УНИВЕРЗИТЕТ У БЕОГРАДУ
МАТЕМАТИЧКИ ФАКУЛТЕТ

Имплементација неких алгоритама на квантним рачунарима

Никола Спасојевић

- Мастер рад -

Ментор:
др Миодраг Живковић, проф.

Комисија:
др Саша Малков, ванр. проф.
др Анђелка Ковачевић, ванр. проф.
др Александар Картељ, доцент

Београд, 2019.

Сажетак

Квантни рачунари, још од настанка идеје осамдесетих година прошлог века, привлаче пажњу научника, а последњих година постали су редовна тема не само научних радова, већ и популарних чланака. Овај рад представља квантне рачунаре и алгоритме, пре свега из угла информатике и математике, кроз више целина. Дат је општи увод у област квантне механике, као и неопходни елементи за разумевање квантних рачунара. Кроз детаљнији опис и примере једне гране квантних алгоритама заснованих на квантној Фуријеовој трансформацији, приказан је пут развоја алгоритама за квантне рачунаре, њихове имплементације, могућности, али и тешкоће њихове конструкције.

Садржај

1 Увод **1**

2 Квантна механика **3**
2.1 Физика као наука . . . 3
2.2 Почеци квантне физике . . . 4
2.3 Суперпозиција и важност мерења . . . 5
2.4 Уплетеност . . . 5

3 Квантни рачунар и основни алгоритми **7**
3.1 Неопходни математички елементи . . . 7
3.2 Постулати квантне механике . . . 9
3.3 Мешана стања . . . 15
3.4 Телепортација . . . 15
3.5 Супергусто кодирање . . . 17
3.6 Физичка имплементација квантних рачунара и квантни програмски језици . . . 18

4 Предност квантних рачунара - Дојч-Јоза алгоритам **19**

5 Квантни алгоритми засновани на Фуријеовој трансформацији **25**
5.1 Квантна Фуријеова трансформација . . . 25
5.2 Процена квантне фазе . . . 27
5.3 Шорови алгоритми - факторизација и дискретни логаритам 28
5.4 Последице и пост-квантна криптографија . . . 32

6 Општи случај употребе квантних рачунара - за и против **33**
6.1 Кључни елементи квантног убрзања и применљивост . . . 33
6.2 Када? . . . 34

7 Закључак **35**

Библиографија **37**

Глава 1

Увод

Према Муровом закону, граница усложњавања рачунарских кола биће досегнута за 30 до 40 година [1], након чега више неће бити могуће смањивање класичних рачунарских компоненти. Иако се може поставити питање да ли је потребно додатно усложњавати рачунарске системе, чињеница је да ће до тога доћи не само због потреба тржишта, већ и безбедносно-економских ефеката поседовања најбржих рачунара. Следеће логично питање је како то учинити када, уз тренутну технологију, граница величине рачунарске компоненте јесте атом. Управо у томе и лежи одговор - потребно је пронаћи нову технологију. Као једно од решења, појављује се концепт квантног рачунара чије функционисање почива на квантној, а не класичној физици. Као идеја, квантно рачунарство се први пут помиње 1980. године у раду Јурија Манина [2], а пет година касније Дојч формализује појам универзалног квантног рачунара [3], пандана Тјуринговој машини класичног рачунарства.

Како је у питању сложена машина, квантни рачунар је први пут конструисан тек крајем деведесетих година, а највећи квантни рачунар тренутно има само педесет кубита[1], јединица које можемо сматрати битовима квантног рачунарства. Ипак, сам раст интересовања, као и активно ангажовање приватног сектора у истраживању ове технологије оправдава и већи рад академске заједнице у овој области. Протекле године ИБМ је објавио конструкцију до тада највећег квантног рачунара, а канадски Дивејв(енг. D-vawe) је пустио у продају специјализовани квантни рачунар од чак 2000 кубита. Квантно рачунарство је неизбежна тема на великим конференцијама, а нарочито у области криптографије, у којој је пост-квантна криптографија постала саставни део курсева на свим већим универзитетима.

Циљ овог рада јесте да на једноставан начин пружи основне информације и покаже могућности квантног рачунарства свима које интересује ова област. Рад је писан тако да буде разумљив информатичарима и подразумева знање из области алгоритмике, програмирања и математике. Са друге стране, дубље знање математике и квантне механике није неопходно и делови рада ће бити посвећени управо њима.

[1] У раду ће бити коришћен израз кубит, као реч српског језика. Неки аутори користе и израз кјубит као транскрипцију оригиналне енглеске речи “qubit” или “qbit”. Како се ради о појму, а не о имену, у овом раду је ипак коришћено кубит, у складу са правилима српског језика.

Након поглавља која се баве самим квантним рачунарима, рад се фокусира на алгоритме за квантне рачунаре и то на групу алгоритама заснованих на квантној Фуријеовој трансформацији. Кроз постепено усложњавање, представљају се предности квантних рачунара, начин развоја алгоритама и њихова имплементација у хипотетичким квантним колима. У последњим поглављима, рад се осврће на општи случај имплементације алгоритма на квантном рачунару, тешкоће које том приликом могу настати и предности и мане самог приступа.

Глава 2

Квантна механика

Квантна механика или квантна физика је најмлађа грана физике, односно њено најмлађе проширење. Оно што ово проширење чини изузетно занимљивим јесте то што није монолитно нити јасно дефинисано попут Њутнове механике или Ајнштајнове релативности, већ је знатно шире и разноврсније описано кроз више радова разних научника [4]. У овом поглављу, описаћемо најбитније елементе квантне механике за квантно рачунарство, како би читалац који није имао додира са том облашћу могао да са разумевањем настави читање овог рада.

2.1 Физика као наука

> *„There is an expanding frontier of ignorance"*
>
> — Richard Feynman, The Feynman Lectures on Physics [5]

Цитат Ричарда Фајнмена са почетка овог поглавља би грубо могао да се преведе као „Границе незнања су растуће", мада тај превод нема снагу оригиналне изјаве. Ипак, суштина остаје јасна, колико год да проширујемо наше знање, толико проширујемо и видик ка свему што не знамо. Физика, као једна од најстаријих наука, то показује већ хиљадама година. Парадоксално, за науку која покушава да објасни свет не постоји јединствена дефиниција.

Дефиниција 2.1.1 *Физика је грана науке која се бави природом и својствима материје и енергије[6].*

Дефиниција 2.1.2 *Физика је наука која се бави материјом и енергијом и њиховим интеракцијама[7].*

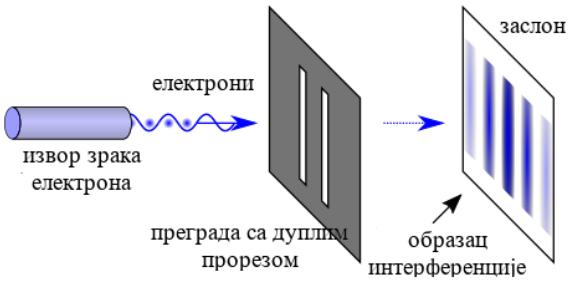
Дефиниција 2.1.3 *Физика је наука о природи уопште; у ужем смислу: наука о законима природних појава уколико ове нису изазване органским или хемијским силама [8].*

Физика се може описати као наука која се бави описивањем света, узрочно-последичним везама феномена, односно законитостима по којима се они одвијају. Са друге стране, напредовање физике је подстакнуто жељом за откривањем узрока тих законитости. Језик физике је математика којом се формално описују законитости, а у зависности од потреба, пре свега резултата експеримената, употребљавају се различити математички алати. У наредном поглављу ћемо детаљно размотрити неке од елемената неопходних за изучавање квантног рачунарства.

2.2 Почеци квантне физике

Почетак квантне физике обележила су два догађаја, удаљена скоро стотину година један од другог. Почетком деветнаестог века, Томас Јанг (енг. Thomas Young) изводи Експеримент са двоструким прорезом којим доказује таласну природу светлости. Поставка експеримента се састоји од извора хомогене светлости и плоче са два уска прореза између извора и платна. У случају да је светлост честица, очекивано понашање би било њено концентрисање на местима директно иза прореза. Међутим, на платну иза прореза долази до формирања периодичне шаре - последица интерференције таласа светлости.

Почетком двадесетог века, Макс Планк (нем. Max Planck), на основу идеја Лудвига Болцмана (нем. Ludwig Boltzmann) формира прву квантну теорију која укључује идеју да је енергија квантизована, односно дискретна, и да се зрачи и апсорбује у "квантима". Алберт Ајнштајн (нем. Albert Einstein) користи ову теорију да објасни фотоелектрични ефекат, а последица је откривање честичне природе светлости. Дакле, светлост је и талас и честица. Луј де Број (фр. Louis de Broglie) 1924. године предлаже дуалну природу честица, а Ервин Шредингер (нем. Erwin Schrödinger) таласном функцијом описује кретање електрона у атому. Овиме је формализована идеја о дуалности талас-честица, према којој све честице имају и таласну природу. У наставку ћемо размотрити још два феномена квантне механике, нарочито битна за квантно рачунарство.



Слика 2.1: Експеримент са двоструким прорезом који показује таласну природу електрона. [9]

2.3 Суперпозиција и важност мерења

Како бисмо објаснили суперпозицију, почећемо описом чувеног мисаоног експеримента Ервина Шредингера, познатом као "Шредингерова мачка". Поједностављено, експеримент се може замислити на следећи начин; у затвореној кутији налази се мачка. Заједно са мачком, у кутији је ампула смртоносног отрова и чекић повезан са механизмом. Механизам је тако подешен да је вероватноћа 0.5 да ће отпустити чекић и поломити ампулу са отровом, усмрћујући мачку, а вероватноћа 0.5 да неће. Питање је да ли је мачка жива или мртва?

Заправо, одговор је чуднији од питања, мачка је и жива и мртва са вероватноћом 0.5 да ћемо отварањем кутије наћи живу мачку и истом вероватноћом супротног исхода. Наравно, квантна механика се бави системима на атомском нивоу, али овај експеримент једноставно приближава једно веома битно питање - да ли се мерењем врши посматрање стања које већ постоји или се мерењем ствара стање. Експериментима је утврђено да је мерење далеко сложеније него што се мислило [4] и да је мерење оно што одређује конкретно стање. Стање честица или система пре мерења је формулисано као *суперпозиција* - комбинација свих могућих стања честице са придруженим вероватноћама чији је збир 1. Мерењем, честица се "спушта"у неко од основних стања у коме остаје и након мерења. Наравно, овде, као и у остатку рада, подразумевамо статистичку (пробабилистичку) интерпретацију квантне механике, иако постоје и друге, попут "Теорије више светова", где приликом отварања кутије долази до стварања два универзума - једног у коме је мачка жива и другог у коме је мртва.

Важно је нагласити аспект суперпозиције који може довести до забуне. Наиме, експериментално[4] је доказано да систем јесте у суперпозицији пре мерења, односно постоји разлика између мерења над системом који је већ у неком од основних стања и над системом који је у суперпозицији. Експериментални доказ саме суперпозиције постоји у виду модификованог експеримента са двоструким прорезом, као и експеримента са два огледала[10], које нећемо описивати, а могу се наћи у литератури. Из свега овога следи да, иако су сваком стању квантног система који је у суперпозицији придружени коефицијенти који могу бити тумачени као вероватноћа исхода, то не значи да је систем у неком од тих стања, а ми немамо информацију о томе. Напротив, систем је у суперпозицији свих стања, а тек мерењем прелази у неко од основних стања.

