Kvantno Računarstvo

Veljko Petrović
Januar, 2023

Motivacija

- Svaki moderan računar se oslanja na kvantne efekte.
- Ovo nije to: kvantno računarstvo se oslanja direktno na kvantne bite: kubite koji nemaju jednu vrednost nego su u superpoziciji vrednosti.
- Ovo omogućava takvim računarima da izvršava algoritme koje klasični računari ne mogu.
- Tačnije rečeno: algoritmi su izvršivi na klasičnim računarima ali ono što na kvantnom računaru može u polinomijalnom vremenu, na klasičnom računaru može u eksponencijalnom vremenu.
- Ovo ima ogromne posledice na praktičnost rešavanja određenih algoritama.

Kvantno Računarstvo

Novi tip računarstva

Izvori

- Ovo je jednostavan uvod u oblast kome je cilj da vas zainteresuje za dalje istraživanje.
- Prezentacija je bazirana donekle na radu prof. Skota Aronsona, naročito na njegovom blogu (Shtetl Optimized) i u knjizi Quantum Computing since Democritus.

Izvinjenje

- Nisam imao vremena da se konsultujem sa nekim ko predaje ovo na PMFu.
- Šta znam o kvantnoj mehanici sam naučio na engleskom jeziku, ne srpskom.
- Rezultat je to što je sasvim moguće da je terminologija loše prevedena. U slučaju zbunjenosti, notacija je univerzalna, termini ne.
- Takođe: na par mesta sam jako pojednostavljivao stvari budući da je ovo jedno predavanje, a ne trideset.
- Konačno, ja *nisam ekspert* u ovoj oblasti računarstva. Ovo predavanje je informativno, opciono, i ima namenu da vas zainteresuje, ništa više od toga.

Kvantna mehanika

Veoma brz uvod

Pristup

- Ovde se nećemo baviti kvantnom mehanikom kakva se obično radi.
- Ovo je zato što nas, fundamentalno, ne zanimaju iste stvari kao fizičare
- Ne želimo da računamo zračenje ili bilo šta slično. Zanimaju nas kvantna stanja ne i kojim fizičkim fenomenima odgovaraju.
- Baš kao što kada razmišljamo o klasičnim računarima nas zanima 0 i 1 i prelaz između njih. Nigde nas ne zanima da li su električni ili optički ili mehanički. Fundamentalno nema razlike u tome kako ih programiramo.

Kvantna mehanika kao progresija

- **Deterministički** sistemi koji koriste **logičke vrednosti** vode u...
- **Probabilističke** sisteme koji koriste **verovatnoće** koji vode u...
- **Kvantne** sisteme koje koriste **amplitude.**

Šta je amplituda?

- Fundamentalno ono što karakteriše amplitude (za razliku od verovatnoća) jeste da mogu biti negativne, pozitivne, ili kompleksne.
- Ovo je jako teško zamisliti: mogli bi da zamislimo šta znači biti 50% na jednoj i 50% na drugoj poziciji. Ali šta znači biti -70.71% na jednoj i 70.71% na drugoj?
- Ova teškoća vizualizacije je jedan od glavnih razloga zašto kvantna mehanika izaziva glavobolje i danas.
- Uprkos tome matematički aparat koji se koristi nije tako strašan.
  - Ne, ozbiljno.

Hajde da počnemo od verovatnoće

- Zamislimo vektor mogućih događaja $\Omega = (p_1, p_2, \ldots, p_N)$
- U klasičnoj verovatnoći uspostavljenoj aksiomatskim sistemom Kolmogorova važi da:
- $\sum \Omega = \sum_{i=1}^{N} p_i = 1$
- Ima smisla, zar ne? Verovatnoća da će se *nešto* desiti je ravno 1.

Norme

- Ovo ograničenje se može formulisati i tako što se kaže da, u verovatnoći, 1-norma skupa događaja mora biti 1.
- 1-norma je način računanja magnitude vektora tako što se sumiraju apsolutne vrednosti svih dimenzija
- Ovo se još zove i Menhetn Razdaljina.
- Šta se desi ako koristimo, recimo, 2-normu?

2-norma?

