



# 10—Kvantno računarstvo

NOVI TIP RAČUNARSTVA

# 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.

# 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

- ▶ U ovoj prezentaciji ću biti prinuđen da vas izložim matematičkoj tipografiji u PowerPoint-u.
- ▶ Ona je mučna za gledanje i mučnija za pisanje, ali sam hteo da su sve prezentacije u istom formatu umesto da imate samo jednu u LaTeX formi.
- ▶ Zbog toga što je tako užasna tipografija, na nekim mestima ću umesto notacije koristiti reči tipa alfa-kvadrat i slično. Molim izvinite zbog toga.

# Izvinjenje #2

- ▶ 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.



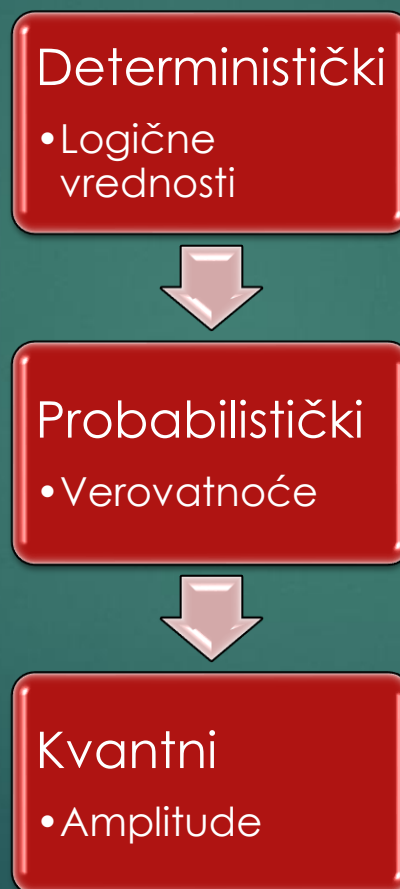
# Kvantna mehanika

VEOMA BRZI 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.

# Kvantna mehanika kao progresija





# 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 prvo vektor mogućih događaja omega
- ▶  $\Omega = (p_1, \dots, p_N)$
- ▶ U klasičnoj verovatnoći važi kao uslov:
- ▶  $\sum \Omega = \sum_{i=1}^N p_i = 1$
- ▶ Ovo možemo opisati i ovako: za vektor klasičnih verovatnoća mogućih ishoda nekog događaja važi da je 1-norma tog skupa jednaka 1.
- ▶ 1-norma jeste kada merimo vektor tako što sumiramo apsolutne vrednosti svih dimenzija. To je još poznato (u 2D slučaju) kao Menhetn Razdaljina
- ▶ Ali šta bude ako pokušamo da koristimo 2-normu?

# 2-norma

- ▶ 2-norma vam je poznatija i kao Pitagorina razdaljina. Drugim rečima
- ▶  $\|\Omega\|_2 = \sqrt{\sum_{i=1}^N p_i^2}$
- ▶ Šta onda bude ako zamislimo da vrednosti p moraju da zadovoljavaju uslov da:
- ▶  $\|\Omega\|_2 = 1$
- ▶ Dobijemo kvantnu mehaniku.

# Bit u kvantnoj mehanici

- ▶ Ako je bit u klasičnoj verovatnoći onda može da bude ili 0 ili 1 i to sa vrednošću  $p$  za 0 i  $1-p$  za 1.
- ▶ Ali u kvantnoj mehanici imamo nešto drugo. Naš kvantni bit (kubit) ima amplitude alfa i beta, za koje važe da je suma njihovih *kvadrata* jedan. Drugim rečima, moguće vrednosti alfa i beta opisuju *krug*.
- ▶  $\alpha^2 + \beta^2 = 1$  nasuprot  $p + 1 - p = 1$
- ▶ Ako je bit u stanju alfa-nula i beta-jedan, šta bude kada pogledamo šta je stanje bita?

# Merenje

- ▶ Pre ili kasnije, moramo da vidimo šta naš kvantni sistem radi.
- ▶ Merenje proizvodi klasičan rezultat, tj. naš bit će biti *ili* 0 *ili* 1 sa nekim verovatnoćama.
- ▶ Kojim? Pa  $\alpha^2$  i  $\beta^2$ , naravno.
- ▶ Kada se merenje izvrši, rezultat je *uništenje* kvantnog stanja.
- ▶ 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
- ▶  $A^T A = A A^T = I$  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
- ▶  $A^*A = AA^* = I$  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.



