# Шоров алгоритам и квантна надмоћ

Ментор: Игор Салом

Аутор: Лука Невајда 4ц

Математичка гимназија Београд

јун 2020.

# Садржај

# 1 Увод

Област квантног рачунарства је млада и перспективна, међутим знање широке популације о њима је мало. Ове машине се користе принципима рада квантне механике, области физике која постоји тек мало више од 100 година. Функционисање квантних рачунара и алгоритама који се извршавају на њима је доста другачији у односу на "класичне", бинарне рачунаре. Циљ овог рада је да барем мало појасни концепт квантних рачунара, али и једног од алгоритама који се на њему извршавају, Шоровог алгоритма. Испоставиће се да ови рачунари нуде решења која бинарни рачунари не могу ефикасно понудити и самим тим шире могућности онога што је могуће извршити на рачунару. Такође се покреће питање која од ове две врсте рачунара је боља и како се то може доказати, па ће бити и речи о квантној надмоћи која се бави овим питањем. Посветићемо се и потенцијалној примени квантних рачунара, из разлога што њихова експанзија још није почела.
Да бисмо боље разумели концепт квантних рачунара, разлоге зашто могу постати надмоћније машине од бинарних рачуанра, али и схватили концепт самог Шоровог алгоритма, морамо знати догађаје и открића из поља квантне механике и рачунарства која су им претходили.

## 1.1 Кратка историја квантне механике

*Са сигурношћу могу да кажем да квантну механику нико није разумео.*

**Richard Feynman**
**(1918-1988.)**-амерички физичар

Од настанка човека као бића, приписује му се епитет *радозналост*. Човек од својег најранијег доба истражује и покушава да што боље разуме самог себе, свет чији је он део и појаве које чине тај свет. Као резултат ове човекове особине, настанком првих цивилизација и писма, временом настају и науке: биологија, историја, географија, хемија... које покушавају да на што објективнији начин опишу и класификују разна питања која су занимала човечанство и пренесу их будућим генерацијама. Наука која проучава и тежи да дефинише својства природних појава и тела назива се физика. Кроз векове физика је успела да опише бројне феномене који су до тад интригирали човечанство (разна кретања, гравитацију, електричну струју, карактеристике гаса и флуида) и до краја 19. века физика је описала велики број тада познатих појава.

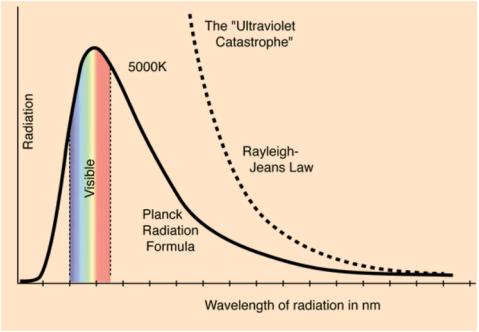
Међутим, крајем 19. и почетком 20. века откривен је низ проблема који се нису могли доказати "класичном" физиком. Неки од тих појава, ефеката и експеримената су ултраљубичаста катастрофа, фотоелектрични ефекат и Мајкелсон-Морлијев експеримент. Решавањем ових проблема настају три нове гране физике, које су показале да свет, ипак, није онакав како је замишљан. Ове гране се и данас активно продубљују и то су: општа теорија релативности, квантна механика и квантна теорија поља, која их обједињује и повезује.

Први проблем којим се бавила квантна механика је **ултраљубичаста катастрофа**. Наиме, класичном физиком није било могуће описати расподелу енергије електромагнетног

зрачења апсолутно црног тела. Рејли-Џинсовим[1] законом је покушана апроксимација ове расподеле, међутим за високе вредности фреквенце Рејли-Џинсовим законом се добија бесконачна вредност, што би значило да би апсолутно црно тело у тренутцима емитовало целу своју енергију до апсолутне нуле, што се наравно не дешава. Бројни физичари су покушавали да реше овај феномен, да би 1900. године Макс Планк [2] извео закон помоћу кога се савршено описује ову расподелу. Приликом извођења ове формуле Планк је користио хипотезу:

$$E = nh\nu, \quad n \in \mathbb{N}$$

којом показује да енерија емитује у дискретним порцијама које је он назвао **квант енергије** ($h\nu$). Ово је супротно прећашњем мишљењу да се енергија емитује континуално. Планк није први коме је ова идеја пала на памет, још 1877. Болцман[3] претпоставља да се енергија емитује дискретно. Међутим, Планк је први који је доказао да је то заправо истина.




Слика 1: *Приказ ултраљубичасте катастрофе*

На причу коју је Планк започео надовезао се Ајнштајн[4] открићем формуле за фотоелектрични ефекат. Овај феномен је открио Хајнрих Херц [5] 1887. године и представља емисију електрона из металне кристалне решетке под утицајем електромагнетног зрачења. Ајнштајнова формула:

$$h\nu = A_i + T_{max}$$

где $A_i$ представља излазни рад електрона, а $T_{max}$ његову максималну кинетичку енергију, показује да се енергија и апсорбује у **квантима**, али и да се светлост (или било које друго

[1]James Jeans (1877-1946.)-енглески физичар
John William Rayleigh (1842-1914.)-енглески физичар, добитник Нобелове награде 1904. године
[2]Max Planck (1858-1947.)-немачки физичар, добитник Нобелове награде 1918. године
[3]Ludwig Boltzmann (1844-1906.)-аустријски физичар
[4]Albert Einstein (1879-1955)-немачки физичар, за откриће формуле фотоелектричног ефекта добио Нобелову награду 1921. године
[5]Heinrich Rudolf Hertz (1857-1894.)-немачки физичар

електромагнетно зрачење) дели на коначан број кванта енергије који се даље не деле. Недуго након ових открића, кванти енергије добијају нови назив који и данас носе: **фотони**. Ајнштајново откриће је један од првих показатеља да светлост има дуалну природу: у неким ситуацијама се понаша као талас, а у другим као честица.
У поприлично кратком временском периоду квантна механика је окренула дотадашње догме физике наглавачке, али томе дефинитвно није био крај већ, напротив, само почетак. 1913. године Нилс Бор[6] излаже своја два постулата и приказује свој модел атома по којем се електрони крећу по фиксним радијусима, односно да се налазе на дискретним енергетским нивоима на којима не добијају, али и не губе енергију. Међутим, како је могуће да електрон не губи енергију ако знамо када се креће по кружној путањи? Одговор на ово питање дао је Луј де Брољ[7] 1923. године постављањем своје хипотезе: ако се путањи електрона додели стојећи талас такав да се на путањи електрона налази цео број таласних дужина ($2\pi r = n\lambda$) и ако не постоји никакав отпор средине, тај стојећи талас ће осциловати бесконачно дуго, без икаквих губитака енергије. Запис хипотезе:

$$\lambda = \frac{h}{p}$$

где је $p$ импулс честице, $\lambda$ таласна дужина таласа, а $h$ Планкова константа. Према томе, електрон и друге микрочестице се по де Брољу понашају дуално. Његова теорија се поклапа са првим Боровим постулатом ($L = n\hbar$) и касније је и експериментално доказана. Након овог револуционарног открића поставља се питање: ако микрообјекат испољава таласна и честична својства, како описати његова могућа стања? Одговор на ово питање дао је Ервин Шредингер[8] 1925. године дефинисањем диференцијалне једначине која је понела име по њему. Решавањем ове једначине добијају се функције које описују стања микрообјекта. Ове функције су познате као **таласне функције** ($\psi(\vec{r}, t)$ у општем случају; $\psi(x)$ у специјалном случају када се честица налази на једној оси координатног система и $t = 0$). Наредне године Макс Борн открива статистичку природу таласне функције: $|\psi(x)|^2$ представља густину вероватноће налажења честице у тачки $x$. Ова формула указује на пробабилистичку природу квантне механике и чињеницу да колико год параметара о неком објекту, нећемо добити сигуран податак, већ вероватноћу. Ситуација се компликује када желимо да добијемо две особине честице у истом тренутку. 1927. године су откривене Хајзенбергове[9] релације неодређености:

$$\Delta x \cdot p_x \geqslant h, \quad \Delta y \cdot p_y \geqslant h, \quad \Delta z \cdot p_z \geqslant h, \quad \Delta t \cdot \Delta E \geqslant h$$

Ове релације показују да не можемо у исто време са тачношћу знати положај честице и њен импулс, већ само једне од те две особине. Исто важи и за сопствено време живота честице и њену енергију. Релацијама неодређености се прикључује и Боров принцип комплементарности (1928.година) који каже да је немогуће посматрати и таласну и честичну

[6]Niels Bohr (1885-1962.)-дански физичар, добитник Нобелове награде 1922. године
[7]Louis de Broglie (1892-1987.)-француски физичар, добитник Нобелове награде 1929. године
[8]Erwin Schroedinger (1887-1961.)-аустријски физичар, добитник Нобелове награде 1933. године
[9]Werner Heisenberg (1901-1976.)-немачки физичар, добитник Нобелове награде 1932. године

природу микрообјекта у истом тренутку.
У наредном периоду квантна механика се усредсредила на проучавање елементарних честица и решавање бројних парадокса, ефеката и загонетки, али је и наишла на скептицизам њеног описивања реалности. Највећи противник пробабилистичке природе квантне механике је био, помало иронично, Алберт Ајнштајн. Остала је упамћена његова изјава: "*Уверен сам да Бог не баца коцкицу*". Као реакција настаје ЕПР (Ајнштајн-Подолски-Розен) парадокс из 1935. године. Овај мисаони експеримент покушава да аргументује став да физичка реалност коју описује квантна механика није потпуна и има неке недостатке. Дејвид Бом је касније прилагодио ЕПР да би га било лакше разумети. Уопштено, парадокс каже:
Имамо две честице у квантној спрези[10] и извршимо мерење неке особине на једној од њих две. До тог тренутка ми не знамо коју вредност та особина има и може узимати било коју вредност коју она може да узима, односно до тог тренутка те честице у квантној суперпозицији. Оног тренутка када извршимо мерење ми суперпозицију прекидамо и добијамо тачну вредност те особине за честицу на којој смо вршили мерење, а пошто су честице у квантној спрези, у истом тренутку можемо знати и вредност те особине за другу честицу, без обзира што на њој није вршено мерење. Пошто се на неки начин дешава да друга честица "зна" коју вредност у истом тренутку када сазнамо вредност прве честице, а честице се могу у теорији наћи на великим удаљеностима, делује као да та информација путује брзином већом од брзине светлости, што је по теорији релативности немогуће. С тога је Ајнштајн био присталица **теорије скривених варијабли**, односно веровао је да је квантној мехници неопходно додати још параметара да би тачно описала стања у универзуму.
1964. Џон Бел[11] формулише теорему и у оквиру ње неједнакост, која када је њено нарушење експериментално проверено показује да је Ајнштајн погрешио, односно да ниједна теорија скривених променљивих не може да рекреира ефекте квантне механике, а ти ефекти су реални.
Оно што се дефинитивно показало је да математика иза квантне механике функционише беспрекорно. Половином 20. века и све присутнијом темом рачунаства, полако је настајала идеја о уређају који би симулирао квантна стања-квантном рачунару. 1981. године Ричард Фајнман[12] у раду "*Simulating physics with computers*" први разматра концепт квантног рачунара који би могао да симулира квантне системе и објашњава зашто такав рачунар може да их симулира, а обичан не. На основу овог модела настали су многи квантни алгоритми, међу којима је и тема овог рада: Шоров алгоритам. Ови алгоритми су се показали као много бољи и бржи у обради података у односу на класичне алгоритме. Иако ови алгоритми већ постоје, нису још увек није у масовној примени. Међутим, уз брз развој технологије какав је трентно присутан, питање је времена када ће они бити у широкој употреби.

[10]quantum entanglement-стања групе честица где није могуће одредити стање једне честице независно од других
[11]John Bell (1928-1990.)-британски физичар
[12]Richard Feynmann(1918-1988.)-амерички физичар

## 1.2 Кратка историја рачунарства

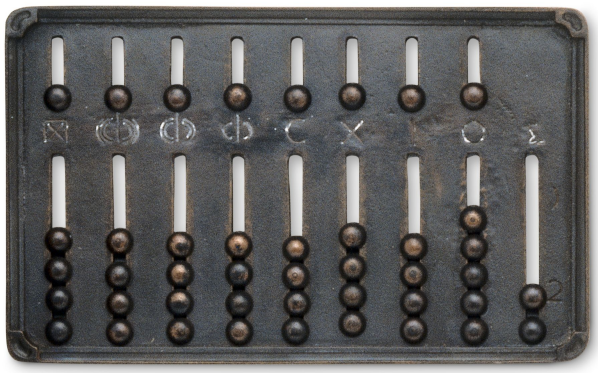
*Компјутери су бескорисни. Могу вам дати само одговоре.*

**Pablo Picasso(1881-1973.)**-чувени шпански уметник

Још једна корисна особина човека је *домишљатост*. Још од саме праисторије човек кроти природу и прилагођава је својим потребама. Ова особина има корене који нас воде 2 милиона година уназад када је тадашњи човеколики примат *Homo habilis* почео да прави оруђа која би му олакшавала лов. Због ове особине потом настаје точак, али и писмо. Домишљатост човека и његова жеља да себи што више олакша свакодневне проблеме довеле су и до проналаска разних уређаја који су имали разне примене, између осталог и процесуирање разних подтака. Из оваквих уређаја ненепосредно настају и данашњи рачунари.

Пошто се дефиниција речи рачунар кроз време мењала и данашња дефиниција се односи само на електронске системе, њихове механичке претке ћу називати "рачунарима".

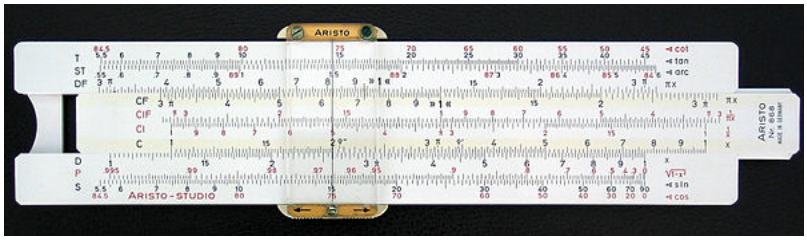
Једна од направа које су започеле идеју о "рачунарима" је абакус[13]. Ова справа за рачунање је постојала код многих народа. Први примерци су настали на територији Кине око 1100. године пре нове ере и као примену су имали рачунање у декадном систему. Временом су настали грчки, римски, јапански, руски и древноамерички абакуси. Римски абакуси су се највише употребљавали у Европи и користили су се до 16. века. Ова справа је заправо била плоча са подељеним пољима по којима се померају каменчићи или метални дугмићи и у зависности од њиховог шположаја добија се одређена вредност. Од латинског назива за те каменчиће (*calculus*) је настала реч *calculare*, што значи рачунати. Други абакуси и дан данас имају примену: у Јапану и Русији су и даље саставни део културе, многа деца у вртићима уче да рачунају помоћу упрошћених абакуса, а постоје и абакуси за слепе људе, који помажу слепим људима да рачунају.