О суперпозицији ће бити још речи у наредном поглављу, у делу о постулатима квантне механике.

2.4 Уплетеност

Уплетеност је још један важан и интересантан феномен квантне механике који може бити искоришћен за конструкцију квантних алгоритама. Феномен је доказан 2015. године[11], али у тренутку писања овог рада још увек није објашњен у потпуности.

Две или више честица могуће је "уплести", односно довести у такво стање да су њихове особине у корелацији без обзира на њихову удаљеност. Уплитањем честице постају један систем који постоји до тренутка мере-

ња, када ће бити одређена вредност особина обе честице. Првобитна идеја је била да су честице самом акцијом уплитања доведене у крајња стања. Међутим, експериментално је потврђено да то није случај, већ да је тек самим мерењем одређено стање једне честице и тиме истовремено и друге. На пример, ако се уплету два електрона и раздвоје, након што се измери спин (једна од особина електрона) једног електрона, спин другог електрона ће бити супротан. Са друге стране, пре мерења, електрони су чинили сложени систем несепарабилног[1] стања. Овај аспект ће такође бити детаљније објашњен у делу о постулатима квантне механике, као и у делу о телепортовању.

[1] Несепарабилно стање система јесте оно стање у ком се не може разлучити индивидуално стање компоненти система, већ искључиво стање система у целини.

Глава 3

Квантни рачунар и основни алгоритми

Као концепт, квантни рачунар се први пут помиње почетком осамдесетих година прошлог века [2] [12]. Деведесетих настају битни алгоритми [13] [14], а већ крајем прошлог столећа настају и први покушаји физичке реализације квантних рачунара [15] [16].

Квантни рачунар је замишљен као машина која користи концепте квантне механике попут суперпозиције и уплетености како би решила неки проблем брже него што је то могуће на класичним рачунарима. Уобичајена верзија теоријског квантног рачунара је блиска по концептима класичном рачунару и може се посматрати као његово проширење. Уместо битова, користе се кубити који осим два основна стања могу бити и у суперпозицији, а квантна кола преузимају улогу логичких кола класичних рачунара. У наставку ћемо формализовати ову идеју на темељима квантне механике.

3.1 Неопходни математички елементи

Као што је већ речено, квантна механика је, као и физика уопште, математички формализована, тако да је неопходно упутити се у неке појмове линеарне алгебре. Како бисмо се задржали на практичном аспекту, а и избегли претерано улажење у детаље Хилбертових простора и оператора који се користе у квантној механици, претпостављаћемо да се бавимо пре свега векторским простором над комплексним бројевима.

Ако је $A = \begin{bmatrix} z_{11} & z_{12} \\ z_{21} & z_{22} \end{bmatrix}$ матрица комплексних бројева, тада је:

A^T - транспонована матрица

$$A^T = \begin{bmatrix} z_{11} & z_{21} \\ z_{12} & z_{22} \end{bmatrix}$$

A^* - конјугована матрица

$$A^* = \begin{bmatrix} \overline{z_{11}} & \overline{z_{12}} \\ \overline{z_{21}} & \overline{z_{22}} \end{bmatrix}$$

$A^\dagger$ - адјунгована (транспонована конјугована) матрица

$$A^\dagger = \begin{bmatrix} \overline{z_{11}} & \overline{z_{21}} \\ \overline{z_{12}} & \overline{z_{22}} \end{bmatrix}$$

Најважнију новост у математичку нотацију квантне механике увео је Дирак 1939. године [17]. Иако наизглед мала измена, увођење бра-кет нотације је олакшало запис формула и данас постало широко распрострањено:

$|\psi\rangle$ - **кет**, вектор Хилбертовог простора, у нашем случају: $\begin{bmatrix} z_1 \\ z_2 \\ \vdots \\ z_n \end{bmatrix}$

$\langle\psi|$ - **бра**, адјунг $|\psi\rangle$ вектора, у случају матрица над комплексним бројевима, то је транспонована конјугована матрица, односно транспонована матрица конјугата: $\begin{bmatrix} \overline{z_1} & \overline{z_2} & \dots & \overline{z_n} \end{bmatrix}$

$\langle\phi|\psi\rangle$- унутрашњи (скаларни) производ $|\phi\rangle$ и $|\psi\rangle$

Пример 3.1.1 *Ако је* $|\phi\rangle = \begin{bmatrix} 2 \\ 6i \end{bmatrix}$ *и* $|\psi\rangle = \begin{bmatrix} 3 \\ 4 \end{bmatrix}$ *тада је њихов унутрашњи производ:* $\langle\phi|\psi\rangle = \begin{bmatrix} 2 & -6i \end{bmatrix} \begin{bmatrix} 3 \\ 4 \end{bmatrix} = 6 - 24i$

$|\phi\rangle \otimes |\psi\rangle$ - тензорски (векторски) производ $|\phi\rangle$ и $|\psi\rangle$:

$$|\phi\rangle = \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix} \qquad |\psi\rangle = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix}$$

$$\begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix} \otimes \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix} = \begin{bmatrix} a_1 * |\psi\rangle \\ a_2 * |\psi\rangle \\ \vdots \\ a_n * |\psi\rangle \end{bmatrix} = \begin{bmatrix} a_1 * b_1 \\ a_1 * b_2 \\ \vdots \\ a_1 * b_n \\ a_2 * b_1 \\ \vdots \\ a_n * b_n \end{bmatrix}$$

Особине тензорског производа:

1. $(a+b) \otimes c = a \otimes c + b \otimes c$; $a \otimes (b+c) = a \otimes b + a \otimes c$
2. $a \otimes b \neq b \otimes a$
3. Ако је $c = const$, тада $c * (a \otimes b) = c * a \otimes b$

$\forall x \in \{0,1\}_m, y \in \{0,1\}_m : |xy\rangle \stackrel{\text{def}}{=} |x\rangle \otimes |y\rangle$

$\| |\psi\rangle \|$ - норма, $\| |\psi\rangle \| = \sqrt{\langle\psi|\psi\rangle}$

3.2 Постулати квантне механике

Ово поглавље пружа неопходну везу квантне механике и рачунарства објашњавајући суштину квантног рачунара. Кроз постулате квантне механике, представљене су основе конструкције и функционисања квантних рачунара. Поглавље се заснива на једној од најопширнијих књига ове области [18] као и корисним белешкама [19].

Квантни бит

Дефиниција 3.2.1 *Сваком изолованом физичком систему може се придружити Хилбертов простор (комплексни векторски простор са унутрашњим производом) - простор стања система. Стање система је потпуно описано вектором дужине 1 у овом простору.*

За различите физичке системе могу се користити разни простори стања, међутим, у случају квантног рачунарства, битан је само један систем - кубит. Кубит је изоловани физички систем са два базна вектора и представља основну јединицу информације квантног рачунара. Два базна вектора могу бити различито означена и могу узимати различите вредности, али по конвенцији важи следеће:

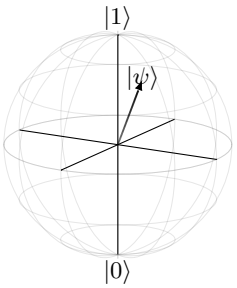
$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

У простору стања са овим базним векторима, свако стање система $|\psi\rangle$ се може описати једначином:

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

где су коефицијенти $\alpha, \beta \in \mathbb{C}$ и важи $\|\alpha\|^2 + \|\beta\|^2 = 1$. Последње следи из услова пробабилистичке интерпретације квантне механике о чему је било речи у претходном поглављу, а биће детаљније разматрано у делу о мерењу. Пример стања кубита јесте:

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



Слика 3.1: Блохова сфера која представља сва могућа стања кубита

Уобичајен начин визуелизације кубита јесте Блохова сфера(фр. Felix Bloch), приказана на слици 3.1. Полови сфере су основна стања кубита, $|0\rangle$ и $|1\rangle$, а сама сфера сва могућа стања суперпозиције.

Ознаке $|0\rangle$ и $|1\rangle$ означавају класична стања бита 0 и 1, односно резултат добијен мерењем кубита у неком од тих стања ће бити класично стање 0 или 1. Ипак, квантно стање кубита које се означава на овај начин зависи од конкретне имплементације, тако да $|0\rangle$ и $|1\rangle$ представљају искључиво ознаке, а не вредности.

Ако се вратимо на дефиницију кубита, приметићемо да су α и β комплексни бројеви. Дакле, на први поглед да би се описао кубит потребна су четири реална броја, по два за сваки од комплексних коефицијената. Како бисмо разјаснили овај детаљ, прећи ћемо на поларне координате $\alpha = r_\alpha e^{i\phi_\alpha}$, $\beta = r_\beta e^{i\phi_\beta}$. Тада је кубит изражем једначином $|\psi\rangle = r_\alpha e^{i\phi_\alpha} |0\rangle + r_\beta e^{i\phi_\beta} |1\rangle$. Међутим, један степен слободе је већ елиминисан ограничењем $\|\alpha\|^2 + \|\beta\|^2 = 1$, тако да је битна само фазна разлика, а не свака фаза појединачно. Тако добијамо $|\psi\rangle = r_\alpha |0\rangle + r_\beta e^{i(\phi_\beta - \phi_\alpha)} |1\rangle$ и могућност да представимо кубит у три димензије у визуелизацији која је и најближа стварном стању кубита.

Еволуција

Дефиниција 3.2.2 *Еволуција (промена стања у току времена) изолованог квантног система се описује унитарним трансформацијама*[1]*. Ако је $|\psi\rangle$ стање система у времену t, а стање $|\psi'\rangle$ у тренутку t', тада $|\psi'\rangle = U|\psi\rangle$ за неки унитарни оператор U који зависи искључиво од t и t'.*

$$U : \mathbb{C}^{2^n} \to \mathbb{C}^{2^n}$$

Карактеристике U:

1. U је линеарно и циркуларно; $U(\alpha|0\rangle + \beta|1\rangle) = \alpha U|0\rangle + \beta U|1\rangle$
2. U чува норму; $\|U|\psi\rangle\| = \||\psi\rangle\| = 1$, за валидно стање $|\psi\rangle$
3. $U^{-1} = U^\dagger$
4. U чува скаларни производ; $U\langle\phi|\psi\rangle = \langle U\phi|U\psi\rangle$

Најчешћи унитарни оператори[2] јесу они који трансформишу систем од једног или два кубита. Неки од њих су дати у наставку:

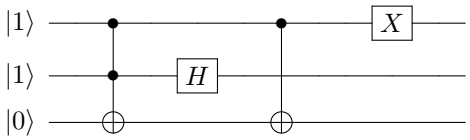
[1] Унитарна трансформација(функција) је изоморфизам између два Хилбертова простора који чува скаларни производ.

[2] Ако су домен и кодомен унитарне трансформације исти, тада се она може назвати унитарним оператором.

