Математичка гимназија

МАТУРСКИ РАД
- из предмета физика -

КВАНТНА ЛОГИЧКА КОЛА

Ученик

Марко Шушњар IVд

Ментор

Александра Димић
Физички факултет

Београд, јун 2017.

Садржај

1 Увод **1**

2 Квантни битови - кубити **3**
2.1 Основна својства кубита . . . 3
2.2 Блохова сфера . . . 4
2.3 Вишеструки кубити . . . 5

3 Квантна логичка кола **7**
3.1 Унитарне матрице . . . 7
3.2 Логичка кола над једним кубитом . . . 7
3.3 Ротације око x, y и z-осе . . . 9
3.4 Логичка кола над више кубита . . . 9
3.5 Идентитети са квантним логичким колима . . . 11

4 Квантно процесирање **12**
4.1 Структура квантних кола . . . 12
4.2 Матрице еквивалентних логичких кола . . . 13
4.3 Примери квантних кола . . . 14
4.4 Мерење у колима . . . 16
4.5 Универзална логичка кола . . . 17

5 Класе сложености проблема **21**
5.1 Теорија сложености . . . 21
5.2 Класе сложености у класичном рачунарству . . . 21
5.3 Класе сложености у квантном рачунарству . . . 22

6 Предности квантних рачунара **24**
6.1 Паралелно процесирање . . . 24
6.2 Дојч-Јожа алгоритам . . . 25
6.3 Гроверов алгоритам . . . 27
6.4 Шоров алгоритам . . . 28

7 Закључак **31**

Литература **32**

1. Увод

Прве кораке у сфери рачунарства и рачунарске обраде информације направио је Алан Тјуринг, који је у свом раду 1936. године[1], математички увео модел програмабилног компјутера, односно Тјурингове машине. Показао је да постоји Универзална Тјурингова машина која може да реши сваки проблем за који постоји алгоритам на било којем другом уређају. На тај начин је успостављена аналогија између математичког модела и реалних уређаја, попут данашњих рачунара. Штавише, сваки проблем који може бити решен временски ефикасно на неком уређају, може бити решен ефикасно и на Тјуринговој машини. То представља Черч-Тјурингову тезу.

До прве допуне ове тезе долази услед алгоритма за утврђивање да ли је број прост који се заснива на насумичним бројевима. Наиме, на основу неколико понављања алгоритма, могуће је утврдити да је број прост са одређеном вероватноћом или да је сигурно сложен. Како није познат сличан ефикасан алгоритам на детерминистичкој Тјуринговој машини, теза је допуњена тако да тврди да се сваки процес може ефикасно симулирати на пробабилистичкој Тјуринговој машини.

Концепт рачунара какав данас користимо поставио је Џон фон Нојман. Након тога долази до проналаска транзистора и развоја рачунарства значајном брзином. У прилог томе говори и закон који је 1965. године емпиријски поставио Гордон Мур, један од оснивача компаније Интел. Према том закону, сваке две године моћ рачунара и број транзистора у њима се удвостручи за исту цену израде. Тако се, од 2000 транзистора почетком 70-их година, дошло до преко милијарду транзистора у микропроцесорима. Повећање броја транзистора природно прати и смањивање њихових димензија. Тако је могуће применити Муров закон на још две или три генерације пре него што постану толико мали да до изражаја дођу квантни ефекти. Алтернатива смањивању димензија је употреба нових полупроводничких материјала, као и прављење вишејезгарних процесора, али свакако можемо очекивати да се смањивање не може потпуно избећи.

Квантна механика предвиђа појаве на које нисмо навикли у класичној физици. Честице се често понашају као таласи, па је успостављен таласно-честични дуализам. Саму „талас-честицу" описује таласна функција, а њен положај и импулс не можемо тачно одредити, о чему говоре Хајзенбергове релације неодређености. Изузетно је значајан постулат квантне механике по којем, ако систем може да буде у стању А и у стању Б, онда може да буде и у произвољној суперпозицији стања А и Б. Стање система може се одредити мерењем након којег систем прелази у измерено стање. Такође, квантна механика предвиђа постојање увезаних стања, односно ситуација при којима се одређивањем стања једне честице тренутно утиче на стање друге. Иако су нека од ових предвиђања деловала контраинтуитивно и као да нарушавају неке основне принципе физике, квантна механика је једна од досад најбоље потврђених теорија у физици и налази своју даљу примену.

[1] A. M. Turing – *On computable numbers, with an application to the Entscheidungsproblem*, 1936.

Још 1982. године, Ричард Фајнман приметио је да је симулирање квантних система на класичним рачунарима изразито тешко. Како би то избегао, предлаже прелазак на рачунаре који би били засновани на принципима квантне механике. Након тога, 1985. године, Давид Дојч дефинише уређај, Универзални квантни рачунар, који би био способан да ефикасно симулира произвољни физички систем. Због квантно-механичких особина природе, претпоставља да би и такав уређај био базиран на квантној механици. Још увек није познато да ли би Универзални квантни рачунар могао да постоји, али постоје алгоритми за квантне рачунаре који омогућавају ефикасно решавање проблема за које се сматрало да не могу бити ефикасно решени на Тјуринговој машини, односно на класичним рачунарима.

Први такав пример навео је сам Дојч када је искористио основне принципе квантне механике како би омогућио паралелно израчунавање за више различитих стања. То је 1992. године искоришћено у Дојч-Јожином алгоритму за ефикасно решавање проблема који на класичним рачунарима захтева експоненцијалну сложеност. Године 1994, Питер Шор долази до алгоритма који омогућава брзо растављање великог броја на просте факторе, што се раније сматрало да није могуће и стога је коришћено за шифровање са такозваним приватним кључем. Две године касније, Лов Гровер објављује алгоритам за квантну претрагу података у сложености мањој од линеарне.

Дакле, квантни рачунари омогућавају решавање проблема за које се раније веровало да не могу бити ефикасно решени или нуде мању сложеност од класичних. На квантним рачунарима је могуће симулирати све што је могуће и на класичним, али се ослањају и на физичке појаве које нису у основи рада класичних рачунара. Тако се квантни системи могу користити за телепортовање информације, генерисање истински насумичних бројева, пробијање кодова, али и за преношење информације са сигурношћу откривања евентуалног прислушкивања. Примене и могућност даљег развоја су велики, због чега су квантни рачунари у жижи интересовања данашњих информатичара и физичара. Циљ је омогућити услове у којима би квантни рачунари постојали и могли да раде онако како ми очекујемо. До сада је објављено успешно формирање рачунара са преко 1000 квантних битова.

У овом раду биће представљен модел квантних рачунара преко квантних логичких кола, аналогних логичким колима на која смо навикли у класичним рачунарима. Формално ћемо увести квантне битове и операције које се у колима врше над њима. Навешћемо најважнија квантна кола и детаљније описати предности квантних рачунара кроз већ наведене алгоритме. Видећемо и какав значај имају открића у сфери квантног рачунарства за груписање проблема у класе сложености.

2. Квантни битови - кубити

2.1 Основна својства кубита

У класичној теорији, основна јединица информације је бит. Битови могу имати само једну од две вредности - 0 или 1, и она је јединствено одређена независно од тога да ли је претходно измерена. Битови се могу копирати, преносити и читати без утицаја на остале битове у систему.

На сличном концепту је заснована и квантна теорија информације и квантно рачунарство. Основна јединица је квантни бит, односно кубит. За разлику од класичних битова, кубити представљају квантне системе који могу бити у два стања (0 и 1), али и у њиховој суперпозицији. Стања 0 и 1 се, по Дираковој нотацији, записују кет векторима, који су математички заправо вектори колоне: $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ и $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. Онда се кубит уводи као математички објекат који представља линеарну комбинацију ова два стања:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}.$$

Овде су α и β комплексни бројеви који се називају амплитуде одговарајућих стања, а сразмерни су вероватноћи налажења честице у том стању. Кубити могу узимати бесконачно много стања, односно читав континум стања између $|0\rangle$ и $|1\rangle$. Мерењем кубита не добија се информација о појединачним амплитудама, већ само коначно стање $|0\rangle$ или $|1\rangle$. Вероватноћа добијања стања $|0\rangle$ је $|\alpha|^2$, а стања $|1\rangle$ је $|\beta|^2$. Онда мора да важи: $|\alpha|^2 + |\beta|^2 = 1$. У већини случајева у квантном рачунарству, амплитуде су реални бројеви. Важно је напоменути да након мерења, кубит прелази у измерено стање, односно из стања $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ прелази у стање $|0\rangle$ или $|1\rangle$.

За свако стање записано кет вектором, може се увести запис бра вектором, односно вектором врстом, који носи еквивалентну информацију:

$$\langle 0| = \begin{pmatrix} 1 & 0 \end{pmatrix}, \langle 1| = \begin{pmatrix} 0 & 1 \end{pmatrix}, \langle\psi| = \alpha^*\,\langle 0| + \beta^*\,\langle 1| = \begin{pmatrix} \alpha^* & \beta^* \end{pmatrix},$$

где су α^* и β^* конјуговане вредности амплитуда. Посматрајмо два различита кубита: $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$ и $|\phi\rangle = c\,|0\rangle + d\,|1\rangle$. Производ бра и кет вектора је:

$$\langle\psi| \cdot |\phi\rangle = \langle\psi|\phi\rangle = \begin{pmatrix} a^* & b^* \end{pmatrix} \begin{pmatrix} c \\ d \end{pmatrix} = a^*c + b^*d$$

и одговара преклапању између стања ψ и ϕ. Тако се за међусобно нормална стања добија резултат 0, за једнака стања $\langle\psi|\psi\rangle = |\alpha|^2 + |\beta|^2 = 1$, а вероватноћа налажења кубита $|\psi\rangle$ у стању $|0\rangle$ се може одредити као $|\langle\psi|0\rangle|^2$.

Са друге стране, производ кет и бра вектора даје матрицу:

$$|\psi\rangle \cdot \langle\phi| = |\psi\rangle \langle\phi| = \begin{pmatrix} a \\ b \end{pmatrix} \begin{pmatrix} c^* & d^* \end{pmatrix} = \begin{pmatrix} ac^* & ad^* \\ bc^* & bd^* \end{pmatrix}$$

која ће нам бити од значаја када будемо анализирали логичка кола.

Стања $|0\rangle$ и $|1\rangle$ формирају ортонормирану базу векторског простора. У зависности од физичког система који описују, могу се бирати различите базе, а резултат мерења зависи од базе. На пример, ако одређујемо поларизацију линеарно поларизованог фотона, измерена вредност ће бити дуж осе поларизатора (односно зависи од њеног одабира), а смер зависи од одговарајућих амплитуда. Слично, и кубит можемо посматрати у различитим ортонормираним базама.
Посматрајмо кубит који је у стању $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$. Његовим мерењем у односу на уобичајену базу добија се стање $|0\rangle$ са вероватноћом $\frac{1}{2}$, односно стање $|1\rangle$ са истом вероватноћом. Међутим, ако уведемо стања $|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$ и $|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$, добијамо још једну ортонормирану базу. Како је принципијелно могуће извршити мерење у односу на сваку ортонормирану базу, резултат мерења у односу на ову базу ће увек бити $|+\rangle$. Дакле, одавде је јасно да, иако начин на који представљамо кубит не утиче на њега, резултат самог мерења и те како зависи од изабране базе.

На крају, пре него што пређемо на графичко представљање кубита, напоменимо још једну важну разлику у односу на класичне битове која ће бити касније детаљније објашњена. Поред тога што се читањем, односно мерењем кубита мења његово стање, немогуће је копирати[1] или пренети кубит без промене стања. Такође, читање једног кубита у рачунару може утицати на остале кубите, што свакако није случај са класичном информацијом.

2.2 Блохова сфера

Ослањајући се на услов $|\alpha|^2 + |\beta|^2 = 1$, вредност кубита се може илустровати тачком на јединичној сфери - тзв. Блоховој сфери. Прво ћемо показати да се сваки кубит $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, може представити у облику $|\psi\rangle = e^{i\gamma}(\cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle)$. Притом γ одговара фазној разлици која нема приметних ефеката и самим тим се не представља на Блоховој сфери.