Слика 2: *примерак римског абакуса*

[13]Назив потиче из 14. века и изведен је од грчке речи абах

Након абакуса, од 17. века се користи логаритмар, направа која је служила за израчунавање природних логаритама, али и других математичких операција (множења, дељења, дизања броја на други и трећи степен, вађења квадратног и кубног корена). Логаритмар се најчешће састоји од две летве исте дужине различите ширине и од прозирне плочице са уцртаном линијом која клизи по широј плочици. Шира плочица је удубљена по дужини тако да ужа по њој може да клизи. Обе плочице су баждарене по логаритамској скали, што логаритмар чини јако добрим за мултипликативне операције, али и лошим за адитивне операције. Зато се на логаритмарима није могло сабирати и одузимати. Понегде се још увек користе.




Слика 3: *примерак логаритмара*

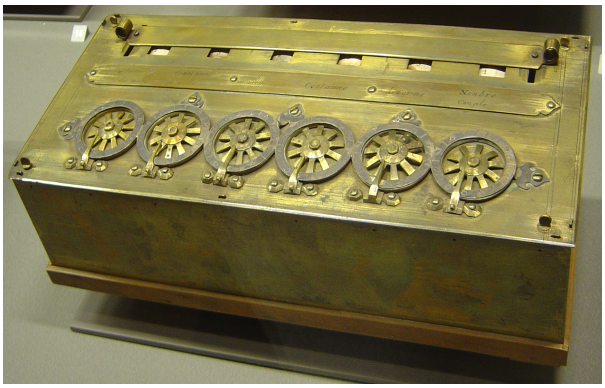
Иако су ове две направе помагале човеку да брже савлада и обради податке, не могу се баш сматрати рачунарима, јер да би процесуирале податке потребан им је човек (човек помера куглице на абакусу и човек помера дашчице на логаритмару). Да бисмо добили уређај који можемо назвати "рачунаром"тај уређај мора имати одређену аутономију од човека приликом процесуирања података, односно мора имати неки механизам или код по коме функционише.

Иако се заправо не зна када је откривен први "рачунар", многи историчари се слажу да је најстарији откривени "рачунар" механизам из Антикитере, који потиче из 1. века нове ере. Овај уређај откривен је на самом почетку 20. века (1901. године) првих педесет година након свог открића је био врло мистериозан, јер се није знало како функционише и која му је била примена. На самом почетку су постојала нагађања да је служио за астрономска прорачунавања и то је закључено на основу астрономских термина записаних на једном зупчанику. Ова нагађања су се испоставила као тачна, када је Дерек де Сола Прајс[14] 1952.године написао рад о овом механизму. Де Сола Прајс закључује да је механизам служио као симулатор кретања планета око Сунца, чинећи га тиме првим познатим аналогним "рачунаром". Овај механизам се чува у Националном археолошком музеју у Атини и слични механизми нису постојали (или такви уређаји нису пронађени) следећих хиљаду година.

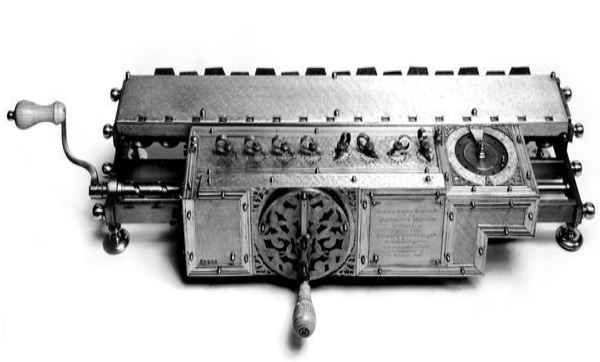
[14]Dereck de Sola Price-британски научник и историчар

Слика 4: *механизам из Антикитере*

Следећи корак у развоју "рачунара"нас води у 1645. годину када је Блез Паскал [15] изумео **паскалину**-први аритметички калкулатор. Паскалина је била децимална машина и могла је само да сабира и одузима. 1671. Лајбниц[16] осмишља *рачуналъку са бубњем* (нем. *Staffelwalze*, енг. *Stepped reckoner*), прву машину која може да ради основне четири математичке опрације. Уз њих је могла да рачуна квадратни корен. Ове две машине иако су пионири данашњих рачунара нису биле за комерцијалну употребу. Биле су јако тешке, скупе и нису биле много јаке. До првог комерцијалног калкулатора ће проћи још 150 година.



(а) Паскалова *Паскалина*



(б) Лајбницов *Staffelwalze*

Први калкулатор за комерцијалну употребу је 1820. године изумео Шарл Томас де Колмар[17] и назвао га је **аритмометар**. Могао је да врши све четири основне аритметичке операције и био је у продаји следећих деведесет година. 1822. Чарлс Бебиц[18] осмишља први озбиљнији "рачунар-"**Диференцијалну машину**". Ова машина је користила децимални бројевни систем и служила је за табелирање полиномских функција. Међутим, многе функције је могуће апроксимирати интерполационим полиномима, па је "Диференцијална машина"

[15]Blaise Pascal (1623-1662.)-француски математичар, физичар и филозоф
[16]Gotfried Wilhelm Leibnitz (1646-1716.)-немачки математичар и филозоф
[17]Charles Tomas de Colmar (1785-1870.)-француски проналазач
[18]Charles Babbage (1791-1871.)-енглески математичар

могла да рачуна и приближне вредности логаритамских и тригонометријских функција. Међутим, функционални прототип "Диференцијалне машине"никада није завршен.Бебиџ је био у конфликту са главним инжењером пројекта, а финансијска потпора коју је пружала влада Велике Британије је у једном треутку нестала.Тридесетак година касније Бебиџ представља побољшану верзију названу "**Диференцијална машина 2**" и постоји пар ових машина које су настале независно од Чарлса Бебица. Бебиџ се, међутим, није зауставио на "Диференцијалној машини"и још 1833. године ради на њеном наследнику: "**Аналитичкој машини**". Први пут ју је описао 1837.године. Ова машина је практично била прави предак данашњем рачунару који се користи у генералне сврхе са свим карактеристикама које ће се касније појавити у рачунарима, међу којима је и програмабилност. Идеју програмабилности Бебиџ је пронашао у тадашњој текстилној индустрији у којој су машине за ткање биле прогамиране помоћу бушених картица. 1843. године Ада Ловлејс [19] је преводећи рад Луиђија Менабрее[20] везаног за "Аналитичку машину" са француског на енглески писала додатне белешке дуже од самог превода. Испоставило се да је Лоблејсова написала "код" за рачунање Бернулијевих бројева. Ово се сматра првим компутерским програмом.

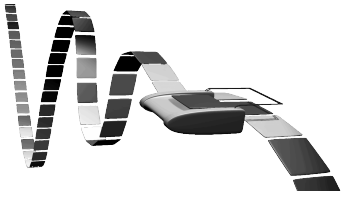
1936. Алан Тјуринг[21] даје апстрактни модел свог рачунара: "**Тјурингову машину**", као и услов који друге машине треба да испуне да би се могле звати "**Тјуринг комплетним**". "Тјурингова машина" је замишњена као математички модел машине која ради помоћу бесконачно дуге траке која је подељена на ћелије које садрже неке симболе. Машина може да очитава те симболе и у зависности од симбола или неког утврђеног алгоритма машина ће се другачије понашати. Она поседује такозвану "главу за писање" која очитава симбол који се налази директно испод ње. Под дејством тог симбола или алгоритма, машина ради следеће три ствари у датом редоследу:

1. Пише симбол у ћелију (симбол може бити цифра или слово коначног алфабета)

2. Помера се за једну ћелију на леву или десну страну

3. Извршава следећу наредбу или прекида рачунање

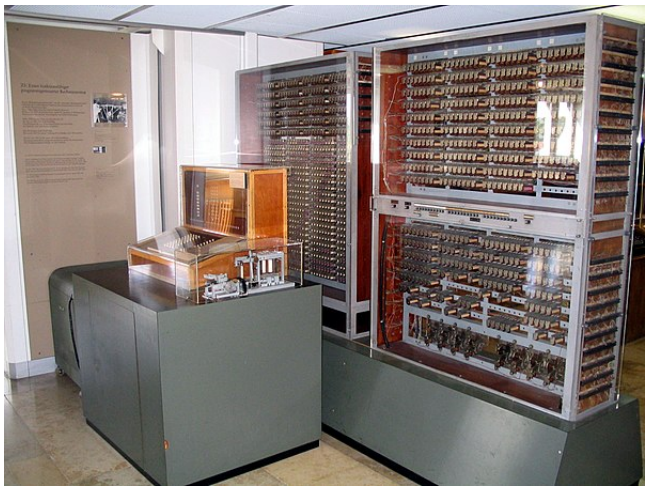
Машина која може да симулира "Тјурингову машину"је "Тјуринг-комплетна". Данас је "Тјуринг-комплетност"стандард и скоро сви модерни рачунари јесу "Тјуринг-комплетни".



Слика 6: *приказ Тјурингове машине*

[19]Ada Lovelace (1815-1852.)-енглеска маематичарка, ћерка чувеног енглеског песника Џорџа Бајрона
[20]Luigi Menabrea (1809-1896.)-италијански математичар и генерал
[21]Alan Turing (1912-1954.)-енглески математичар и криптограф

Следећи велики искорак у историји рачунарства се десио између 1939. и 1940. године када је на Државном универзитету Ајове настао **Атанасов-Бери компјутер**[22]. Ово је први аутоматски електронски дигитални рачунар. Такође је и први рачунар који је користио бинарни бројевни систем за рачунање и чување података. Јединице одређене за рачунање и чување података су биле физички одвојене, што је била још једна новина. Имао је регенеративну меморију (може да се пуни и празни изнова и изнова) од 3000 бита. Атанасов-Бери компјутер је служио за рачунање система линеарних једначина и могао је да решава системе од 29 линеарних једначина. Његова мана је била што није "Тјуринг-комплетан" и што за разлику од следеће машине на листи није био програмабилан.
У јеку Другог светског рата 1941. године у Берлину Конрад Цузе[23] је представио **Z3**, први комплетно функционалан програмабилан потпуно аутоматски електромеханички компјутер. Z3 је користио речи од 22 бита и могао је да обавља 5 операција у секунди. Функционисао је помоћу 2600 релеја и технички није био потпуно дигиталан. Цузе је тражио од Немачке владе да финансира пројекат да би релеје заменио електричним прекидачима, међутим влада је одбила да га финансира назвавши пројекат *"небитним за рат"*. Оригинални примерак "Z3"машине је страдао у савезничком бомбардовању 1943. године, међутим направљено је пар реплика. 1998. године је показано да је "Z3" делимично Тјуринг-комплетан (мисли се само на укупан број исхода јер Z3 није имао условно гранање).

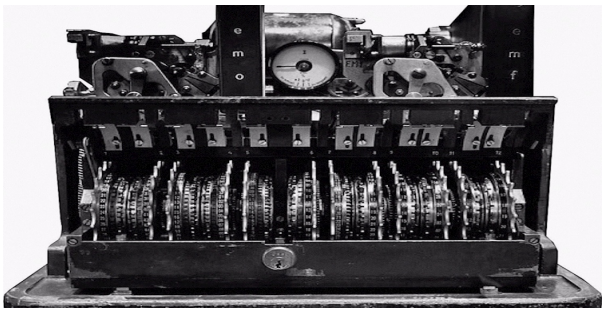


Слика 7: *Цузеов Z3*

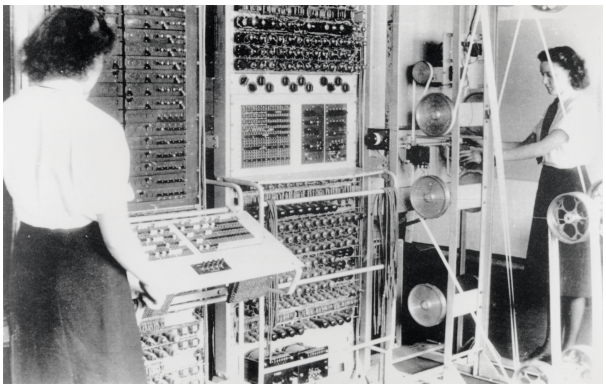
Немачка је у Другом светском рату поседовала машине за криптовање порука зване "**Енигма**"и групу сличних "**Лоренцових машина**". Као реакција на ове машине настаје Британска тајна лабораторија за дешифривање података **Блечли парк** (енг. *Bletchley Park*). Већ поменути Алан Тјуринг креира машину која дешифрује "Енигму", а 1943. Флауерс и Њуман[24] пројектују рачунар "**Колос**"(енг. *Colossus*). "Колос" је коришћен за дешифровање

[22]John Vincent Atanasoff (1903-1995.)-амерички физичар
Clifford Berry (1918-1963.)-амерички инжењер
[23]Konrad Zuse (1910-1995)-немачки рачунарски пионир
[24]Thomas Flowers (1905-1998.)-енглески инжењер

"Лоренцових машина". Користио је вакуумске цеви (тада коришћених у радио пријемницима, а данас коришћеним у аудио појачалима високог квалитета) да би врши нумеричке, али и логичке операције. Први је потпуно дигитални, програмабилни рачунар. Програмиран је помоћу електричних прекидача и полуга и прва је "Тјуринг-комплетна" машина.



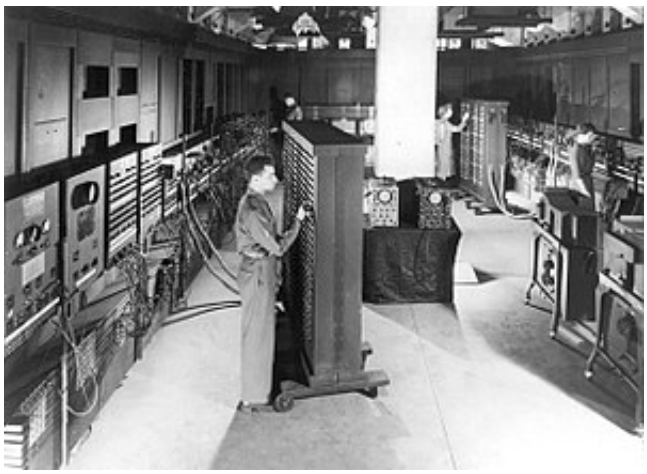
(а) Лоренцова машина



(б) Колос, дешифровао Лоренцову машину

Слика 8: Приказ Лоренцове машине и Колоса

Након другог светског рата 1946. године на универзитету у Пенсилванији настаје **ENIAC** (енг. *Electronic Numerical Integrator And Computer*)-први рачунар за решавање великог броја математичких проблема. Ова машина је била огромна: заузимала је простор од 167 квадратних метара и тежила је читавих 27 тона. Сасројала се од око 17500 вакуумских цеви, 7200 кристалних диода, 1500 релеја и 70000 отпорника. Улазни и излазни параметри су биле бушене картице и овај рачунар је користила америчка војска приликом креирања хидрогенске бомбе.