Паулијева - X	$X: \begin{cases} \|0\rangle \to \|1\rangle \\ \|1\rangle \to \|0\rangle \end{cases}$	$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
Паулијева - Z	$Z: \begin{cases} \|0\rangle \to \|0\rangle \\ \|1\rangle \to \|-1\rangle \end{cases}$	$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
z - ротација	$R_z(\rho): \begin{cases} \|0\rangle \to \|0\rangle \\ \|1\rangle \to e^{i\rho}\|1\rangle \end{cases}$	$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\rho} \end{bmatrix}$
Адамарова	$H: \begin{cases} \|0\rangle \to \frac{\|0\rangle+\|1\rangle}{\sqrt{2}} \\ \|1\rangle \to \frac{\|0\rangle-\|1\rangle}{\sqrt{2}} \end{cases}$	$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
CNot	$CNot: \begin{cases} \|00\rangle \to \|00\rangle \\ \|01\rangle \to \|01\rangle \\ \|10\rangle \to \|11\rangle \\ \|11\rangle \to \|10\rangle \end{cases}$	$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$
Тофолијева	$CCNot: \begin{cases} \|000\rangle \to \|000\rangle \\ \|001\rangle \to \|001\rangle \\ \|010\rangle \to \|010\rangle \\ \|011\rangle \to \|011\rangle \\ \|100\rangle \to \|100\rangle \\ \|101\rangle \to \|101\rangle \\ \|110\rangle \to \|111\rangle \\ \|111\rangle \to \|110\rangle \end{cases}$	$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$

Две трансформације, Адамарова и Тофолијева, јесу значајне због тога што имају шири смисао од самог трансформисања кубита. Адамарова (фр. Jacques Hadamard) трансформација је битна јер уводи суперпозицију на основу улаза који је у основном стању. Ово је изузетно корисна трансформација што ће бити показано у описаним алгоритмима. Тофолијева (ит. Tommaso Toffoli) трансформација је значајна јер је универзална, односно било која Булова функција се може представити квантним колом које је сачињено само од њих [20]. Овиме је такође демонстрирана универзалност квантног рачунара.

Попут логичких капија у класичном случају, основне унитарне трансформације се могу сматрати "интегрисаним"приликом конструкције квантних кола и могу се употребљавати као словне ознаке без појашњавања. Квантна кола се приказују као хоризонталне линије које представљају кубите, обележене правоугаонике који представљају унитарне трансформације и могу обухватати једну или више линија (кубита) и вертикалне линије које представљају CNot и CCNot трансформације. Почетна вредност кубита дата је на почетку (са леве стране) линије која га представља. У колу постоји вертикална кохерентност, односно сматра се да је свака замишљена вертикална линија исти тренутак времена за све кубите. На слици 3.2 је приказан квантни систем са три кубита.

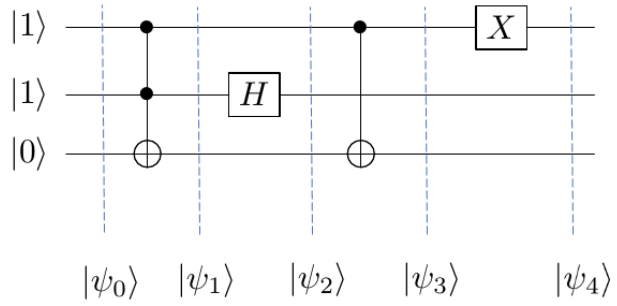


Слика 3.2: Пример квантног кола са CCNot трансформацијом (први и други контролишу трећи кубит), Адамаровом трансформацијом, CNot трансформацијом (први контролише трећи кубит) и Паулијевом X трансформацијом (инверзијом)

Сложени системи

Дефиниција 3.2.3 *Простор стања сложеног квантног система је тензорски производ простора стања физичких система који га чине.*

За систем од n кубита важи$|\phi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \otimes ... \otimes |\psi_n\rangle$ Као пример сложеног система, узећемо 3.2. На слици 3.3 приказан је исти систем са додатим вертикалним линијама које означавају тренутак.



Слика 3.3: Квантно коло са означеним стањима у зависности од времена

Размотрићемо стање система након сваке трнасформације. На почетку стање система је:

$$|\psi_0\rangle = |1\rangle \otimes |1\rangle \otimes |0\rangle$$

Ознаку $\otimes$ је могуће изоставити:

$$|\psi_0\rangle = |1\rangle\,|1\rangle\,|0\rangle$$

Такође је дозвољен и кондензовани запис:

$$|\psi_0\rangle = |110\rangle$$

Стање након примене CCNot трансформације:

$$|\psi_1\rangle = |111\rangle$$

Након примене Адамарове трансформације, други кубит је у суперпозицији:

$$|\psi_2\rangle = |1\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} \otimes |1\rangle$$
$$= \frac{1}{\sqrt{2}}(|101\rangle - |111\rangle)$$

Вредност првог кубита је $|1\rangle$, као и трећег, те се применом трансформације трећи кубит мења у $|0\rangle$:

$$|\psi_3\rangle = \frac{1}{\sqrt{2}}(|100\rangle - |110\rangle)$$

На крају, применом Паулијеве трансформације која је заправо инверзија, мења се и први кубит:

$$|\psi_4\rangle = \frac{1}{\sqrt{2}}(|000\rangle - |010\rangle)$$

Уплетени системи

Неки сложени системи, попут претходно приказаног, могу да се разложе на компоненте, односно на стања која их чине:

$$\frac{1}{\sqrt{2}}(|000\rangle - |010\rangle) = |0\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} \otimes |0\rangle$$

Са друге стране, постоје и системи који не могу, попут: $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$. Ови системи представљају уплетене системе.

Дефиниција 3.2.4 *$|\psi\rangle \in \mathbb{C}^{2^n}$ је уплетен ако за све $n1, n2$ такве да $n_1 + n_2 = n$ важи:*

$$\forall\, |\psi_1\rangle \in \mathbb{C}^{2^n_1}, |\psi_2\rangle \in \mathbb{C}^{2^n_2} : |\psi\rangle \neq |\psi_1\rangle \otimes |\psi_2\rangle$$

Ови системи су од пресудне важности за протоколе комуникације својствене квантном рачунарству попут телепортације и супергустог кодирања. Од посебног значаја су четири максимално уплетена двокубитна стања, такозвана Белова стања:

$$|\psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$
$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$
$$|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$
$$|\phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

Ова стања су први пут представљена 1964. у раду Џона Бела (ен. John Bell) о уплетеним стањима[21], а њихов значај потиче од чињенице да имају највећу могућу меру корелације од $2\sqrt{2}$. Белово мерење јесте мерење Беловог стања. У случају да кубити нису уплетени, односно у Беловом стању, Белово мерење ће их прво довести у одговоарајуће Белово стање.

Квантно мерење

Дефиниција 3.2.5 *Квантна мерења су описана скупом оператора M_m на систему над којим се врши мерење. Индекс m се односи на могуће исходе експеримената. Ако је стање система непосредно пре мерења $|\psi\rangle$, тада је вероватноћа резултата (класичног исхода) m при мерењу:*

$$P(m) = \langle\psi| M_m^\dagger M_m |\psi\rangle = \| M_m |\psi\rangle \|^2$$

Стање система након мерења је:

$$\frac{M_m |\psi\rangle}{\sqrt{\langle\psi| M_m^\dagger M_m |\psi\rangle}} = \frac{M_m |\psi\rangle}{\| M_m |\psi\rangle \|}$$

Како вероватноће морају у суми бити 1 и оператори мерења морају да задовоље једначину:

$$\sum_m \langle\psi| M_m^\dagger M_m |\psi\rangle = I$$

Мерење није унитарни оператор. Ово доводи до тога да је његовом применом неповратно изгубљено стање система које му је претходило.

Стандардно мерење

Стандардно мерење у квантном рачунарству је представљено операторима $M_0 = |0\rangle\langle 0|$ и $M_1 = |1\rangle\langle 1|$. Приметимо да је ефекат било ког мерења $M_\phi = |\phi\rangle\langle\phi|$ пројекција на ϕ, па се тако и при стандардном мерењу добијају вредности пројекције на неко од класичних стања. Резултат мерења, осим вредности 0 или 1, јесте и спуштање самог стања у основно стање $|0\rangle$ или $|1\rangle$. У наставку су детаљније приказане особине стандардног мерења.

$$M_0 = |0\rangle\langle 0| = \begin{bmatrix}1\\0\end{bmatrix}\begin{bmatrix}1 & 0\end{bmatrix} \qquad M_1 = |1\rangle\langle 1| = \begin{bmatrix}0\\1\end{bmatrix}\begin{bmatrix}0 & 1\end{bmatrix}$$

$$M_0 |0\rangle = |0\rangle\langle 0|0\rangle = |0\rangle \qquad M_1 |1\rangle = |1\rangle\langle 1|1\rangle = |1\rangle$$

$$M_0 |1\rangle = |0\rangle\langle 0|1\rangle = 0 \qquad M_1 |0\rangle = |1\rangle\langle 1|0\rangle = 0$$

У општем случају, ако је $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, тада је дејство оператора:

$$M_0 |\psi\rangle = \alpha |0\rangle \qquad M_1 |\psi\rangle = \beta |1\rangle$$

Стање система након мерења M_0 ће бити:

$$\frac{M_0 |\psi\rangle}{\sqrt{\langle\psi| M_0^\dagger M_0 |\psi\rangle}} = \frac{\alpha|0\rangle}{\|\alpha\|} = |0\rangle$$

Односно, након мерења M_1:

$$\frac{M_1 |\psi\rangle}{\sqrt{\langle\psi| M_1^\dagger M_1 |\psi\rangle}} = \frac{\beta|1\rangle}{\|\beta\|} = |1\rangle$$

Теорема 3.2.1 *(Каскадно мерење) Нека су M_m и L_l два скупа оператора мерења. Узастопно мерење оператором из скупа M_m, па оператором из скупа L_l физички је еквивалентно мерењу оператором из скупа N_{ml}, где је $N_{ml} = M_m L_l$.*

Теорема 3.2.2 *(Неразлучивост квантних стања) Неортогонална квантна стања не могу бити прецизно разликована, односно измерена са потпуном тачношћу.*

Теореме 3.2.1 и 3.2.2 наводимо без доказа, али ћемо дати интуицију иза њих. Прва теорема је директна последица саме дефиниције мерења. Друга теорема не следи директно, али је такође последица дефиниције. Вероватноћа погрешног мерења се не своди на 0, као код ортогоналних стања, већ увек постоји могућност грешке. Комплетан доказ се може наћи у [18].

3.3 Мешана стања

Дефиниција 3.3.1 *Мешано стање је статистички ансамбл чистих стања са расподелом вероватноћа $(|\psi_i\rangle, p_i)$.*

Мешана стања се јављају у случајевима када није познато стање система или елемената система, али су позната његова могућа стања и њихова вероватноћа.