Амплитуде α и β су комплексни бројеви, па се могу представити у облику $\alpha = x_1 + iy_1$ и $\beta = x_2 + iy_2$, односно $\alpha = r_1 e^{i\phi_1}$ и $\beta = r_2 e^{i\phi_2}$ у поларним координатама. Ако извучемо релативну фазу добијамо $|\psi\rangle = e^{i\phi_1}(r_1|0\rangle + r_2 e^{i(\phi_2-\phi_1)}|1\rangle)$, односно $|\psi\rangle = e^{i\phi_1}(r_1|0\rangle + (x+iy)|1\rangle)$. Сада, знајући да важи $|r_1|^2 + |x+iy|^2 = 1$, односно $r_1^2 + x^2 + y^2 = 1$ можемо овом стању придружити тачку на јединичној сфери. Ако уведемо сферне координате θ' и ϕ, добијамо:

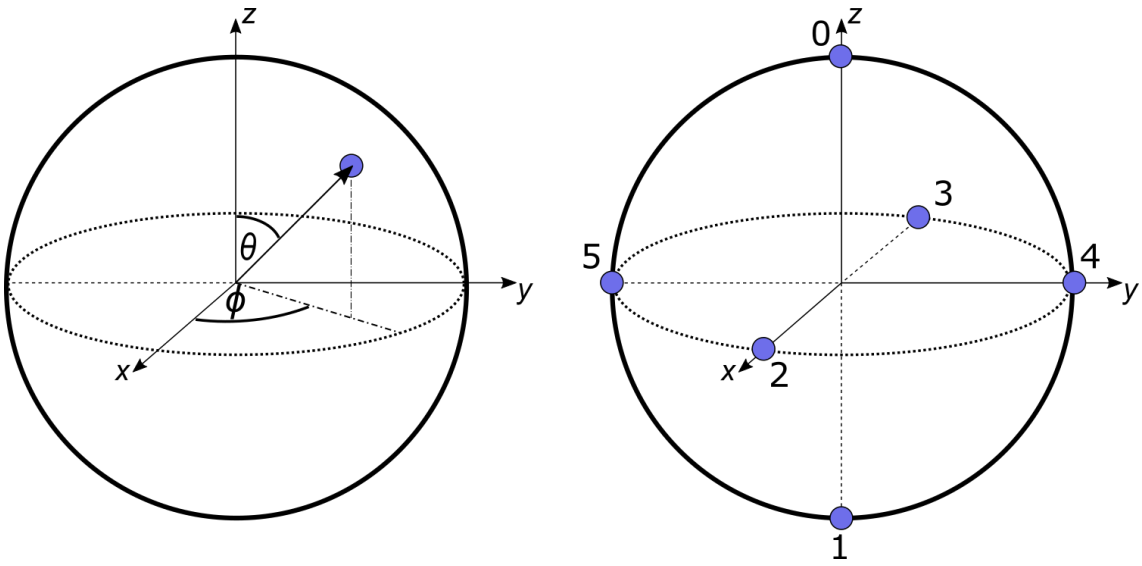
$$\begin{aligned} x &= \sin\theta' \cos\phi \\ y &= \sin\theta' \sin\phi \\ r_1 &= \cos\theta' \end{aligned}$$

Међутим, како се сва стања налазе између $\theta' = 0$ (стање $|0\rangle$) и $\theta' = 90°$ (стање $|1\rangle$), овако уведене координате ће сва стања пресликати на полусферу. Стога уместо угла θ' уводимо

[1] No − cloning theorem; W. K. Wootters, W. H. Zurek, *A single quantum cannot be cloned*, 1982.

угао $\theta = 2\theta'$ и коначно добијамо: $|\psi\rangle = e^{i\phi_1}(\cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle)$, што је облик који смо тражили.

Дакле, сваки кубит можемо представити на јединичној Блоховој сфери тако што његове амплитуде запишемо у одговарајућем облику и придружимо им одговарајуће сферне координате. Приметимо да при оваквом представљању северном полу сфере одговара стање $|0\rangle$, а јужном стање $|1\rangle$. Иако су та два стања математички ортогонална (нормална), на сфери се представљају дијаметрално супротним тачкама. Исто важи и за остала ортогонална стања.



Слика 1: Представљање произвољног кубита на Блоховој сфери у зависности од углова θ и ϕ (лево); Карактеристични кубити на сфери: тачкама 0, 1, 2, 3, 4 и 5 редом одговарају стања $|0\rangle$, $|1\rangle$, $|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$, $|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$, $|R\rangle = \frac{|0\rangle + i|1\rangle}{\sqrt{2}}$ и $|L\rangle = \frac{|0\rangle - i|1\rangle}{\sqrt{2}}$ (десно)

2.3 Вишеструки кубити

Посматрајмо сада два кубита. Они појединачно могу бити у стањима $|0\rangle$ и $|1\rangle$, па резултат њиховог мерења могу бити стања $|00\rangle$, $|01\rangle$, $|10\rangle$ и $|11\rangle$. Стога, систем се пре мерења налази у суперпозицији ових стања, односно:

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

Као и до сада, вероватноћа добијања сваког појединачног стања једнака је квадрату модула одговарајуће амплитуде. Укупна вероватноћа је 1, па важи: $|\alpha_{00}|^2+|\alpha_{01}|^2+|\alpha_{10}|^2+|\alpha_{11}|^2 = 1$. Базу коју узимамо за представљање целокупног стања система више кубита називамо база израчунавања.

Слично, за три кубита добијамо следеће:

$$|\psi\rangle = \alpha_{000}\,|000\rangle + \alpha_{001}\,|001\rangle + \alpha_{010}\,|010\rangle + \alpha_{011}\,|011\rangle + \alpha_{100}\,|100\rangle + \alpha_{101}\,|101\rangle + \alpha_{110}\,|110\rangle + \alpha_{111}\,|111\rangle.$$

Тада мерењем добијамо један од резултата $|000\rangle$, $|001\rangle$, $|010\rangle$, $|011\rangle$, $|100\rangle$, $|101\rangle$, $|110\rangle$ и $|111\rangle$.

Аналогно, систем вишеструких кубита може бити сачињен од произвољног природног броја појединачних кубита. Важно је напоменути да поред истовременог мерења свих кубита, можемо мерити појединачне подскупове. На пример, полазећи од стања $|\psi\rangle = \alpha_{00}\,|00\rangle + \alpha_{01}\,|01\rangle + \alpha_{10}\,|10\rangle + \alpha_{11}\,|11\rangle$, ако измеримо само први кубит, добијамо резултат $|0\rangle$ са вероватноћом $|\alpha_{00}|^2 + |\alpha_{01}|^2$ и долазимо у стање $|\psi\rangle = \frac{\alpha_{00}|00\rangle + \alpha_{01}|01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}$. Слично важи и за добијање резултата $|1\rangle$.

Ако полазимо од два кубита $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$ и $|\phi\rangle = c\,|0\rangle + d\,|1\rangle$, регистар сачињен од њих можемо формирати једноставно њиховим Декартовим производом:

$$|\psi\rangle \otimes |\phi\rangle = \begin{pmatrix} a \\ b \end{pmatrix} \otimes \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} ac \\ ad \\ bc \\ bd \end{pmatrix} = ac\,|00\rangle + ad\,|01\rangle + bc\,|10\rangle + bd\,|11\rangle.$$

Потпуно анологно се поступа и за више од два кубита. Регистар сачињен од више кубита има значајне разлике у односу на класиче регистре са битовима. Наиме, кубити могу међусобно интерферирати и тако утицати на резултат који добијамо, што се са битовима очигледно не дешава. Такође, вишеструки кубити могу бити у такозваним квантним увезаним (спрегнутим) стањима. За стање кажемо да је увезано ако и само ако се не може представити као Декартов производ више појединачних стања. Најпознатије такво стање је Белово стање познато и као ЕПР[2] пар: $|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$. У Беловом стању, вредност првог и другог кубита су увек једнаке, па се тако мерењем само једног од њих директно одређује и стање другог. Занимљиво је да оваква стања немају одговарајућу паралелу у класичној физици.
Значај увезаних стања у квантном рачунарству биће приметан код паралелног процесирања које је осетно оптималније него у класичим рачунарима.

[2] A. Einstein, B. Podolsky, N. Rosen; ЕПР парадокс: *Can Quantum – Mechanical Description of Physical Reality be Considered Complete*?, 1935.

3. Квантна логичка кола

3.1 Унитарне матрице

Квантни рачунари се, као и класични, састоје од кола сачињених од ситнијих квантних логичких кола. Улога квантних логичких кола је манипулисање информацијом тако што се на једном или више улазних кубита извршава одређена операција и преводе се у ново стање.

Квантна логичка кола се могу представити матрицама. Тако се, на пример, квантна логичка кола над једним кубитом представљају матрицама са две врсте и две колоне. Онда, ако је дато логичко коло $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ и улазни кубит $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, излазно стање је:

$$A|\psi\rangle = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \alpha a + \beta b \\ \alpha c + \beta d \end{pmatrix} = \begin{pmatrix} \alpha' \\ \beta' \end{pmatrix} = |\psi'\rangle.$$

Испоставља се да је потребан и довољан услов да матрица одговара квантном логичком колу то да буде унитарна. Матрица U је унитарна ако важи $UU^\dagger = I$, где је $U^\dagger$ матрица која се добија транспоновањем и конјуговањем матрице U, а I је јединична матрица.
Ако је U унитарна матрица, онда важи да је и њен инверз U^{-1} такође унитарна матрица, односно $U^{-1} = U^\dagger$. То значи да за свако квантно логичко коло постоји његов инверз, па се његовом применом улазни кубит враћа у почетно стање. Врсте и колоне унитарне матрице представљају ортонормиран скуп вектора, што је и очекивано, јер на неки начин одговарају бази израчунавања. Још једно значајно својство је $\det U = 1$, као и то да је сума квадрата модула свих елемената матрице 1.

3.2 Логичка кола над једним кубитом

Као што је већ наведено, логичка кола над једним кубитом заправо представљају унитарне матрице 2×2. Међу њима постоји неколико карактеристичних и врло применљивих које ћемо овде навести.

Прво ћемо увести аналогон класичном NOT колу (логичком инвертору). Уместо резултата $|0\rangle$ треба да добијамо $|1\rangle$ и обрнуто, односно матрица треба да замењује коефицијенте уз стања $|0\rangle$ и $|1\rangle$. Тражена матрица је:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

која се још назива и Паулијева X матрица. Приметимо да је $X = |0\rangle\langle 1| + |1\rangle\langle 0|$, одакле је интуитивно јасно шта заправо она ради. Дакле, стања $|0\rangle$ и $|1\rangle$ се сликају у себи дијаметрално супротна на Блоховој сфери, али то заправо не важи у општем случају, тј. ова матрица не представља увећање лонгитуде (угао ϕ) за 180° и превођење латитуде (угао θ) у угао $180° - \theta$.

Следеће уводимо Паулијеву Z матрицу (односно Z квантно логичко коло):

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = |0\rangle\langle 0| - |1\rangle\langle 1|.$$

Она од кубита $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ прави кубит $|\psi'\rangle = \alpha|0\rangle - \beta|1\rangle$.

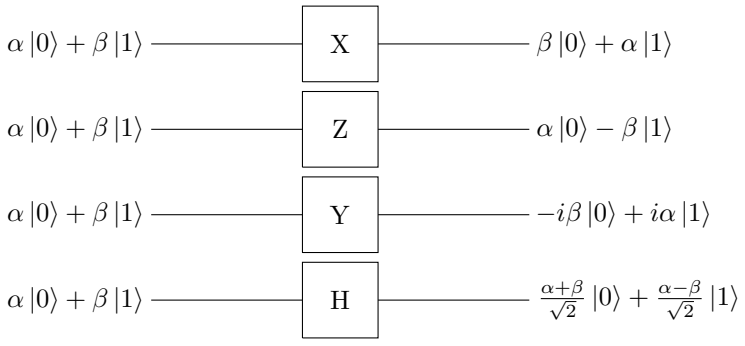
Трећа Паулијева матрица која се такође користи је $Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = i(|1\rangle\langle 0| - |0\rangle\langle 1|)$.