# Primeri unitarne matrice

▶  $\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$  - Hadamardova matrica.

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

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

▶ Tofolijeva matrica.

# Dirakova ket notacija

- ▶ Kada pričamo o stanjima nekog kvantnog sistema (kod nas uvek jednog ili više kubita) zgodno je imati kompaktnu notaciju.
- ▶ U toj notaciji onaj kubit sa početka priče izgleda ovako
- ▶  $\alpha|0\rangle + \beta|1\rangle$
- ▶ Ishodi su 0 i 1, a amplitude alfa i beta.

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

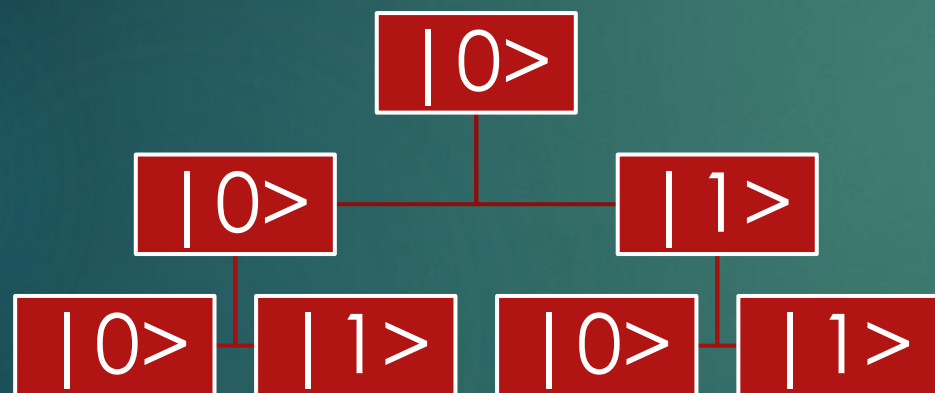
$$v' = Uv = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle, \text{ a ako primenimo transformaciju opet onda bude}$$
$$v'' = Uv' = 1|1\rangle$$

## Primer kvantne interakcije

# 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.

# Primer kvantne interakcije



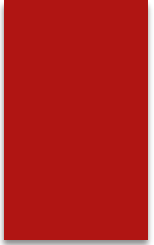
- ▶ Jedna interpretacija ovoga jeste da se posmatraju staze kroz ovaj dijagram prelaza stanja. Do konačne 0 dolaze dve staze (0 do 0, pa do 0, i 0 do 1 pa do 0) ali te staze, kada se pogleda, imaju pozitivnu i negativnu amplitudu.
- ▶ Ovo znači da su u poziciji *destruktivne interferencije*.
- ▶ Kao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

# Mešana stanja

- ▶ Šta bude ako imamo *mešana* stanja.
- ▶ 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,  $N \times N$  matrica gde je svaki element  $i, j$  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.



Za 25% verovatnoću  $\alpha|0\rangle + \beta|1\rangle$  i 75% verovatnoću  $\alpha|0\rangle - \beta|1\rangle$  imali bi:

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

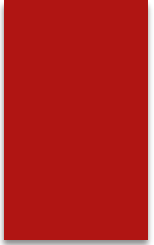
Operacije sa istom matricom gustine nisu razlučive, tj. u istom su pomešanom stanju.

# Matrica gustine



# 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*.


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

Gde se notacija  $|00\rangle$  koristi kao skraćenica za  $|0\rangle \otimes |0\rangle$  radi kompaktnosti notacije.