- Znate je, ali verovatnije kao Pitagorinu Razdaljinu ili Euklidovu Razdaljinu ili jednostavno magnitudu vektora
- $\|\Omega\|_2 = \sqrt{\sum_{i=1}^{N} p_i^2}$
- Ako onda umesto uslova $\|\Omega\|_1 = 1$ važi $\|\Omega\|_2 = 1$
- Umesto verovatnoće onda imamo kvantnu mehaniku.
- Manje-više.

Bit u kvantnoj mehanici

- Deterministički bit je ili 1 ili 0.
- Ako zamislimo probabilistički bit, on je ili 0 ili 1 sa verovatnoćom p i $1-p$.
- A kvantni bit? Kvantni bit ima dve amplitude, α i β čija je suma kvadrata 1
- $\alpha^2 + \beta^2 = 1$ (što opisuje krug) nasuprot $p + 1 - p = 1$
- Neka da je naš kvantni bit u stanju da je amplituda α 1 i amplituda β 0, što je OK jer zadovoljava uslov. Šta je onda stanje bita ako odemo i pogledamo?

Merenje

- Pre ili kasnije, moramo meriti stanje našeg kvantnog sistema.
- Merenje proizvodi 'klasičan' rezultat, tj. ili će biti 0 ili 1 kada se ode i pogleda.
- Postoje naravno verovatnoće da će biti 0 i verovatnoća da će biti 1. Koje su to verovatnoće?
- Pa $p_0 = \alpha^2$ i $p_1 = \beta^2$ naravno.

Merenje

- Drugim rečima, naše kvantno stanje može da bude pomešano koliko god hoćete, u jednom trenutku će se svesti na merenje koje će proizvesti stohastički rezultat.
- Kada merimo, moramo da stanje merimo u nekoj bazi. To su dimenzije u odnosu kojih merimo stanje.

Čemu amplitude?

- Zašto je onda ikome korisno da priča o amplitudama kada se uvek stvari završe u verovatnoćama i konkretnim vrednostima?
- Zato što, ako imamo amplitude, onda možemo da radimo potpuno drugačije operacije nad našim kubitima (i drugim kvantnim sistemima) koje proizvode razna neobična stanja koja eventualno kolabiraju u verovatnoće.
- Ono što je između je ono što čini kvantne sisteme čudnim.

Kako izgledaju transformacije?

- Ne možemo kvantnima stanjima da radimo šta god hoćemo: šta god da bude slučaj, svako kvantno stanje mora i dalje, predstavljeno kao vektor, da zadovoljava 2-normu.
- Kako izgleda, onda, opšta forma operacije koja normu čuva?
- To mora biti **unitarna** matrica. Unitarna matrica zadovoljava vrlo specifične uslove, naime, unitarna matrica A koja ima samo realne elemente mora da zadovoljava
- $$A^T A = A A^T = I$$
- Dakle, unitarna realna matrica (takođe: ortogonalna matrica) je takva da joj je inverzija jednaka transpoziciji.

Unitarne matrice sa kompleksnim elementima

- U opštijem slučaju unitarne matrice sa kompleksnim elementima važi $A^* A = A A^* = I$ odnosno, inverzija matrice je jednaka njenoj hermitijanskoj transpoziciji.
- Hermitijanska transpozicija je rezultat koji se dobije ako se za neku matricu prvo nađe transponovana, a onda se za svaki element individualno uzme kompleksna konjugovana vrednost, tj. obrne se znak imaginarnog dela.
- Bilo koja matrica koja ispunjava ovaj uslov predstavlja smislenu transformaciju nad nekim kvantnim stanjem.

Primer unitarne matrice

$$\begin{bmatrix} 1 & 0 \\ 0 & -i \end{bmatrix}$$

Matrica Hadamardove transformacije prvog reda

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

Tofolijeva matrica

$$T = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

Dirakova ket notacija

- Kad pričamo o kvantnom sistemu dobro je imati lepu kompaktnu notaciju
- Istorijski se koristi Dirakova ket notacija
- Tako da ako želimo da opišemo onaj kubit sa početka priče gde je ampltuda nula α a amplituda jedan β pisali bi
- $\alpha|0\rangle + \beta|1\rangle$