3.4 Телепортација

Телепортација као концепт подразумева размену "кубита", односно информације о стању кубита, без физичке размене кубита између две стране у комуникацији. Протокол се заснива на квантној уплетености једног пара кубита који се користе као веза између саговорника [22]. Циљ је да се пренесе стање кубита $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ без преноса самог кубита. Опис је дат у наставку:

Алиса и Боб деле (први је код Алисе, други код Боба) уплетени пар кубита q_a и q_b у стању $|\phi\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$. Алиса жели да пошаље Бобу кубит $|\psi\rangle$. Она то чини на следећи начин:

1. Врши Белово мерење свог кубита $|\psi\rangle$ и уплетеног кубита $|q_a\rangle$. Како два кубита нису уплетена, Белово мерење их прво доводи у Белово стање применом CNot и Адамаровог оператора, а затим врши мерење којим се добијају класична стања два кубита

2. Шаље Бобу два класична бита p и a која садрже резултате мерења

Након што је примио два класична бита, Боб ће искористити свој уплетени кубит (који је Алиса мерењем спустила у класично стање) како би код себе направио копију оригиналног Алисиног кубита $|\psi\rangle$:

1. У зависности од бита добијених од Алисе, Боб примењује одговарајући оператор на свој кубит $|q_b\rangle$:

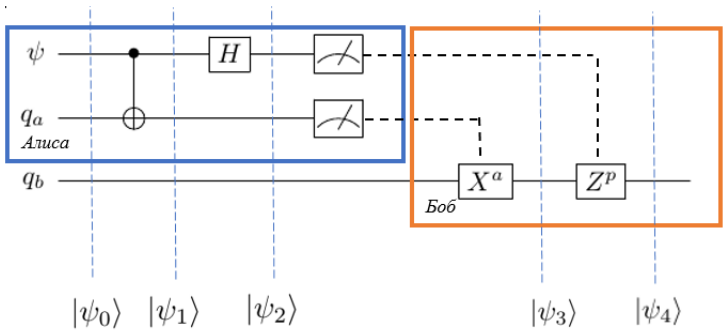
а) Ако су вредности битова 00, не примењује ништа (примењује I)

б) Ако су вредности битова 01, примењује X

в) Ако су вредности битова 10, примењује Z

г) Ако су вредности битова 11, примењује X и Z

Вредност Бобовог кубита сада одговара Алисином оригиналном кубиту



Слика 3.4: Квантно коло телепортације једног кубита од Алисе Бобу

Размотрићемо шта се дешава приликом телепортације у колу датом на слици 3.4, ако су Алисин и Бобов кубит уплетени у Белово стање $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$:

$$
\begin{aligned}
|\psi_0\rangle &= |\psi\rangle\,|\phi^+\rangle = (\alpha\,|0\rangle + \beta\,|1\rangle)\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\
&= \frac{1}{\sqrt{2}}(\alpha\,|0\rangle\,(|00\rangle + |11\rangle) + \beta\,|1\rangle\,(|00\rangle + |11\rangle) \\
|\psi_1\rangle &= \frac{1}{\sqrt{2}}(\alpha\,|0\rangle\,(|00\rangle + |11\rangle) + \beta\,|1\rangle\,(|10\rangle + |01\rangle) \\
|\psi_2\rangle &= \frac{1}{2}(\alpha(|0\rangle + |1\rangle)(|00\rangle + |11\rangle) + \beta(|0\rangle - |1\rangle)(|10\rangle + |01\rangle) \\
&= \frac{1}{2}(|00\rangle\,(\alpha\,|0\rangle + \beta\,|1\rangle) + |01\rangle\,(\alpha\,|1\rangle + \beta\,|0\rangle) + |10\rangle\,(\alpha\,|0\rangle - \beta\,|1\rangle) + |11\rangle\,(\alpha\,|1\rangle - \beta\,|0\rangle))
\end{aligned}
$$

p	a	$\lvert\psi_2\rangle$	$\lvert\psi_3\rangle$	$\lvert\psi_4\rangle$
0	0	$\alpha\,\lvert0\rangle + \beta\,\lvert1\rangle$	$\alpha\,\lvert0\rangle + \beta\,\lvert1\rangle$	$\alpha\,\lvert0\rangle + \beta\,\lvert1\rangle$
0	1	$\alpha\,\lvert1\rangle + \beta\,\lvert0\rangle$	$\alpha\,\lvert0\rangle + \beta\,\lvert1\rangle$	$\alpha\,\lvert0\rangle + \beta\,\lvert1\rangle$
1	0	$\alpha\,\lvert0\rangle - \beta\,\lvert1\rangle$	$\alpha\,\lvert0\rangle - \beta\,\lvert1\rangle$	$\alpha\,\lvert0\rangle + \beta\,\lvert1\rangle$
1	1	$\alpha\,\lvert1\rangle - \beta\,\lvert0\rangle$	$\alpha\,\lvert0\rangle - \beta\,\lvert1\rangle$	$\alpha\,\lvert0\rangle + \beta\,\lvert1\rangle$

Табела 3.2: Анализа стања Бобовог уплетеног кубита кола 3.4. По окончању протокола, Бобов кубит је у стању кубита који је Алиса послала.

3.5 Супергусто кодирање

Суперпозиција као моћан алат у квантном рачунарству има два аспекта, рачунарски, када се користи ради паралелизације и информациони када се користи за пренос више информација од класичних бита. Као што смо већ нагласили, кубит може бити у неком од два основна стања или у било ком стању на Блоховој сфери. Са друге стране, информације чувамо уз помоћ само два основна стања и логично питање је како да у том контексту искористимо све могућности кубита. Одговор је употреба уплетености.

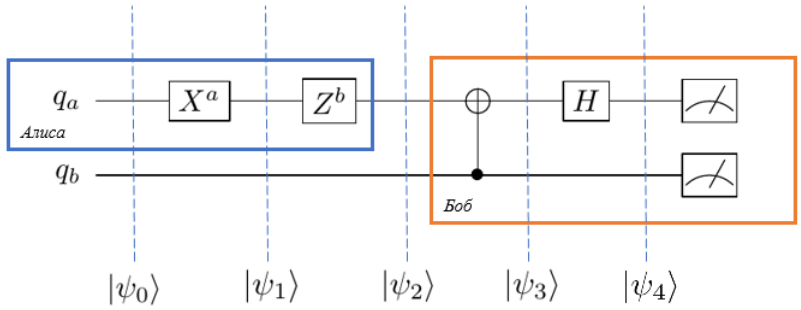
Супергусто кодирање[23] се најлакше описује на примеру комуникације између два ентитета које ћемо звати Алиса и Боб. Нека Алиса и Боб деле (први је код Алисе, други код Боба) уплетени пар кубита q_a и q_b у стању $|\psi\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$. Алиса жели да пошаље Бобу два бита, $a, b \in [0, 1]$. Она то чини на следећи начин:

1. Ако је први бит $a = 1$, примењује X оператор на свој кубит q_a
2. Ако је други бит $b = 1$, примењује Z оператор на свој кубит q_a
3. Шаље свој кубит Бобу

Боб прима кубит q_a од Алисе и, како би добио информацију:

1. Примењује CNot оператор на свој и Алисин кубит$q_a q_b$
2. Примењује Адамаров оператор на Алисин кубит
3. Врши мерење оба кубита; вредност првог кубита је вредност другог бита који је Алиса послала, а вредност другог прва.

Тиме је само једним слањем кубита послата информација од два бита. Јасно је да су Алиса и Боб морали у једном тренутку да добију по кубит уплетеног пара, тако да је заправо у почетку извршено једно слање (преузимање) кубита, а касније и друго које је овде приказано, али поента овог примера је пре свега осликавање могућности квантних рачунара у домену информација.



Слика 3.5: Квантно коло два уплетена кубита Алисе и Боба

У односу на телепортацију, важна разлика јесте што при супергустом кодирању постоји размена кубита, што осликава различите намене две методе. Иако обе користе уплетеност, главни циљ телепортације је избегавање размене кубита између два ентитета. Супергусто кодирање, са друге

a	b	$\|\psi_0\rangle$	$\|\psi_1\rangle$	$\|\psi_2\rangle$	$\|\psi_3\rangle$	$\|\psi_4\rangle$
0	0	$\frac{\|00\rangle+\|11\rangle}{\sqrt{2}}$	$\frac{\|00\rangle+\|11\rangle}{\sqrt{2}}$	$\frac{\|00\rangle+\|11\rangle}{\sqrt{2}}$	$\frac{\|00\rangle+\|10\rangle}{\sqrt{2}}$	$\|00\rangle$
0	1	$\frac{\|00\rangle+\|11\rangle}{\sqrt{2}}$	$\frac{\|00\rangle+\|11\rangle}{\sqrt{2}}$	$\frac{\|00\rangle-\|11\rangle}{\sqrt{2}}$	$\frac{\|00\rangle-\|10\rangle}{\sqrt{2}}$	$\|10\rangle$
1	0	$\frac{\|00\rangle+\|11\rangle}{\sqrt{2}}$	$\frac{\|10\rangle+\|01\rangle}{\sqrt{2}}$	$\frac{\|10\rangle+\|01\rangle}{\sqrt{2}}$	$\frac{\|11\rangle+\|01\rangle}{\sqrt{2}}$	$\|01\rangle$
1	1	$\frac{\|00\rangle+\|11\rangle}{\sqrt{2}}$	$\frac{\|10\rangle+\|01\rangle}{\sqrt{2}}$	$\frac{-\|10\rangle+\|01\rangle}{\sqrt{2}}$	$\frac{-\|11\rangle+\|01\rangle}{\sqrt{2}}$	$\|11\rangle$

Табела 3.3: Анализа стања уплетених кубита 3.5

стране, тежи ка смањењу броја кубита који су неопходни за размену информација.

На крају, приметићемо једну могућу замерку. Наиме, претпоставка је да се информација чува у класичним битовима. Међутим, није незамислив систем у коме би се информације чувале у виду стања самог кубита на много сложенији начин.

3.6 Физичка имплементација квантних рачунара и квантни програмски језици

Још од настанка концепта квантног рачунара, разни тимови су покушавали да направе машину која би имала карактеристике квантног система, односно која би била у складу са постулатима квантне механике, примењеним на рачунарски концепт бита. У том смислу, формирани су и оквири у којима би таква машина требало да ради, попут Ди Виченцових постулата [24].

Прве физичке реализације делимично квантних рачунара развијене су у Великој Британији [15] и Америци [16] и биле су засноване на магнетној резонанцији. То су такозване НМР машине, а не могу се сматрати квантним рачунаром јер не омогућавају уплетеност, кључни елемент телепортације и квантне комуникације. Данас, квантни рачунари се најчешће заснивају на суперпроводницима [25], имају неколико десетина кубита, а на њиховом развоју раде тимови ИБМ-а [26], Гугл-а [27] и других великих компанија.

Са друге стране, квантни рачунари представљају велику промену не само у физичкој конструкцији, већ и у софтверским могућностима рачунара. То је довело до развоја нових програмских језика предвиђених за рад на квантним рачунарима. Две парадигме које имају највише представника јесу императивна (QCL, LanQ) и функционална (QML, Quipper). Ови језици подразумевају синтаксу популарних програмских језика попут C-а и Haskell-а уз додатне уграђене инструкције које се изводе над кубитима као и уграђене рутине за које се може претпоставити да ће бити стандардно имплементиране на квантним рачунарима.