## Tenzorski proizvod kvantnih stanja

# 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 (EPR):
- ▶  $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$

# Teorema o nemogućnosti kloniranja

- ▶ *Nema te procedure konzistentne sa kvantnom mehanikom koja kao ulaz uzme nepoznato kvantno stanje i proizvede dva primerka tog istog nepoznatog stanja.*

Neka je stanje koje kopiramo jedan kubit koji izgleda ovako:  $\alpha|0\rangle + \beta|1\rangle$  onda neka naša procedura kloniranja uzima taj kubit i prazan kubit i proizvede dve kopije našeg kubita. To izgleda ovako:  
 $(\alpha|0\rangle + \beta|1\rangle|0\rangle) \mapsto (\alpha|0\rangle + \beta|1\rangle) \otimes (\alpha|0\rangle + \beta|1\rangle) = \alpha^2|0\rangle|0\rangle + \alpha\beta|0\rangle|1\rangle + \alpha\beta|1\rangle|0\rangle + \beta^2|1\rangle|1\rangle$   
Ali jedine konzistentne operacije su unitarne matrice a one su uvek *linearne*. Stoga nema takve unitarne matrice koja efektira kloniranje.

# Teorema o nemogućnosti kloniranja

- ▶ 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.

# Teorema o nemogućnosti kloniranja

- ▶ 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

KAPIJE, KOLA I OSNOVE

# BPP klasa problema

- ▶ Pre nego se zaletimo na priču o kvantnom računarstvu 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

- ▶ 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 slučaju 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  $\sim 99.9983\%$ .
- ▶ 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  $2^n$  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 duži 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 klasični kompjuteri

- ▶ 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.

# Šorov algoritam

PRIMER PRIMENE

# 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  $d^{1/3}$  gde je  $d$  broj cifara. Dakle vreme je, za neku bazu  $b$ ,  $b^{\sqrt[3]{d}}$
- ▶ 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

- ▶ 1995 Šor je pokazao da, sa kvantnim računarom, je moguće problem rešiti u vremenu koje je *polinomijalno*. Trenutni najbolji rezultati 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  $a \bmod N$ .
- ▶ 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.



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

$$7^1 - 1 = 6$$

$$7^2 - 1 = 48$$

$$7^3 - 1 = 342$$

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

Dakle, očekuje se da će periodičnost biti 4 i zaista ako sračunamo opštu formulu  $7^i \bmod 15$  za  $i$  od 1 do 9 dobje se: 1, 7, 4, 13, 1, 7, 4, 13, 1, 7. Mesto gde imamo da je modulo jednak 1 je tačka perioda, i prvo takvo mesto je tamo gde baza ide na  $r$ -ti smer.

## Primer traženja perioda

# 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  $a^i \bmod N$  koji je  $r$ .
- ▶ Peto, ako je  $r$  neparan, skačemo na prvi korak.

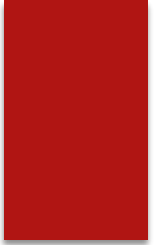
Sada imamo  $r$  koje je parno i koje je takvo da je  $r$  najmanji celi broj takav da je  $a^r - 1$  je neka vrednost puta  $N$ . Onda je slučaj da:

$$a^r - 1 = (a^{r/2} - 1)(a^{r/2} + 1)$$

Znamo da  $a^{r/2} - 1$  nije umnožak broja  $N$  zato što bi onda period bio  $r/2$ , a znamo da nije. Ako uzmemo da  $a^{r/2} + 1$  takođe nije umnožak broja  $N$ , onda imamo slučaj dva broja koji nijedan nije umnožak  $N$ , ali njihov proizvod jeste. U tom slučaju jedina mogućnost je da je  $p_1$  koji traimo je prost činilac  $a^{r/2} - 1$ , a  $p_2$  isto za  $a^{r/2} + 1$  ili obrnuto.

# Od periodičnosti do faktORIZACIJE





U ovom slučaju važi da se  $p_1$  i  $p_2$  mogu naći tako što se računa najveći zajednički delilac  $N$  i  $a^{r/2} \pm 1$ . Jedini izuzetak je šta činiti ako je  $a^{r/2} + 1$  baš umnožak broja  $N$ . Onda se vrednost  $a$  napušta, i računa se sledeći pokušaj. Srećom ovo je retko za  $N = 15$ , jedina vrednost  $a$  koja ne rezultuje sa uspehom je 14.