На крају, наведимо веома значајно Адамарово логичко коло. Оно, полазећи од стања $|0\rangle$ даје $|+\rangle$, а полазећи од $|1\rangle$ даје $|-\rangle$. У општем случају, за кубит $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ враћа $|\psi'\rangle = \alpha|+\rangle + \beta|-\rangle = \frac{\alpha+\beta}{\sqrt{2}}|0\rangle + \frac{\alpha-\beta}{\sqrt{2}}|1\rangle$, односно у матричном облику:

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

Занимљиво је да је Адамарова матрица сама свој инверз, односно њеним поновљеним коришћењем се кубит враћа у почетно стање.

Све ове операције над кубитима се могу представити на Блоховој сфери (слика 1). Тако, на пример, Адамарово логичко коло представља ротацију за 90° око y-осе и осну рефлексију у односу на xy-раван. На слици 2 су приказане шематске ознаке логичких кола и преглед њиховог деловања на кубите.



Слика 2: Шематски приказ квантних логичких кола над једним кубитом

3.3 Ротације око x, y и z-осе

Вратимо се сада на Блохову сферу, односно на представљање операција које логичко коло врши над кубитом на њој. Постоје три матрице, које се добијају из Паулијевих матрица, и које представљају ротације око x, y и z-осе (које су претходно уведене) за неки угао α. Дефинишемо их на следећи начин:

$$R_x(\alpha) = e^{-i\alpha X/2} = \begin{pmatrix} \cos(\frac{\alpha}{2}) & -i\sin(\frac{\alpha}{2}) \\ -i\sin(\frac{\alpha}{2}) & \cos(\frac{\alpha}{2}) \end{pmatrix}$$

$$R_y(\alpha) = e^{-i\alpha Y/2} = \begin{pmatrix} \cos(\frac{\alpha}{2}) & -\sin(\frac{\alpha}{2}) \\ \sin(\frac{\alpha}{2}) & \cos(\frac{\alpha}{2}) \end{pmatrix}$$

$$R_z(\alpha) = e^{-i\alpha Z/2} = \begin{pmatrix} e^{-i\frac{\alpha}{2}} & 0 \\ 0 & e^{i\frac{\alpha}{2}} \end{pmatrix}.$$

Наводимо доказ за ротацију око z-осе стања $|\psi\rangle = \cos(\frac{\theta}{2}) + e^{i\phi}\sin(\frac{\theta}{2})$:

$$\begin{pmatrix} e^{-i\frac{\alpha}{2}} & 0 \\ 0 & e^{i\frac{\alpha}{2}} \end{pmatrix} \begin{pmatrix} \cos(\frac{\theta}{2}) \\ e^{i\phi}\sin(\frac{\theta}{2}) \end{pmatrix} = e^{-i\frac{\alpha}{2}}\cos(\tfrac{\theta}{2})\,|0\rangle + e^{i\frac{\alpha}{2}}e^{i\phi}\sin(\tfrac{\theta}{2})\,|1\rangle = \\ = e^{-i\frac{\alpha}{2}}(\cos(\tfrac{\theta}{2})\,|0\rangle + e^{i(\phi+\alpha)}\sin(\tfrac{\theta}{2})\,|1\rangle).$$

Овде опет напомињемо да се релативна фаза стања $|0\rangle$ и $|1\rangle$ не означава на Блоховој сфери, јер је не можемо опазити, па се ново стање на сфери добија ротацијом за угао α око z-осе. Занимљиво је да на основу овог рачуна следи да се ротацијом за $\alpha = 2\pi$ од стања $|\psi\rangle$ добија стање $-|\psi\rangle$. Дакле, да бисмо кубит вратили у почетно стање, потребно је да извршимо ротацију за 4π.

На крају, наводимо још једно својство ових матрица ротације. На основу ортонормираности врста и колона унитарних матрица, произвољно квантно логичко коло над једним кубитом се може представити као:

$$U = e^{i\alpha}R_z(\beta)R_y(\gamma)R_z(\delta),$$

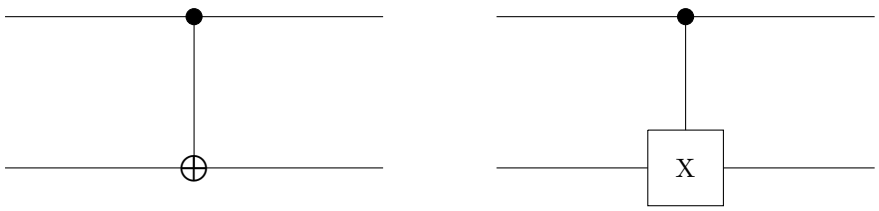
односно као композиција две ротације у односу на z и једне у односу на y-осу.

3.4 Логичка кола над више кубита

Операције над више кубита такође се представљају унитарнима матрицама, а димензије матрица зависе од броја кубита. Најзначајније логичко коло над два кубита је контролисано NOT коло (често се означава као CNOT), која у зависности од стања првог кубита делује на други као обичан квантни NOT или на њега уопште не делује. CNOT је матрица са четири врсте и четири колоне са следећим елементима:

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 11| + |11\rangle\langle 10|,$$

односно стања $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$ преводи редом у стања $|00\rangle$, $|01\rangle$, $|11\rangle$, $|10\rangle$. Приметимо да први кубит остаје непромењен, а други у класичном смислу представља збир по модулу два (што се у рачуну и у колима обележава са $\oplus$).



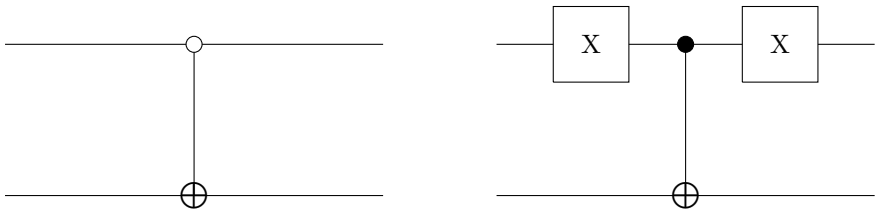
Слика 3: Лево: Шема NOT-а који се извршава ако је контролни кубит 1 (CNOT); Десно: Приказ преко Пауилијевог X (квантног NOT) логичког кола

У квантном смислу, могуће је извршити мерење контролног кубита пре CNOT логичког кола, али и није неопходно, поготово ако нам је циљ да очувамо суперпозицију више стања. Значај CNOT кола ћемо тек касније истакнути и доказати, а огледа се у томе да се сва логичка кола над два или више кубита могу представити само преко јединичних кола и CNOT-а. Зато се CNOT назива и универзално логичко коло.

За свако логичко коло над једним кубитом могуће је увести коло над два или више кубита, тако да су додатни кубити контролни. На пример, ако је дата унитарна матрица $U = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, онда је матрица која описује логичко коло са једним контролним кубитом (U се извршава ако је једнак 1):

$$U_c = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & a & b \\ 0 & 0 & c & d \end{pmatrix}.$$

Такође, можемо уводити логичка кола која се извршавају ако је контролни кубит једнак 0. Математички нема разлике у односу на кола која смо досад увели, док се у колима они могу реализовати употребом два Паулијева X логичка кола, пре и после циљане операције.



Слика 4: NOT који се извршава ако је контролни кубит 0; Шема са белим кружићем (лево) и приказ преко два Паулијева X логичка кола (десно)

Истакнућемо на крају најважније логичко коло над три кубита: NOT коло са два контролна кубита, познато као CCNOT, које оперише као обичан NOT над трећим кубитом само ако су прва два кубита једнака 1. У матричном облику:

$$CCNOT = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix},$$

односно преводи кубите a, b, c у $a, b, c \oplus ab$. CCNOT, познато и као Тофоли коло, је реверзибилно и само је себи инверз, али је његов посебан значај у томе што показује да се све класичне операције могу извршити и са кубитима. Наиме, помоћу Тофоли логичког кола се могу представити сва класична логичка кола, па самим тим и све класиче операције.
Као пример наводимо представљање Шеферовог (НИ) кола, које је универзално за класича кола. За $c = 1$, трећи излазни кубит ће бити $1 + ab = \neg ab$, што је заправо оно што ради НИ коло. Дакле, онда је могуће представити и сва остала класична логичка кола.

3.5 Идентитети са квантним логичким колима

На крају овог поглавља доказаћемо неколико идентитета са квантним логичким колима који се могу користити за упрошћавање кола.

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

$$XYX = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix} = Y$$

$$HXH = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \tfrac{1}{2}\begin{pmatrix} 2 & 0 \\ 0 & -2 \end{pmatrix} = Z$$

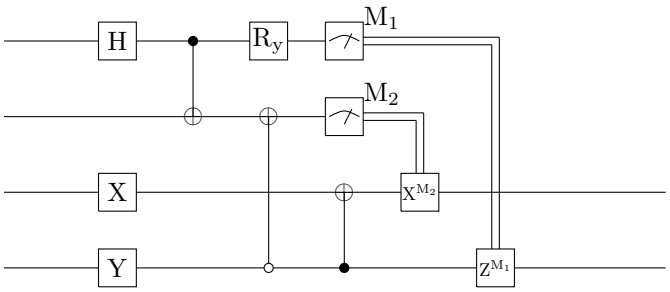
$$HYH = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} i & -i \\ -i & -i \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \tfrac{1}{2}\begin{pmatrix} 0 & 2i \\ -2i & 0 \end{pmatrix} = -Y$$

$$HZH = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \tfrac{1}{2}\begin{pmatrix} 0 & 2 \\ 2 & 0 \end{pmatrix} = X$$

4. Квантно процесирање

4.1 Структура квантних кола

Повезивањем више квантних логичких кола са циљем вршења конкретне операције над кубитима добијају се квантна кола. Визуелно се представљају дијаграмима, сличним као и класична кола, где се поред логичких кола употребљавају и линије, такозване жице. Ипак, линија не мора да означава стварну жицу, већ еволуцију кола у времену, које тече са леве на десну страну. Кубити се такође обележавају једном линијом, па тако на улазу у коло над n кубита има n линија. У квантним колима је могуће вршити мерење кубита и тада се добија информација о његовом стању, а он прелази у измерено стање и надаље се понаша као класичан бит. Обележавамо га са две линије.



Слика 5: Пример једног квантног логичког кола. Ознаке M_1 и M_2 одговарају мерењима кубита

Иако је теоретски могуће све класиче операције извршавати са квантним колима, у квантном рачунарству се у раду са битовима, ради једноставности, могу употребљавати и касична логичка кола. Ипак, због особина кубита, неке ствари на које смо навикли нису дозвољене у квантним колима. Петље нису дозвољене, односно кола су ациклична. Није дозвољено ни да већи број кубита улази у квантно логичко коло него што излази из њега, јер су сва логичка кола описана унитарним матрицама. Обрнуто, један кубит се не може умножити и употребити више пута у истом стању. Заправо, клонирање кубита је принципијелно немогуће, о чему ће касније бити речи. Сетимо се да су овакве манипулације са класичним битовима дозвољење, а примери су обична И и ИЛИ кола или декодери и мултиплексери.

Све операције се извршавају над n кубита у такозваној бази израчунавања $|x_1 x_2 \dots x_n\rangle$. Сваки кубит x_i може бити 0 или 1, па база израчунавања одређује векторски простор стања са 2^n различитих стања. Сва мерења у колу се извршавају у бази израчунавања. Могу се вршити над једним циљаним кубитом или над било којим подскупом базе израчунавања.

Улазни кубити су најчешће у стањима $|0\rangle$, али се узима да се и свако друго стање може припремити у највише n корака.