Primer kvantne interakcije

Neka imamo stanje $v = 1|0\rangle$ i matricu

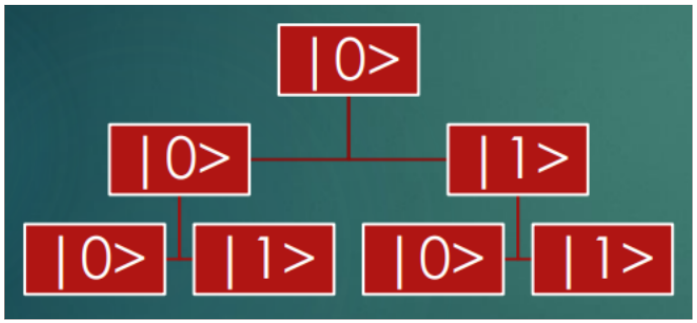
$$U = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix}$$

onda $v' = Uv = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ A ako primenimo transformaciju opet onda $v'' = Uv' = 1|1\rangle$

Primer kvantne interakcije

- Šta se ovde desilo?
- Imamo operaciju koja bi trebalo da ubacuje slučajnost. Počnemo sa apsolutno sigurnim stanjem i ubacimo transformaciju koja čini obe mogućnosti jednako verovatnim. Tj. ako merimo vrednost međurezultata dobićemo ili 1 ili 0. sa verovatnoćom ravno 0.5.
- Onda primenimo istu tu operaciju. U svetu obične verovatnoće, nema tih slučajnosti koje bi mogli dodati koji bi nas vratili na sigurnu verovatnoću.
- Ali ovde, ista ta operacija nam obrne vrednost, drugim rečima pretvori ekviprobabilne događaje u sigurno dobijanje vrednosti 1.

Dijagram prelaza stanja



Dijagram prelaza stanja

- Jedna interpretacija ovoga jeste da se posmatraju staze kroz ovaj dijagram prelaza stanja. Do konačne 0 dolaze dve staze (0 do 0, pa do 0, i 0 do 1 pa do 0) ali te staze, kada se pogleda, imaju pozitivnu i negativnu amplitudu.
- Ovo znači da su u poziciji *destruktivne* interferencije.
- Kao rezultat: nikad se ne dese.
- Putanje koje vode do 1 imaju pozitivne amplitude te interferiraju *konstruktivno.*

Mešana stanja

- Šta bude ako imamo mešana stanja: malo probabilistička, malo kvantna.
- U takvim stanjima imamo određenu verovatnoću da smo u jednom kubit-stanju, i određenu, drugu, verovatnoću da smo u drugom kubit-stanju.
- Ovo se rešava kroz matematički konstrukt poznat kao matrica gustine.
- Za neki vektor amplituda sa N elemenata se posmatra, prvo, NxN matrica gde je svaki element $N_{i,j}$ proizvod i-tog i j-tog elementa tog vektora amplituda.
- Da skratimo priču, to zovemo NN matrica. (Nije zvaničan termin).

Matrica gustine

- Ako imamo nekoliko vektora nad kojim imamo distribuciju verovatnoće (klasične verovatnoće) onda je matrica gustina ponderisana suma NN matrica za sve te vektore gde su faktori ponderisanja relativne verovatnoće.

Matrica gustine

Za 0.25 verovatnoću $\alpha|0\rangle + \beta|1\rangle$ i 0.75 verovatnoću $\alpha|0\rangle - \beta|1\rangle$ imali bi

$$D = 0.25 \cdot \begin{bmatrix} \alpha^2 & \alpha\beta \\ \beta\alpha & \beta^2 \end{bmatrix} + 0.75 \cdot \begin{bmatrix} \alpha^2 & -\alpha\beta \\ -\beta\alpha & \beta^2 \end{bmatrix} = \begin{bmatrix} \alpha^2 & -0.5\alpha\beta \\ -0.5\beta\alpha & \beta^2 \end{bmatrix}$$

Matrica gustine i nerazlučivost

- Mešana stanja su nerazlučiva
- To znači da ako odradimu kvantnu operaciju nad mešanim stanjem opisanim matricom gustine kao izlaz dobijemo još jedno mešano stanje

Kombinovanje kvantnih stanja

- Šta da radimo ako imamo više kvantnih stanja sa poznatim amplitudama i hoćemo da opišemo kvantno stanje koje je rezultat kombinacije svih tih stanja?
- Ovo nije nerealistična situacija: ako imamo kvantni računar koji operiše nad reči sa, npr, 16 kubita možemo da pričamo o stanju celog računara kao jednom kvantnom stanju? Da li je to moguće?
- Da, kroz operaciju *tenzorskog proizvoda.*