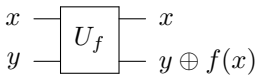
Глава 4

Предност квантних рачунара - Дојч-Јоза алгоритам

Дојч-Јоза алгоритам[28] један је од најједноставнијих детерминистичких алгоритама квантног рачунарства, али истовремено и најбољи практични пример предности квантних над класичним рачунарима. Алгоритам су креирали Дејвид Дојч (енг. David Deutsch) и Ричард Јоза (енг. Richard Jozsa) 1992. године са специфичним циљем демонстрације могућности квантних рачунара. Како би се то постигло, алгоритам је посебно дизајниран да буде тежак при извршавању на класичном рачунару, али не и при извршавању на квантном. Прво ћемо представити првобитну верзију алгоритма коју је дизајнирао Дојч, а односи се на одређивање типа функције у бинарном систему.

Нека је $f : B \to B, B = \{0, 1\}$ функција Булове алгебре која је константна, резултата увек 0 или увек 1, или је балансирана, резултата 0 при једном улазу, а 1 при другом. При томе, сама функција није позната, односно алгоритам мора да даје исправно решење за сваку функцију која одговара условима. У класичном случају, задата функција мора да се изврши два пута како би се утврдило да ли је балансирана или константна. Међутим, у квантном случају неопходан је само један пролазак кроз функцију и то на следећи начин.

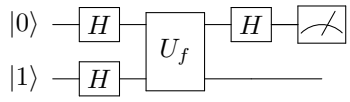
Сама бинарна функција не представља унитарни оператор[1] јер не мора бити бијекција, те као оператор не задовољава услов инвертибилности. Како би се функција представила у квантном систему, дефинишемо нови унитарни оператор U_f коме су улаз вредности два кубита, а излаз такође два (трансформисана) кубита. Први кубит улаза чува вредност која ће представљати улазне параметре фунције f, а други кубит служи за уписивање резултата.



Слика 4.1: Унитарни оператор који представља функцију која се тестира

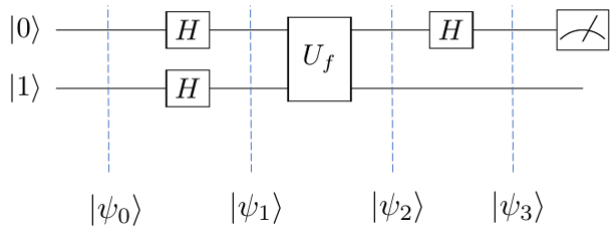
[1] Поглавље 3.2

Квантна варијанта функције f представља квантно пророчиште (енг. oracle), односно алгоритам се не бави њеном имплементацијом, али захтева да она не доводи до декохеренције[2] улазног стања. Да би се избегло двоструко извршавање функције користи се суперпозиција чији је ефекат паралелизација, те се једним проласком испитују оба могућа случаја. За постизање паралелизације користи се Адамарова трансформација, а до тачног распореда капија (оператора) у квантном колу могуће је доћи наивном методом, односно комбиновањем капија до задовољавајућег решења. Оно је представљено на слици 4.2.



Слика 4.2: Поставка квантног кола Дојчовог алгоритма

Разматрањем стања кола при свакој трнсформацији, биће појашњени разлози такве конструкције квантног кола.



Почетно стање представља два улазна кубита:

$$|\psi_0\rangle = |0\rangle\,|1\rangle \tag{4.1}$$

Након Адамарових трансформација, стање кола је:

$$|\psi_1\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}\,\frac{|0\rangle - |1\rangle}{\sqrt{2}} \tag{4.2}$$

Дејство унитарног оператора U_f ће бити размотрено у два одвојена случаја, у зависности од вредности функције f:

$$f(x) = 0 \qquad\qquad f(x) = 1 \tag{4.3}$$

$$y \oplus |0\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \oplus |0\rangle \qquad y \oplus |1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \oplus |1\rangle \tag{4.4}$$

$$= \frac{1}{\sqrt{2}}(|0\rangle \oplus |0\rangle - |1\rangle \oplus |0\rangle) \qquad = \frac{1}{\sqrt{2}}(|0\rangle \oplus |1\rangle - |1\rangle \oplus |1\rangle) \tag{4.5}$$

$$= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \qquad = \frac{1}{\sqrt{2}}(|1\rangle - |0\rangle) \tag{4.6}$$

[2] Декохеренција - нарушавање квантног стања, спуштање честице у класично стање.

Из овога следи:

$$y \oplus f(x) = (-1)^{f(x)} \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \tag{4.7}$$

Даље следи да се оператор може дефинисати на следећи начин:

$$U_f(|x\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)) = (-1)^{f(x)} |x\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \tag{4.8}$$

Стање након примене унитарног оператора ће бити:

$$\begin{aligned} |\psi_2\rangle &= U_f(\frac{|0\rangle + |1\rangle}{\sqrt{2}} \frac{|0\rangle - |1\rangle}{\sqrt{2}}) \\ &= \frac{1}{2}((-1)^{f(|0\rangle)} |0\rangle (|0\rangle - |1\rangle) + (-1)^{f(|1\rangle)} |1\rangle (|0\rangle - |1\rangle)) \end{aligned} \tag{4.10}$$

Ако је функција константна, $f(0) = f(1) = const.$:

$$\begin{aligned} |\psi_2\rangle &= \frac{1}{2}((-1)^{f(|0\rangle)}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle)) \\ &= (-1)^c \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{aligned} \tag{4.12}$$

Ако је функција балансирана, $f(0) \neq f(1)$:

$$\begin{aligned} |\psi_2\rangle &= \frac{1}{2}((-1)^c |0\rangle (|0\rangle - |1\rangle) + (-1)^{1-c} |1\rangle (|0\rangle - |1\rangle)) \\ &= \frac{1}{2}((-1)^c |0\rangle (|0\rangle - |1\rangle) + (-1)(-1)c |1\rangle (|0\rangle - |1\rangle)) \\ &= \frac{1}{2}(-1)^c(|0\rangle - |1\rangle)(|0\rangle - |1\rangle) \\ &= (-1)^c \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{aligned} \tag{4.14}$$

На крају, како би се из стања првог бита добила информација о функцији, неопходно је применити Адамарову капију још једном како би се из суперпозиције добило основно стање:

$$|\psi_3\rangle = \begin{cases} \frac{1}{\sqrt{2}}(-1)^c|\mathbf{0}\rangle(|0\rangle - |1\rangle), \text{ако је функција константна} \\ \frac{1}{\sqrt{2}}(-1)^c|\mathbf{1}\rangle(|0\rangle - |1\rangle), \text{ако је фунција балансирана} \end{cases} \tag{4.15}$$

Резултат анализе квантног кола потврђује да је на овај начин могуће добити решење задатог проблема на основу крајње вредности првог кубита.

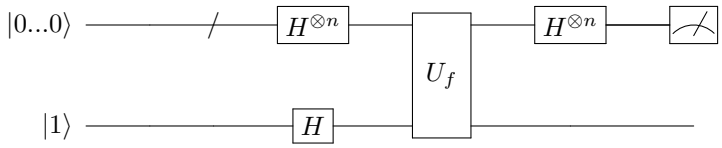
Приликом анализе алгоритма, користили смо се разлагањем првог улазног кубита оператора U_f. Међутим, пророчиште по дефиницији не врши разлагање, односно декохеренцију, већ извршава операцију над суперпонираним кубитом. На тај начин функција се извршава само једном, за разлику од два пута колико се извршава у класичном случају.

Сада ћемо размотрити генерализацију Дојчовог алгоритма на функције са доменом природних бројева. Нека је $f : B^n \to B, B = \{0, 1\}$ функција

Булове алгебре која је константна или балансирана. Од алгоритма се захтева да одреди о каквој функцији се ради што ефикасније. У најгорем класичном случају, неопходно је испитати $n/2+1$ улаза да би се утврдило о каквој функцији се ради. Са друге стране, у квантном случају, временска сложеност је само $\mathcal{O}(1)$.

$$f : B^n \to B \begin{cases} (\forall x \in B^n) f(x) = c \\ \begin{cases} (\forall x \in X), f(x) = 0 \\ (\forall y \in Y), f(y) = 1 \end{cases} \end{cases} , |X| = |Y| = |B^n|/2, X \cup Y = B^n$$

Квантно коло Дојч-Јоза алгоритма је слично колу коришћеном у оквиру Дојчовог алгоритма уз разлику што има $n+1$ улаза, а унитарни оператор је такође модификован за нову улазну димензију.



Слика 4.3: Поставка квантног кола Дојч-Јоза алгоритма

Како смо већ детаљно образложили Дојчов алгоритам, у овом делу се нећемо бавити детаљима Дојч-Јоза алгоритма, имајући у виду да је идеја која омогућава убрзање потпуно иста. Сви могући улазни аргументи се уз помоћ Адамарове трансформације суперпонирају у ново стање које представља улаз за пророчиште-квантну функцију. Оно због чега је овај алгоритам битан јесте убрзање које пружа. Док Дојчов алгоритам само пружа двоструко убрзање, Дојч-Јоза алгоритам потпуно мења ред временске сложености од линеарне $\mathcal{O}(n)$ на константну $\mathcal{O}(1)$. Сложеност класичног алгоритма јесте у провери, неопходно је испитати бар половину свих могућих улаза функције да би се утврдило да ли је балансирана, што доводи до сложености $\mathcal{O}(n)$. У квантном случају, као и у Дојчовом алгоритму, сложеност је $\mathcal{O}(1)$ јер ће се функција (пророчиште) увек позивати само једном.

Постоје два елемента овог алгоритма која могу деловати збуњујуће. Прво, у оригиналној поставци функција која се испитује је дата класично, а у самом алгоритму се разматра њена квантна верзија, што су неки аутори посебно нагласили[29]. Међутим, тако нешто није у супротности са самом идејом да функција која се тестира мора бити имплементирана у самој машини на којој ће се испитивати њене карактеристике. У класичном случају, функција ће бити имплементирана и моћи ће да се изврши на класичном рачунару. У квантном случају, функција ће бити имплементирана на квантном рачунару и моћи ће да се изврши, а као што смо видели у претходном поглављу, то је могуће уз помоћ Тофолијевих трансформација за било коју функцију. Даље, управо због тога што је имплементирана на квантном рачунару, функција ће моћи да се изврши и у случају када је улаз суперпозиција, па није неопходно тестирати одвојено све случајеве.

Други потенцијално збуњујући елемент јесте сложеност, јер се за сваки кубит врше и додатне Адамарове трансформације. Ту долазимо до из-

узетка у ефикасности алгоритма, а то јесу просте функције. Ако је цена извршавања функције иста или мања од цене извршавања Адамарове трансформације, класично тестирање функције је ефиксаније. Ипак, ако се узме у обзир да је Адамаров оператор једна од основних трансформација које би биле имплементиране на квантном рачунару, у општем случају овај алгоритам јесте бржи од класичног.

