nedelja informatike v7.0

Kvantni algoritmi: Kraj kriptografije?

Lazar Galić

Matematička gimnazija

11. april 2022.

Za početak...

Furijeov niz

Aproksimacija proizvoljne periodične $f(x) : \mathbb{R} \to \mathbb{R}$ sa periodom 2π:

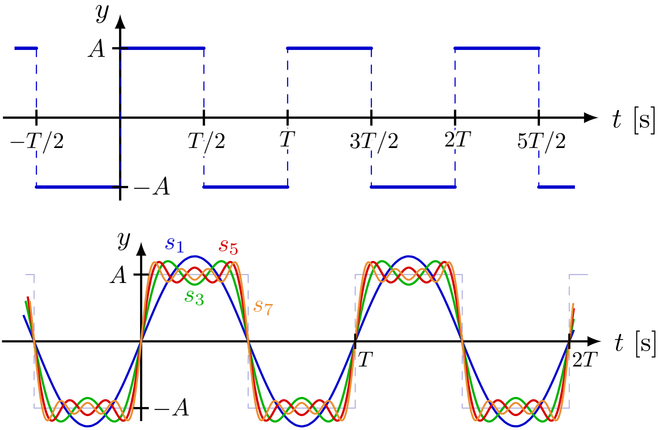
$$f(x) = \frac{1}{2}a_0 + \sum_{n=1}^{\infty} a_n \cos(nx) + \sum_{n=1}^{\infty} b_n \sin(nx)$$

gde se konstante a_0, a_i i b_i ($i \in \mathbb{N}$) nalaze kao:

$$\begin{aligned} a_0 &= \frac{1}{\pi}\int_{-\pi}^{\pi} f(x)dx \\ a_i &= \frac{1}{\pi}\int_{-\pi}^{\pi} f(x)\cos(ix)dx \\ b_i &= \frac{1}{\pi}\int_{-\pi}^{\pi} f(x)\sin(ix)dx \end{aligned}$$

Ukoliko je period funkcije $T \neq 2\pi$, koristimo zamenu $x' = \frac{2\pi}{T}x$

Prikaz Furijeovog niza



Prikaz Furijeovog niza

Kompleksan oblik Furijeovog niza

Poznato je da važi $\cos(\varphi) = \frac{e^{i\varphi}+e^{-i\varphi}}{2}$ i $\sin(\varphi) = \frac{e^{i\varphi}-e^{-i\varphi}}{2i}$.
Furijeov niz se može predstaviti i pomoću kompleksnih funkcija:

$$
\begin{aligned}
f(x) &= \frac{a_0}{2} + \sum_{k=1}^{\infty} \left(a_k \cos kx + b_k \sin kx\right), \\
&= \frac{a_0}{2} + \sum_{k=1}^{\infty} \left(a_k \frac{e^{ikx} + e^{-ikx}}{2} + b_k \frac{e^{ikx} - e^{-ikx}}{2i}\right), \\
&= \frac{a_0}{2} + \sum_{k=1}^{\infty} \frac{a_k - ib_k}{2} e^{ikx} + \sum_{k=1}^{\infty} \frac{a_k + ib_k}{2} e^{-ikx}, \\
&= \sum_{k=-\infty}^{\infty} c_k e^{ikx},
\end{aligned}
$$

Furijeova transformacija

Furijeova transformacija je generalizacija Furijeovog niza za $T \to \infty$.

Umesto diskretnog niza $\{c_k\}$ $(k \in \mathbb{C})$, dobijamo kontinualnu funkciju $F(k)$:

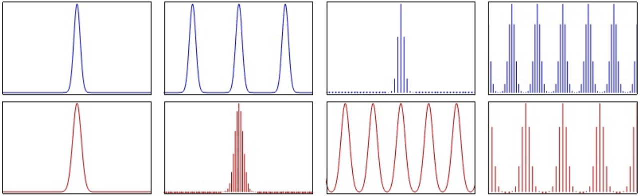
$$f(x) = \int_{-\infty}^{\infty} F(k) e^{2\pi i k x} dk$$
$$F(k) = \int_{-\infty}^{\infty} f(x) e^{2\pi i k x} dx$$

Diskretna Furijeova transformacija

Vrednosti obe funkcije se mogu aproksimirati diskretnim vrednostima na pravilnim intervalima, čime one postaju periodične.