Tenzorski proizvod kvantnog stanja

$$(\alpha|0\rangle + \beta|1\rangle) \otimes (\gamma|0\rangle + \delta|1\rangle) = \alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|10\rangle + \beta\delta|11\rangle$$

Razdvojiva i spregnuta stanja

- Ako neko dvo-kubitno stanje možemo da napišemo kroz tenzorski proizvod dva jednokubitna stanja, onda za to stanje kažemo da je razdvojivo (eng. Separable).
- Ako, sa druge strane, imamo dvokubitno stanje takvo da je predstavljanje stanja kroz tenzorski proizvod jednokubitnih stanja nemoguće, onda imamo spregnuto (eng. Entangled) stanje.
- Da, ono koje je legendarno u naučnoj fantastici i popularnoj nauci.
- Evo čuvenog primera, prilagođenog iz rada Ajnštajna, Podolskog, i Rozena $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$

Interpretacija EPR

- Iz primera se može videti što se ovo zove i ‘upletenost’
- Zamislite za momenat (znam da smo obećali da nas ne zanima šta su fizički nosioci kvantnog ponašanja) da su u pitanju dva elektrona i kvantno obeležije je spin koji može biti $-\frac{1}{2}$ ili $\frac{1}{2}$
- Ovo kaže da ako izmerimo ovaj sistem 50% vremena će imati stanja koja su 00 i 50% vremena 11, odnosno, spin će biti ili jedan ili drugi, ali će biti isti u oba stanja.
- Ova dva elektrona su, onda, upletena.

Teorema o nemogućnosti kloniranja

Nema te procedure konzistentne sa kvantnom mehanikom koja kao ulaz uzme nepoznatno kvantno stanje i kao izlaz proizvede dva primerka tog istog, nepoznatnog stanja.

Dokaz teoreme o nemogućnosti kloniranja

Neka je kopirano stanje kubit $\alpha|0\rangle + \beta|0\rangle$ onda procedura kloniranja uzima taj kubit i prazan kubit i proizvede kao izlaz taj isti kubit i kopiju u praznom kubitu. Dakle:

$$(\alpha|0\rangle + \beta|1\rangle|0\rangle) \mapsto (\alpha|0\rangle + \beta|1\rangle) \otimes (\alpha|0\rangle + \beta|1\rangle)$$

$$= \alpha^2|0\rangle|0\rangle + \alpha\beta|0\rangle|1\rangle + \alpha\beta|1\rangle|0\rangle + \beta^2|1\rangle|1\rangle$$

Ali ovo je jasno nelinearno, a sve unitarne matrice su i linearne. Dakle nema takve matrice i konsekventno nema takve operacije koja klonira proizvoljno stanje.

Fizička interpretacija

- Ova teorema takođe proizilazi direktno iz Hajzenbergovog principa neodređenosti, budući da ako bi imali kvantni sistem od jedne čestice, i ako bi mogli da ga kloniramo, onda bi mogli da napravimo dve kopije i kod jedne izmerimo impuls, do proizvoljne preciznosti, a kod druge poziciju, do proizvoljne preciznosti, te ako ima kloniranja nema principa neodređenosti.
- Sa druge strane, ako nema principa neodređenosti, onda bi u principu merenjem mogli da odredimo sve osobine nekog stanja i da ga kloniramo tako.

Programerska interpretacija

- Ovo je jako bizarno budući da to predstavlja nešto što rad sa klasičnim sistemima čini trivijalnim, a kvantni sistemi čine nemogućim.
- Ako imamo bajt 1010 1100 možemo ga kopirati u 1010 1100 trivijalno. To je manje-više i najlakša stvar koju možemo raditi sa njim.
- Ista stvar sa kubitima je apsolutno nemoguća. Ovo čini transfer kubita jako teškim.
- Jedini mogući metod je 'kvantna teleportacija' koja omogućava da se neki kubiti prebace sa jednog mesta na drugo kroz klasičan kanal, uz to da se original uništi.
- Ovo se sa klasičnom informacijom ne zove 'teleportacija' no samo, 'premeštanje.'