Глава 5

Квантни алгоритми засновани на Фуријеовој трансформацији

У претходном поглављу описали смо први алгоритам који је указао на предност квантних над класичним рачунарима и који је подстакао велики напредак у конструкцији квантних алгоритама. У овом поглављу, описаћемо настанак и потенцијалну употребу квантних алгоритама заснованих на Фуријеовој трансформацији кроз неколико примера. Кроз цело поглавље, пратићемо развој квантног алгоритма, од основних алгоритама (Квантна Фуријеова трансформација и Процена фазе), преко комплексног алгоритма (Шоров алгоритам) и примене, до последица по постојеће класичне алгоритме.

5.1 Квантна Фуријеова трансформација

Фуријеова трансформација слика простор стања величине 2^n из домена амплитуда у домен фреквенција [19] и представља битан математички алат у разним областима науке и технике [30]. У квантном рачунарству она је много значајнија као градивни елемент сложенијих алгоритама, а нарочито битна за ефикасну факторизацију на квантним рачунарима. Дискретна Фуријеова трансформација (ДФТ) у основи представља пресликавање вектора комплексних бројева дужине N у други вектор исте дужине, при чему се сваки елемент првог слика у суму елемената другог вектора.

Квантном Фуријеовом трансформацијом се назива имплементација класичне инверзне ДФТ квантним колима. Поћи ћемо од њене класичне дефиниције, користећи нотацију из[18]:

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{\frac{2\pi i j k}{N}} \tag{5.1}$$

Овај облик трансформације се добија употребом поларних координата, y_k и x_j су комплексни бројеви, а разлика квантне у односу на дискретну Фуријеову трансформацију је знак експонента. Преведено на ниво квантне механике, ДФТ за ортонормирану базу $|0\rangle \ldots |N-1\rangle$ има облик:

$$|j\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} |k\rangle \, e^{\frac{2\pi i j k}{N}} \tag{5.2}$$

Тада у општем случају, за произвољно стање, квантна Фуријеова трансформација јесте пресликавање:

$$\sum_{j=0}^{N-1} x_j \left|j\right\rangle \rightarrow \sum_{k=1}^{N-1} y_k \left|k\right\rangle \tag{5.3}$$

где се вредности y_k одређују класичном методом. Ради лакше имплементације у квантном колу, овај израз се даље трансформише. Подразумевајући да су k и j бинарни бројеви, могуће је извршити следеће трансформације:

$$\begin{aligned}
\left|j\right\rangle &\rightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \left|k\right\rangle e^{\frac{2\pi i j k}{N}}, N = 2^n \\
&= \frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} \left|k\right\rangle e^{2\pi i j k/2^n} \\
&= \frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} e^{2\pi i j \sum_{l=1}^{n} k_l 2^{n-l}/2^n} \left|k\right\rangle \\
&= \frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} e^{2\pi i j \sum_{l=1}^{n} k_l 2^{-l}} \left|k\right\rangle \\
&= \frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} e^{2\pi i j k_1 2^{-1}} e^{2\pi i j k_2 2^{-2}} ... e^{2\pi i j k_n 2^{-n}} \left|k\right\rangle \\
&= \frac{1}{2^{n/2}} \sum_{k_1=0}^{1} \sum_{k_2=0}^{1} ... \sum_{k_n=0}^{1} e^{2\pi i j k_1 2^{-1}} e^{2\pi i j k_2 2^{-2}} ... e^{2\pi i j k_n 2^{-n}} \left|k_1 k_2 ... k_n\right\rangle \\
&= \frac{1}{2^{n/2}} \sum_{k_1=0}^{1} e^{2\pi i j k_1 2^{-1}} \left|k_1\right\rangle \sum_{k_2=0}^{1} e^{2\pi i j k_2 2^{-2}} \left|k_2\right\rangle ... \sum_{k_n=0}^{1} e^{2\pi i j k_n 2^{-n}} \left|k_n\right\rangle \\
&= \frac{1}{2^{n/2}} (\left|0\right\rangle + e^{2\pi i j 2^{-1}} \left|1\right\rangle)(\left|0\right\rangle + e^{2\pi i j 2^{-2}} \left|1\right\rangle) ... (\left|0\right\rangle + e^{2\pi i j 2^{-n}} \left|1\right\rangle)
\end{aligned} \tag{5.5}$$

У наставку ћемо се бавити само једном компонентом, где ћемо j представити сумом, као што је већ урађено са k:

$$\begin{aligned}
e^{2\pi i j 2^{-k}} &= e^{2\pi i \sum_{l=1}^{n} j_l 2^{n-l} 2^{-k}} \\
&= e^{2\pi i j_1 2^{n-1} 2^{-k}} e^{2\pi i j_2 2^{n-2} 2^{-k}} ... e^{2\pi i j_n 2^{n-n} 2^{-k}} \\
&= e^{2\pi i j_1 2^{n-1-k}} e^{2\pi i j_2 2^{n-2-k}} ... e^{2\pi i j_n 2^{-k}}
\end{aligned} \tag{5.7}$$

За бинарни индекс $j_l = 0$ постоје две могуће вредности, ако је вредност 0, тада ће вредсност $e^{2\pi i j 2^{-k}}$ бити 1. Са друге стране за индекс $j_l = 1$ можемо добити две вредности степена са различитим последицама:

$$e^{2\pi i j_l 2^{n-l-k}} = \begin{cases} e^{2\pi i 2^{n-l-k}} = e, 2^{n-l-k} \geq 0 \\ e^{2\pi i 0.j_{n-k} ... j_n}, 2^{n-l-k} < 0 \end{cases} \tag{5.8}$$

Прва вредност је последица тога што је експонент умножак 2π, а друга тога што (могући) степен зависи од k, чиме је ограничена и вредност l. Из

тога следи облик Фуријеове трансформације који ће бити имплементиран квантним колом:

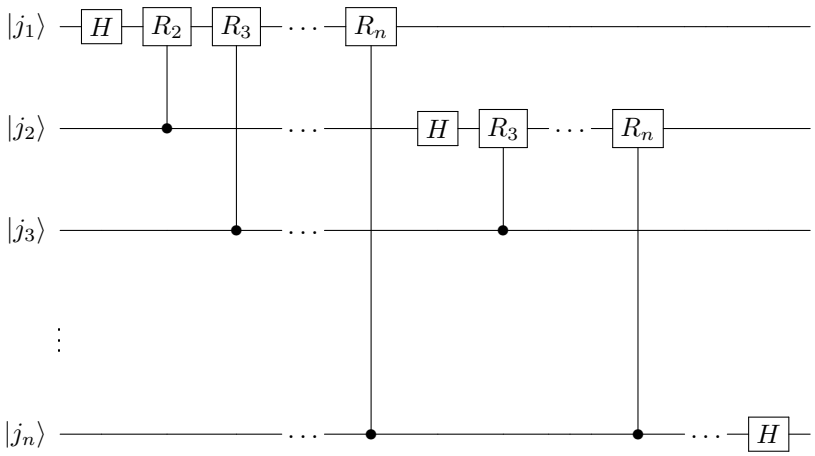
$$\frac{1}{2^{n/2}}(|0\rangle + e^{2\pi 0.j_n}|1\rangle)(|0\rangle + e^{2\pi i 0.j_{n-1}j_n}|1\rangle)...(|0\rangle + e^{2\pi i 0.j_1 j_2 ... j_n}|1\rangle) \quad (5.9)$$

Овакав израз можемо да имплементирамо коришћењем унитарних трансформација које смо већ описали, Адамарове трансформације и z-ротације и које имају облик:

z - ротација $\quad R_z(\theta): \begin{cases} |0\rangle \to |0\rangle \\ |1\rangle \to e^{i\rho}|1\rangle \end{cases} \quad \begin{bmatrix} 1 & 0 \\ 0 & e^{i\rho} \end{bmatrix}$

Адамарова $\quad H: \begin{cases} |0\rangle \to \frac{|0\rangle+|1\rangle}{\sqrt{2}} \\ |1\rangle \to \frac{|0\rangle-|1\rangle}{\sqrt{2}} \end{cases} \quad \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$

Употребом само ове две трансформације, добија се имплементација Фуријеове трансформације представљена на 5.1.



Слика 5.1: Имплементација Фуријеове трансформације у квантном колу

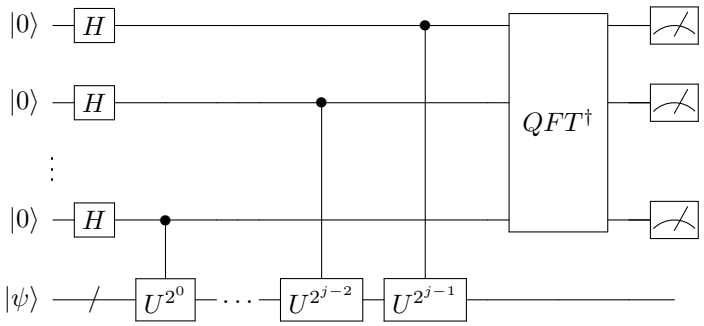
Са аспекта сложености, Квантна Фуријеова трансформација је квадратне сложености, док је Брза Фуријеова трансформација експоненцијалне сложености. Међутим, ово се односи само на неке примене, то јесте на оне случајеве употребе који подразумевају квантно окружење, што искључује велики број тренутних примена ове трансформације. Са друге стране, КФТ има веома битну улогу у неким сложенијим квантним алгоритмима.

5.2 Процена квантне фазе

Приликом описивања Блохове сфере поменули смо релативну фазу кубита. Иако за индивидуални кубит не представља битну одлику, фаза јесте значајна приликом трансформација и операција над више кубита.

Нека је U унитарна операција, таква да постоји сопствени вектор $|\psi\rangle$ за који важи $U|\psi\rangle = e^{2\pi i\phi}|\psi\rangle$. Проблем јесте одредити фазу ϕ. Алгоритам

који одговара на ово питање састоји се из више делова, а представљен је квантним колом на слици 5.2.



Слика 5.2: Имлементација процене фазе у квантном колу

Квантно коло за процену фазе састоји се из два дела - регистра кубита. Први регистар чини суперпонирани сет кубита који контролишу примену трансформације U^{2^j}. Други сет представља сопствени вектор $|\psi\rangle$ за који сматрамо да је познат. Како бисмо објаснили овакву структуру, уочимо прво да важи $U^{2^j} = e^{2\pi i\phi 2^j}$. Из овога следи да ће након примене свих U^{2^j} трансформација (као последица контролне улоге) стање првог регистра бити:

$$1/2^{t/2}(|0\rangle + e^{2\pi i\phi 2^{j-1}}|1\rangle)(|0\rangle + e^{2\pi i\phi 2^{j-2}}|1\rangle)\dots(|0\rangle + e^{2\pi i\phi 2^0}|1\rangle)$$

Ако претпоставимо да се ради о идеалном случају, где се дужина регистра и дужина записа фазе поклапају, овај израз постаје:

$$1/2^{t/2}(|0\rangle + e^{2\pi i 0,\phi_j}|1\rangle)(|0\rangle + e^{2\pi i 0,\phi_{j-1}\phi_j}|1\rangle)\dots(|0\rangle + e^{2\pi i 0,\phi_1\dots\phi_j}|1\rangle)$$

Сада је могуће применити претходно описану инверзну квантну Фуријеову трансформацију и добити оцену фазе $\overline{\phi}$. У идеалном случају, та вредност ће бити једнака фази, међутим то захтева предзнање о дужини децималног записа вредности фазе како би му и број кубита првог регистра био једнак. Ипак, како прецизност фазе није позната, за дужину првог регистра се узима број у зависности од примене, жељене прецизности приказа фазе и жељене тачности мерења. Како би се избегла грешка при мерењу већег броја кубита, могуће је понављање поступка.