# Od periodičnosti do faktORIZACIJE

# Šta to može kvantni računar?

- ▶ Kvantni računari *ne mogu* da 'probaju sve opcije' kako se to često kaže u popularnoj literaturi.
- ▶ Tako ne radi kvantni paralelizam.
- ▶ Uprkos tome, kvantni paralelizam *postoji*.
- ▶ Ono što kvantni računari mogu da urade jeste da evaluiraju globalne osobine kompleksnih funkcija koje nisu takve da se mogu zaključiti na osnovu evaluacije funkcije na samo par tačaka.
- ▶ Periodicitet modularne eksponencijacije je baš takva osobina.

# Magični algoritam za računanje perioda

- ▶ Dokazivo je da ako imamo unitarni operator koji implementira funkciju za modularno množenje onda su sopstvene vrednosti relevantne matrice zavisne od perioda  $r$ .

Za unitarni operator  $U_a$  koji implementira modularno množenje  $x \mapsto ax \bmod N$  sopstvene vrednosti  $U_a$  imaju formu  $e^{j\phi}$  gde je  $\phi = \frac{2\pi k}{r}$  za neki celi broj  $k$ .

# Sopstvena vrednost

- ▶ Ovde se mora reći da je računanje kvantne faze nekog operatora *neverovatno bitan* gradivni element mnogih algoritama.
- ▶ Nažalost, razumevanje ovoga zahteva prilično gadnu matematiku koja već prelazi opseg ovako jednog predavanja.
- ▶ Ako vam treba više:
- ▶ <https://qiskit.org/textbook/ch-algorithms/quantum-phase-estimation.html>
- ▶ Kratko rečeno: možemo da nađemo fazu koju bilo koji unitarni operator nameće ulazu. Neka nazovemo tu operaciju QPE.

# Šorov algoritam za QPE

- ▶ Proračunaćemo QPE vrednost za porodicu operatora  $U_b$  gde je  $b = a, a^2, a^4, a^8, \dots$  i tako sve do vrednosti koja grubo odgovara  $N^2$
- ▶ Ova porodica može da se meri u paraleli i merenje na svim ovim vrednostima pomaže da se smanji greška merenja.
- ▶ Uz dovoljno ponavljanja QPE, čak i ako je jako zašumljen rezultat, moguće je proceniti fazu sa proizvoljnom preciznošću.
- ▶ Kada imamo fazu, možemo da vrlo lako nađemo  $r$ .

# Pod-algoritam za modularno množenje

- ▶ Kvanti algoritmi *smeju* da pozivaju klasične funkcije.
- ▶ Ima smisla: BPP je podskup BQP, pa valjda su i naši klasični programi (glupi) kvantni programi?
- ▶ Ne baš ali blizu.
- ▶ Ako ne želimo da pokvarimo našu superpoziciju, onda moramo da konvertujemo klasičan kod u reverzibilnu formu.
- ▶ To znači da mora da bude napravljena od kapija koje su i klasične i kvantne (kao što je Tofoli kapija i CNOT kapija), prvo.
- ▶ Zatim, mora da 'počisti iza sebe' tako da na kraju izvršavanja samo rezultat ostaje u memoriji, ništa od međurezultata.

# Reverzibilna forma klasična kola

- ▶ Ideja je da se svaka klasična kapija (AND recimo) pretvori u verziju sa istim brojem ulaza i izlaza koja radi jednako dobro unapred i unazad.
- ▶ Onda se napravi blok koji radi proračun kroz neke takve kapije  $G_{1,2,3,4,5}$ .
- ▶ Zbog osobine kapija tu ulazi neki ulaz  $x$ , te biti memorije koju koristimo kao lokalnu promenljiv. Nas zanima neko  $f(x)$  koje je poenta cele vežbe.
- ▶ Zbog reverzibilnosti,  $x$  koji uđe će biti  $x$  i koji izađe, ništa posebnu tu.
- ▶ Da bi se rešili memorije mi uradimo 'dekomputaciju' gde imamo drugi blok koji ima kapije  $G_{5,4,3,2,1}$ .



# Reverzibilna forma klasična kola

- ▶ Time  $x$  koje je izašlo i sada ušlo i dalje ostane  $x$ , pošto ga kapije ne diraju.
- ▶ Međurezultatski biti kako su nastali, tako budu i poništeni.
- ▶ A  $f(x)$  se kopira u registar sa strane i sačuva.



# Dijagram opšte forme reverzibilnosti