Kvantno računarstvo u praksi

Kapije, kola, i osnove

BPP klasa problema

- Pre nego se zaletimo na priču o kvantnom računarsvu malo o teoriji kompleksnosti.
- BPP klasa problema (bounded-error probabilistic polynomial time) je klasa problema gde:
  - Algoritam daje odgovor koji je DA ili NE
  - Sme da 'baca novčić' da dobije slučajan bit i sme da pravi nasumične odluke.
  - Algoritam garantovano radi u polinomijalnom vremenu.
  - Na bilo kom izvršavanju algoritma BPP ima verovatnoću od najviše 1/3 da da netačan odgovor, bez obzira da li je odgovor DA ili NE.

BPP klasa problema

- Ova klasa je više zanimljiva zbog svojih teoretskih osobina.
- Štaviše trenutna intuicija struke je BPP = P
- No ono što mi treba da ponesemo iz ovoga je ideja algoritma koji moramo izvršiti N puta da bi dobili odgovarajuću verovatnoću uspeha.
- U slušaju BPP-a ako izvršimo algoritam, npr. 10 puta i prihvatimo odgovor samo ako dobijemo 10 istih rezultata, onda možemo da očekujemo verovatnoću tačnog rezultata od ~99.9983%.
- Ako hoćemo veću verovatnoću, moramo probati više puta.

BQP

- BQP je BPP izvršavan na kvantnom računaru, odn. računaru koji operiše sa ne klasično-izmerenim vrednostima no sa kvantnim vrednostima.
- Intuitivno govoreći BPP je klasa svih problema koji su efektno rešivi na klasičnom računaru.
- BQP je klasa svih problema koji su efektno rešivi na kvantnom računaru.
- Ideja bavljenja kvantnim računarstvom se vrti oko teze da BQP nije jednak BPP no sadrži BPP.
- Ovo je dokazano.

BQP i NP

- Da li je NP podskup BQP?
- Ne znamo. *Nemamo ni najblažu predstavu.*
- Kada su u pitanju klase kompleksnosti lista stvari koje ne možemo da dokažemo je... poduža.
- Ako imamo problem gde pretražujemo prostor od 2n mogućnosti i sve što možemo jeste da testiramo svaki kandidat to je problem nestruktuirane pretrage za koji važi:
  - Kvantni računari daju ubrzanje
  - To ubrzanje je kvadratno, ne eksponencijalno (Groverov algoritam)
  - Groverov algoritam je optimalan.

Koraci BQP problema

- **Incijalizacija.** Gde imamo na početku sistem od n kubita koji su svi na početku na nekom unapred poznatom stanju. Tipično to je ulaz u algoritam x i onoliko 0 vrednosti sa amplitudom 1 koliko nam treba za naš algoritam.
- **Transformacija.** Naš sistem od n qubita je u bilo kom trenutku superpozicija svih mogućih bit stringova sa n bita sa različitim amplitudama za svaku mogućnost. Mi vršimo transformaciju svih tih sa kvantim kapijama. Ovo su operacije sasvim analogne bulovim kapijama koje koristi običan računar.
- **Merenje.** Na kraju algoritma neki kubit je naš odgovor. Izmerimo ga i dobijemo ili 0 ili 1. Naš algoritam treba da je takav da grešimo najviše 1/3 vremena, baš kao BPP. Ako hoćemo veću verovatnoću, probamo više puta.

Neke kvantne kapije

- Svaka kvantna kapija je u duši unitarna matrica, ali je lakše ponekad posmatrati ih ne kao matrice, nego kao mapiranja, tj. kao tabele istinosnih vrednosti. Drugim rečima tretirati ih kao bilo kakvu drugu kapiju.
- U praksi, želimo da formiramo sve naše transformacije kao kompozicije određenih fundamentalnih kapija koje su efikasne za implementaciju.
- Deo te efikasnosti jeste da kvantne kapije operišu na 1, 2, ili 3 kubita.

Hadamardova kapija 1 kubita

Ulaz	Izlaz
$\|0\rangle$	$\frac{\|0\rangle+\|1\rangle}{\sqrt{2}}$
$\|1\rangle$	$\frac{\|0\rangle-\|1\rangle}{\sqrt{2}}$

Tofolijeva kapija 3 kubita

Ulaz	Izlaz
000	000
001	001
010	010
011	011
100	100
101	101
110	111
111	110

Tofolijeva kapija i klasičan računar

- Možda ste primetili da Tofolijeva kapija radi sasvim veselo i na klasičnom računaru.
- Ovo je sasvim tačno.
- Naravno to znači da ako bi samo imali Tofolijevu kapiju naš kvantni računar bi bio sasvim lak za simulaciju kroz klasičan računar.
- To bi značilo da ne bi mogli da ostvarimo nikakvo ubrzanje.
- Ovo je loše.