Квантна логичка кола могу описати са једним кубитом или са било којим подскупом кубита у систему. Постоје универзалне фамилије квантних логичких кола, односно скуп логичких кола преко којих се могу представити сви остали. Један такав скуп чине већ споменути CNOT и логичка кола над једним кубитом.

4.2 Матрице еквивалентних логичких кола

Дату шему кола је могуће поједноставити коришћењем правила за еквивалентно логичко коло у случајевима када су два или више логичких кола везана редно, паралелно или када се односе на исти контролни кубит.

Прво посматрајмо случај када на кубит у стању $|\psi\rangle$ делују логичка кола A и B тако да се над кубитом прво врши операција A. Након проласка кроз A, кубит је у стању $A|\psi\rangle = |\psi'\rangle$, што заправо представља матрицу истих димензија као и матрица полазног стања. Сада на то ново стање делује B, па је коначан резултат $|\psi''\rangle = B|\psi'\rangle = BA|\psi\rangle$. Дакле, одавде видимо да је еквивалентна матрица производ матрица B и A. Како множење матрица није комутативно, на резултат утиче редослед логичких кола у главном колу. Уопштено, ако посматрамо дејство n редно везаних логичких кола $A_1, A_2, \ldots, A_n$, еквивалентна матрица је производ $A_nA_{n-1}\ldots A_2A_1$.

Ако суседна квантна логичка кола делују на дисјунктне подскупове кубита, кажемо да су везана паралелно и самим тим се могу и извршавати истовремено. Нека су дата паралелно везана логичка кола A и B представљена матрицама димензија $m \times n$ и $p \times q$. Тада се еквивалентна матрица добија Декартовим производом матрица A и B и има димензије $mp \times nq$:

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & \ldots & a_{1n}B \\ a_{21}B & a_{22}B & \ldots & a_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}B & a_{m2}B & \ldots & a_{mn}B \end{pmatrix} = \begin{pmatrix} a_{11}b_{11} & a_{11}b_{12} & \ldots & a_{1n}b_{1q} \\ a_{11}b_{21} & a_{11}b_{22} & \ldots & a_{1n}b_{2q} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}b_{p1} & a_{m1}b_{p2} & \ldots & a_{mn}b_{pq} \end{pmatrix}$$

Наравно, када се ради о квантним логичким колима, матрице су квадратне, а број врста је степен двојке. Аналогно, када имамо n паралелно везаних логичких кола, еквивалентна матрица је $A_1 \otimes A_2 \otimes \cdots \otimes A_n$.

Слика 6: Редно (лево) и паралелно (десно) везана логичка кола A и B

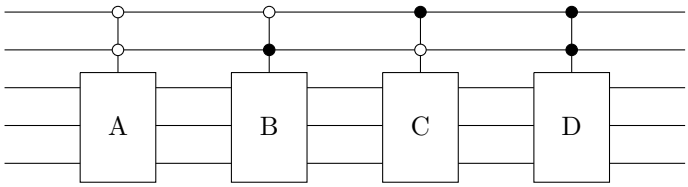
Када се над истим скупом кубита логичко коло A $(m \times n)$ извршава ако је резултат контролног кубита 0, а B $(p \times q)$ ако је резултат 1, онда се њихов еквивалент представља као матрица $(m + p) \times (n + q)$:

$$A \oplus B = \begin{pmatrix} A & 0_{m\times q} \\ 0_{p\times n} & B \end{pmatrix}$$

Аналогно, када имамо више од две матрице, еквивалент је њихов горе дефинисан збир:

$$A_1 \oplus A_2 \oplus \cdots \oplus A_n.$$

Овде је $n = 2^s$, где је s број контролних кубита. Свако од логичких кола оперише само за једно стање контролних кубита. Матрица A_1 одговара стању где су сви кубити 0, а матрица A_n стању где су сви једнаки 1.



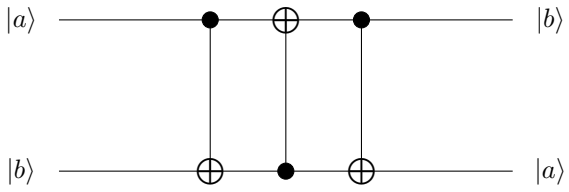
Слика 7: Пример са два контролна кубита; еквивалентна матрица је $A \oplus B \oplus C \oplus D$

Користећи три наведена правила, кола се могу поједноставити и често свести само на извршавање једне еквивалентне матрице, што значајно олакшава рачун и омогућава једноставније праћење квантних кола.

4.3 Примери квантних кола

Као што је већ објашњено, главно коло можемо састављати од произвољног броја логичких кола над коначним бројем кубита, докле год је све повезано према наведеним правилима. Наравно, квантно коло може бити састављено и само од једног логичког кола и једног кубита. У наставку ћемо навести неколико примера, крећући од једноставнијих.

Користећи само три CNOT логичка кола можемо саставити коло које размењује стања два кубита (слика).



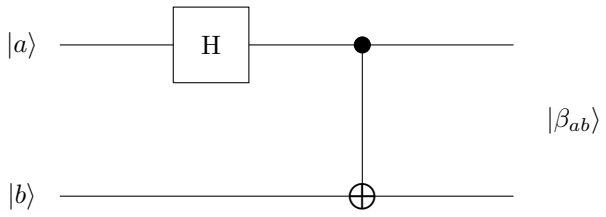
Слика 8: Коло које размењује стања два кубита - SWAP коло

Проверимо шта ово коло заправо ради. Ако су улазни кубити $|a\rangle$ и $|b\rangle$, онда се након првог CNOT-а добија $|a, b \oplus a\rangle$, а после другог $|a \oplus (b \oplus a), b \oplus a\rangle$. Како је за свако стање $a \oplus a = 0$, то је заправо добијено стање $|b, b \oplus a\rangle$. На крају, после треће операције добијамо $|b, (b \oplus a) \oplus b\rangle$, што је у ствари $|b, a\rangle$. Дакле, ово коло заиста размењује стања два кубита.

Следеће наводимо коло које на основу два кубита у стањима $|0\rangle$ или $|1\rangle$ формира кубите у Беловим стањима. Подсетимо се да смо већ увели Белово стање као $|\beta_{00}\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$, међутим сродна су и стања:

$$|\beta_{01}\rangle = \frac{|01\rangle+|10\rangle}{\sqrt{2}}$$
$$|\beta_{10}\rangle = \frac{|00\rangle-|11\rangle}{\sqrt{2}}$$
$$|\beta_{11}\rangle = \frac{|01\rangle-|10\rangle}{\sqrt{2}}.$$

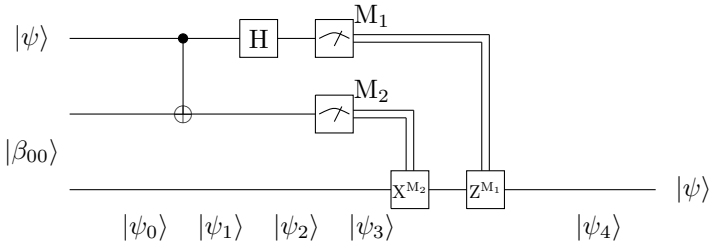
Као и стање $|\beta_{00}\rangle$, и остала Белова стања су увезана и представљају ЕПР парове. Стога, мерењем једног кубита, одређена је и вредност другог. Особине ових стања користићемо у наредном примеру, а сада наводимо шему жељеног кола:



Слика 9: Коло за стварање ЕПР парова

Проучимо механизам овог кола. Ако су улазна стања $|0\rangle$ и $|0\rangle$, након Адамаровог логичког кола, први кубит је у стању $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$. Након CNOT-а се други кубит из стања $|0\rangle$ обрће само ако је први једнак један, односно добијамо стање $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$, што представља $|\beta_{00}\rangle$. Слично је и за остале могућности за a и b.

Занимљив и значајан пример је квантна телепортација. Проблем се састоји у следећем: Ана и Бојан су удаљени, али свако у свом поседу има један кубит из ЕПР пара β_{00} који су генерисали док су били заједно. Анин циљ је да непознато стање $|\psi\rangle$ пренесе Бојану тако што ће му послати само два класична бита.



Слика 10: Шема кола које омогућава квантну телепортацију

На приказаној слици, прва два кубита припадају Ани, а трећи Бојану. На почетку, Ана има кубит у стању $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ и један део ЕПР пара, а Бојан други део, односно укупно стање је:

$$|\psi_0\rangle = (\alpha|0\rangle + \beta|1\rangle)\frac{|00\rangle + |11\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}}(\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|00\rangle + |11\rangle)).$$

Ана пропушта своја два кубита кроз CNOT логичко коло и мења други кубит када је први једнак 1:

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}(\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|10\rangle + |01\rangle)).$$

Након тога, Ана пропушта први кубит кроз Адамарово логичко коло и добија:

$$|\psi_2\rangle = \frac{1}{2}(\alpha(|0\rangle + |1\rangle)(|00\rangle + |11\rangle) + \beta(|0\rangle - |1\rangle)(|10\rangle + |01\rangle)) =$$
$$= \frac{1}{2}(|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle) + |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(\alpha|1\rangle - \beta|0\rangle)).$$

Мерењем, Ана утврђује стања првог и другог кубита, а самим тим, због увезаности, и стање трећег кубита који се налази код Бојана. Резултат који добије шаље Бојану (само два класична бита), а на основу њега Бојан реконструише стање $|\psi\rangle$. Ако Ана измери $|00\rangle$, Бојанов кубит је већ у стању $\alpha|0\rangle + \beta|1\rangle = |\psi\rangle$. Ако Ана измери $|01\rangle$, Бојан треба да употреби X логичко коло како би добио $|\psi\rangle$. Слично, Ако Ана измери $|10\rangle$, Бојан употребљава Z логичко коло, а у сличају резултата мерења $|11\rangle$ користи прво X, па Z логичко коло. Дакле, на основу два резултата M_1 и M_2 која добије од Ане, Бојан од трећег кубита стања $|\psi_3\rangle$, употребом трансформације $Z^{M_1}X^{M_2}$ (редно везани), добија почетно непознато стање $|\psi\rangle$.

На овај начин је, само на основу два бита класиче информације, користећи својства увезаних стања, пренет (телепортован) непознат кубит $|\psi\rangle$ од Ане до Бојана. Телепортација није тренутна, јер се мора пренети класична информација од Ане до Бојана, па је њена брзина ипак мања од брзине светлости. Међутим, важно је разумети да кубит није дуплиран, већ је само пренет, зато што Ани уместо стања $|\psi\rangle$ остаје оно стање које је добила мерењем M_1. Заправо, принципијелно није могуће копирати непознато стање кубита.

У класичним колима, умножавање бита се може реализовати класичним CNOT логичким колом где су на улазу циљани бит x и нула, а на излазу x и $x \oplus 0 = x$. Међутим, у квантном случају, ако је контролни кубит $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, а други $|0\rangle$, излаз ће бити стање $\alpha|00\rangle + \beta|11\rangle$. Како је заправо $|\psi\rangle \otimes |\psi\rangle = \alpha^2|00\rangle + \alpha\beta|01\rangle + \alpha\beta|10\rangle + \beta^2|11\rangle$, то су ова два стања иста ако и само ако је $\alpha\beta = 0$. Дакле, копирање успешно ради само за $|0\rangle$ или $|1\rangle$, тј. само за класичан бит.

Уопштено, може се показати да је теоретски могуће клонирати ортогонална стања, али није могуће клонирати произвољна стања. Ово је једна од кључних разлика између квантних и класичних битова коју смо навели још када смо математички уводили кубите.