Слика 9: *приказ ENIAC-а*

Maxwell Newman (1897-1984.)-енглески математичар

1945. године. годину дана пре пуштања ENIAC-а у рад, Џон фон Нојман[25] објављује свој модел рачунара, познатији као "**фон Нојманова архитектура**" или "**Принстонска архитектура**". Овај модел се састоји од:
1.**Централне процесорске јединице** (енг.CPU-*Central Processing Unit*) која се даље дели на три дела:

a)**Аритметичко-логичке јединицу**(енг. ALU-*Arithmetic/Logic Unit*) : врши обраду података (врши сва рачунања);

b)**Контролну јединицу** : управља свим функцијама CPU, у себи садржи **регистар инструкција** (чува инструкцију која се тренутно извршава) и **бројач инструкција** (садржи број инструкција пре оне која се тренутно извршава);

c)**Регистре** : складиште унете параметре и резултате које је обрадила ALU;
2.**Меморију** : чува инструкције и податке ван које се тренутно користе, или су се до недавно користиле;
3.**Спољно складиштење података** : чува инструкције и податке које се тренутно не користе;
4.**Улазно-излазне механизме** : механизми помоћу којих човек комуницира са машином и машина комуницира са човеком.

Принстонска архитектура је први модел рачунара који има електронски чуван програм и овај модел се и данас користи. Даљи развој рачунара се сводио на смањивање димензија самих рачунара и повећавање рачунске снаге смањивањем димензија транзисторских гејтова[26] и флип-флопова[27], саставних делова процесора. Раст рачунске снаге је кроз време био експоненцијалан и америчка компанија Интел се педесетих година прошлог века хвалила како ће сваке две године избацивати процесоре са двоструко мањим транзисторима. Данас је тај раст све мањи и мањи, јер се приближавамо физичкој граници величини једног транзистора. Смањивање броја иновација бинарних рачунара не значи да ћемо достићи максимум у развијању рачунара. Могло би се рећи да је револуција у рачунарству никад ближа. Питање је времена када ће квантни рачунари бити у широј употреби и када ће потиснути тренутне, бинарне рачунаре. Бројна питања тек следе: како се квантни рачунари разликују од бинарних? Зашто се сматрају бољим решењем? Како функционишу? Зашто још увек нису у масовнијој употреби? На ова и многа друга питања одговориће следеће поглавље.

[25]John von Neumann (1903-1957.)-америчко-мађарски математичар и физичар
[26]gate-капија која извршава операцију над битом и не чува податке
[27]flip-flop-капија која чува податке

# 2 Основе квантног рачунарства

У овом поглављу ћемо сазнати шта то тачно чини квантни рачунар, како функционишу у најгрубљим цртама и како се разликују од "обичних", бинарних рачунара. Ово знање ће нам значајно помоћи да разумемо функционисање Шоровог алгоритма. Међутим, пре него што се упознамо са основним знањем квантног рачунара, неопходно је да уведемо пар математичких појмова да бисмо лакше описали појаве у квантној механици. Упознаћемо се и са нотацијом Пола Дирака, али и постулатима квантнима механике. Како бисмо могли да увидимо разлике између бинарних и квантних рачунара, описаћемо најосновнији ниво бинарног рачунара: бит и Булова логичка која сачињавају бинарни рачунар.

## 2.1 Неопходни математички појмови

### 2.1.1 Векторски простори

Векторски простори су нам вековима помагали да математички опишемо појаве и стања у свету којем припадамо. Зато је врло битно да их дефинишемо:
**Дефиниција**: P се сматра линеарним векторским простором ако га чине скупови $V$(скуп структура званих **вектори**, означених словима грчког алфабета $(\psi, \phi, \theta, ...)$) и $F$(скуп структура званих скалари, означених словима алфабета$(a, b, c, ...)$) и две бинарне операције $+$ (класично сабирање, $+ : V \times V \longrightarrow V$) и $\cdot(, \cdot : \mathrm{F} \times V)$, и да притом важи следеће:

- За структуру $(V, +)$ важе затвореност на скупу $V$, комутативност, асоцијативност, постојање неултралног елемента из $V$, као и постојање инверзног пара за сваки елемент скупа $V$, који је такође из $V$. Другим речима, $(V, +)$ је Абелова група[1].
- $(a+b)\cdot\psi = a\psi + b\psi, \quad a, b \in F, \psi \in V$
- $a(\psi + \phi) = a\psi + a\phi, \quad a \in F, \psi, \phi \in V$
- $a(b\psi) = (ab)\psi, \quad a, b \in F, \psi \in V$, при чему операција између $a$ и $b$ и $b$ и $\psi$ нису исте операциије
- $1\cdot\psi = \psi, \quad \psi \in V, \quad$ при чему је 1 јединични елемент из $F$

Сва стања приказујемо преко вектора које добијамо операцијама на базним векторима векторског простора, а при тим операцијама користимо скаларе из истог тог векторског простора.

Нама најпознатији и најлакше појмљив векторски простор је **Еуклидски тродимензионални векторски простор**[2]. У Еуклидском простору произвољан вектор $\vec{p}$ може приказати на следећи начин:

$$\vec{p} = a\vec{e_x} + b\vec{e_y} + c\vec{e_z},$$

где су $\vec{e_x}, \vec{e_y}, \vec{e_z}$ јединични, међусобно нормални вектори, а $a, b, c$ скалари из $\mathbb{R}$. Дуго се сматрало да је Еуклдски простор тачан опис света у коме живимо. Ипак, показало се да иако

[1] Niels Henrik Abel (1802-1829.)-норвешки математичар
[2] Euclidus-чувени грчки математичар

добро опонаша свет на макроскопском нивоу, није погодан на микроскопском нивоу где важе закони квантне механике. С тога, морамо дефинисати нови векторски производ, чијим уопштењем добијамо Еуклидски простор.
**Дефиниција** Ако направимо линеаран векторски простор са произвољно много димензија и изаберемо скуп $\mathbb{C}$ као скуп скалара, добијамо **Хилбертов векторски простор**[3] $H$, за који важи:

- Дефинисан је скаларни производ два вектора $(x, y)$
- Дефинисано је растојање два вектора: $d(x, y) = \sqrt{(x - y, x - y)}$
- Дефинисан је интензитет вектора: $||x|| = \sqrt{(x, x)}$
- Важи неједнакост торуглова: $d(x, z) \leq d(x, y) + d(y, z)$
- $H$ је комплетан векторски простор: За сваки конвергентан низ из $H$, лимес којем тежи припада $H$.

Преостаје нам само да дефинишемо дуални Хилбертов простор $H_d$ и оператор у скупу $H$:
**Дефиниција** Сваки векторски простор има свој дуални векторски простор који представља простор линеарних функционала[4], с тога уз Хилбертов векторски простор постоји и **дуални Хилбертов векторски простор** $H_d$ који је простор линеарних функционала који све векторе из $H$ сликају у $\mathbb{C}$.
**Дефиниција** Оператор $A$ ($A : H \longrightarrow H$) је математичко правило које када применимо на вектор $x \in H$ добијемо вектор $x'$. Математички записано:

$$x' = A(x)$$

Мала напомена: због лакшег објашњења следећих појмова, сматраћемо да $H$ и $H_d$ имају дискретну базу вектора помоћу којих се сваки други вектор може приказати.

### 2.1.2 Диракова нотација

Британски научник Пол Дирак[5] 1939. године уводи такозвану бра-кет нотацију. Ова нотација се доста користи у квантној механици и омогућава нам да лакше прикажемо векторе и операторе, без коришћења матрица.

- $|\psi\rangle \in H$ се назива **кет** и представља вектор из изабраног $H$. Матрично се представља као колона-матрица:

$$|\psi\rangle = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \end{pmatrix}$$

[3]David Hilbert (1862-1943.)-немачки математичар
[4]функционал је трансформација (или скуп трансформација) које почетни векторски простор слика у његово скаларно поље
[5]Paul Dirac (1902-1984.)-енглески физичар, добитник Нобелове награде 1933. године

- $\langle\phi| \in H_d$ се назива **бра** и представља функцију одговарајућег дуалног Хилбертовог простора која одговара вектору $\phi$ из одабраног $H$. Матрично се представља као ред-матрица:

$$\langle\phi| = \begin{pmatrix}\overline{b_1} & \overline{b_2} & \dots\end{pmatrix}$$

- $\langle\phi|\psi\rangle \in \mathbb{R}$ се назива **бра-кет** и представља скаларни производ вектора $\phi$ и $\psi$. Матрични приказ:

$$\langle\phi|\psi\rangle = \begin{pmatrix}\overline{b_1} & \overline{b_2} & \dots\end{pmatrix}\begin{pmatrix}a_1\\a_2\\\vdots\end{pmatrix} = \sum_{i=1}^{\infty} a_i\overline{b_i}$$

- $A : H \longrightarrow H$ (уједно и $A : H_d \longrightarrow H_d$) је оператор над одабраним Хилберовим простором (и дуалним Хилбертовим простором), који се може представити као матрица[6]. Матрични приказ:

$$A = \begin{pmatrix}A_{11} & A_{12} & \dots\\A_{21} & A_{21} & \dots\\\vdots & \vdots & \ddots\end{pmatrix}$$

### 2.1.3 Својства кет-ова, бра-ова и оператора

Пошто смо у претходним потпоглављима (погледати потпоглавља 2.1 и 2.2) дефинисали шта је кет, бра и оператор и показали како се они означавају, време је и да покажемо нека од њихових својстава, не доказујући их:

- За сваки кет $|\psi\rangle$ постоји јединствени бра $\langle\psi|$ и свака координата кета има свог комплексно-коњугованог пара у координатама браа(координати $a_1$ кета одговара $\overline{a_1}$ координата браа, координати $a_2$ кета одгоавара $\overline{a_2}$ координата браа...) Обратно важи исто.

- $|\psi\rangle\langle\phi|$ је линеаран оператор (очувавају се операције сабирања вектира и множења скалара и вектора)

- Оператори међусобно могу, али не морају бити комутативни. Пошто су оператори матрице, савршени примери ове особине су сабирање и множење матрица. Сабирање 2 матрице је комутативно, док множење две матрице није. Према томе:

$$AB \neq BA$$

- Оператори су међусобно асоцијативни:

$$A(BC) = (AB)C$$

[6]Иако оператор може представљати било које математичко правило (може бити функција, извод...), за потребе квантног рачунарства су нам потребни само линеарни оператори, с тога ћемо на даље операторе сматрати матрицама

- Оператори делују са десна на лево на браове и са лева на десно на кетове:

$$\langle\psi| AB = (\langle\psi| A)B,\ AB|\psi\rangle = A(B|\psi\rangle)$$

- Ако се оператор нађе између браа и кета (било $\langle\phi|(A|\psi\rangle)$ или $(\langle\phi| A)|\psi\rangle$, небитно је, јер је операција асоцијативна) добија се комплексни број:

$$\langle\phi| A|\psi\rangle \in \mathbb{C}$$

Увешћемо и следеће појмове, који су име добили по француском математичару Хермиту[7]:

- **Хермитска коњугација комплексног броја** је његов коњуговано-комплексни пар:

$$a^\dagger = \overline{a}$$

- **Хермитска коњугација кета** $|\psi\rangle$ је његов одговарајући бра $\langle\psi|$, аналогно је хермитска коњугација браа $\langle\psi|$ његов одговарајучи кет $|\psi\rangle$:

$$|\psi\rangle^\dagger = \langle\psi|,\ \langle\psi|^\dagger = |\psi\rangle$$

- **Хермитска коњугација оператора** $A$ (означава се са $A^\dagger$) је транспозиција матрице оператора чији елементи су коњуговано-комплексни парови елемената из $A$.

- **Хермитски оператор** $A$ је онај оператор који је једнак свом хермитски коњугованом пару:

$$A = A^\dagger$$

- **Унитарни оператор** $A$ је онај оператор код кога је инверзна матрица једнака његовом хемритски коњугованом пару:

$$A^\dagger = A^{-1}$$

Ови појмови ће нам бити важни приликом формулације шест постулата квантне механике, које ћемо детаљније обрадити у следећем потпоглављу.

## 2.2 Постулати квантне механике

Постулат(или аксиом) је тврдња чија се истинитост подразумевана без доказивања. Квантна механика се заснива на 6 постулата, који дају нове дефиниције класичним физичким величинама и повезују квантну механику са математиком и тиме нам омогућавају да вршимо одређена израчунавања. Следи формулација свих 6 постулата квантне механике.

**Постулат 1.** *У сваком тренутку стање физичког система је приказано као кет* $|\psi\rangle$ *у простору стања.*

[7]Charles Hermite (1822-1901.)-француски математичар

Коментар: Простор стања је Хилбертов векторски простор (погледати потпоглавње 2.1.). Овај постулат је поприлично радикалан, јер и суперпозиција нека два стања система $|\psi_1\rangle$ и $|\psi_2\rangle$ коју ћемо назвати $|\psi\rangle$ ће припадати Хилберовом простору ($|\psi\rangle = a_1 |\psi_1\rangle + a_2 |\psi_2\rangle$ , $a_{1,\,2} \in \mathbb{C}$, коришћене су само операциије множења скалара и вектора и сабирање вектора), што би значило да је и $|\psi\rangle$ стање система.

**Постулат 2.** *Сваки посматрани атрибут $A$ физичког система је описан оператором $\hat{A}$ који делује на кетове који описују стања система.*

Коментар: Оператори су детаљно описани у претходна три потпоглавља.
Деловањем са оператором на систем углавном долази до промене стања система. Ипак, за сваки оператор постоје стања која се након примене оператора не мењају (осим што бивају помножена константом).

$$A |\psi_a\rangle = a |\psi_a\rangle$$

Ова стања се називају **сопствни вектори**, а бројеви $a$ се називају **сопствене вредности**.

**Постулат 3.** *Једине могуће вредности опсервабле $A$ (величине (атрибута) која се може директно измерити) је једна од сопствених вредности одговарајућег оператора $\hat{A}$*

Пошто можемо да меримо само реалне вредности, сопствене вредности $a_n$ које одговарају оператору  морају бити из скупа реалних бројева. Оператори који имају реалне сопствене вредности су хермитски. Сопствени вектори хермитских база су ортогонални и формирају базу посматраног Хилбертовог векторског простора (ово својство неће бити доказивано).