Može se predstaviti kao preslikavanje vektora $(x_1, x_2, \dots, x_n)$ u vektor $(y_1, y_2, \dots, y_n)$, gde je $\varepsilon_n = e^{\frac{2\pi i}{N}}$ N-ti netrivijalni koren od 1, tako da:

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j \cdot \varepsilon_n{}^{-jk}$$



Primene

Prepoznavanje periodičnih komponenti funkcija

Veliki broj primena:

- Modulacija/demodulacija signala
- Kompresija zvuka - MP3
- Kompresija slika - JPEG
- Obrada slika (oštrina slike, prepoznavanje ivica)
- **Kvantno računarstvo**

1. Furijeove transformacije
2. **Kvantno računarstvo**
3. Šorov algoritam
4. Uticaj na kriptografiju

Kubiti

Osnovna stanja bita - $|0\rangle$ i $|1\rangle$.
Mogu se predstaviti kao vektori:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Kubit - superpozicija osnovnih stanja:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$$

gde su koeficijenti $\alpha, \beta \in \mathbb{C}$.

$|\alpha|^2$ i $|\beta|^2$ - verovatnoće $|0\rangle$ i $|1\rangle$:

$$|\alpha|^2 + |\beta|^2 = 1$$

$|0\rangle$

$|1\rangle$

$$|\psi\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

Kubiti

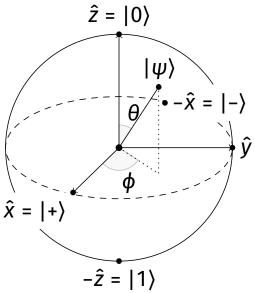
Šta je **superpozicija**?

Objekat se nalazi istovremeno u oba stanja.

Kada dođe do merenja, univerzum će prihvatiti jedno od stanja.

Superpozicija se urušava.

Blohova sfera - vizuelizacija kubita:



Kubiti

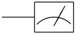
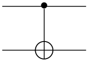
Višestruki kubiti - više osnovnih stanja grupe kubita:

$$
\begin{aligned}
|\psi\rangle = \alpha_{00}\,|00\rangle + \alpha_{01}\,|01\rangle \\
+ \alpha_{10}\,|10\rangle + \alpha_{11}\,|11\rangle
\end{aligned}
$$

Na pojedinačne i višestruke kubite se mogu primeniti kvantne logičke kapije, koje predstavljaju linearne transformacije vektora:

$$
H(q) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \leftarrow \text{Adamarova kapija}
$$

$$
H\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \cdot \frac{1}{\sqrt{2}} \left(\begin{pmatrix} 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right) = \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}
$$

Adamarova kapija	$H(q)$	$\boxed{H}$	$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$
Paulijeva X kapija	$X(q)$	$\boxed{X}$	$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
Paulijeva Y kapija	$Y(q)$	$\boxed{Y}$	$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$
Paulijeva Z kapija	$Z(q)$	$\boxed{Z}$	$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
Kapija faznog pomeraja θ	$R_\theta(q)$	$\boxed{R_\theta}$	$S = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}$
Merenje	$M(q)$		M
Kontrolisano NE	$CNOT(q)$		$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$

Kvantna Furijeova transformacija

Kvantna Furijeova transformacija je preslikavanje kvantnog stanja $|X\rangle = \sum_{j=0}^{N-1} x_j \, |j\rangle$ u kvantno stanje $|Y\rangle = \sum_{k=0}^{N-1} y_k \, |k\rangle$ tako da:

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j \cdot {\varepsilon_n}^{-jk}$$

Ovo je ekvivalentno preslikavanju:

$$|j\rangle \rightarrow \frac{1}{\sqrt{N}} x_j \cdot {\varepsilon_n}^{-jk}$$

Kvantna Furijeova transformacija

Pogledajmo vrednost koja odgovara $|j\rangle$ posle transformacije:

$$
\begin{aligned}
|j\rangle &\to \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{jk\frac{2\pi i}{2^n}} \\
&= \frac{1}{2^{n/2}} \sum_{k_1=0}^{1} \sum_{k_1=0}^{1} \dots \sum_{k_n=0}^{1} e^{2\pi i j\left(\sum_{l=1}^{n} k_l 2^{-l}\right)} \left|k_1 k_2 \dots k_n\right\rangle \\
&= \frac{1}{2^{n/2}} \bigotimes_{l=1}^{n} \sum_{k_l=0}^{1} e^{2\pi i j k_l 2^{-l}} \left|k_l\right\rangle \\
&= \frac{1}{2^{n/2}} \bigotimes_{l=1}^{n} \left(|0\rangle + e^{2\pi i j 2^{-l}} |1\rangle\right)
\end{aligned}
$$