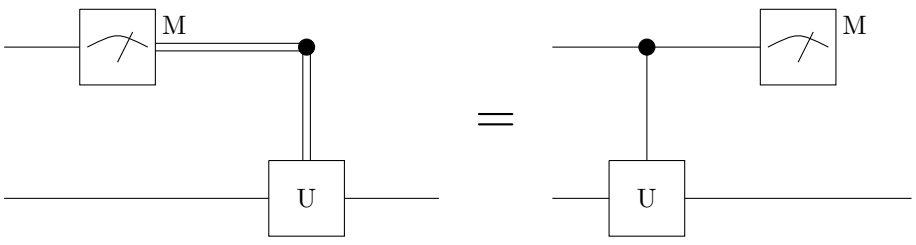
4.4 Мерење у колима

До сада смо се упознали са основним механизмом мерења кубита. Дакле, резултат мерења је једно конкретно стање из базе израчунавања, а након мерења кубит прелази у то стање. Видели смо да се након тога кубит понаша као класичан бит, те га у колима представљамо са две линије.

Постоје две теореме које се односе на мерења кубита у колима и које нам могу бити од користи.

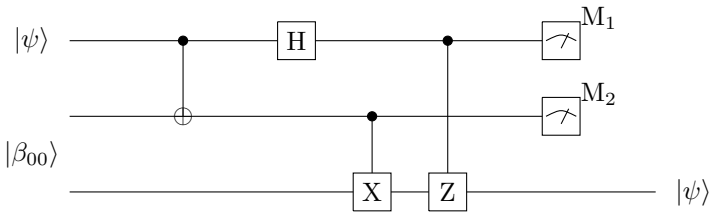
Принцип одложеног мерења: Мерења се увек могу померити са средине квантног кола на његов крај. Уколико се негде у колу користи резултат мерења, класичне операције могу бити замењене квантним контролисаним операцијама.

Принцип одложеног мерења графички можемо приказати на следећи начин:



Слика 11: Илустрација Принципа одложеног мерења

Као пример можемо навести коло које смо користили за квантну телепортацију. Ако мерења у средини кола заменимо контролисаним операцијама, изгубићемо преношење класичне информације између Ане и Бојана, али ће резултат рада кола бити исти. Дакле, операција X се извршава ако је други, а операција Z ако је први Анин кубит једнак 1. Приметимо да је ово ефективно исто као и када смо први пут наводили телепортацију, само што нема мерења кубита до самог краја.



Слика 12: Шема кола за квантну телепортацију добијена коришћењем Принципа одложеног мерења

За мерење смо досад навели да је иреверзибилан (неповратан) процес, јер квантну информацију претвара у класичну. Ипак, ако мерење не открива информацију о квантном стању, испоставља се да онда оно може бити повратно. Наведимо сада један логичан принцип.

Принцип имплицитног мерења: Без умањења општости, за све кубите који нису измерени може се на крају кола претпоставити да су измерени.

Заиста, ако је неки кубит измерен у средини кола, а неки други на самом крају, резултат мерења кубита на крају кола не сме утицати на претходно мерење првог кубита у средини кола. На томе почива овај принцип.

4.5 Универзална логичка кола

У овом одељку ћемо доказати, као што смо раније навели, да постоје универзалне фамилије квантних логичких кола, односно скупови логичких кола преко којих се могу представити сви остали. Доказаћемо универзалност CNOT логичког кола и навести неколико логичких кола над једним кубитом који са њим чине тражену фамилију.

Прво ћемо показати како се произвољна унитарна матрица U може представити као производ неколико унитарних матрица које се разликују од јединичне само по пољима у пресеку врста и колона са индексима $i, j \in \{1, 2, \ldots, d\}$, где је d димензија матрице U. На пример, такве су матрице:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & a & b \\ 0 & 0 & c & d \end{pmatrix} \text{ и } \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & a & 0 & b \\ 0 & 0 & 1 & 0 \\ 0 & c & 0 & d \end{pmatrix}$$

Овакве матрице делују нетривијално на највише два вектора из простора стања.

Илустроваћемо поступак представљања произвољне матрице на матрици U димензија 3×3 преко три матрице које имају претходно описано својство.

Нека је дата матрица:

$$U = \begin{pmatrix} a & d & g \\ b & e & h \\ c & f & i \end{pmatrix}.$$

Наш циљ је да нађемо три матрице U_1, U_2, U_3 такве да важи $U_3U_2U_1U = I$ (I је јединична матрица 3×3), јер ће тада важити $U = U_1^\dagger U_2^\dagger U_3^\dagger$.

Први корак је да поништимо елемент b. То постижемо на следећи начин: Ако је $b = 0$, онда је $U_1 = I$, иначе:

$$U_1 = \begin{pmatrix} \frac{a^*}{\sqrt{|a|^2+|b|^2}} & \frac{b^*}{\sqrt{|a|^2+|b|^2}} & 0 \\ \frac{b}{\sqrt{|a|^2+|b|^2}} & \frac{-a}{\sqrt{|a|^2+|b|^2}} & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Онда се добија: $U_1U = \begin{pmatrix} a' & d' & g' \\ 0 & e' & h' \\ c' & f' & i' \end{pmatrix}$. Следећи корак је да на месту c' стоји нула, а у горњем левом углу јединица. То постижемо тако што је:

$$U_2 = \begin{pmatrix} a'^* & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \text{ за } c' = 0, \text{ а иначе } U_2 = \begin{pmatrix} \frac{a'^*}{\sqrt{|a'|^2+|c'|^2}} & 0 & \frac{c'^*}{\sqrt{|a'|^2+|c'|^2}} \\ 0 & 1 & 0 \\ \frac{c'}{\sqrt{|a'|^2+|c'|^2}} & 0 & \frac{-a'}{\sqrt{|a'|^2+|c'|^2}} \end{pmatrix}.$$

Добијамо као резултат унитарну матрицу чија је прва колона $(1, 0, 0)$, па је и њена прва врста иста таква, јер мора да има норму 1:

$$U_2U_1U = \begin{pmatrix} 1 & 0 & 0 \\ 0 & e'' & h'' \\ 0 & f'' & i'' \end{pmatrix}.$$

Сада одговарајућим избором $U_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & e''^* & f''^* \\ 0 & h''^* & i''^* \end{pmatrix}$, постижемо да је $U_3U_2U_1U = I$, односно $U = U_1^\dagger U_2^\dagger U_3^\dagger$, што нам је и био циљ.

На сличан начин поступамо и када је матрица већих димензија. Ако матрица U има d врста, можемо наћи $d-1$ унитарних матрица које нетривијално делују највише на два вектора тако да је њихов производ са U матрица која у првој врсти и првој колони има све нуле осим јединице у горњем левом углу. Сада поступак понављамо за подматрицу без прве врсте и прве колоне (димензија $(d-1) \times (d-1)$). Поступак се понавља за сваку следећу подматрицу све док се не добије јединична матрица. За то је потребно највише:

$$(d-1) + (d-2) + \cdots + 2 + 1 = \frac{d(d-1)}{2} \text{ унитарних матрица.}$$

Следећи корак је да представимо деловање једне од њих преко квантних логичких кола. Како свака нетривијално делује на највише два стања, нека су то $|s\rangle$ и $|t\rangle$, од јединичне матрице се разликује само за унитарну матрицу 2×2, коју ћемо звати V. Ако се регистар са којим радимо састоји од n кубита, онда се стања $|s\rangle$ и $|t\rangle$ могу представити као n-тоцифрени бинарни бројеви: $s = s_1 \dots s_n$ и $t = t_1 \dots t_n$. Представићемо прелаз од стања $|s\rangle$ до стања $|t\rangle$, користећи Грејев код, као прелаз од броја s до броја t тако да се свака два узастопна броја

разликују за тачно једну цифру. Овакво представљање има највише $n+1$ корак, где су s и t редом први и последњи. Обележимо ове кораке са $|g_1\rangle, |g_2\rangle, \ldots, |g_m\rangle$.
Нека се стања $|g_1\rangle$ и $|g_2\rangle$ разликују на i-том кубиту. Тада прелаз $|g_1\rangle \to |g_2\rangle$ обезбеђујемо обртањем i-тог кубита под условом да су сви остали једнаки. Слично се обезбеђују и прелази од $|g_2\rangle \to |g_3\rangle$ до $|g_{m-2}\rangle \to |g_{m-1}\rangle$. Дакле, овакво коло постиже следеће промене:

$$\begin{gathered} |g_1\rangle \to |g_{m-1}\rangle \\ |g_2\rangle \to |g_1\rangle \\ |g_3\rangle \to |g_2\rangle \\ \vdots \\ |g_{m-1}\rangle \to |g_{m-2}\rangle \end{gathered}$$

Нека се $|g_{m-1}\rangle$ и $|g_m\rangle$ разликују на j-том кубиту. Онда је потребно на j-ти бит стања $|g_{m-1}\rangle$ применити матрицу V под условом да су сви остали кубити одговарајући. Поновном применом првог дела кола у инверзном поретку добија се жељени резултат.

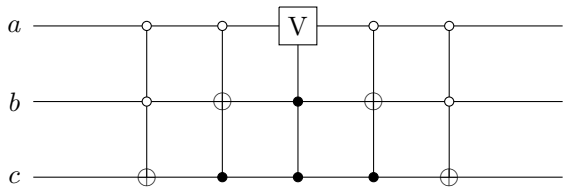
Применимо све претходно наведено на једном примеру. Нека је дата матрица:

$$U_k = \begin{pmatrix} a & 0 & 0 & 0 & 0 & 0 & 0 & c \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ b & 0 & 0 & 0 & 0 & 0 & 0 & d \end{pmatrix}.$$

Она нетривијално делује на стања $|000\rangle$ и $|111\rangle$, а одговарајућа матрица $V = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$.
Грејев код између ових стања је:

a	b	c
0	0	0
0	0	1
0	1	1
1	1	1

Одговарајуће коло за интерпретацију матрице U преко квантних логичких кола је приказано на слици. Оно прво мења трећи кубит ако су прва два нуле, па мења други ако је први 0 и трећи 1, а потом примењује V ако су други и трећи јединице. У наставку ради исто што и у прва два корака, само у обрнутом редоследу.



Слика 13: Представљање матрице U преко квантних логичких кола

Дакле, за представљање произвољне унитарне матрице U_k која делује на два вектора простора стања у рачунару са n кубита потребно је највише $2(n-1)$ операција од $|g_1\rangle$ до $|g_{m-1}\rangle$ и назад. Свака од ових операција се може представити преко CNOT-а и логичких кола над једним кубитом у сложености $O(n)$. Како се и контролисани V може представити у сложености $O(n)$, то једну овакву матрицу можемо представити преко $O(n^2)$ CNOT-а и логичких кола над једним кубитом.

Раније смо добили да се произвољна унитарна матрица U може представити преко $2^{n-1}(2^n-1)$ матрица попут U_k, па је укупно потебно $O(4^n n^2)$ логичких кола над једним кубитом и CNOT-а. Видимо да је ово експоненцијална зависност од n, што нам говори да не можемо произвољан алгоритам на овај начин имплементирати ефикасно у квантним рачунарима. Ипак, постоје алгоритми који имају значајно мању сложеност и у предности су у односу на класичне алгоритме, а којима ћемо се касније детаљније позабавити.

На крају, важно је напоменути и да се произвољно логичко коло над једним кубитом може апроксимирати до жељене тачности користећи само четири логичка кола: Адамаров H, CNOT и два која сада уводимо:

$$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \text{ и } T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$$

и који се редом зову фазно и $\pi/8$ логичко коло. Стога ова четири логичка кола чине једну фамилију универзалних логичких кола. Доказ за ову тврдњу лежи у чињеници да се преко њих могу представити ротације око све три осе до произвољне тачности.

5. Класе сложености проблема

5.1 Теорија сложености

Теорија сложености изучава ресурсе који су потребни да се одређени проблеми реше у општем случају, односно када улазни подаци могу бити изузетно велики. Постоје различите процене сложености, па је тако важно колико је времена, колико основних операција у рачунару, меморијских ресурса или упита потребно за одређено израчунавање. Најчешће се процена врши у такозваном најгорем случају и довољно ју је прецизирати до одређеног реда величине. Тако се као класе издвајају логаритамске, линеарне, полиномијалне и експоненцијалне сложености. Углавном ћемо се бавити бројем операција, за које се узима да су сразмерне времену извршавања, али јако значајни могу бити и просторни ресурси. Често се за проблеме који се могу решити у полиномијалном броју операција каже да могу бити ефикасно решени.