**Постулат 4.** *Када је извршено мерење опсервабле $A$ над стањем $|\psi\rangle$ одређеног Хилбертовог простора, вероватноћа да ће се остварити сопствена вредост $a_n$ је задата квадратом модула скаларног производа $|a_n\rangle$ и $|\psi\rangle$, односно квадратом модула бракета $a_n$ и $\psi$.*

$$P(a_n) = |(a_n, \psi)|^2 = |\,\langle a_n|\psi\rangle\,|^2$$

Коментар: Вероватноћа мора бити реални број.

**Постулат 5.** *Одмах након што је извршено мерење опсервабле  и као резултат добијена вредност $a_n$, стање система је сопствено стање $|a_n\rangle$*

Овај постулат је познат и као "колапс таласне функције"и најконтроверзнији је од свих постулата квантне механике. Ако направимо експериментални систем у стању $|\psi\rangle$ и хоћемо да извршимо мерење опсервабле  која има више могућих сопствених вредности $a_n$, свака од њих ће имати вероватноћу $|\,\langle a_n|\psi\rangle\,|^2$. Оно што је занимљиво је да потпуно идентични експериментални системи могу имати различите излазне вредности, али оне морају бити из скупа могућих вредности опсервабле $A$ (постулат 4). Оно што овај постулат говори је да када једном измеримо да је вредност опсервабле $A$ у ствари $a_n$ и ако одмах поновимо мерење опсервабле , опет ћемо за вредност добити $a_n$.

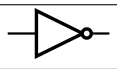
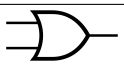
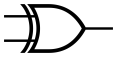
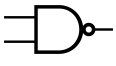
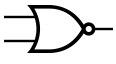
**Постулат 6.** *Временска еволуција стања $|\psi(t)\rangle$ квантног система је дефинисана на следећи начин:*

$$i\hbar\frac{d}{dt}|\psi(t)\rangle = \hat{H}|\psi(t)\rangle$$

Коментар:$\hat{H}$ је хермитски оператор који се зове Хамилтонијан.

## 2.3 Логичка кола бинарног рачунара

Да бисмо могли упоредити бинарне рачунаре са квантним, у најкраћим цртама ћемо описати основу бинарног рачунара и објаснити нека од логичких кола од којих је сачињен.
Као што и само име говори, бинарни рачунари функционишу по **бинарном бројевном систему** и основу бинарног рачунара чини јединица података звана **бит**(енг.*binary digit*). Бит може чувати само два стања: **нулу** или **јединицу**. У преводу, бинарни рачунар може да чува два стања новчића за бацање: главу (1) или писмо (0). Да бисмо могли да добијемо резултат неког комплекснијег задатка, потребно је да над више битова одрадимо неке логичке операције које ће променити стање битова, на основу којег ћемо тај резултат и добити. Интуитивно је јасно да **Булова алгебра**[8] савршено функционише са бинарним бројевним системом, с тога су логичка кола бинарног рачунара на њој и заснована. У табели ће бити приказане неке од капија бинарног рачунара.

| Назив у асемблеру | Назив | Графички приказ | Улазни подаци | Излазни подаци |
|---|---|---|---|---|
| NOT(p) | негација |  | $p$ | $\neg p$ |
| AND(p,q) | коњукција |  | $p, q$ | $p \wedge q$ |
| OR(p,q) | дисјункција |  | $p, q$ | $p \vee q$ |
| XOR(p,q) | екслузивна дисјункција |  | $p, q$ | $p \veebar q$ |
| NAND(p,q) | негативна конјукција |  | $p, q$ | $\neg(p \wedge q)$ |
| NOR(p,q) | негативна дисјункција |  | $p, q$ | $\neg(p \vee q)$ |
| XNOR(p,q) | еквиваленција |  | $p, q$ | $\neg(p \veebar q)$ |

Табела 1: *Неке од логичких капија бинарног рачунара*

Да бисмо вршили сва логичка израчунавања, потребне су нам NOT, AND и OR капије (све исказне формуле се могу свести на различит број $\neg$, $\wedge$ и $\vee$ операција које се могу, а и не морају понављати). Међутим, функцију капије OR можемо добити помоћу повезивања NOT и AND капија, исто као што функцију капије AND можемо добити повезивањем NOT и OR капија. Дакле, да бисмо направили неко логичко коло, не морамо користи две различите врсте капија. NAND и NOR капије се називају и **универзалне капије**, јер само уз помоћ великог броја NAND или само уз помоћ великог броја NOR капија можемо направити било које логичко коло.
Пошто смо увели све потребне појмове и у најкраћим цртама описали основу бинарног рачунара, коначно можемо да се ближе упознамо са светом квантних рачунара.

[8]George Boole (1815-1864)-енглески математчар

## 2.4 Кубит

Кубит(енг. *Quantum binary digit*) квантном рачунару представља исто што и бит бинарном рачунару: његову основну јединицу информације. У овом потпоглављу ћемо се детаљно упознати са кубитом, како се подаци у њему чувају, како се разликује од бита, како би изгледала његова репрезенатција у нама лако појмљивом тродимензионалном простору и како се систем од више кубита понаша.

### 2.4.1 О кубиту и поређење са битом

Баш као и бит, кубит има два основна стања: $|1\rangle = \begin{bmatrix}1\\0\end{bmatrix}$ и $|0\rangle = \begin{bmatrix}0\\1\end{bmatrix}$. Ипак, за разлику од бита који може да чува само та два стања, кубит може да чува стања која су суперпозиције $|1\rangle$ и $|0\rangle$. Да бисмо што боље разумели ову ситуацију, вратићемо се на аналогију новчића коју смо први пут користили у причи о биту. Бит може да чува оба стања новчића: главу(1) и писмо(0). Кубит такође може да чува стања која представљају главу (100 посто глава, 0 посто писмо) и писмо (0 посто глава, 100 посто писмо), али и да чува стања 75 посто глава 25 посто писмо и обратно. У теорији може чувати било које вероватноће за главу и писмо докле год је њихов збир 100 посто. Одређено стање $|\psi\rangle$ се приказује преко стања $|1\rangle$ и $|0\rangle$ на следећи начин:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,,\ \alpha, \beta \in \mathbb{C}$$

У прошлом параграфу се такође може приметити једна очигледна разлика између бита и кубита: излазни подаци. Бит ће увек имати одређену вредност: 1 или 0. Кубит ће увек имати две вредности: $|\alpha|^2$ и $|\beta|^2$, односно вероватноћу за $|0\rangle$ и вероватноћу за $|1\rangle$ (постулат 4). Оно што је карактеристично за $|\alpha|^2$ и $|\beta|^2$ је да у збиру увек дају 1 (збир вероватноћа мора бити 100 посто):

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

### 2.4.2 Репрезентација кубита у тродимензоналном простору

Пошто су $\alpha$ и $\beta$ комлексни бројеви чији збир квадрата модула једнак 1, имаћемо велики број стања. Ипак имамо стања код којих су парови вероватноћа идентични, а ипак нису у питању иста стања. Као пример дајем следећа стања:

$$|\psi_1\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}},\ |\psi_2\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}},\ |\psi_3\rangle = \frac{|0\rangle + i\,|1\rangle}{\sqrt{2}},\ |\psi_4\rangle = \frac{|0\rangle - i\,|1\rangle}{\sqrt{2}}$$

Сва ова стања имају исте парове вероватноћа $(\frac{1}{2}, \frac{1}{2})$, али ипак нису иста стања. Њих је поприлично тешко замислити. Много би нам било лакше ако бисмо на неки начин могли да их визуализујемо у тродимензионалном. Да бисмо то урадили, потребно нам је основно знање комплексних бројева и поларних координата.
Комплексне бројеве $\alpha$ и $\beta$ ћемо приказати на следећи начин:

$$\alpha = r_0 e^{i\phi_0},\ \beta = r_1 e^{i\phi_1},\quad 0 \leqslant \theta_0, \theta_1 \leqslant 2\pi$$

$r_0$ и $r_1$ су модули ових комплексних бројева, а $\theta_0$ и $\theta_1$ су њихови аргументи.

$$|\psi\rangle = r_0 e^{i\phi_0}|0\rangle + r_1 e^{i\phi_1}|1\rangle$$

Следећи корак је извући $e^{i\theta_0}$ испред зграде:

$$|\psi\rangle = e^{i\phi_0}(r_0 + r_1 e^{i(\phi_1-\phi_0)})$$

Број $e^{i\phi_0}$ неће утицати на резултат (може се доказати) и може се одстранити из израза:

$$|\psi\rangle = r_0 + r_1 e^{i(\phi_1-\phi_0)}$$

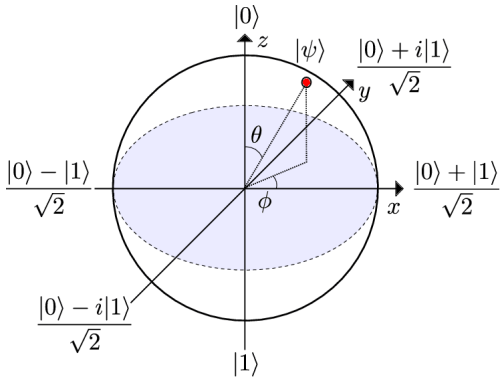
$r_0$ и $r_1$ су, као што је речено, модули ових комплексних бројева и за њих знамо да важи $r_0^2+r_1^1$, иста особина важи и за sin и cos истог угла. Увешћемо следеће смене које ће бити објашњене ускоро:

$$r_0 = \cos\frac{\theta}{2},\ r_1 = \sin\frac{\theta}{2}, \quad 0 \leqslant \theta \leqslant \pi$$

Ове смене уз смену $\theta = \theta_1 - \theta_0$ ћемо убацити у израз:

$$|\psi\rangle = \cos\frac{\theta}{2} + \sin\frac{\theta}{2}e^{i\phi},$$

Геометријска интерпретација овог израза у тродимензионалном простору је чувена Блохова сфера[10]:




Слика 10: Графички приказ Блохове сфере

Координата вектора $|\psi\rangle$ на Блоховој сфери је одређена његовим поларним координатама: његовим радијус вектором (он је увек један јер је полупречник Блохове сфере), углом који његова пројекција на $xOy$ раван гради са $x$-осом ($\angle\phi$) и углом који он заклапа са $z$-осом ($\angle\theta$). Разлог зашто смо се одлучили за смену $r_0 = \cos\frac{\theta}{2},\ r_1 = \sin\frac{\theta}{2}, \quad 0 \leqslant \theta \leqslant \pi$ је једноставан: овако су стања $|0\rangle$ и $|1\rangle$ на истој оси, док су иначе ортогонални. Исто ће важити и за стања код којих се коефицијенти испред$|0\rangle$ и $|1\rangle$ разликују само у знаку. Још једно лепо својство Блохове сфере је да се сва стања који имају исти уређени пар вероватноћа (a,b) налазе на једном кругу који је нормалан на $z$-осу. Стања која се налазе на $x$-оси $(|+\rangle\ |-\rangle)$y$-(|i+\rangle\ |i-\rangle)j$.

[10]Felix Bloch(1905-1983)-швајцарски физичар, добитнк Нобелове награде 1952.године

### 2.4.3 Систем више кубита

У претходним одељцима (2.4.1. и 2.4.2.) смо се упознали са кубитом и његовим својствима. Иако је кубит у поређењу са битом, осим могућности чувања већег броја стања и нема неке велике предности, следи прича која ће зацементирати надмоћ квантних рачунара у односу на бинарне рачунаре: систем више кубита.

Баш као што можемо да посматрамо више битова бинарног рачунара истовремено, можемо посматрати и више кубита квантног рачунара истовремено. Ради једноставности, на почетку ћемо посматрати систем који се састоји од два кубита. Оваквав систем има четири основна стања: $|00\rangle$, $|01\rangle$, $|10\rangle$ и $|11\rangle$. Ово опет, као ни код једног кубита, није никаква новина. Два бита могу исто могу бити у једном од ова 4 стања. Ипак, овде се појављујује први феномен квантне механике, који се јавља и код једног кубита, али овде долази до много већег изражаја: **квантна суперпозиција**.
Аналогно једном кубиту, где смо имали суперпозицију два основна стања система, код система са два кубита ћемо имати суперпозицију четири основна стања:

$$|\psi\rangle = \alpha_{00}\,|00\rangle + \alpha_{01}\,|01\rangle + \alpha_{10}\,|10\rangle + \alpha_{11}\,|11\rangle\,, \quad \alpha_{00}, \alpha_{01}, \alpha_{10}, \alpha_{11} \in \mathbb{C}$$

За бројеве $\alpha_{00}$, $\alpha_{01}$, $\alpha_{10}$ и $\alpha_{11}$ важи исто што је важило и за бројеве $\alpha$ и $\beta$ код једног кубита: вероватноћа да је систем у неком од основних стања је једнака квадрату модула коефицијента који је испред тог стања:

$$P(|00\rangle) = |\alpha_{00}|^2,\ P(|01\rangle) = |\alpha_{01}|^2,\ P(|10\rangle) = |\alpha_{10}|^2,\ P(|11\rangle) = |\alpha_{11}|^2.$$

Збир ових бројева је такође једнак јединици као и код једног кубита:

$$|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$$

Суперпозиција је огромна предност квантног рачунара: иако систем од два кубита има исти скуп основних стања, он ће бити у свим тим стањима са одређеном вероватноћом (све док се не изврши мерење), за разлику од бинарног система који ће бити само у једном од тих стања. Ситуација само више иде у прилог квантним рачунарима ако повећавамо број кубита: системи од $n$ бита и $n$ кубита ће имати $2^n$ стања и квантни систем ће истовремено бити у $2^n$ стања (са одређеним вероватноћама), док ће бинарни систем бити и даље само у једном. То значи да релативно мали број кубита може да чува екстремно велики број информација.
Сада ћемо приказати како изгледа опште стање система од $n$ кубита:

$$|\psi\rangle = \sum_{i=1}^{n} \alpha_{q_1 q_2 ... q_n}\,|q_1 q_2 ... q_n\rangle\,, \quad q_1, q_2, ..., q_n \in \{\,0, 1\,\}$$

Вероватноћа одређеног основног стања $|q_1 q_2 ... q_n\rangle$ се рачуна исто као и код система од једног или два кубита:

$$P(|q_1 q_2 ... q_n\rangle) = |\alpha_{q_1 q_2 ... q_n}|^2, q_1, q_2, ..., q_n \in \{\,0, 1\,\}$$

За коефицијенте испред основних стања и даље важи да је збир свих модула квадрата 1:

$$\sum |\alpha_{q_1 q_2 ... q_n}|^2 = 1, \quad q_1, q_2, ..., q_n \in \{ 0, 1 \}$$

Ако извршимо мерење над одређеним кубитима или некако сазнамо да је неко стање немогуће, добићемо скуп могућих стања који је подскуп почетног скупа основних стања. Овиме ће се променити и вероватноће преосталих могућих стања. Да бисмо ово својство илустровали, вратићемо се на систем од два кубита: Ако извршимо мерење над првим кубитом и утврдимо да је његова вредност 1, од почетног скупа од 4 стања завршили смо на скупу од 2 стања: $|10\rangle$ и $|11\rangle$. Тада ће свако стање $|\psi\rangle$ изгледати овако:

$$|\psi\rangle = \frac{\alpha_{10}\,|10\rangle + \alpha_{11}\,|11\rangle}{\sqrt{|\alpha_{10}|^2 + |\alpha_{11}|^2}}$$

Преостале вероватноће се, као што је напоменуто, променити:

$$P(|10\rangle) = |\frac{\alpha_{10}}{\sqrt{|\alpha_{10}|^2 + |\alpha_{11}|^2}}|^2 = \frac{|\alpha_{10}|^2}{|\alpha_{10}|^2 + |\alpha_{11}|^2}, \quad P(|11\rangle) = \frac{|\alpha_{11}|^2}{|\alpha_{10}|^2 + |\alpha_{11}|^2}$$

Корен у имениоцу се јавља да би збир свих преосталих могућности и даље био један.