Kvantna Furijeova transformacija

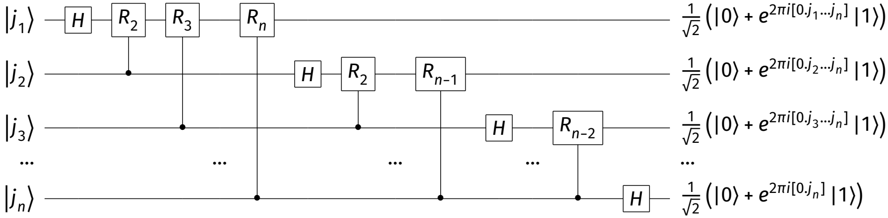
Eksponent u ovom izrazu odgovara:

$$e^{2\pi i j 2^{-l}} = e^{2\pi i [j_1 j_2 \ldots j_n] 2^{-l}} = e^{2\pi i [j_1 j_2 \ldots j_l . j_{l+1} \ldots j_n]} = e^{2\pi i [0.j_{l+1} \ldots j_n]}$$

Rezultat kvantne Furijeove transformacije je onda:

$$|j_1 j_2 \ldots j_n\rangle \to \frac{1}{2^{n/2}} \bigotimes_{l=0}^{n} \left(|0\rangle + e^{2\pi i [0.j_{l+1} \ldots j_n]} |1\rangle\right)$$

Kvantno kolo Furijeove transformacije



Procena faze

Podsetnik: Sopstveni vektor $|u\rangle$ i sopstvena vrednost $\alpha \in \mathbb{C}$ za datu linearnu matricu M predstavljaju rešenje jednačine:

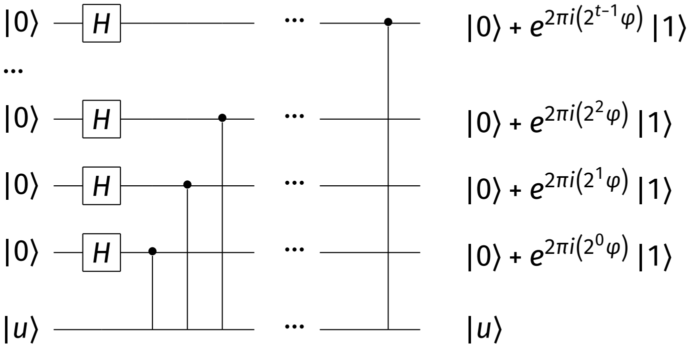
$$M\,|u\rangle = \alpha\,|u\rangle$$

Za sopstveni vektor $|u\rangle$ proizvoljne transformacije (matrice, kapije kola) U, možemo izračunati fazu primenom KFT na $|00...00\rangle$:

$$|0\rangle \to \frac{1}{2^{n/2}}\left(|0\rangle + e^{2\pi i 2^{t-1}\varphi}\,|1\rangle\right)\ldots\left(|0\rangle + e^{2\pi i 2^{0}\varphi}\,|1\rangle\right) = \frac{1}{2^{n/2}}\sum_{k=0}^{2^n-1} e^{2\pi i k\varphi}\,|k\rangle$$

Ukoliko primenimo inverznu kvantnu Furijeovu transformaciju, dobijamo procenu za φ.

Procena faze



Kolo za generisanje Furijeove transformacije za operator U

Šorov algoritam

Red broja x po modulu n je najmanji broj ρ tako da:

$$x^{\rho} \equiv 1 \pmod{n}$$

Posmatrajmo operator (koji se može napraviti kao logičko kolo):

$$U\,|y\rangle = \left|xy \pmod{n}\right\rangle$$

Takođe, smatramo da za $y \geq n$ važi $U\,|y\rangle = |y\rangle$.

Šorov algoritam

Za $0 \leq s < \rho$, sopstveni vektori U sa sopstvenim vrednostima $e^{-\frac{2\pi i s}{\rho}}$ su:

$$|u_s\rangle = \frac{1}{\sqrt{\rho}} \sum_{k=0}^{\rho-1} e^{\frac{2\pi i s k}{\rho}} \left|x^k \bmod n\right\rangle$$

$$U\,|u_s\rangle = \frac{1}{\sqrt{\rho}} \sum_{k=0}^{\rho-1} e^{k\cdot\frac{2\pi i s}{\rho}} \left|x \cdot (x^k \bmod n) \bmod n\right\rangle$$

$$= \frac{1}{\sqrt{\rho}} \cdot e^{-\frac{2\pi i s}{\rho}} \sum_{k=0}^{\rho-1} e^{(k+1)\cdot\frac{2\pi i s}{\rho}} \left|x^{k+1} \bmod n\right\rangle = e^{-\frac{2\pi i s}{\rho}} |u_s\rangle$$

Ako primenimo KFT na U, dobijamo fazu $e^{\frac{2\pi i s}{\rho}}$, odakle određujemo ρ.