Детаљнији опис алгоритма може се наћи у [18]. Овај алгоритам, као и Квантна Фуријеова трансформација, има највећи значај као градивни елемент сложенијих алгоритама, а посебно у налажењу реда броја и факторизацији.

5.3 Шорови алгоритми - факторизација и дискретни логаритам

Два алгоритма Питера Шора (енг. Peter Shore) за факторизацију целих бројева и решавање проблема дискретног логаритма припадају најзначајнијим алгоритмима квантног рачунарства до сада [31]. Пример су не само

квантног убрзања, јер проблеме који су класично експоненцијалне сложености решавају у полиномијалном времену, већ и могућег утицаја квантних рачунара на алгоритме који се тренутно користе, односно потенцијалних ефеката на нашу (информатичку) свакодневицу. Алгоритми су изложени у раду [13] деведесетих година и сматрају се првим револуционарним алгоритмима квантног рачунарства који су касније пратили и други попут Гроверовог алгоритма [14].

Факторизација целих бројева

Сваки природни број могуће је разложити на просте чиниоце (факторе) чијим множењем се добија тај број. Ова чињеница позната је још од античког времена, међутим тек у модерном добу добија на значају захваљујући сложености факторизације бројева за коју су и најефикаснији познати алгоритми скоро експоненцијалне сложености. У свом раду [13], Шор излаже пробабилистички квантни алгоритам за факторизацију бројева у полиномијалном времену. Алгоритам се састоји из два дела; свођења проблема факторизације на проблем налажења реда по модулу (класични део) и алгоритам за налажење реда елемента (квантни део).

Први део алгоритма се бави математичким проблемом свођења факторизације броја на проблем налажења реда по модулу. Претпоставимо да имамо ефикасан начин за израчунавање реда r броја x по модулу N. Такође, претпоставићемо да N није парно, као и да се не може добити степеновањем, како су оба ова случаја тривијална. Тада, можемо применити следећи поступак:

1. Насумично изабери x у интервалу $(1, N-1)$.
2. Ако је $NZD(x, N) > 1$, врати $NZD(x, N)$ као фактор.
3. У супротном, израчунај ред r од x по модулу N.
4. Ако је r парно и $x^{r/2} \neq -1(modN)$, израчунај $NZD(x^{r/2}-1, N)$ и $NZD(x^{r/2}+1, N)$.
5. У супротном, понови поступак
6. Провери (дељењем) да ли су $NZD(x^{r/2}-1, N)$ и $NZD(x^{r/2}+1, N)$ фактори N и ако јесу, врати одговарајуће факторе.

Корак овог поступка који може изазвати забуну јесте последњи који претпоставља да ће бар један од два заједничка делиоца бити фактор. Једини случај где заједнички делилац неће донети резултат јесте да је тај делилац управо N, односно да је $x^{r/2}-1$ или $x^{r/2}+1$ дељиво са N. Међутим, $N \| (x^r - 1)$ јер је r ред од x, у супротном $r/2$ би био ред од x. Тиме смо сигурни да ће бар $NZD(x^{r/2}-1, N)$ бити фактор.

Још једно питање јесте које је вероватноћа да нећемо морати да поновимо алгоритам, односно да важи да је r парно и $x^{r/2} \neq -1(modN)$. У складу са Кинеском теоремом о остацима, та вероватноћа јесте већа од $1 - 1/2^m$ где је m број простих фактора N.

Други део алгоритма јесте решавање проблема налажења реда елемента по модулу N помоћу алгоритма за процену фазе. Овде ћемо изложити

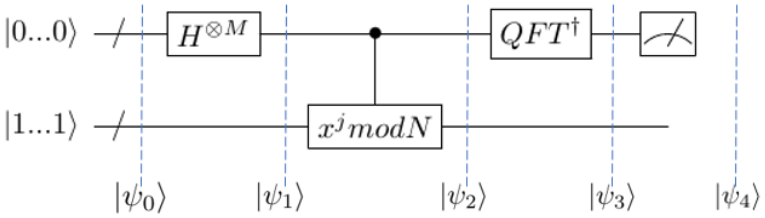
алгоритам на начин представљен у [18], имајући у виду да смо и посебно изложили алгоритам за процену фазе, док је у оригиналној верзији [13] овај део дат са комплетном разрадом алгоритма сличног оном за процену квантне фазе.

Проблем је следећи; за познате узајамно просте x и N, $x < N$ одредити најмање r такво да важи $x^r = 1(modN)$.

Суштински, алгоритам је исти као алгоритам за процену фазе где је оператор чија фаза се процењује:

$$U\left|y\right\rangle = \left|xy(modN)\right\rangle$$

Односно, у овом случају, одређивање реда елемента ће бити посматрано као проналажење периода функције $f(r) = x^r(modN)$. Олакшавајућа околност у овом случају јесте то што знамо на основу дужине броја који факторишемо, $L = log(N)$, да је неопходна дужина првог регистра за идентификовање периода $t = 2 * L + 1$. Одговарајуће квантно коло је приказано фигуром 5.3



Слика 5.3: Одређивање периода применом процене фазе

Размотрићемо и детаљније стање која. Припрема кола подразумева иницијализацију првог редистра на 0, а другог на 1:

$$\left|\psi_0\right\rangle = \left|0...0\right\rangle \left|1...1\right\rangle$$

Суперпозиција првог редистра након примене Адамарове трансформације:

$$\left|\psi_1\right\rangle = \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} \left|j\right\rangle \left|1...1\right\rangle$$

Примена $U = x^j modN$ и растављање трансформације:

$$\begin{aligned}\left|\psi_2\right\rangle &= \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} \left|j\right\rangle \left|x^j modN\right\rangle \\ &= \frac{1}{\sqrt{r2^t}} \sum_{s=0}^{r-1} \sum_{j=0}^{2^t-1} e^{2\pi isj/r} \left|j\right\rangle \left|u_s\right\rangle\end{aligned}$$

После примене инверзне Фуријеове трансформације:

$$\left|\psi_3\right\rangle = \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} \left|\overline{s/r}\right\rangle \left|u_s\right\rangle$$

Након мерења, резултат је:

$$\sim s/r$$

Оно што након мерења преостаје да се уради јесте екстракција података о периоду. Наиме, резултат мерења ће бити s/r, те самим мерењем не добијамо коначно решење. Оно се рачуна помоћу верижних разломака за које постоји ефикасан алгоритам.

Физички, алгоритам за факторизацију је имплементиран 2001. године на НМР рачунару [32].

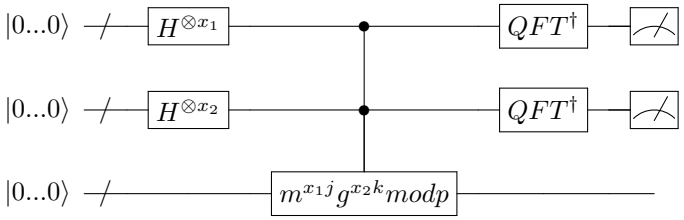
Проблем дискретног логаритма

Проблем дискретног логаритма је још један од битних алгоритама који се масовно користе у криптографији, а такође и још један за чије решавање је Шор конструисао адекватан алгоритам. Проблем је следећи; нека је p прост број и g генератор групе $modp$. Ако је m елемент групе, одредити s такво да важи $g^s = m(modp)$.

Слично факторизацији, применићемо алгоритам за процену фазе, овог пута на функцију:

$$U\left|x_1\right\rangle\left|x_2\right\rangle = \left|m^{x_1} g^{x_2} (modp)\right\rangle$$

Редослед m и g у трансформацији је дат у складу са [18]. Битна разлика у односу на факторизацију јесте што у случају дискретног логаритма, фигурирају два броја g и x, поред непознате r. То је разлог зашто ћемо користити три регистра као што је приказано на слици 5.4.



Слика 5.4: Одређивање дискретног логаритма

Након примене трансформације (функције) на суперпозицију, стање кола је:

$$\begin{aligned}\left|\psi\right\rangle &= \frac{1}{p-1}\sum_{x_1=0}^{p-2}\sum_{x_2=0}^{p-2}\left|x_1\right\rangle\left|x_2\right\rangle\left|m^{x_1} g^{x_2} modp\right\rangle \\ &= \frac{1}{(p-1)\sqrt{r}}\sum_{l=0}^{r-1}\sum_{x_1=0}^{p-2}\sum_{x_2=0}^{p-2} e^{2\pi i(slx_1+lx_2)/r}\left|x_1\right\rangle\left|x_2\right\rangle\left|\hat{f}(sl,l)\right\rangle\end{aligned}$$

После примене инверзне Фуријеове трансформације:

$$\left|\psi\right\rangle = \frac{1}{\sqrt{r}}\sum_{l=0}^{r-1}\left|sl/r\right\rangle\left|l/r\right\rangle\left|\hat{f}(sl,l)\right\rangle$$

Након мерења, резултат је:

$$\sim (sl/r, l/r)$$

Из резултата мерења, преко заједничких елемената и верижних разломака, добија се вредност s. Овиме је, преко периодичности функције степеновања по модулу за конкретан случај, решен проблем дискретног логаритма.

5.4 Последице и пост-квантна криптографија

Проблеми представљени у претходна два дела, факторизација на просте чиниоце и проблем дискретног логаритма, чине окосницу модерних криптографских алгоритама са јавним кључем. Управо то је чести извор интересовања за квантне рачунаре (иако је већа вероватноћа да ће неко за живота видети слетање човека на Марс, него разбијање криптографског алгоритма квантним рачунаром).Очигледно је да ће овакви алгоритми постати превазиђени једном кад квантни рачунари постану довољно брзи и зато је настала нова грана криптографије - пост-квантна криптографија. Ова област се бави проблемима који, бар тренутно, не могу бити ефикасно решени квантним путем и тиме постају кандидати за кључне елементе криптографских протокола.

Најпознатији алгоритам који је тренутно угрожен квантним рачунарима јесте RCA, а заснива се управо на претпоставци да је налажење фактора броја екпоненцијално тешко. RCA као основу узима два велика проста броја, односно њихов производ. Како је у питању алгоритам са јавним кључем, тај број ће бити јаван и ту се налази проблем, јер поента алгоритма јесте да нико не може да факторише јавни кључ. Ако би се то постигло, а Шоров алгоритам то омогућава, било ко би могао да дешифрује тајну поруку и тиме је алгоритам обесмишљен.

Оно што се тренутно намеће као решење јесте коришћење другачијих проблема за које није тренутно познато квантно решење. Проблем који остаје јесте могућност да ће се појавити ефикасни алгоритми и за таква решења јер квантно рачунарство, за разлику од класичног, прати не само развој технике, већ и развој физике, те је подложно изненадним резултатима.