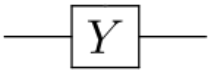
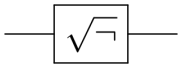
Још једна лепа особина система од два или више кубита је да они могу бити у **квантној спрези** (енг. *quantum entanglement*). Као што је показано Беловом теоремом (за више погледати одељак 1.1), два објекта која су у квантној спрези као да комуницирају међу собом брзином већом од брзине светлости. Експериментално, то би значило да ако измеримо неку особину једног од та два објекта, истог тренутка, без извршеног мерења над другим објектом, знаћемо вредност те особине другог објекта. Уз паметно постављене везе између кубита, са јако малим бројем извршених мерења ћемо знати вредности великог броја кубита готово инстантно. Ово је кључ брзине квантних рачунара. О стањима где су кубити у квантној спрези ће бити речи даље у тексту.

## 2.5 Логичка кола квантног рачунара

Логичке капије су, у суштини, унитарни оператори који делују на један или више кубита мењајући им стање. Пошто смо у претходним одељцима подразумевали да је оператор матрица, већина логичких капија ће бити унитарне матрице. У овом одељку ћемо се детаљно посветити логичким колима, на неки начин их класификовати и објаснити како се могу повезивати.

### 2.5.1 Логичке капије на једном кубиту

Ако посматрамо и оператор $A$ и вектор стања $|\psi_1\rangle$ као матрице, ново стање $|\psi_2\rangle$ које настаје деловањем оператора на стање можемо приказати као производ матрице оператора $A$ и матрице стања $|\psi_1\rangle$. Сада ћемо се упознати са неким капијама које делују на један кубит.

| Назив | Графички приказ | Приказ оператора | Коментар |
|---|---|---|---|
| Адамарова капија |  | $\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$ | излаз у општем случају $\frac{1}{\sqrt{2}}((a+b)\|0\rangle+(a-b)\|1\rangle)$ за стање $\|0\rangle$ претвара у $\frac{1}{\sqrt{2}}(\|0\rangle+\|1\rangle)$ |
| Паулијева X капија |  | $\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$ | Еквивалент NOT капије, Ротира око X-осе Блохове сфере за $\pi$ |
| Паулијева Y капија |  | $\begin{bmatrix}0 & -i\\ i & 0\end{bmatrix}$ | Ротира око Y-осе Блохове сфере за $\pi$ |
| Паулијева Z капија |  | $\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}$ | Ротира око Z-осе Блохове сфере за $\pi$ |
| Капија фазног помераја $\phi$ |  | $\begin{bmatrix}1 & 0\\ 0 & e^{i\phi}\end{bmatrix}$ | Помера поларну координату $\theta$ (погледати Блохову сферу) за неки угао$\phi$ |
| Корен NOT капија |  | $\frac{1}{2}\begin{bmatrix}1+i & 1-i\\ 1-i & 1+i\end{bmatrix}$ | Двоструким понављањем добијамо Паулијеву X капију. Ову капију је немогуће рекреирати на бинарном рачунару |

Табела 2: Неке од капија које делују на један кубит

Једини изузетак од ових капија је капија која извршава мерење. Ово је једина капија која није матрица и која је иреверзибилна (долази до колапса таласне функције). Када једном извршимо мерење, не можемо вратити систем у суперпозицију. Ова капија има два излазна параметра: вероватноћу за стање $|0\rangle$ и вероватноћу за стање $|1\rangle$.

Слика 11: Графички приказ капије за мерење

### 2.5.2 Логичке капије на два или више кубита; Контролисане капије

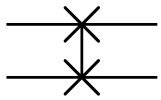
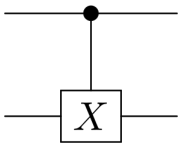
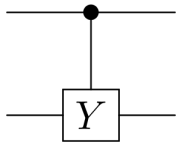
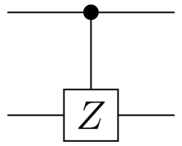
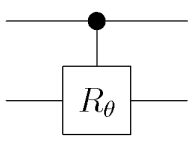
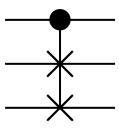
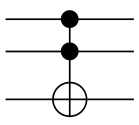
Пре него што излистамо логичке капије над два или више кубита, морамо да дефинишемо шта су то контролисане капије. Контролисане капије делују на два или више кубита, при томе бар један кубит контролише операцију која се врши на другим кубитима који пролази кроз капију.

Поред капија које делују на два кубита, постоје и капије које делују на три кубита. Најпознатије капије које делују на три кубита су Тофолијева[11] (CCNOT) капија и Фредкинова[12]

[11] Tomasso Toffoli (1943- )-италијанско-амерички научник

[12] Edward Fredkin (1934- )-амерички научник

(CSWAP) капија. Занимљива ствар везана за ове две капије је да су оне универзалне за било коју логичку и аритметичку операцију, што значи да искључиво од Фредкинових или Тофолијевих капија можемо да направимо било које логичко или аритметичко коло. Ово потврђује чињеницу да квантни рачунари могу обављати све што могу и бинарни рачунари.

| Назив | Графички приказ | Приказ оператора | Коментар |
|---|---|---|---|
| SWAP капија |  | $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$ | размењује стања између два кубита |
| Контролисана X (CNOT) капија |  | $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$ | Ако је вредност првог кубита $\|1\rangle$, примењује Паули X капију на други, а ако је вредност првог $\|0\rangle$ не ради ништа |
| Контролисана Y (CY) капија |  | $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & i \\ 0 & 0 & -i & 0 \end{bmatrix}$ | Ако је вредност првог кубита $\|1\rangle$, примењује Паули Y капију на други, а ако је вредност првог $\|0\rangle$ не ради ништа |
| Контролисана Z (CZ) капија |  | $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$ | Ако је вредност првог кубита $\|1\rangle$, примењује Паули Z капију на други, а ако је вредност првог $\|0\rangle$ не ради ништа |
| Контролисана капија фазног помераја $\theta$ |  | $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\theta} \end{bmatrix}$ | Ако је вредност првог кубита $\|1\rangle$, врши фазни померај на други, а ако је вредност првог $\|0\rangle$ не ради ништа |
| Фредкинова (CSWAP) капија |  | $\begin{smallmatrix} 1&0&0&0&0&0&0&0 \\ 0&1&0&0&0&0&0&0 \\ 0&0&1&0&0&0&0&0 \\ 0&0&0&1&0&0&0&0 \\ 0&0&0&0&1&0&0&0 \\ 0&0&0&0&0&0&1&0 \\ 0&0&0&0&0&1&0&0 \\ 0&0&0&0&0&0&0&1 \end{smallmatrix}$ | Ако је стање контролног кубита $\|1\rangle$ размењује стања између преостала два кубита, а ако није, не ради ништа |
| Тофолијева (CCNOT) капија |  | $\begin{smallmatrix} 1&0&0&0&0&0&0&0 \\ 0&1&0&0&0&0&0&0 \\ 0&0&1&0&0&0&0&0 \\ 0&0&0&1&0&0&0&0 \\ 0&0&0&0&1&0&0&0 \\ 0&0&0&0&0&1&0&0 \\ 0&0&0&0&0&0&0&1 \\ 0&0&0&0&0&0&1&0 \end{smallmatrix}$ | Ако је вредност контролних кубита $\|11\rangle$, примењује Паули X капију на трећи, а ако није, не ради ништа |

Табела 3: Неке од капија које делују на два и три кубита

Лепа особина свих ових оператора је то што су они унитарне матрице, односно да им је њихов хермитски пар инверз (у специјалним случајевима су једнаке и инверзу). Ова особина нам говори да су промене стања изазваних овим логичким капијама реверзибилне, односно ако применимо инверзну капију одмах након капије (или у специјалном случају ако применимо исту капију двапут) вратићемо се у почетно стање.

### 2.5.3 Повезивање капија у коло

Слично као што правимо класична електрична кола, правићемо и кола квантног рачунара. Капије у коло можемо да повежемо редно или паралелно. Да бисмо математички дефинисали један од начина везивања капија и како функционишу стања која обухватају кубите у квантној спрези када се на један од кубита примени капија, морамо дефинисати Кронекеров производ матрица[13]:

**Кронекеров производ матрица** (означава се са $\bigotimes$): Ако имамо два матрице $A(m \times n$ матрица) и $B(p \times q$ матрица), Кронекеров производ матрица $A \bigotimes B$ је $pm \times qn$ матрица која се гради на следећи начин:

$$A \bigotimes B = \begin{bmatrix} a_{11}B & a_{12}B & \dots & a_{1n}B \\ a_{21}B & a_{22}B & \dots & a_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}B & a_{m2}B & \dots & a_{mn}B \end{bmatrix} =$$

$$= \begin{bmatrix} a_{11}b_{11} & a_{11}b_{12} & \dots & a_{11}b_{1q} & \dots & \dots & a_{1n}b_{11} & a_{1n}b_{12} & \dots & a_{1n}b_{1q} \\ a_{11}b_{21} & a_{11}b_{22} & \dots & a_{11}b_{2q} & \dots & \dots & a_{1n}b_{21} & a_{1n}b_{22} & \dots & a_{1n}b_{2q} \\ \vdots & \vdots & \ddots & \vdots & \dots & \dots & \vdots & \vdots & \ddots & \vdots \\ a_{11}b_{p1} & a_{11}b_{p2} & \dots & a_{11}b_{pq} & \dots & \dots & a_{1n}b_{p1} & a_{1n}b_{p2} & \dots & a_{1n}b_{pq} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \ddots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \ddots & \ddots & \vdots & \vdots & \vdots & \vdots \\ a_{m1}b_{11} & a_{m1}b_{12} & \dots & a_{m1}b_{1q} & \dots & \dots & a_{mn}b_{11} & a_{mn}b_{12} & \dots & a_{mn}b_{1q} \\ a_{m1}b_{21} & a_{m1}b_{22} & \dots & a_{m1}b_{2q} & \dots & \dots & a_{mn}b_{21} & a_{mn}b_{22} & \dots & a_{mn}b_{2q} \\ \vdots & \vdots & \ddots & \vdots & \dots & \dots & \vdots & \vdots & \ddots & \vdots \\ a_{m1}b_{p1} & a_{m1}b_{p2} & \dots & a_{m1}b_{pq} & \dots & \dots & a_{mn}b_{p1} & a_{mn}b_{p2} & \dots & a_{mn}b_{pq} \end{bmatrix}$$

Кронекеров производ матрица је лакше схватити на примеру, с тога ћемо увести једноставан пример:

$$A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}, B = \begin{bmatrix} 5 & 6 \\ 7 & 8 \end{bmatrix}$$

Кронекеров производ $A \bigotimes B$ је једнак:

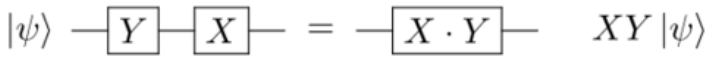
$$A \bigotimes B = \begin{bmatrix} 1\begin{bmatrix} 5 & 6 \\ 7 & 8 \end{bmatrix} & 2\begin{bmatrix} 5 & 6 \\ 7 & 8 \end{bmatrix} \\ 3\begin{bmatrix} 5 & 6 \\ 7 & 8 \end{bmatrix} & 4\begin{bmatrix} 5 & 6 \\ 7 & 8 \end{bmatrix} \end{bmatrix} = \begin{bmatrix} 1\cdot 5 & 1\cdot 6 & 2\cdot 5 & 2\cdot 6 \\ 1\cdot 7 & 1\cdot 8 & 2\cdot 7 & 2\cdot 8 \\ 3\cdot 5 & 3\cdot 6 & 4\cdot 5 & 4\cdot 6 \\ 3\cdot 7 & 3\cdot 8 & 4\cdot 7 & 4\cdot 8 \end{bmatrix} = \begin{bmatrix} 5 & 6 & 10 & 12 \\ 7 & 8 & 14 & 16 \\ 15 & 18 & 20 & 24 \\ 21 & 24 & 28 & 32 \end{bmatrix}$$

[13] Leopold Kronecker (1823-1891)-немачки математичар

Битна особина Кронекеровог производа је да ако је сачињен од унитарних матрица и сам ће бити унитарна матрица. Инверз матрице $A \bigotimes B$, сачињене од унитарних матрица $A$ и $B$ је ${}^{\dagger} \bigotimes B^{\dagger}$ (може се доказати). Важност ове особине ће доћи до изражаја на крају одељка.
Сада када смо дефинисали све математичке појмове битне за повезивање капија у коло, можемо им се детаљније посветити.

