k dobimo

$$\begin{aligned} &\frac{1}{\sqrt{n}} \sum_{q=0}^{\frac{n}{r}-1} \sum_{s=0}^{r-1} f(s)\chi^k(qr)\chi^k(s) \\ &= \frac{1}{\sqrt{n}} \sum_{s=0}^{r-1} f(s)\chi^k(s) \sum_{q=0}^{\frac{n}{r}-1} \chi^k(qr). \end{aligned}$$

Če k ne deli $\frac{n}{r}$, potem je $\chi^k(qr) \neq 1$ za vsak $q = 0, \ldots, \frac{n}{r} - 1$ in po formuli za geometrijsko vrsto velja

$$\sum_{q=0}^{\frac{n}{r}-1} \chi^k(qr) = \frac{e^{2\pi i k} - 1}{e^{\frac{2\pi i r k}{n}} - 1} = 0.$$

Sicer je $\chi^k(qr) = 1$ za vsak $q = 0, \ldots, \frac{n}{r} - 1$ in velja

$$\sum_{q=0}^{\frac{n}{r}-1} \chi^k(qr) = \frac{n}{r},$$

kar dokaže lemo.

□

5.2 Kvantni del algoritma

Vrnimo se sedaj k našemu začetnemu algoritmu. V drugem poglavju smo problem izračuna prafaktorjev števila

$$N = pq$$

prevedli na problem iskanja najmanjšega števila r, da velja

$$y^r = 1 \mod N$$

za nek $y \in \mathbb{Z}_N^*$. To pa je ekvivalentno iskanju periode funkcije $f\colon \mathbb{Z}_N \to \mathbb{Z}_N$ s predpisom

$$f(k) = y^k \mod N.$$

Označimo njeno periodo z r. Naj bo n takšno število, da je

$$2^{n-1} < N \leq 2^n.$$

V nadalje bomo enačili N z 2^n, kar lahko storimo, saj se bo končni rezultat le malo razlikoval od pravega.

Začnimo z dvema n-registroma $V_n \otimes V_n$ v začetnem stanju $|0\rangle \otimes |0\rangle$.

(1) Na prvem registru uporabimo Walsh-Hadamardovo preslikavo W_n in dobimo

$$\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle \otimes |0\rangle.$$

Dobljeno stanje nato preslikamo z U_f, kar nam da

$$\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle \otimes |f(x)\rangle.$$

(2) Sedaj opazimo drugi register, kar nam da neko vrednost y_0 in nam kolabira stanje v

$$\frac{1}{\sqrt{|f^{-1}(y_0)|}} \sum_{x \in f^{-1}(y_0)} |x\rangle \otimes |y_0\rangle.$$

Ker je f periodična, obstaja natanko eno število $0 \leq x_0 < r$, da je $f(x_0) = y_0$. Če označimo $K = \frac{N}{r}$, je zgornje stanje v prvem registru potem enako

$$\frac{1}{\sqrt{K}} \sum_{q=0}^{K-1} |x_0 + qr\rangle = \sum_{x=0}^{N-1} \psi(x)\, |x\rangle,$$

kjer je

$$\psi(x) = \begin{cases} \frac{1}{\sqrt{K}}; & \text{če } r \mid x - x_0 \\ 0; & \text{sicer.} \end{cases}$$

Po definiciji je ψ periodična s periodo r.

(3) Na prvem registru sedaj uporabimo kvantno Fourierjevo transformacijo in po prejšnji lemi pridemo do stanja (po definiciji funkcije velja $r \mid N$)

$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} \chi^{\frac{sN}{r}}(x_0) \left| \frac{sN}{r} \right\rangle \otimes |y_0\rangle.$$

(4) Za konec opazimo to stanje v prvem registru, kar nam vrne vrednost c, ki je večkratnik števila $\frac{N}{r}$. Ker je bila vrednost y_0 naključna, je $c = \frac{sN}{r}$ za naključen $s \in \{0, \ldots r-1\}$, oziroma, $\frac{c}{N} = \frac{s}{r}$. Preko zapisa ulomka $\frac{c}{N}$ v okrajšani obliki $\frac{c'}{N'}$ in upoštevanja enakosti

$$c'r = sN'$$

ugotovimo, da je r večkratnik števila N'. Ta korak ponavljamo, dokler nismo zadostno gotovi, da je največji skupni večkratnik dobljenih vrednosti res perioda r funkcije f.

Literatura

[1] J. P. Buhler, H. Lenstra in C. Pomerance, *Factoring integers with the number field sieve*, v: The development of the number field sieve (ur. A. K. Lenstra), Lecture Notes in Mathematics, Springer, Berlin, 2006, str. 50–94.

[2] C. Pittet, *Mathematical aspects of Shor's algorithm*, 2013, dostopno na `https://cel.hal.science/cel-00963668/document`.