Univerzalnost

- Ali ako imamo Tofolijevu kapiju i Hadamardovu kapiju, iznenada smo spašeni.
- Te dve kapije su univerzalan skup koji zahvaljujući Šijevoj teoremi znamo da može da simulira bilo koju kvantnu kapiju (čija je unitarna matrica matrica realnih vrednosti što je za proračune dosta) sa proizvoljnom tačnošću.
- Još bolje, kroz rezultat kojise zove Solovaj-Kitajeva teorema, možemo da tvrdimo da je makoji univerzalni skup kapija efikasno (sa najviše polinomijalnim povećanjem broja kapija) simulira bilo koji univerzalni skup kapija.
- Drugim rečima koje kapije koristimo je tehnički problem, ništa više.

Šta je naš problem

- Imamo složeni broj N koji hoćemo da razbijemo na proste činioce. Ovo se još zove faktorizacija tog broja.
- Ovo je teško: klasični računari ovo rade u eksponencijalnom vremenu.
- Najefikasniji glasični algoritam ovo radi sa eksponentom od $d^{\frac{1}{3}}$ gde je d broj cifara. Dakle vreme je, za neku bazu b, $b^{d^{\frac{1}{3}}}$
- Rekord je d = 232 što je, distribuirano, oduzelo oko 2000 CPU-godina na modernim procesorima.
- Drugim rečima, dovoljno veliki brojevi ne mogu da se razbiju na proste činioce. Moderna kriptografija je bazirana na ovome.

Šorov algoritam

Pojednostavljen primer primene

Šorov algoritam

- 1995 Šor je pokazao da, sa kvantnim računarom, je moguće problem rešiti u vremenu koje je polinomijalno. Trenutni najbolji rezulatti zahtevaju $10d$ kubita i d^3 vremena.
- Ovo znači da sa dovoljno dobrim kvantnim računarom, faktorizacija brojeva je trivijalan problem.
- Ovo je... uzbudljiv rezultat budući da se trenutno jako puno uzdamo u kriptografiju.

Traženje perioda

- Šorov algoritam počinje napadom na problem vezan za faktorizaciju: traženje perioda modularne eksponent funkcije.
- Kratko rečeno: Ako imamo celi broj N i a, treba da nađemo najmanji pozitivni celi broj r, takav da je $a^r - 1$ umnožak N. Broj r je onda period $amodN$.
- Šta to znači? To znači da kada bi posmatrali niz stepena modulo N neke baze a, onda bi ona počela da ponavlja vrednosti posle r koraka.

Primer traženja perioda

Neka je N=15 i a=7. Onda se vidi da:

$$7^1 - 1 = 6$$

$$7^2 - 1 = 48$$

$$7^3 - 1 = 342$$

$$7^4 - 1 = 2400 = 160 * 15$$

Primer traženja perioda

Dakle, iz ovoga sledi da je periodičnost 4, i zaista ako izračunamo ostatak sa 15 za vrednosti 7^i za i od 1 do 9 dobijemo: 1, 7, 4, 13, 1, 7, 4, 13, 1, 7. Mesto gde je modulo 1 je tačka perioda i prvo takvo mesto je mesto gde će baza otići na r-ti stepen.

Od periodičnosti do faktorizacije

- Ako zamislimo da imamo magični algoritam za traženje perioda (uskoro) onda kako da to pretvorimo u sistem faktorizacije?
- Zamislimo da znamo da je $N = p_1 p_2$, broj sa dva faktora. Ako napadamo RSA to je i slučaj.
- Prvo: Odaberemo slučajno a između 2 i $N - 1$
- Drugo: Proračunamo najveći zajednički delilac N i a.
- Treće, ako je rezultat različit od 1, to je p_1, i mi smo gotovi.
- Četvrto, ako je rezultat 1, magično sračunamo period $a_i modN$ koji je r.
- Peto, ako je r neparan, skačemo na prvi korak.