**Редна кола** Ако имамо две капије $P$ и $Q$, при чему је капија $Q$ делује на кубите након $P$, њих две ће симулирати једну капију $R$ која се може репрезентовати као матрични производ $Q$ и $P$:

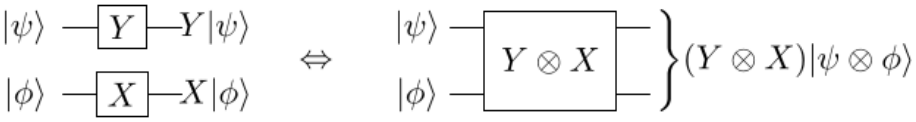
$$R = Q \cdot P$$




Слика 12: Пример Паулијевих X и Y кола која су везана редно

**Паралелна кола** Ако имамо две капије $P$ и $Q$ при чему је капија на $P$ делује на кубите који су у стању $|\psi\rangle$, а $Q$ делује на кубите који су у стању $|\phi\rangle$, њих две ће симулирати једну капију $R$ која се може репрезентовати као Кронекеров производ капија $P$ и $Q$ које делују на стање које је Кронекеров производ $\psi$ и $\phi$, или математички речено:

$$(P \bigotimes Q)\,|\psi \bigotimes \phi\rangle$$




Слика 13: Пример Паулијевих X и Y кола, која делују на $|\phi\rangle$ и $|\psi\rangle$ редом, везаних паралелно

Пошто су све капије унитарне матрице, а матрични и Кронекеров производ матрица које су унитарне матрице је у оба случаја унитарна матрица, то значи да ће сва логичка кола такође бити унитарна. Инверзно коло датог кола $A \cdot (B \bigotimes C)$ добијамо на следећи начин:

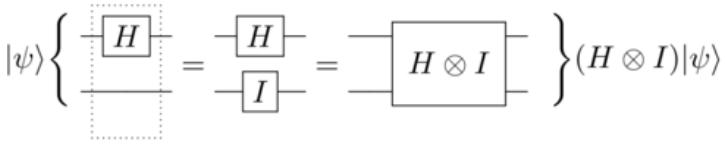
$$(A \cdot (B \bigotimes C))^{\dagger} = (B \bigotimes C)^{\dagger} \cdot A^{\dagger} = (B^{\dagger} \bigotimes C^{\dagger}) \cdot A^{\dagger}$$

### 2.5.4 Стања са кубитима у квантној спрези

У овом одељку ћемо се посветити стањима која укључује два или више кубита који су повезани квантном спрегом. Без умањења општости, посматраћемо само стања која укључују два кубита повезана квантном спрегом. Једно од најпознатијих оваквих стања је Белово стање:

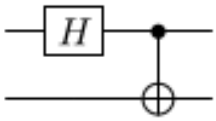
$$|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

Ово стање ће нам савршено показати својства квантне спреге. Овде се лако може приметити својство квантне спреге које већ знамо, а то је да ако одредимо стање само једног кубита, аутоматски ћемо знати вредност другог кубита без икаквог мерења. Друга занимљива чињеница је да су оваква стања нераздвојива, односно не могу се приказати преко Кронекеровог производа стања кубита који су у спрези. То се може приметити и у нашем примеру. С тога треба водити рачуна када примењујемо капије на оваква стања. На пример, ако желимо да применимо капију $A$ која делује на један кубит из Беловог стања, наићићемо на проблем. Наиме, матрица капије $A$ која делује на један кубит је димензија $2 \times 2$, док је матрица Беловог стања димензија $4 \times 1$, што значи да множење ових матрица није могуће. Морамо проширити матрицу капије $A$ тако да буде димензија $4 \times 4$, а то ћемо извести тако што ћемо извршити Кронекеров производ ње и јединичне матрице $I$ димензија $2 \times 2$. То значи да ћемо паралелно везати капију  која ће деловати на први кубит и капију $I$ која неће уопште деловати на други кубит.




Слика 14: Пример Адамарове капије која делује на стање $|\psi\rangle$ које је сачињено од два кубита у спрези

Постоје кола која стандардна стања претварају у стања са квантном спрегом. На пример, стање $|00\rangle$ се може претворити у Белово стање помоћу кола $CNOT(H \bigotimes I)$ кола, познатог и као Белово коло.




Слика 15: Графички приказ Беловог кола

## 2.6 Квантна Тјурингова машина

У одељку 1.2. је било речи о Тјуринговој машини, Тјуринговој комплетности и чињеници да је скоро сваки модерни рачунар Тјуринг-комплетан. Причу о овоме ћемо мало проширити и објаснити шта је то квантна Тјурингова машина.
Тјурингова машина се може представити као уређена седморка симбола звана $M$

$$M = [Q, \Gamma, b, \Sigma, q_0, F, \delta]$$

- $Q$ представља коначан непразан скуп стања, на пример $\{ A, B, C, HALT \}$
- $\Gamma$ представља коначан непразан скуп симбола на траци, на пример $\{ 0, 1 \}$

- $b \in \Gamma$ представља празан симбол, на пример 0
- $\sigma \in \Gamma$ представља непразан скуп улазних симбола, на пример 1
- $q_0 \in Q$ представља иницијално стање, на пример $A$
- $F \subseteq Q$ представља непразан скуп крајњих стања, на пример $HALT$
- $\delta$ представља транзициону функцију која помера траку лево или десно у зависности од стања

Да бисмо имали квантну Тјурингову машину, неопходно је да редефинишемо горе наведене скупове и повежемо их са Хилбертовим простором, према томе:

- $Q$ је замењен Хилбертовим простором стања
- $\Gamma$ је такође замењен Хилбертовим простором, углавном различитим од простора стања
- $b \in \Gamma$ је повезан са нултим вектором
- $\sigma$ остаје непромењен, јер улазни и излазни симболи не морају бити квантна стања
- $q_0 \in Q$ је стање из $Q$
- $F \subseteq Q$ је потпростор $Q$
- $\delta$ представља скуп унитарних матрица које су изоморфизми простора $Q$ на самог себе

У овом поглављу смо се детаљно посветили квантним рачунарима и макар у цртама објаснили како они функционишу. У следећим поглављима ћемо се детаљно посветити можда најпознатијем алгоритму створеном за квантне рачунаре, Шоровом алгоритму, његовом детаљном објашњењу и потенцијалној примени, али и потенцијалној примени квантних рачунара, као и питању зашто још увек нису у широј употреби.

# 3 Опис и објашњење Шоровог алгоритма

Како смо се у претходним поглављима детаљно упознали са квантним рачунарима, њиховим начином рада и стекли довољно знања о њима да бисмо наставили даље, време је да се упознамо и са вероватно најпознатијим квантним алгоритмом, Шоровим алгоритмом. Ово поглавље ће се детаљно посветити овом алгоритму, сазнаћемо чему је намењен, објаснити његову математичку и квантномеханичку позадину и на крају објаснити његову брзину.

## 3.1 О алгоритму

Амерички математичар и професор америчког универзитета MIT (енг. *Massachusetts Institute of Technology*) Питер Шор (енг. Peter Shor) је 1994. године конструисао овај алгоритам као **ефикасни алгоритам факторизације природних бројева**. Иако множење бројева бинарним рачунарима не изазива проблем и довољно је ефикасно, исто се не може рећи и за факторизацију природних бројева. Иако за релативно мале бројеве извршавање њихове факторизације не одузима пуно времена, време обраде чак и најбољих бинарних алгоритама са повећањем броја цифара расте експоненцијално. Иако је математика иза Шоровог алгоритма позната и технички је могуће користити Шоров алгоритам и на бинарним рачунарима, кључ ефикасности Шоровог алгортима лежи у могућностима квантних рачунара. 2001. године у америчкој компанији IBM, уз помоћ квантног рачунара са 7 кубита, применом Шоровог алгоритма је успешно извршена факторизација броја 15. Највећи број на којем је, у правом смислу, извршена факторизација Шоровим алгоритмом је 21 и то је учињено 2012. године. Следе математичка и квантномеханичка основа Шоровог алгоритма.

## 3.2 Математичка основа Шоровог алгоритма

Математичка основа Шоровог алгоритма се заснива на теорији бројева, области математике којој смо се детаљно посветили у другој години предмета "Анализа са алгебром". Кроз низ дефиниција и теорема које ћемо доказати, показаћемо како Шоров алгоритам функционише из математичке перспективе.

**Теорема 1.** *Сваки природан број* $n$, $n \geqslant 2$ *је или прост или је производ простих бројева*

*Доказ.* Тврђење доказујемо индукцијом:
1) За $n = 2$ знамо да је тврђење тачно, јер је 2 прост број
2) Нека је $n \geqslant 2$ природан број. Претпоставимо да тврђење важи за све бројеве $k$, $k < n$.Тада ћемо за наше $n$ имати две могућности: или је $n$ прост број, чиме тврђење важи, или је сложен, што значи да се може приказати као производ бројева $k_1$ и $k_2$ који су мањи од $n$. Међутим, како за $k_1$ и $k_2$ важи да су или прости или производи простих бројева, то ће значити и да је $n = k_1 \cdot k_2$ производ простих бројева, чиме је тврђење доказано. ■

Увешћемо и једну теорему без доказа:

**Теорема 2.** *Ако* $p|ab$, *а притом* $p$ *и* $a$ *немају заједничких делилаца изузев 1, онда* $p|b$

**Теорема 3.** *Ако је $p$ прост број и $p|ab$, онда $p|a$ или $p|b$.*

*Доказ.* Ако претпоставимо да $p|a$, тврђење важи. Ако пак тврдимо да $p$ не дели $a$, пошто је $p$ прост број, они немају заједничких делилаца изузев 1. По теореми 2, онда ће важити $p|b$, чиме је ова теорема доказана. ■

**Теорема 4.** *Сваки природан број $N$ већи од 1 се може јединствено приказати у облику производа простих чинилаца (са тачношћу до њиховог поретка).*

*Доказ.* Због теореме 1 знамо да је сваки природни број $N$ већи од 1 или прост или се може приказати као производ простих чинилаца. Сада је ред да докажемо да је тај производ чинилаца јединствен. За почетак, претпоставићем супротно и тврдићемо да природан број $N$ може да се прикаже преко два оваква производа:

$$N = p_1 p_2 \dots p_k = q_1 q_2 \dots q_l$$

Изабраћемо један произвољан број $p_i$ из првог производа бројева. Производ $q_1 q_2 \dots q_l$ мора бити дељив са $p_i$, што по теореми 3 имплицира да $p_i$ дели неки од бројева из производа. Како је производ $q_1 q_2 \dots q_l$ сачињен искључиво од простих бројева, онда ће број $p_i$ бити једнак неком од бројева из $q_1 q_2 \dots q_l$, рецимо $p_i = q_j$. Аналогно, за сваки број $q_j$ из другог производа постојаће број $p_i$ који ће му бити једнак. Када скратимо ове бројеве из њихових производа, поступак се понавља, чиме је теорема доказана. ■

**Дефиниција 1.** *Ако се у разлагању броја $N$ неки чиниоци понављају, па се, рецимо $p_1$ јавља $\alpha_1$ пута,$p_2$ јавља $\alpha_2$ пута,..., $p_k$ јавља $\alpha_k$ пута, онда се облик*

$$N = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$$

*назива* ***канонска факторизација*** *броја $N$.*

Као што смо навели, процес факторизације природних бројева на бинарним рачунарима није претерано ефикасан. Посебан проблем представља факторизација великих бројева $N$ чија је канонска факторизација дефинисана на овај начин:

$$N = q_1 \cdot q_2$$

где су $q_1$ и $q_2$ прости бројеви приближно исте дужине. На овом принципу је чак створена енкрипција која се данас јако често користи на интернету (о овоме ће бити речи касније). Овакве бројеве ћемо користити као пример при објашњавању Шоровог алгоритма, накнадно ћемо додати како алгоритам функционише у општем случају.
Под претпоставком да нам је број $N$ познат, ако желимо да сазнамо његова два чиниоца $q_1$ и $q_2$, тривијално је јасно да нам је потребно да знамо само један и да ћемо знати оба. Међутим, то нам не олакшава претерано овај проблем, јер су $q_1$ и $q_2$ велики прости бројеви, за које не знамо практично ништа осим да кад се множе чине $N$. Оно што нам иницијално преостаје је да погађамо. Већина алгоритама то и ради: генеришу произвољне бројеве и проверавају да ли је то један од наших тражених бројева. Овај процес за велике бројеве може трајати и

годинама. Један од начина на који можемо да олакшамо себи овај процес је да погодимо неки број $M$ који ће делити са $N$ један од чинилаца. Ове бројеве је доста лакше погодити него неки од чинилаца $N$ (има их много више), а ако погодимо бар један од њих, помоћу познатог **Еуклидовог алгоритма**[1] ћемо утврдити један од чинилаца броја $N$.

**Дефиниција 2.** *Највећи међу заједничким делиоцима бројева $a$ и $b$ је највећи заједнички делилац бројева $a$ и $b$.(Обележава се са НЗД$(a,b)$). За целе бројеве кажемо да су узајамно прости ако је НЗД$(a,b)$=1.*

**Теорема 5.** *Ако је $a = bq + r,\ 0 \leqslant r < b$(може се доказати да се сваки цео, па и природаан број може овако приказати), онда је НЗД$(a,b)$=НЗД$(b,r)$.*

*Доказ.* Нека је $d$ заједнички делилац бројева $a$ и $b$. Тада из $a = bq + r$ следи да је $d$ делилац $r$, односно да је $d$ заједнички делилац $b$ и $r$. Слично, ако је $d$ заједнички делилац $b$ и $r$, онда је $d$ заједнички делилац бројева $a$ и $b$, што значи да се се скупови заједничких делилаца $a$ и $b$ и $b$ и $r$ поклапају, па им се и највећи елементи поклапају. Према томе, НЗД$(a,b)$=НЗД$(b,r)$ ■

Процес налажења НЗД$(a,b)$ функционише на следећи начин:

$$a = bq_1 + r_1,\ 0 \leqslant r_1 < b,$$

$$b = r_1q_2 + r_2,\ 0 \leqslant r_2 < r_1,$$

$$r_1 = r_2q_3 + r_3,\ 0 \leqslant r_3 < r_2,$$

$$\dots$$

$$r_{n-2} = r_{n-1}q_n + r_n,\ 0 \leqslant r_n < r_{n-1},$$

$$r_{n-1} = r_nq_{n-1}$$

Како бројеви $r_k$ чине опадајући низ природних бројева, лако је схватити да ћемо након коначног броја корака завршити, односно доћи до једнакости $r_{n-1} = r_nq_{n-1}$ и броја $r_n$ о којем ће нам више рећи следећа теорема.

**Теорема 6.** *Последњи остатак $r_n$ који је различит од нуле и претходном поступку представља НЗД$(a,b)$.*

*Доказ.* Ако се осврнемо на теорему 5, видећемо да је задовољен следећи низ једнакости: НЗД$(a,b)$=НЗД$(b,r_1)$=НЗД$(r_1,r_2)$= $\dots$ =НЗД$(r_{n-2},r_{n-1})$=НЗД$(r_{n-1},r_n)$. Како $r_n|r_{n-1}$, то значи да је НЗД$(r_{n-1},r_n)$= $r_n$, односно НЗД$(a,b)$= $r_n$. ■

Еуклидов алгоритам је јако ефикасан и доста нам олакшава посао ако насумично изабран природан број $M$ и $N$ имају заједничких делилаца. Проблем, међутим настаје када су они узајамно прости. Да не бисмо стално бирали $M$ и проверавали НЗД њега и $N$, морамо користити другачији метод. Увешћемо још појмова који ће нас увести у један ефективан метод налажења нетривијалних делилаца (делиоци који нису 1 и $N$):

[1] Euclidus(око 365-300.године п.н.е.)