Šorov algoritam

Lema 1 - Kako pogoditi broj reda 2

Neka je $n = p_1^{\alpha_1} \cdot \ldots \cdot p_m^{\alpha_m}$ faktorizacija neparnog složenog broja n, neka je x uniformno nasumično odabran broj za koji $2 \leq x \leq n$ i $\mathrm{NZD}(x, n) = 1$, i neka je ρ red broja x po modulu n. Tada važi:

$$P(2|r \wedge x^{\rho/2} \not\equiv -1 (\mathrm{mod}\ n)) \geq 1 - \frac{1}{2^m}$$

Lema 2 - Kako pogoditi delioc ako znamo broj reda 2

Za složen broj n (sa l bitova), i rešenje x jednačine $x^2 \equiv 1$ (mod n), za koje važi $x \not\equiv \pm 1$ (mod n) i $2 \leq x \leq n - 1$, bar jedan od brojeva $\mathrm{NZD}(x - 1, n)$ i $\mathrm{NZD}(x + 1, n)$ je netrivijalni faktor n koji možemo računati u $O(l^3)$.

Šorov algoritam

Postupak Šorovog algoritma, koji vraća neki faktor datog broja n, je:

Ako je broj paran, vrati 2.
Odaberi nasumičan $2 \leq a \leq n - 1$.
Izračunaj $k = NZD(a, n)$. Ako $k \neq 1$, vrati k.
Pomoću KFT izračunaj period ρ funkcije:

$$f(x) = a^x \bmod n$$

Ako je r neparno, vrati se na početak.
Ako je $a^{\rho/2} \equiv -1 \pmod{n}$, vrati se na početak.
Inače, bar jedan od $NZD(a^{\rho/2} + 1, n)$ i $NZD(a^{\rho/2} - 1, n)$ je faktor n, što se lako može proveriti. Vratiti onaj koji je delioc.

Kako radi enkripcija?

Enkripcija - šifrovanje podataka pomoću ključeva *koji su teški za pogoditi u realnom vremenu*, u svrhu bezbednog prenosa podataka.

2 glavna pristupa enkripciji:

- **Simetrična enkripcija** - isti ključ za šifrovanje i dešifrovanje.
- **Asimetrična enkripcija** - različit ključ za šifrovanje i dešifrovanje.

Kod simetrične enkripcije, ključ je poznat samo pošiljaocu i primaocu.

Kod asimetrične enkripcije, postoje 2 tipa ključa:

- **Javni ključ** - ključ koji je poznat svima.
- **Privatni ključ** - ključ koji je poznat samo kreatoru para ključeva.

TLS (i HTTPS) koristi asimetričnu enkripciju za deljenje simetričnog ključa, a zatim koristi simetričnu enkripciju za razmenu podataka.

RSA algoritam

Rivest-Shamir-Adleman (RSA) - algoritam za asimetričnu enkripciju.

Zasniva se na ideji da, za tri veoma velika broja n, d i e, čak iako su e, n i m poznati, veoma je teško pronaći d, ako $\forall m \in \mathbb{N}$ važi:

$$(m^e)^d \equiv m \pmod{n}.$$

Pojednostavljeni algoritam:

Odaberi 2 nasumična prosta broja p i q, i izračunaj $n = pq$.
Odredi $\lambda(n) = NZS(p-1, q-1)$ ($\lambda(n)$ je Karmajklova funkcija)
Odaberi nasumičan $1 \leq e \leq \lambda(n)$, tako da $NZD(e, \lambda(n)) = 1$.
Pronađi $d \equiv e^{-1} \pmod{\lambda(n)}$.

Pošto $d \cdot e \equiv 1 \pmod{\lambda(n)}$, ovi brojevi odgovaraju zahtevima RSA, pa se e koristi za pravljenje javnog ključa, a d za pravljenje privatnog ključa.

Post-kvantna kriptografija

Šorov algoritam omogućava znatno bržu faktorizaciju $n = p \cdot q$.

Ovo omogućava lako računanje $\lambda(n)$, a zatim i d, što izlaže privatni ključ.

Kvantni računari su i dalje u ranom razvoju - najveći faktorisan broj je:

$$1.099.551.473.989 = 1.048.589 \times 1.048.601$$

Limitacije - stabilnost više kubita, interferencije, spoljni šum.

Zaštita podataka se zasniva na težini pogađanja rešenja problema.

Većina trenutno korišćenih problema imaju efikasnija kvantna rešenja.

Postoje problemi koji su i dalje teški - npr. problemi rešetki.

Pitanja?

Hvala na pažnji!