Ово је само један од примера како квантно рачунарство може да утиче на свет, у случају да се у кратком року конструише квантни рачунар, велика количина информација би постала тренутно доступна. Али, колико год ово деловало застрашујуће, то је такође и добар показатељ моћи квантних рачунара која у зависности од примене може знатно допринети пре свега науци, а затим и свакодневном животу.

Глава 6

Општи случај употребе квантних рачунара - за и против

У претходним поглављима, представили смо квантне алгоритме засноване на Фуријеовој трансформацији. Оно што се може закључити јесте да је главни фактор убрзања код ових алгоритама квантна суперпозиција. Међутим, приказана група алгоритама није изузетак, већ су и други алгоритми попут оних заснованих на квантној претрази такође мотивисани суперпозицијом. Осим суперпозиције, у поглављу о квантним рачунарима, приказали смо два основна протокола, супергусто кодирање и телепортацију који су засновани на квантној уплетености. У овом поглављу ћемо се детаљније осврнути на ова два чиниоца квантног убрзања, али и на проблеме који се појављују приликом имплементације алгоритама, како теоријски, тако и практично.

6.1 Кључни елементи квантног убрзања и применљивост

Основни елемент квантног убрзања јесте квантна суперпозиција која омогућава паралелизацију израчунавања и претраге, односно паралелну примену функције без битног повећања просторне сложености. Очигледно је да алгоритми који би могли да се убрзају класичном паралелизацијом, могу да се квантно имплементирају знатно ефикасније. Међутим, неколико чинилаца квари слику о идеалном рачунару.

Прво, алгоритми који не могу да се убрзају на овај начин биће исте ефикасности, под условом да брзина класичних операција на квантним рачунарима буде приближна класичним. Друго, надовезујући се на претходно, квантни рачунари су по брзини далеко од класичних, а нека предвиђања [25] говоре о томе да они још дуго неће по брзини претећи класичне рачунаре. Решење за ове проблеме јесте селективна примена квантних рачунара, односно примена само у случајевима када долази до битног убрзања у тренутном контексту, као у случају факторизације. У осталим случајевима, препорука јесте коришћење класичних рачунара.

Трећи проблем јесте сложеност развоја алгоритама. Наиме, како би се развио нови алгоритам потребно је широко знање математике и физике, услов који испуњавају креатори представљених алгоритама, Дејвид Дојч

је физичар, а Ричард Јоза и Питер Шор математичари. На први поглед, главна препрека јесте начин размишљања о проблемима и о могућим рачунарским решењима која су у случају квантних рачунара разноврснија. Међутим, то није тако једноставно, јер квантни рачунари у једном аспекту представљају напредак, али са друге стране, због тренутног степена развоја, представљају и назадовање. Као што се може видети из претходних примера, алгоритми баратају са појединачним битовима и битовским операцијама, те је са тог аспекта квантно рачунарство на нивоу на ком је класично било пре седамдесет година - на нивоу машинског кода. Тако да, слично првим рачунарима, захтевају елементарнија знања о самој структури како би се употребили на прави начин. Покушаји да се произведе програмски језик за квантне рачунаре углавном за резултат имају необичан спој класичног програмског језика и језика који барата кубитима на машинском нивоу.

Други елемент квантног убрзања јесте уплетеност која омогућава квантну комуникацију. У случају када је квантни рачунар имплементиран у складу са Ди Виченцовим правилима, могуће је уплитање кубита, те је самим тим омогућена и телепортација, односно пренос кубита у сложеном стању. Ово је занимљив аспект чак и у овом тренутку јер је експериментално показана могућност телепортације на већој удаљености. Ово би значило велики напредак у комуникацији, а нарочито у безбедности преноса информација. Такође, уплетеност већ сад имплицира не само квантну комуникацију у оквиру рачунара, већ и на мрежи.

6.2 Када?

Питање када има двоструко значење у случају квантних рачунара; та значења морају се посматрати паралелно. Прво питање се односи на временаску одредницу. Примена квантног рачунара данас није могућа јер једноставно нису довољно велики ни брзи да би подржали основне рачунске операције. Примена у будућности нас доводи до другог питања када, односно у којим случајевима примењивати квантне рачунаре. Претходно смо изложили елементе квантног убрзања и од могућности њихове употребе у конкретном случају зависи да ли ће алгоритам бити имплементиран квантно или класично. Напослетку, ако квантни рачунари при основним операцијама буду имали брзину класичних, ово питање ће бити питање саме конструкције алгоритама, а имплементација ће увек бити квантна. Ако у алгоритму постоје делови који би се убрзали квантним елементима рачунара, онда би било логично формирати квантни алгоритам. Са друге стране, не би постојала потреба за променом постојећих ефикасних алгоритама.

Глава 7

Закључак

Напретком квантних рачунара достићи ће се нове могућности израчунавања са разноврсним применама. Како би се то најбоље искористило, биће неопходно трансформисати начин конструкције алгоритама у будућности са једне стране, а са друге и начин конструкције квантних рачунара. Дизајн и имплементација алгоритама у квантном окружењу захтевају сасвим нови концептуални приступ проблемима, веома различит од класичних рачунара. Како би се тај процес олакшао, у наредном периоду би требало развијати не само операције на нивоу кубита, већ и сложеније, формализовати појам квантног регистра, као и других структура података. У овом смеру већ постоје кораци [33], а структуре података ће (бар до следећег великог скока у физици) имати двоструку улогу, са једне стране ће постојати у квантној унутрашњости рачунара, а са друге ће омогућавати комуникацију рачунара са нашим класичним светом.

Квантни рачунари, посматрано из тренутне перспективе, нису свемогући, што се огледа и у њиховој немогућности да реше NP комплетне проблеме. Међутим, убрзања која пружају при одговарајућим применама јесу реална и доносе сасвим нове могућности. У овом раду, приказани су само неки од представника квантних алгоритама заснованих на Фуријеовој трансформацији, који, иако најзначајнији, нису и једини. Осим већ познатих квантних алгоритана, морамо узети у обзир и то да се ради о релативно младој области, те је разумно очекивати велики број нових моћних алгоритана у наредним деценијама.

На крају, конструкција и имплементација алгоритама у квантним колима без физичке имплементације на видику може деловати бесмислено, али није, јер представља припрему за нешто што ће тек да се деси. Квантни рачунари представљају поглед у будућност и можда прву прилику да технолошки скок дочекамо потпуно припремљени.

Библиографија

[1] Laszlo B. Kish. End of moore's law: thermal (noise) death of integration in micro and nano electronics. *Physics Letters A*, 305(3-4):144–149, 2002.

[2] Yuri Manin. Computable and uncomputable. *Sovetskoye Radio, Moscow*, 128, 1980.

[3] David Deutsch. Quantum theory, the church–turing principle and the universal quantum computer. *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences*, 400(1818):97–117, 1985.

[4] David J. Griffiths and Darrell F. Schroeter. *Introduction to quantum mechanics*. Cambridge University Press, 2018.

[5] Richard P. Feynman, Robert B. Leighton, and Matthew Sands. The feynman lectures on physics; vol. i. *American Journal of Physics*, 33(9):750–752, 1965.

[6] John Simpson. *Oxford English Dictionary*. Oxford University Press, 2 edition, 2009.

[7] Merriam-Webster. *Merriam-Webster's Elementary Dictionary*. Merriam Webster, 1 edition, 2009.

[8] Милан Вујаклија. *Лексикон страних речи и израза*. Просвета Београд, 1954.

[9] Johannes Kalliauer. File:double-slit.svg. https://commons.wikimedia.org/wiki/File:Double-slit.svg, Aug 2017.

[10] Fedor Herbut. *Kvantna mehanika: za istraživače*. Prirodno matematički fakultet Univerziteta u Beogradu, 1982.

[11] Bas Hensen, H. Bernien, A.E. Dréau, A. Reiserer, N. Kalb, M.S. Blok, J. Ruitenberg, R.F.L. Vermeulen, R.N. Schouten, C. Abellán, et al. Experimental loophole-free violation of a bell inequality using entangled electron spins separated by 1.3 km. *Nature*, (526):682–686, 2015.

[12] Richard P. Feynman. Simulating physics with computers. *International journal of theoretical physics*, 21(6):467–488, 1982.

[13] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, 41(2):303–332, 1999.

[14] Lov K. Grover. A fast quantum mechanical algorithm for database search. pages 212–219, 1996.

[15] Jonathan A. Jones, Michele Mosca, and Rasmus H. Hansen. Implementation of a quantum search algorithm on a quantum computer. *Nature*, 393(6683):344, 1998.

[16] Isaac L. Chuang, Neil Gershenfeld, and Mark Kubinec. Experimental implementation of fast quantum searching. *Physical review letters*, 80(15):3408, 1998.

[17] Paul Adrien Maurice Dirac. *The principles of quantum mechanics*. Number 27. Oxford university press, 1981.

[18] Michael A. Nielsen and Isaac Chuang. *Quantum computation and quantum information*. AAPT, 2002.

[19] Mark Oskin. Quantum computing-lecture notes. *Notes to CSE590mo*, 2004.

[20] Tommaso Toffoli. Reversible computing. In *International colloquium on automata, languages, and programming*, pages 632–644. Springer, 1980.

[21] John S. Bell. On the einstein podolsky rosen paradox. *Physics Physique Fizika*, 1(3):195, 1964.

[22] Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K. Wootters. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Physical review letters*, 70(13):1895, 1993.

[23] Charles H. Bennett and Stephen J. Wiesner. Communication via one-and two-particle operators on einstein-podolsky-rosen states. *Physical review letters*, 69(20):2881, 1992.

[24] David P. DiVincenzo. The physical implementation of quantum computation. *Fortschritte der Physik: Progress of Physics*, 48(9-11):771–783, 2000.

[25] John Preskill. Quantum computing in the nisq era and beyond. *Quantum*, 2:79, 2018.

[26] Chris Fisher. Quantum starts here. https://www.research.ibm.com/ibm-q/, Apr 2009.

[27] Google quantum. https://ai.google/research/teams/applied-science/quantum/.

[28] David Deutsch and Richard Jozsa. Rapid solution of problems by quantum computation. *Proc. R. Soc. Lond. A*, 439(1907):553–558, 1992.

[29] Zhengjun Cao, Jeffrey Uhlmann, and Lihua Liu. Analysis of deutsch-jozsa quantum algorithm. *IACR Cryptology ePrint Archive*, 2018:249, 2018.

[30] Ronald Newbold Bracewell and Ronald N. Bracewell. *The Fourier transform and its applications*, volume 31999. McGraw-Hill New York, 1986.

[31] Richard Jozsa. Quantum factoring, discrete logarithms, and the hidden subgroup problem. *Computing in science & engineering*, 3(2):34, 2001.

[32] Lieven M.K. Vandersypen, Matthias Steffen, Gregory Breyta, Costantino S. Yannoni, Mark H. Sherwood, and Isaac L. Chuang. Experimental realization of shor's quantum factoring algorithm using nuclear magnetic resonance. *Nature*, 414(6866):883, 2001.

[33] Maximilian Fillinger. Data structures in classical and quantum computing. *arXiv preprint arXiv:1308.0833*, 2013.