Сложеност процеса се изучава и у класичном рачунарству, али квантно рачунарство доноси нови приступ и могућност да неки проблеми за које није постојало ефикасно решење сада буду решени. Наиме, сложеност симулације квантних система на класичним рачунарима експоненцијално расте са порастом димензије система, док је у квантном рачунарству зависност линеарна. Према Муровом закону, сваке две године моћ класичних рачунара се удвостручи, што је еквивалентно додавању само једног кубита у квантним рачунарима. То већ говори о њиховој видљивој предности. Међутим, као што смо досад видели, линеаран број кубита, када се измери, даје само линеаран број класичних битова, па одређена количина информација остаје скривена. Стога, иако се сви процеси који се могу извести на класичним рачунарима могу извести и на квантним, није доказано да квантни рачунари заиста имају предност у односу на класиче.

Теорија сложености израчунавања дели проблеме у класе тако да су у истој класи проблеми који захтевају сличне количине ресурса. У наставку ћемо навести неке основне у класичном и квантном рачунарству.

5.2 Класе сложености у класичном рачунарству

Најзначајније класе проблема су **P** (полиномијално време) и **NP** (недетерминистичко полиномијално време). Прва група представља проблеме који за кратко време могу бити експлицитно решени на класичном рачунару. То су, на пример, множење два броја или рачунање детерминанте матрице. Са друге стране, за проблеме у **NP** је могуће брзо проверити да ли одређено решење испуњава услове, али није пронађено ефикасно решење у општем

случају. Један такав пример је растављање броја на просте чиниоце: лако је проверити да ли су дати бројеви прости фактори неког већег броја, али је растављање великог броја на просте чиниоце на класичном рачунару веома споро. Очигледно, сви проблеми који су у **P**, морају бити и у **NP**, па важи $\mathbf{P} \subseteq \mathbf{NP}$, али није познато да ли је $\mathbf{P} \neq \mathbf{NP}$ или важи $\mathbf{P} = \mathbf{NP}$. Постоји подскуп **NP**, такозвани **NP**-комплетни проблеми, чијим би решавањем уз мање прилагођавање били решени и сви остали проблеми из тог подскупа, али до сада ниједан **NP**-комплетан проблем није решен.

Може се увести и класа **BPP**, која представља скуп проблема који се са одређеном вероватноћом, произвољном мањом од 1, али се обично узима $\frac{2}{3}$, могу решити у полиномијалном времену.

Следећа важна класа је **PSPACE**, класа проблема који у неограниченом времену могу бити решени са полиномијалним бројем битова. Очигледно, **P** је подскуп класе **PSPACE**, јер ако је проблем решив у полиномијалном броју корака, онда не може захтевати више од полиномијалног броја битова. Такође важи и да је **NP** подскуп **PSPACE**, јер ако је могуће проверити решење у полиномијалном времену, могуће је и обрадити све могуће случајеве у неограниченом времену и полиномијалној меморији тако што не меморишемо претходне провере. Иако се верује да је **PSPACE** строго већи од **P**, није пронађен проблем у **PSPACE** који није у **P**. Стога, за сада знамо само да важи $\mathbf{P} \subseteq \mathbf{NP} \subseteq \mathbf{PSPACE}$.

Класа која садржи **PSPACE** је **EXP**, односно класа проблема који могу бити решени у експоненцијалном времену. Разлог за то је што, иако решења проблема који су у у **PSPACE** немају ограничено време, имају ограничену меморију, па и максимално експоненцијалан број стања у којима се могу наћи. Дакле, важи $\mathbf{PSPACE} \subseteq \mathbf{EXP}$.

5.3 Класе сложености у квантном рачунарству

Увођењем квантног рачунарства настају и нове класе проблема који се могу решавати на квантним рачунарима. Могуће је и успостављати везе између већ постојећих класа, али и између постоћих и нових класа.

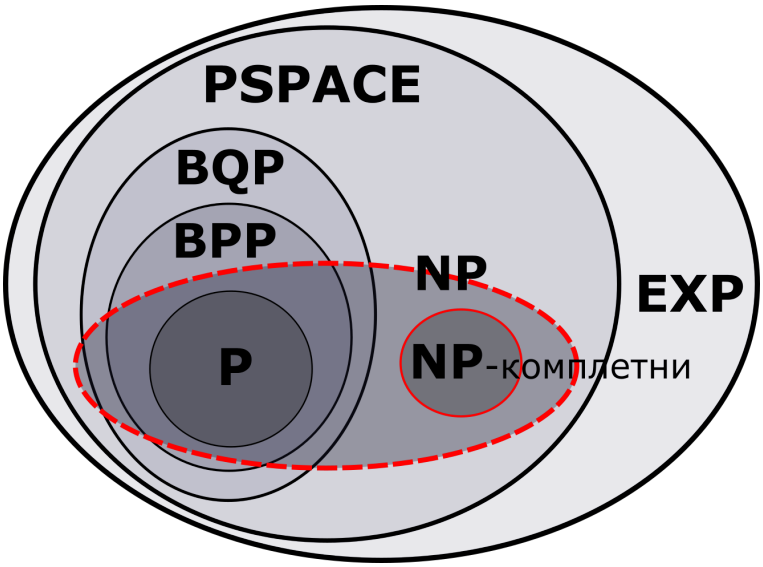
Најзначајнија нова класа која се природно намеће је **BQP** - проблеми који могу са одређеном вероватноћом (на пример $\frac{2}{3}$) бити решени на квантном рачунару у полиномијалном времену. Већ смо навели да се класична логичка кола могу представити преко квантних. Такође, могуће је симулирати насумичне битове користећи Адамарово логичко коло. Дакле, сви проблеми решени на класичном рачунару у полиномијалном времену могу бити решени и на квантним рачунарима ефикасно, па вжи $\mathbf{P} \subseteq \mathbf{BQP}$ и $\mathbf{BPP} \subseteq \mathbf{BQP}$. Додатно, познато је да сваки проблем који може бити решен у полиномијалном времену на квантним рачунарима, може бити решен са полиномијалном меморијом на класичним, односно $\mathbf{BQP} \subseteq \mathbf{PSPACE}$. Разлог за то је што свако квантно логичко коло може бити до произвољне тачности представљено на класичном рачунару са полиномијалним просторним ресурсима.

Ипак, још увек није познато да ли је заиста квантни рачунар моћнији од класичног. Стога није познато ни да ли је $\mathbf{BPP} \neq \mathbf{BQP}$. Проналажење доказа за то би водило и до закључка да је $\mathbf{BPP} \neq \mathbf{PSPACE}$, али овако стаје могуће и да је $\mathbf{P} = \mathbf{PSPACE}$.

Један од проблема који нису за сада ефикасно решени на класичном рачунару, а познат је алгоритам за његово ефикасно решавање на квантном рачунару је растављање броја на просте чиниоце. То је, као што смо већ описали, проблем који припада класи **NP**, односно постоји пресек класа **NP** и **BQP**, али није познат њихов тачан однос. Нажалост, растављање

броја на просте чиниоце није **NP**-комплетан проблем, па његовим решавањем нису решени остали проблеми из те класе.

Алгоритам за ефикасно растављање броја на просте чиниоце је један од неколико познатих алгоритама који остварују боље перформансе при решавању одређених проблема него класични рачунари. Ипак, као што смо видели, не доказује надмоћ квантних рачунара. Тек евентуални формални доказ би допринео бољем схватању односа међу калсама сложености проблема. На слици испод је илустровано оно што је до сада познато.



Слика 14: Однос између класа сложености проблема. Познато је да важи **P** ⊆ **NP** ⊆ **PSPACE** и **P** ⊆ **BPP** ⊆ **BQP** ⊆ **PSPACE** ⊆ **EXP**

6. Предности квантних рачунара

6.1 Паралелно процесирање

Основна предност квантних рачунара у односу на класичне је могућност паралелног процесирања. Оно се заснива на квантномеханичком својству које смо досад сретали - суперпозицији. Када кубит доведемо у суперпозицију више жељених стања, једним извршавањем операције над њим заправо паралелно извршавамо операцију над сваким стањем појединачно.

Испитајмо то на следећем примеру. Нека је $f : \{0,1\} \to \{0,1\}$ функција која оперише над вредностима кубита. Формирајмо логичко коло U_f које за улазно стање два кубита $|x, y\rangle$ враћа стање $|x, y \oplus f(x)\rangle$. Ако је $y = 0$, излазна вредност другог кубита је заправо $f(x)$. Ако први кубит доведемо у суперпозицију више стања, могуће је рачунати вредност функције f у више различитих тачака истовремено.
То можемо постићи полазећи од стања $|0\rangle$ за оба кубита. Ако пре извршавања логичког кола U_f применимо H логичко коло над првим кубитом, почетно стање ће бити $\frac{|0\rangle+|1\rangle}{\sqrt{2}}|0\rangle$, а излазно $\frac{|0,f(0)\rangle+|1,f(1)\rangle}{\sqrt{2}}$. Дакле, успели смо да једним примењивањем U_f логичког кола израчунамо вредност функције $f(x)$ за два различита x.

Овај поступак је могуће уопштити и израчунавати за произвољан број кубита. Ако имамо два кубита које пропуштамо кроз Адамарово логичко коло, постижемо суперпозицију:

$$\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) = \frac{|00\rangle + |01\rangle + |10\rangle + |11\rangle}{2}$$

и можемо вршити израчунавање за четири тачке истовремено.
Слично, за n кубита, ако применимо H логичко коло n пута добијамо суперпозицију стања:

$$\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle$$

где x узима сва могућа стања од $|00\ldots0\rangle$ (n нула), до $|11\ldots1\rangle$ (n јединица). Постављањем $(n+1)$-ог кубита у стање $|0\rangle$ и коришћењем логичког кола U_f над овим кубитима добијамо излаз:

$$\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x, f(x)\rangle.$$

Ипак, иако смо успели да једном операцијом израчунамо $f(x)$ за чак 2^n различитих вредности x, мерењем овај кубит колапсира у само једно стање, односно само један пар $|x, f(x)\rangle$. Стога, неопходно је осмислити одговарајући алгоритам којим је могуће из суперпонираног стања извући информацију за коју би класичним израчунавањем било потребно више корака. Навешћемо један такав пример.

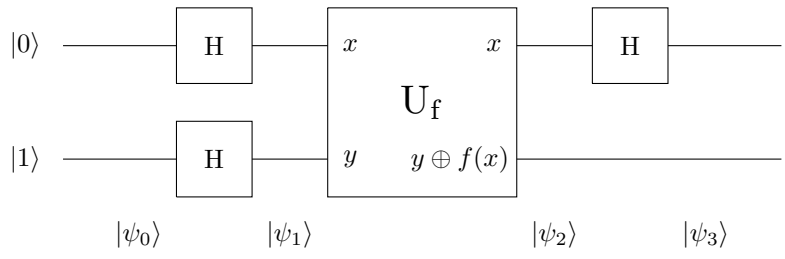
Полазимо од два кубита у стањима $|0\rangle$ и $|1\rangle$ и примењујемо на њима H логичко коло. Добијамо стање $|\psi_1\rangle = \left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$. Погледајмо шта се добија применом U_f логичког кола над кубитима $|x\rangle\,\frac{|0\rangle-|1\rangle}{\sqrt{2}}$. Ако је $f(x) = 0$, излазно стање је $|x\rangle\,\frac{|0\rangle-|1\rangle}{\sqrt{2}}$, а за $f(x) = 1$ добијамо $|x\rangle\,\frac{|1\rangle-|0\rangle}{\sqrt{2}}$. Дакле, у општем случају резултат је $(-1)^{f(x)}\,|x\rangle\,\frac{|0\rangle-|1\rangle}{\sqrt{2}}$. Онда из стања $|\psi_1\rangle$ добијамо:

$$|\psi_2\rangle = \pm\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right), \text{ за } f(0) = f(1);$$
$$|\psi_2\rangle = \pm\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right), \text{ за } f(0) \neq f(1).$$

Даље применом H логичког кола на првом кубиту добијамо:

$$|\psi_3\rangle = \pm\,|0\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right), \text{ за } f(0) = f(1);$$
$$|\psi_3\rangle = \pm\,|1\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right), \text{ за } f(0) \neq f(1),$$

односно општије резултат је: $|\psi_3\rangle = \pm\,|f(0) \oplus f(1)\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$. Мерењем првог кубита сада са вероватноћом 1 добијамо резултат $f(0) \oplus f(1)$. Приметимо да смо опет извршили само једну итерацију U_f, док су у класичном случају за рачунање овог збира потребне две итерације. Дакле, успели смо да одредимо глобално својство функције ефикасније него на класичном рачунару. Алгоритам који смо описали је једноставна верзија Дојчовог алгоритма. На сличном принципу се заснива и алгоритам који ћемо следећи навести.