Od periodičnosti do faktorizacije

- Eventualno r će biti parno i to će biti najmanji celi broj takav da $a^r - 1$ je umnožak N. Onda:
- $a^r - 1 = (a^{\frac{r}{2}} - 1)(a^{\frac{r}{2}} + 1)$
- Znamo da $a^r - 1$ nije umnožak broja N zato što bi onda period bio $\frac{r}{2}$ a znamo da to nije. Ako uzmemo kao predpostavku da $a^r + 1$ takođe nije umnožak N onda imamo situaciju dva broja, nikoji od kojih nije umnožak N čiji proizvod jeste umnožak N. To može samo da bude ako je jedan od činilaca $a^{\frac{r}{2}} - 1\ p_1$ a jedan od činilaca $a^{\frac{r}{2}} + 1\ p_2$ ili obratno.

Od periodičnosti do faktorizacije

- Onda sve što moramo da uradimo jeste da sračunamo najveći zajednički delilac za N i za $a^{\frac{r}{2}} \pm 1$ i rešili smo naš problem.
- Ako je slučaj da je baš $a^{\frac{r}{2}} + 1$ umnožak N onda moramo odbaciti vrednost koju smo izabrali i pokušati opet.
- Ovo će biti retko, ali je moguće.

Šta može kvantni računar

- Popularna miskoncepcija je da kvantni računari, zbog superpozicija, ‘probaju sve opcije odjednom’
- Oni apslutno tako ne rade, uprkos tome, postoji kvantni paralelizam nekakve vrste
- Njega odlikuje sposobnost da se uzme kompleksna funkcija i da se odrede (brzo) njene globalne osobine koje nisu izračunljive iz njene evaluacije na relativno malom broju tačaka
- Periodicitet modularne eksponencijacije je baš jedna takva osobina.

Kako radi ‘magični’ algoritam?

Za unitarni operator U_a koji implementira modularno množenje $x \mapsto axmodN$ sopstvene vrednosti odgovarajuće matrice će imati formu $e^{j\phi}$ gde je $\phi = \frac{2\pi k}{r}$ za $k \in \mathbb{Z}$.

Kako radi ‘magični’ algoritam

- Tačna procedura računanja kvantne faze koju nameće operator (to je ovo ϕ) je spektakularno kompleksna, ali srećom je već odrađena za nas.
- Detalji su ovde: https://qiskit.org/textbook/ch-algorithms/quantum-phase-estimation.html
- Kratko rečeno: ovo je moćna operacija i notacija za nju je QPE.

Šorov algoritam i QPE

- Proračunamo QPE vrednosti za porodicu operatora U_b gde je $b = a, a^2, a^4, a^8 \ldots$ i tako sve do stepena a koji odgovara grubo vrednosti N.
- Ovo merenje se može potpuno paralelizovati
- QPE je jedna od onih stvari koje imaju nasumičnu šansu greške, ali uz dovoljno merenja signal će nadjačati šum.
- Kada imamo fazu, možemo naći r.

Kako raditi modularno množenje?

- Kvantni algoritmi apsolutno mogu da pozivaju potpuno klasične pod-funkcije.
- Ako je BPP podskup BQP onda su valjda naši klasični programi samo ne osobito bistri kvantni programi?
- Ne baš, ali blizu.
- Problem je u tome što klasičan kod kvari superpozicije. Da to ne bi radio mora biti konvertovan u reverzibilnu formu.
- To znači da, prvo, mora biti napravljen od kvantnih kapija i, drugo
- Mora da ‘počisti iza sebe’ odnosno da iza izvršavanja ima samo izlaz, ništa od pod-rezultata, tj. da ne pravi pobočna dejstva.

Reverzibilnost

- Centralna ideja je da se svaka klasična kapija pretvori u varijantu koja ima isti broj ulaza i izlaza i radi jednako dobro u oba smera
- Onda se napravi blok koi radi proračun kroz te kapije, neka su G_1, G_2, G_3, G_4, G_5 recimo
- Zbog toga kako kapije rade u njih ulazi sva memorija koju će da koriste kao ulaz
- Kad dobijemo njihov izlaz mi moramo da počistimo tu memoriju. To radimo tako što pokrenemo G_5, G_4, G_3, G_2, G_1 i uradimo sve što smo radili ranije *unazad*
- Ovo se zove ‘uncomputing’
- Rezultat ovoga je da se ovo ponaša kao žica, a da mi iz sredine ‘ukrademo’ f(x)

Reverzibilnost

Reverzibilnost

Izvor slike: https://quantum-computing.ibm.com/docs/iqx/guide/shors-algorithm (C) IBM.