Слика 15: Коло за имплементацију Дојчовог алгоритма

6.2 Дојч-Јожа алгоритам

Нека је дата функција $f(x)$, где је $x \in \{0, 1, \ldots, 2^n - 1\}$, која је или константна или балансирана, тј. или узима једну исту вредност за све x или узима вредност 0 за тачно пола бројева из домена, а вредност 1 за другу половину. Наш задатак је да одредимо каква је

функција заправо. На класичним рачунарима било би неопходно да израчунамо вредност функције у $2^{n-1}+1$ тачака да бисмо са сигурношћу одговорили на питање. Са друге стране, са квантним рачунарима проблем је могуће решити у линеарној сложености, ако применимо уопштење већ описаног Дојчовог алгоритма, познато као Дојч-Јожин алгоритам.

Први корак је да припремимо n кубита у стању $|0\rangle$ и један у стању $|1\rangle$, односно:

$$|\psi_0\rangle = |00\ldots0\rangle\,|1\rangle \ (n \text{ нула})$$

Након тога примењујемо Адамарово H логичко коло на сваки од њих и добијамо стање:

$$|\psi_1\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

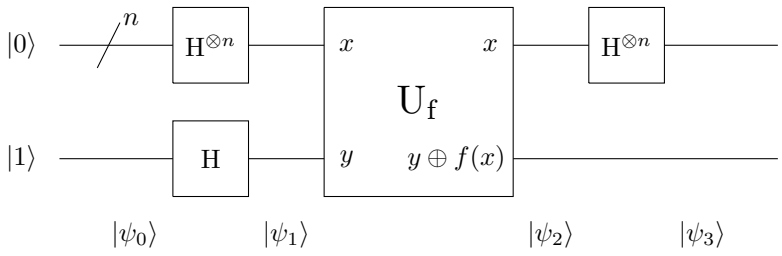
Сада применимо логичко коло $U_f : |x, y\rangle \to |x, y \oplus f(x)\rangle$ на првих n кубита. Већ смо показали да се деловањем U_f на кубит $|x\rangle \frac{|0\rangle-|1\rangle}{\sqrt{2}}$ добија стање $(-1)^{f(x)}\,|x\rangle \frac{|0\rangle-|1\rangle}{\sqrt{2}}$, односно ново стање $(n+1)$-ог кубита је:

$$|\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{f(x)}\,|x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

Поново примењујемо H логичко коло на првих n кубита. Како се, за један кубит, деловање Адамаровог логичког кола може представити као: $H\,|x\rangle = \frac{1}{\sqrt{2}} \sum_{z=0}^{1} (-1)^{xz}\,|z\rangle$, то ће ново стање бити:

$$|\psi_2\rangle = \frac{1}{\sqrt{2^n}} \left(\sum_{x=0}^{2^n-1} (-1)^{f(x)} \frac{1}{\sqrt{2^n}} \sum_{z=0}^{2^n-1} (-1)^{xz}\,|z\rangle \right) \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) =$$
$$\frac{1}{2^n} \sum_{x=0}^{2^n-1} \sum_{z=0}^{2^n-1} (-1)^{f(x)+xz}\,|z\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

Сада мерењем првих n кубита долазимо до решења. Наиме, ако је функција константна, коефицијент уз стање $|00\ldots0\rangle$ (тј. стање $x = 0$) је $+1$ или -1, у зависности од вредности коју $f(x)$ узима. Одатле закључујемо да је амплитуда тог стања 1, односно мерењем морамо добити тај резултат. Ако је функција балансирана, сабирци у коефицијенту уз стање $x = 0$ се потиру, односно амплитуда је 0, па сигурно нећемо добити то стање. Дакле, када измеримо стање првих n кубита, ако добијемо резултат $|00\ldots0\rangle$, функција је константна, за сваки други резултат који измеримо је балансирана. Важно је напоменути да Дојч-Јожин алгоритам ради у свим случајевима, односно са само једном применом U_f увек враћа тачан резултат.



Слика 16: Коло за имплементацију Дојч-Јожиног алгоритма; прва линија представља n кубита

Иако овај проблем није посебно значајан и његово решење није примењено за решавање осталих проблема, показује нам на који начин квантни рачунари могу да превазиђу класичне. Међутим, приметимо да дизајнирање квантних алгоритама уопште није једноставан задатак, поготово када нам је циљ да значајно умањимо сложеност. Тако се, на пример, овај проблем може решити пробабилистички на класичном рачунару до велике сигурности и са знатно мање покушаја од 2^n, али ако проблем желимо да решимо са сигурношћу, циљ је испуњен. Зато се сматра да је Дојч-Јожин алгоритам[1] веома значајан и свакако је настао пре следећа два алгоритма која наводимо.

6.3 Гроверов алгоритам

Квантни рачунари нам омогућавају оптимизацију проналажења решења у скупу од N могућих решења. На класичним рачунарима, потребно је проверити свако могуће решење, па је одговарајућа сложеност $O(N)$. Међутим, користећи квантну претрагу, тачније Гроверов алгоритам[2], могуће је дати проблем решити у сложености $O(\sqrt{N})$.

Прво ћемо увести такозвану црну кутију која проверава да ли је улазни параметар решење које тражимо. У класичном случају, то би била функција $f(x)$ која враћа један ако је одговор потврдан, а нула у супротном. Начин рада црне кутије нећемо разматрати, јер зависи и од самог проблема, али ће наш циљ бити да пронађемо жељено решење са што мање њеног позивања. На пример, ако нам је задатак да пронађемо просте факторе неког броја m претрагом од 2 до $\sqrt{m}$, црна кутија би обављала дељење броја m са улазним параметром и у зависности од остатка враћала 0 или 1.
У квантном случају, смисао црне кутије је исти, али је принцип рада мало другачији. Наиме, као и раније, користићемо стање $|x\rangle \frac{|0\rangle-|1\rangle}{\sqrt{2}}$ и трансформацију $|x,y\rangle \to |x, y \oplus f(x)\rangle$. Ово стање остаје непромењено ако $|x\rangle$ није тражено решење, а у супротном се обрће. У општем случају, ново стање је $(-1)^{f(x)}|x\rangle \frac{|0\rangle-|1\rangle}{\sqrt{2}}$. У наставку ћемо посматрати кубите из регистра без последњег, који се никада не мења, па можемо рећи да црна кутија врши трансформацију:

$$|x\rangle \to (-1)^{f(x)}|x\rangle$$

За претрагу $N = 2^n$ случајева, потребно нам је $n+1$ кубит. Првих n доведемо у стање $|0\rangle$, а последњи у стање $|1\rangle$. Након тога, све их пропустимо кроз H логичко коло. На тај начин, последњи кубит смо довели у жељено стање, а првих n у суперпозицију $\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle$. Приметимо да сва стања имају једнаку амплитуду. Наш задатак је да повећамо амплитуду решења x_0 које тражимо. То се постиже применом Гроверовог оператора на првих n кубита потребан број пута. Гроверов оператор се састоји од црне кутије, два $H^{\otimes n}$ логичка кола и једног фазног логичког кола Z_0 које се понаша на следећи начин: $Z_0|x\rangle = |x\rangle$, за $x = 0$, а иначе $Z_0|x\rangle = -|x\rangle$. Такво логичко коло се може представити преко матрица $n \times n$ као $Z_0 = 2|0^n\rangle\langle 0^n| - I$. Ако означимо $D = H^{\otimes n} Z_0 H^{\otimes n}$, онда је: $D = 2(H^{\otimes n}|0^n\rangle\langle 0^n| H^{\otimes n}) - H^{\otimes n} H^{\otimes n} = 2|+^n\rangle\langle +^n| - I$.

[1] David Deutsch, Richard Jozsa, *Rapid solutions of problems by quantum computation*, 1992.
[2] Lov Grover, *A fast quantum mechanical algorithm for database search*, 1996.

Делујући на стање $|\psi\rangle = \sum_{x=0}^{2^n-1} \alpha_x |x\rangle$, добијамо:

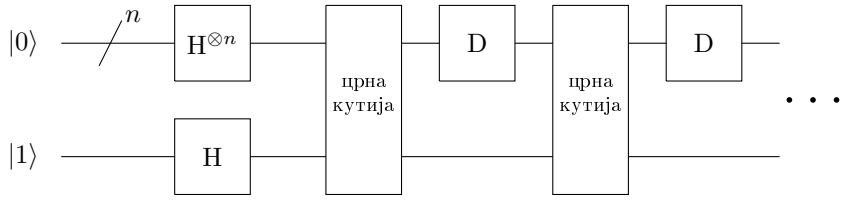
$$D|\psi\rangle = 2|+^n\rangle\langle+^n|\psi\rangle - |\psi\rangle =$$
$$= 2|+^n\rangle \sum_{x=0}^{2^n-1} \left(\frac{\alpha_x}{\sqrt{N}}\langle x|x\rangle\right) - |\psi\rangle = 2|+^n\rangle \mu\sqrt{N} - |\psi\rangle$$

где је $\mu = \frac{1}{N}\sum_{x=0}^{2^n-1} \alpha_x$ средња вредност амплитуда. Даље је:

$$D|\psi\rangle = 2\sum_{x=0}^{2^n-1}\left(\frac{1}{\sqrt{N}}|x\rangle\right)\mu\sqrt{N} - \sum_{x=0}^{2^n-1}\alpha_x|x\rangle = \sum_{x=0}^{2^n-1}(2\mu-\alpha_x)|x\rangle.$$

На почетку су све амплитуде по $\frac{1}{\sqrt{2^n}} = \frac{1}{\sqrt{N}}$,. Проласком кроз црну кутију, амплитуда стања $|x_0\rangle$ постаје $-\frac{1}{\sqrt{N}}$, а остале се не мењају. Како је $\mu = \frac{1}{N}\left(\frac{2^n-1}{\sqrt{N}} - \frac{1}{\sqrt{N}}\right) \approx \frac{1}{N}\frac{N}{\sqrt{N}} = \frac{1}{\sqrt{N}}$, то деловањем D амплитуде стања различитих од $|x_0\rangle$ остају приближно исте, док амплитуда $|x_0\rangle$ постаје $\frac{3}{\sqrt{N}}$. Дакле, једном применом Гроверовог оператора, амплитуда циљаног стања се повећала за $\frac{2}{\sqrt{N}}$. Сваким следећим дејством ће се приближно повећати за исто толико.

Након примене Гроверовог оператора, а самим тим и црне кутије, $O(\sqrt{N})$ пута, амплитуда решења x_0 ће бити већа од $0,1$. Стога, ако алгоритам поновимо 100 пута, вероватноћа налажења решења мерењем првих n кубита прелази $\frac{2}{3}$. Гроверов алгоритам проблем претраге решава у мањој сложености од класичног, али за разлику од Дојч-Јожиног алгоритма нема сигурно решење, већ вероватноћа налажења решења зависи од броја понављања целог процеса.



Слика 17: Коло за имплементацију Гроверовог алгоритма; Гроверов оператор представљају црна кутија и D коло и понавља се $O(\sqrt{N})$ пута

6.4 Шоров алгоритам

Шоров алгоритам представља алгоритам за брзу факторизацију бројева и може бити веома применљив. На пример, већина криптографских система се заснива на немогућности брзог растављања великог броја M на просте чиниоце (**NP** проблем). Међутим, коришћењем Шоровог алгоритма, овај проблем постаје решив у полиномијалном времену, те стога угрожава успостављени систем шифровања.

Шоров алгоритам[3] се састоји од операција које можемо извести и на класичном рачунару и од одређивања поретка s броја A по модулу M (односно најмањег природног броја таквог да је $x^s \equiv 1 \pmod{M}$, где су A и M узајамно прости). Зато ћемо сада описати како се ефикасно може одредити s на квантном рачунару. Потребна су нам два регистра кубита у стању $|0\rangle$. Прво припремимо кубите у првом регистру у суперпозицију $\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle$, где је $N = 2^n$ произвољан број између M^2 и $2M^2$, и добијамо стање $|\psi_1\rangle$. Потом бројеве пропустимо кроз U_f коло које за улазно стање $|x, 0\rangle$ даје стање $|x, a^x \bmod M\rangle$ и добијамо стање:

$$|\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \, |a^x \bmod M\rangle$$

Потом измеримо кубите из другог регистра и као резултат добијамо само један остатак c, односно стање $|c\rangle$. У првом регистру тада остају само кубити који испуњавају услов $a^x \equiv c \pmod{M}$, односно добијамо стање:

$$|\psi_3\rangle = \frac{1}{\sqrt{D}} \sum_{a=0}^{D-1} |x_0 + as\rangle \, |c\rangle$$

где је $D = [\frac{2^n - 1 - x_0}{s}] + 1$ број појављивања остатка c, а x_0 најмањи природан број такав да је $a^{x_0} \equiv c \pmod{M}$.

Уведимо сада коло које представља квантну Фуријеову трансформацију. Оно за стање у простору стања $|0\rangle, |1\rangle, \ldots, |N-1\rangle$ врши следећу трансформацију:

$$|j\rangle \to \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i jk/N} \, |k\rangle$$

и може се представити унитарном матрицом:

$$F_N = \frac{1}{\sqrt{N}} \begin{pmatrix} 1 & 1 & 1 & \ldots & 1 \\ 1 & \omega & \omega^2 & \ldots & \omega^{N-1} \\ 1 & \omega^2 & \omega^4 & \ldots & \omega^{2(N-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{N-1} & \omega^{2(N-1)} & \ldots & \omega^{(N-1)(N-1)} \end{pmatrix}$$

где је $\omega = e^{2\pi i/N}$. Квантну Фуријеову трансформацију примењујемо на први регистар стања $|\psi_3\rangle$ и добијамо:

$$|\psi_4\rangle = \frac{1}{\sqrt{ND}} \sum_{\gamma=0}^{N-1} \sum_{a=0}^{D-1} e^{\frac{2\pi i}{N}\gamma(x_0+sa)} \, |\gamma\rangle \, |c\rangle = \sqrt{\frac{D}{N}} \sum_{\gamma=0}^{N-1} \left(\frac{1}{D} \sum_{a=0}^{D-1} e^{\frac{2\pi i}{N}\gamma sa} \right) e^{\frac{2\pi i}{N}\gamma x_0} \, |\gamma\rangle \, |c\rangle$$

$$\approx \frac{1}{\sqrt{s}} \sum_{\gamma=0}^{N-1} \left(\frac{1}{D} \sum_{a=0}^{D-1} e^{\frac{2\pi i}{D}\gamma a} \right) e^{\frac{2\pi i}{N}\gamma x_0} \, |\gamma\rangle \, |c\rangle$$

јер је $s \approx \frac{N}{D}$. Користећи да је сума $\frac{1}{D} \sum_{a=0}^{D-1} e^{\frac{2\pi i}{D}\gamma a}$ једнака 1 када је γ целобројни умножак броја D, а 0 иначе, добијамо да је:

[3] Peter Shor, *Polynomial – Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*, 1994.

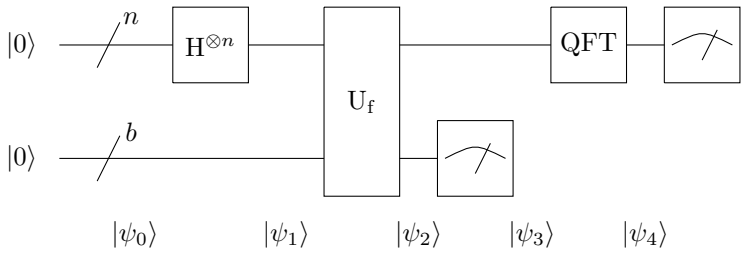
$$|\psi_4\rangle \approx \frac{1}{\sqrt{s}} \sum_{\substack{\gamma=0 \\ \gamma=kD}}^{N-1} e^{\frac{2\pi i}{N}\gamma x_0} |\gamma\rangle |c\rangle.$$

Следећи корак је мерење кубита из првог регистра. Као што видимо, можемо да добијемо само резултат kD (k је цео број) који је приближно једнак $\frac{kN}{s}$, односно $\frac{\gamma}{N} \approx \frac{k}{s}$.

Представљајући измерено $\frac{\gamma}{N}$ у облику верижног разломка $a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\cdots + \cfrac{1}{a_m}}}}}$, где су $a_0, a_1, a_2, \ldots, a_m$ ненегативни цели бројеви, а m такозвани ред конвергенције овог разломка и понављајући цао поступак довољан број пута, можемо одредити поредак s.

Сада се враћамо на растављање броја M на просте факторе. Прво класичним алгоритмима проверимо да ли је M паран или је степен простог броја и у случају да јесте вратимо одговарајући прост фактор. Ако није, изаберемо насумично број A мањи од M. Ако A и M нису узајамно прости, вратимо одговарајући заједнички прост делилац, а у супротном користећи описан алгоритам нађемо поредак s броја A по модулу M. Ако је s паран и $A^{s/2} \not\equiv -1 (\text{mod } M)$, израчунамо НЗД$(A^{s/2} - 1, M)$ и НЗД$(A^{s/2} + 1, M)$ и проверимо да ли је неки од њих прост фактор броја M. Ако јесте, враћамо тај број. У супротном алгоритам није успео да нађе прост фактор и понављамо га за неки други број A.

Цео алгоритам поновимо потребан број пута. Алгоритам нам са великом вероватноћом ефикасно решава проблем налажења простог фактора великог броја.



Слика 18: Коло за имплементацију Шоровог алгоритма; Овде је b најмањи такав број да је $2^b > M$, јер у први регистар иду бројеви до N, а у други бројеви до M

7. Закључак

Кроз овај рад упознали смо се са основама квантног рачунарства кроз три повезане области: математику, физику и информатику. Сам концепт и начин на који уводимо кубите и операције над њима је математички формалан и као такав не мора постојати у реалности, већ може остати на нивоу апстакције Универзалног квантног рачунара. Пошто инспирацију и могућност остваривања концепта у реалности заснивамо на квантној механици, немогуће је процесе дубље анализирати без помоћи физике. Физика нам објашњава интеракције кубита, интерференцију и суперпозиције стања, увезана стања и сличне феномене на које наилазимо. Такође, евентуалним новим открићима у квантној теорији омогућава и даљи развој квантног рачунарства. Наравно, у основи самог рачунарства је обрада информације и потреба за њом, па отуда следи информатички поглед на ствари. Квантна физика уводи квантне особине информације, које се значајно разликују од класичних и које остављу простора за рад квантним информатичарима. Само до сада срели смо се са њеном телепортацијом на велике удаљености, што је последица увезаних стања, али и са немогућношћу њеног копирања.

Класични битови имају само два могућа стања, 0 и 1. Логична надоградња, поготово када имамо сазнања о квантној механици и када смо наилазили на проблем симулације квантних система на класичним рачунарима, представља увођење кубита као линеарне комбинације тих стања, са додатком преласка у једно од њих приликом мерења. Сва даља својства квантних логичких кола и квантних алгоритама следе одатле. Приметимо да слобода коју имамо приликом математичког заснивања логичког кола (једини услов је унитарност матрице) омогућава да све жељене операције заиста можемо да представимо преко логичких кола и изведемо. Са друге стране, постојање универзалних логичких кола обећава у погледу практичне реализације замишљених алгоритама.

Увидели смо да је могуће све процесе са класичних рачунара извести и на квантним, те стога сигурно квантни рачунари неће бити мање моћни од класичних, што оправдава улагања у њихово даље развијање. Чак и ако би се испоставило да је $\mathbf{BQP} = \mathbf{BPP}$, то што смо прво дошли до ефикасних алгоритама за неке проблеме на квантним рачунарима говори о њиховој приступачности. Такође, могуће је да за проблеме који јесу ефикасно решени на класичним рачунарима постоје још ефикаснија решења на квантним, попут квантне претраге. Још једна ствар коју нам пружају квантни системи је генерисање истински насумичних бројева, односно ситуације у којима природа сама бира резултат мерења, што на данашњим рачунарима није постигнуто.

Предности су многе, па би тако само паралелно процесирање и наведени алгоритми могли да имају разноврсне примене, поготово у симулирању физичких система и пробијању шифара које данас користимо. Дизајнирање нових квантних алгоритама је изузетно тежак задатак, јер смо у раду навикли на класичне системе. Такође, није довољно осмислити алгоритам, већ он мора бити за класу бољи од класичног. За сада немамо представу колико тога можемо

да постигнемо на квантним рачунарима, због чега је важно наставити са унапређивањем техничких услова за њихов рад и развијањем нових алгоритама. Довољно је да се сетимо да додавање једног кубита одговара удвостручивању броја класичних битова и да знамо да радимо на правом задатку.

На крају, занимљиво је напоменути да квантно рачунарство не мора бити засновано на кубитима. Као што теоријски класичне рачунаре можемо засновати на системима са различитом основом, тако и квантни рачунари могу радити са другим основама. На пример, уколико одаберемо основу 3, у питању су кутрити који могу бити у стањима $|0\rangle$, $|1\rangle$ и $|2\rangle$ и њиховој суперпозицији. Испоставља се да нека стања која су увезана када их посматрамо у систему са основом 2 нису увезана у неким другим просторима стања. Ипак, то не значи да се увезана стања могу избећи у потпуности, јер је оно што нам омогућавају веома значајно. Коначно, одабир основе 2 је логичан, јер је аналоган класичним рачунарима и као такав највише интуитиван и наравно најједноставнији за рад и даље прорачуне.

Захвалност

Захваљујем се свом ментору, Александри Димић, на сарадњи и помоћи при изради матурског рада. Захваљујем се и својим професорима, Јовици Милисављевићу и Игору Салому, који су ми држали менторске часове из физике. Посебну захвалност дугујем професорки Наташи Чалуковић која ми је физику предавала четири године и која је у великој мери заслужна за све што сам за то време научио и остварио.

Литература

[1] M. A. Nielsen, I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, 2000.

[2] C. P. Williams, *Explorations in Quantum Computing*, Springer, 2011.

[3] C. Li, R. Roberts, X. Yin, *Decomposition of unitary matrices and quantum gates*, arXiv : 1210.7366 [quant − ph]

[4] R. O′Donnell, J. Wright, *Quantum Computation and Information 2015*, Carnegie Mellon University, https : //www.cs.cmu.edu/ odonnell/quantum15/

[5] S. Aaronson, *6.896 Quantum Complexity Theory*, Massachusetts Institute of Technology, http : //stellar.mit.edu/S/course/6/fa08/6.896/materials.html

[6] R. Cleve, A. Ekert, C. Macchiavello, M. Mosca, *Quantum Algorithms Revisited*, arXiv : quant − ph/9708016