**Дефиниција 3.** *Нека је дат природан број $m$, већи од 1. Два цела броја $a$ и $b$ су конгруентна по модулу $m$ ако дају исти остатак при дељењу са $m$*

Ова релација се пише као $a \equiv b \pmod{m}$ или као $a \equiv_m b$. Поред дефиниције увешћемо још неке особине које нису тешке за проверавање:

1. $a \equiv b \pmod{m}$ ако и само ако је $a = mt + b,\ 0 \leqslant b < m$, где је $t$ неки цео број
2. $a \equiv b \pmod{m}$ ако и само ако је разлика бројева дељива са $m$.
3. Бити конгруентан по датом модулу је релација еквиваленције.

Увешћемо још једну теорему коју нећемо доказивати, а која ће нам бити корисна при доказивању леме која следи

**Лема 1.** *Дат је сложен број $N$ и $x$ је нетривијални корен једначине $x^2 \equiv 1 \pmod{N}$ (под нетривијалним решењем се сматра да $x \pm 1$), онда уз помоћу $x$ можемо израчунати нетривијални количник $N$ (под тривијалним количником сматрамо 1 и $N$)*

*Доказ.* Како је $x^2 \equiv 1 \pmod{N}$, то значи да је $(x-1)\cdot(x+1) \equiv 0 \pmod{N}$, а како $x \neq \pm 1 \pmod{N}$, то значи да је $1 < x < N-1$. Одавде знамо да је НЗД$(N, x-1)$ или НЗД $(N, x+1)$ нетривијални делилац броја $N$. ■

Шоров алгоритам се служи овом лемом као главном идејом за налажење нетривијалних делилаца. Следи основа по којој алгоритам тражи $x$

**Дефиниција 4.** *Најмањи од природних бројева $t$ за које важи:*

$$a^t \equiv_m 1$$

*назива се* ***поретком*** *броја $a$ по модулу $m$.*

**Теорема 7.** *Ако је $t$ поредак броја $a$ по модулу $m$ и $a^s \equiv 1 \pmod{m}$, тада $t|s$.*

*Доказ.* Ако $s$ није дељиво са $t$ и представимо га као $s = tq + r,\ 0 < r < t$, тада важи: $a^s = (a^t)^q a^r$, односно $a^r \equiv 1 \pmod{m}$, што је немогуће јер је $t$ најмањи број за који важи $a^t \equiv 1 \pmod{m}$ ■

Ово само значи да је број $t$ период понављања за број $a$ по модулу $m$, што значи да ће $^n \equiv a^{kt+n} \pmod{m}$, $O \leqslant n < t$.

Из ових тврђења следи да ће Шоров алгоритам за почетак насумично изабрати број $a$ ($a \in \mathbb{N}, 0 < a, N$),а затим ће тражити поредак броја $a$ по модулу $N$, који ћемо назвати $y$(подразумевамо да $y \neq 0$)

Када нађемо број $y$, и од броја $a^y$ одузмемо један, добићемо број чији је делилац број $N$ (својство 2), односно другачије написано:

$$a^y - 1 = mN,\ m \in \mathbb{N}$$

Специјално, ако је $y$ паран број, онда $x^y-1$ можемо записати као разлику квадрата природних бројева:

$$a^y - 1 = (a^{\frac{y}{2}} - 1)(a^{\frac{y}{2}} + 1)$$

Одакле следи:

$$(a^{\frac{y}{2}} - 1)(a^{\frac{y}{2}} + 1) = mN,\ m \in \mathbb{N}$$

За бројеве $(a^{\frac{y}{2}} \pm 1)$ имаћемо два исхода:

1. Један бројева је једнак $m_1$, који је чинилац броја $m$, а други је једнак $m_2N$, чији је чинилац $N$. У овом случају морамо почети из почетка, јер не можемо добити један од чинилаца $N$.

2. Један бројева је једнак $m_1q_1$, а други је једнак $m_2q_2$ $(m_1 \cdot m_2 = m)$, један ће делити број $q_1$, а други ће делити број $q_2$. У овом случају изабраћемо један од ових бројева, применити Еуклидов алгоритам за тражење НЗД од $N$ и изабраног броја и добити један од чинилаца броја $N$.

Први исход се, међутим, неће догодити, јер је $0 < \frac{y}{2} < y$, а знамо да је $y$ поредак броја $a$ по модулу $N$, што по дефиницији 4 значи да је он најмањи број после нуле за који важи $a^y \equiv 1 \pmod N$. Ово значи да смо на овакав начин добили да је $a^{\frac{y}{2}}$ нетривијално решење једначине $x^2 \equiv 1 (\mathrm{mod}\ N)$, односно да је тражено $x = a^{\frac{y}{2}}$, под условом да је $y$ парно. Зашто се овај процес сматра исплативим и ефикасним, показаће следеће две леме

**Лема 2.** *Ако је $p$ непаран прост број и $x,\ 0 < x < p$. Тада је вероватноћа да је поредак броја $x$ по модулу $p$ паран број већа од $\frac{1}{2}$.*

**Лема 3.** *Нека је $N$ непаран сложен број и нека је $x$ случајно изабран број ($0 < x < N$). Нека је $r$ поредак броја $x$ по модулу $N$. Тада са вероватноћом већом од $\frac{3}{8}$ ће $r$ бити парно и $x^{r/2} \not\equiv \pm 1$ по модулу $N$.*

Ове две леме су доказане у раду број 8 и показују нам да скоро увек са релативно малим бројем покушаја можемо ефикасно да нађемо нетривијални делилац броја $N$.

Поред већ помињаног специјалног случаја, постоји још један, а то је случај да је број $N$ приказан као неки степен непарног простог броја:

$$N = p^\alpha$$

У овом случају бисмо много пута безуспешно нашим методом тражили нетривијални корен, можда бисмо и успели, али не претерано ефикасно. Уместо тога ћемо користити ефикаснији и овом случају боље прилагођен опште познати алгоритам **бинарне претраге** и тражити $\sqrt[k]{N},\ 1 < k < \log_2 N$ (основа логаритма је 2 јер $N$ посматрамо у бинарном облику). Ако постоји такво $k$ из датог интервала, такво да је $\sqrt[k]{N} \in \mathbb{N}$ можемо одредити о ком непарном простом броју се ради. Овим процесом се може и решити случај када је $N$ степен неког сложеног броја. У том случају када бинарном претрагом нађемо тај број, нека се он зове $s$, већ

познатим алгоритмом ћемо наћи његове нетривијалне делиоце.

Вратимо се на почетак и на општи случај. Како ћемо факторисати број који је представљен као $N = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$? Ићи ћемо поступно, у следећем редоследу:

1. Проверава да ли је почетни број паран или не. Ако јесте, алгоритам враћа 2 и понавља процес све док се не добије непаран број

2. Проверава да ли је број специјални случај $N = p^{\alpha}$ путем горенаведеног алгоритма бинарне претраге. Ако је решење дате претраге прост број, завршава, а ако је решење сложен број на њему примењује корак 3

3. Ако се корак 2 испостави безуспешним, бира произвољан природан број $a$, $1 < a < N$ и помоћу Еуклидовог алгоритма проверава НЗД$(N, a)$. Ако се испостави да је НЗД$(N, a)$>1, као вредност враћа НЗД$(N, a)$, дели $N$ тим бројем и наставља процес рекурзивно за НЗД$(N, a)$ (од корака 2) и количник $N$ и НЗД$(N, a)$ (од корака 3)

4. Ако се деси да је НЗД$(N, a)$=1, тражимо корак броја $a$ по модулу $N$ који смо у тексту обележеавали са $y$

5. Проверава да ли је $y$ парно и да ли $a^y \not\equiv \pm 1 (\mathrm{mod}\ N)$. Ако оба услова важе, $a^{\frac{y}{2}}$ проглашава за $x$ и тражи НЗД$(N, x + 1)$ и НЗД$(N, x - 1)$. Једно од та два, ако не и оба, ће бити нетривијални делилац $N$. Као излаз враћа нетривијални делилац (или делиоце), њиме (или њима) делимо $N$ и наставља програм рекурзивно од корака 2 за делиоце и од корака 3 за нови количник

6. Ако се деси да бар један од два услова не важи, враћамо се на корак 3

Једино што нам преостаје је како ефективно да одредимо корак нашег насумично одабраног броја по модулу $N$. Ако се осврнемо на теорему број 7, приметићемо да је остатак степена неког броја $a$ по модулу неког другог броја $N$ заправо периодична функција, при чему је период те функције заправо поредак броја $a$ по модулу $N$. Срећом, постоји алгоритам за тражење периода функције и користи се квантном механиком. Како функционише овај алгоритам, сазнаћемо у следећем одељку.

## 3.3 Квантномеханичка основа Шоровог алгортима

Као што је већ наведено, конгруентност степена произвољног природног броја $a$ по модулу другог природног броја $N$ је периодична функција, односно може се написати као функција зависна од степена броја $a$:

$$f(x) = a^x \mod N$$

Период ове функције ће бити поредак броја по модулу $N$ (означавали смо га са $y$). За налажење нашег $y$ користићемо поменути алгоритам налажења периода функције, који ћемо детаљно описати. Међутим, пре описивања овог алгоритма морамо се упознати са **квантном Фуријеовом трансформацијом**, на коју се овај алгоритам ослања.

### 3.3.1 Квантна Фуријеова трансформација

Квантна Фуријеова трансформација се поприлично често користи у квантном рачунарству и веома је корисна за решавање нашег проблема. Базира се на класичном алгортиму брзе Фуријеове трансформације насталом да би се ефикасно извршило множење два полинома високог, али једнаког степена. Овај алгоритам ћемо објаснити и показати зашто је, уз мале измене, погодан за коришћење квантних алгоритама.
Почећемо од два полинома степена $d$:

$$A(x) = a_0 + a_1x + a_2x^2 + ... + a_dx^d$$

$$B(x) = b_0 + b_1x + b_2x^2 + ... + b_dx^d$$

Интуитивно нам је познато да ће полином настао производом ова два полинома (на даље ћемо га звати $C(x)$) бити степена $2d$. Класични метод множења два полинома захтева да се сваки члан полинома $A(x)$ помножи са сваким чланом полинома $B(x)$, што је споро и неефикасно. Алгоритам брзе Фуријеове трансформације овај проблем решава у четири корака, од којих су три од та четири кључна.

1. Бирање тачака
2. Евалуација, односно израчунавање вредности $A(x)$ и $B(x)$ у одабраним тачкама
3. Добијање вредности за $C(x)$ у одабраним тачкама. Вредност $C(x)$ у некој тачки као производ вредности $A(x)$ и $B(x)$ у тој истој тачки
4. Интерполација полинома помоћу које из вредности $C(x)$ у тачкама које смо иницијално одабрали одређује све коефицијенте $c_0, c_1, c_2, ..., c_{2d}$ новог полинома $C(x)$

Кораци 1,3 и 4 су нам кључни па ћемо сваки укратко објаснити.

**Корак 1: Бирање тачака** Алгоритам се служи чињеницом да се сваки полином степена $m$ може јединствено представити у својим вредностима у $n$ различитих тачака, при чему је $n \geqslant m + 1$. Пошто наш финални полином $C(x)$ треба да буде $2d$ степена, морамо да изаберемо барем $2d + 1$ различитих тачака. Што више тачака изаберемо грешка при каснијој интерполацији ће бити мања. Најбоље је да наш број одабраних тачака $n$ буде паран, да бисмо тачке могли да бирамо као $\frac{n}{2}$ парова позитивних и негативних бројева:

$$\pm x_0, \pm x_1, \pm x_2, ..., \pm x_{\frac{n}{2}-1}$$

Овако одабрани чланови ће нам доста олакшати евалуацију, што ћемо сада и показати

**Корак 2: Евалуација** Приликом оваквог одабира тачака, доћи ће до доста преклапања. Приметићемо да ће чланови са парним степенима бити потпуно исти, а члановима са непарним степенима ће се само мењати знак. Ово имплицира да бисмо могли наш почетни полином да разбијемо на два полинома, а како, показаћемо на једноставном примеру:

$$P(x) = 6x^5 + 5x^4 + 4x^3 + 3x^2 + 2x + 1$$

све чланове са парним степенима ћемо пребацити на леву страну, а све са непарним на десну страну. Непарним члановима извлачимо једно $x$:

$$P(x) = 5x^4 + 3x^2 + 1 + 6x^5 + 4x^3 + 2x = 5x^4 + 3x^2 + 1 + x(6x^4 + 4x^2 + 2)$$

Леви полином ћемо назвати $P_p(x^2)$, а десни у загради $P_n(x^2)$

$$P(x) = P_p(x^2) + xP_n(x^2)$$

Исти случај ћемо имати и у општем случају са $A(x)$, $A(x) = A_p(x^2) + xA_n(x^2)$. На овакав начин када будемо убацили пар бројева $\pm x_i,\ i \in \{\, 1, 2, ..., \frac{n}{2} - 1 \,\}$ добићемо следећа решења :

$$A(x_i) = A_p(x_i^2) + x_i A_n(x_i^2)$$

$$A(-x_i) = A_p(x_i^2) - x_i A_n(x_i^2)$$

Разлика је, као што се може приметити, само у знаку испред другог сабирка. Користећи се овим методом, ако знамо $A_p(x_i^2)$ и $A_n(x_i^2)$, знаћемо и $A(\pm x_i)$. Процес настављамо рекурзивно за $A_p(x^2)$ и $A_n(x^2)$. Одавде се лако увиђа да ако желимо да при сваком рекурзивном кораку хоћемо да групишемо бројеве у парове, иницијални број бројева $n$ мора бити облика: $2^k,\ k \in \mathbb{N}$. Међутим, ако желимо да на исти начин поделимо полиноме $A_p(x^2)$ и $A_n(x^2)$ као што смо учинили са $A(x)$, мораћемо да $\frac{n}{2}$ чланова $(x_0^2, x_1^2, x_2^2, ..., x_{\frac{n}{2}-1}^2)$ повежемо у $\pm$ парове, што можемо да учинимо само ако користимо комплексне бројеве(негативне вредности квадрата су могуће само код комплексних бројева). Међутим, поставља се питање како ћемо одабрати те комплексне бројеве? Ако посматрамо рекурзију од почетка до краја. На почетку ћемо имати само један полином и $n$ бројева које смо одабрали. На крају ћемо имати $n$ полинома насталих гранањем и само један број, постигнут константним спаривањем и квадрирањем бројева. Ради једноставности, нека је тај број једнак јединици (модул свих бројева је одатле 1). Одавде увиђамо да су сви почетни бројеви комплексни $n$-ти корени тог броја 1, односно записано у облику једначине:

$$x^n = 1$$

Наши иницијални бројеви, односно решења горње једначине (назваћемо их $\omega^l$), су заправо комплексни бројеви и у поларним координатама се приказују на следећи начин:

$$\omega^l = e^{i2\pi\frac{l}{n}},\ l \in \{\, 0, 1, 2, ..., n-1 \,\}$$

С обзиром да смо бирали да је $n$ облика $2^k$, за ове бројеве важе следећа својства:

- $\omega^{l+\frac{n}{2}} = -\omega^l$, односно постоје позитивни и негативни парови

$$e^{(i2\pi\frac{l+n/2}{n})} = e^{i2\pi\frac{l}{n}} e^{i2\pi\frac{n/2}{n}} = e^{i2\pi\frac{l}{n}} e^{i2\pi\frac{2^{k-1}}{2^k}} = e^{i2\pi\frac{l}{2^k}} e^{i2\pi\frac{1}{2}} = e^{i2\pi\frac{l}{n}} e^{i\pi} = -e^{i2\pi\frac{l}{n}}$$

- Квадрирањем се добијају решења једначине $x^{n/2} = 1$

$$e^{(i2\pi\frac{l}{n})2} = e^{i2\pi\frac{2l}{2^k}} = e^{i2\pi\frac{l}{2^{k-1}}} = e^{i2\pi\frac{l}{n/2}}$$

На овај начин смо успели да решимо питање евалуације. Следи објашњење интерполације

**Корак 3: Интерполација** Како смо успели да нађемо вредности $A(x)$ и $B(x)$ за све првобитно одабране тачке и за њих нашли вредности $C(x)$, ми смо практично решили задатак. Оно што је преостало је да извршимо интерполацију како бисмо открили коефицијенте полинома $C(x)$ $(c_0, c_1, c_2, ..., c_{2d})$. У суштини, да одаберемо други начин да прикажемо полином који смо већ добили. Практично, урадићемо само исту ствар инверзно, како тачно, показаћемо ускоро.
Вратимо се на почетак. Алгоритам брзе Фуријеове трансформације ради са полиномима, зашто смо се овиме бавили и како нам то помаже? Вратимо се назад на причу $n$-то димензионих векторски простора. Оба начина приказивања полинома степена $\leqslant n-1$ (преко коефицијената или вредности у одређеним тачкама) се могу приказати као $n$-то димензионих вектора. Из једног у други вектора можемо да пређемо деловањем матрица (евалуација и интерполација):

$$\begin{bmatrix} A(x_0) \\ A(x_1) \\ A(x_2) \\ \vdots \\ A(x_{n-1}) \end{bmatrix} = M_1 \cdot \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_{n-1} \end{bmatrix}, \quad \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_{n-1} \end{bmatrix} = M_2 \cdot \begin{bmatrix} A(x_0) \\ A(x_1) \\ A(x_2) \\ \vdots \\ A(x_{n-1}) \end{bmatrix}$$

Матрице $M_1$ и $M_2$ су **Вандермондове матрице**[2], које су уопштено овог облика:

$$\begin{bmatrix} 1 & x_0 & x_0^2 & \dots & x_0^n \\ 1 & x_1 & x_1^2 & \dots & x_1^n \\ 1 & x_2 & x_2^2 & \dots & x_2^n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_m & x_m^2 & \dots & x_m^n \end{bmatrix}$$

Лепа особина ових матрица која се може доказати јесте да ако су вредности $x_0, x_1, ..., x_m$ различите, што код нас јесте случај, онда је матрица инверзибилна.
Како ми на почетку евалуације радимо са решењима једначине $x^n = 1$, ако са тим вредностима желимо да направимо Вандермондову матрицу, добићемо матрицу $M_1$ димензија $n \times n$:

$$M_1 = \begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \omega & \omega^2 & \dots & \omega^{n-1} \\ 1 & \omega^2 & \omega^4 & \dots & \omega^{2(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{n-1} & \omega^{2(n-1)} & \dots & \omega^{(n-1)(n-1)} \end{bmatrix}$$

Сада ћемо показати да је ова матрица инверзибилна:

[2]Alexandre Vandermonde (1735-1796)-француски математичар

**Лема 4.** *Колоне матрице $M_1$ су нормалне свака са сваком*

*Доказ.* Множење две колоне $i$ и $j$ је представљено скаларним производом хермитског вектора једне колоне и вектора друге колоне.

$$j \cdot i = 1 + \omega^{i-j} + \omega^{2(i-j)} + \ldots + \omega^{n(i-j)}$$

Како је ово сума геометријског низа, можемо је написати другачије:

$$\frac{1-\omega^{n(i-j)}}{1-\omega^{i-j}} = \frac{1-(\omega^n)^{(i-j)}}{1-\omega^{i-j}} = \frac{1-1^{(i-j)}}{1-\omega^{i-j}} = 0$$

Овим доказујемо да су било које две колоне $i$ и $j$ међусобно ортогоналне. Специјалан случај је када $i = j$ када је скаларни производ $n$. ■

Ако је свака колона, односно сваки вектор ортогоналан са сваким другим вектором, односно формираће базис. Ако опет погледамо начине записа полинома, приметићемо да оба приказују исти полином на два начина. Интуитивно нам је јасно да ове матрице заправо мењају базис вектора. Ово ће нам бити битно када будемо повезивали причу са квантним рачунарима. Ако транспонујемо $M_1$ и све чланове матрице заменимо хермитским паровима ($\omega^\dagger = \omega^{-1}$) добићемо матрицу $M_1^\dagger$ и када је помножимо са $M_1$ добићемо јединичну матрицу помножену бројем $N$:

$$M_1 \cdot M_1^\dagger = M_1^\dagger \cdot M_1 = nI$$

Када поделимо $M_1^\dagger$ са $n$, добијамо инверз од $_1$, односно матрицу $M_2$ која је матрица интерполације.

Ако се вратимо на причу квантног рачунарства, приметићемо да су ове две матрице, уз мале измене, потенцијални оператори на стање од $n$ кубита. Разлика ће бити само у коефицијентима који ту морају бити због нормализације:

$$QFT_n = \frac{1}{\sqrt{n}} \begin{bmatrix} 1 & 1 & 1 & \ldots & 1 \\ 1 & \omega & \omega^2 & \ldots & \omega^{n-1} \\ 1 & \omega^2 & \omega^4 & \ldots & \omega^{2(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{n-1} & \omega^{2(n-1)} & \ldots & \omega^{(n-1)(n-1)} \end{bmatrix}$$

$$QFT_n^{-1} = \frac{1}{\sqrt{n}} \begin{bmatrix} 1 & 1 & 1 & \ldots & 1 \\ 1 & \omega^{-1} & \omega^{-2} & \ldots & \omega^{-(n-1)} \\ 1 & \omega^{-2} & \omega^{-4} & \ldots & \omega^{-2(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{-(n-1)} & \omega^{-2(n-1)} & \ldots & \omega^{-(n-1)(n-1)} \end{bmatrix}$$

На овај начин ћемо чак и учинити да је матрица унитарна, што нам још више одговара, јер су сва логичка кола квантног рачунара унитарна. Још једна велика предност је то што су

матрице иницијално креиране за множење полинома, што значи да су операције у оквиру матрице линеарне и самим тиме су валидне квантне операције.

Као што смо рекли, квантна Фуријеова трансформација је заправо промена базиса, односно произвољно стање $|x\rangle = \sum_{i=0}^{N-1} x_i |i\rangle$ ће мапирати у стање $\sum_{i=0}^{N-1} y_i |i\rangle$ на следећи начин:

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{\frac{i2\pi jk}{N}}, \quad j \in \{\, 0, 1, 2, ..., N-1 \,\}$$

На сличан начин дефинишемо и инверзну квантну Фуријеову трансформацију:

$$x_j = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} y_k e^{-\frac{i2\pi jk}{N}}, \quad k \in \{\, 0, 1, 2, ..., N-1 \,\}$$

У специјалном случају, ако је $|x\rangle$ једно од основних стања векторског простора, квантна Фуријеова трансформација се може записати и овако:

$$|x\rangle \longrightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{\frac{i2\pi xk}{N}} |k\rangle$$

Посматрајмо овај случај. Наш систем се састоји од $N$ основних вектора стања $(|0\rangle, |1\rangle, ..., |N-1\rangle)$ који могу представљати бројеве и пошто је $N = 2^n$, систем се може приказати преко $n$ кубита. Произвољно стање система $|x\rangle = |x_1 x_2 ... x_n\rangle$, где су $x_1 x_2 ... x_n$ стања сваког кубита понаособ, можемо представити као Кронекеров производ сваког од тих стања:

$$|x_1 x_2 ... x_n\rangle = |x_1\rangle \otimes |x_2\rangle \otimes ... \otimes |x_n\rangle$$

С тим на уму, расписаћемо запис трансформације:

$$|x\rangle \longrightarrow \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{\frac{i2\pi xk}{N}} |k\rangle =$$

$$= \frac{1}{\sqrt{2^n}} \sum_{k_1 \in \{\, 0,1 \,\}} \sum_{k_2 \in \{\, 0,1 \,\}} ... \sum_{k_n \in \{\, 0,1 \,\}} e^{i2\pi x \sum_{l=1}^{n} k_l 2^{-l}} |k_1 k_2 ... k_n\rangle =$$

$$= \frac{1}{\sqrt{2^n}} \sum_{k_1 \in \{\, 0,1 \,\}} \sum_{k_2 \in \{\, 0,1 \,\}} ... \sum_{k_n \in \{\, 0,1 \,\}} \bigotimes_{l=1}^{n} e^{i2\pi x k_l 2^{-l}} |k_l\rangle =$$

$$= \frac{1}{2^{\frac{n}{2}}} \bigotimes_{l=1}^{n} \sum_{k_n \in \{\, 0,1 \,\}} e^{i2\pi x k_l 2^{-l}} |k_l\rangle = \frac{1}{2^{\frac{n}{2}}} \bigotimes_{l=1}^{n} (|0\rangle + e^{i2\pi x 2^{-l}} |1\rangle)$$

Овај облик се може још мало боље приказати: како је број $x$ приказан у бинарном систему, да бисмо га представили у декадном систему применићемо формулу:

$$x = [x_1 x_2 ... x_n] = x_1 2^{n-1} + x_2 2^{n-1} + ... + x_n 2^0$$

када овај број помножимо са $2^{-l}$, крајњи резултат можемо да прикажемо као:

$$2^{-l}x = [2^{-l}\sum_{r=1}^{n} x_r 2^{n-r} = \sum_{r=1}^{n} x_r 2^{n-l-r} = \sum_{r=1}^{n} x_r 2^{n-l-r} + \sum_{r=n-l+1}^{n} x_r 2^{n-l-r} = s_1(l) + s_2(l)$$

сума $s_1(l)$ ће сигурно припадати скупу $\mathbb{N}$, док ће $s_2$ бити $x_{n-l+1}2^{-1} + x_{n-l+2}2^{-2} + ... + x_n 2^{-l}$ што се записује као $[0.x_{n-l+1}x_{n-l+2}...x_n]$. Ово осматрање ћемо вратити у израз за трансформацију $x$:

$$|x\rangle \longrightarrow \frac{1}{2^{\frac{n}{2}}}\bigotimes_{l=1}^{n}(|0\rangle + e^{i2\pi(s_1+[0.x_{n-l+1}x_{n-l+2}...x_n])}|1\rangle) =$$

$$= \frac{1}{2^{\frac{n}{2}}}\bigotimes_{l=1}^{n}(|0\rangle + e^{i2\pi s_1(l)}e^{i2\pi[0.x_{n-l+1}x_{n-l+2}...x_n 2^{-l}]}|1\rangle) =$$

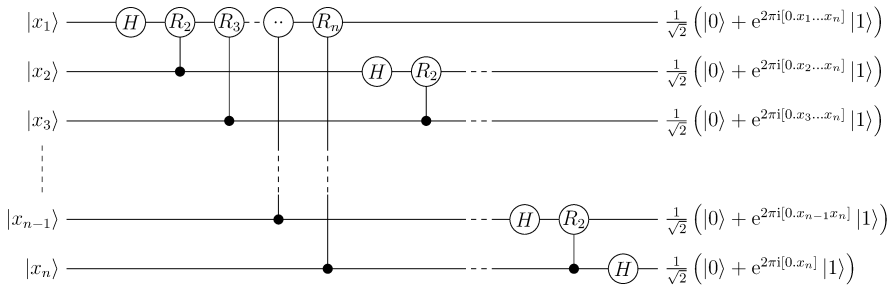
$$= \frac{1}{2^{\frac{n}{2}}}\bigotimes_{l=1}^{n}(|0\rangle + 1^{s_1(l)}e^{i2\pi[0.x_{n-l+1}x_{n-l+2}...x_n]}|1\rangle) =$$

$$= \frac{1}{2^{\frac{n}{2}}}\bigotimes_{l=1}^{n}(|0\rangle + e^{i2\pi[0.x_{n-l+1}x_{n-l+2}...x_n]}|1\rangle)$$

Односно од кубита $x_1$ до кубита $x_n$:

$$|x\rangle \longrightarrow \frac{1}{2^{\frac{n}{2}}}(|0\rangle + e^{i2\pi[0.x_1x_2...x_n]}|1\rangle) \otimes (|0\rangle + e^{i2\pi[0.x_2...x_n]}|1\rangle) \otimes ... \otimes (|0\rangle + e^{i2\pi[0.x_n]}|1\rangle)$$

Ово је финална репрезантација квантне Фуријеове трансформације на основно стање $x$ и доста нам говори о томе како ће изгледати логичко коло.
Коло квантне фуријеове трансформације се састоји само од две врсте капија: Адамарове капије и контролисане капије фазног помераја за $\frac{2\pi}{2^n}$. Адамарова капија ће кубит $|x\rangle = |1\rangle$ претворити у стање$(\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle))$ што одговара стању последњег кубита. Сви кубити ће проћи кроз једну Адамарову капију. Ово такође омогућава контролисаној капији да делује само на $|1\rangle$ компоненту кубита на који делује.




Слика 16: Приказ квантне Фуријеове трансформације над $n$ кубита

### 3.3.2 Алгоритам проналажења периода функције

Након што смо сазнали све што нам је потребно о квантној суперпозицији, можемо се посветити начину на који Шоров алгоритам тражи поредак насумично изабраног броја, решавајући проблем налажења периода функције.
Претпоставимо да фаза $\phi$ настаје дејством неког унитарног оператора $U$(његов сопствени вектор је $|u\rangle$, а његова сопствена вредност је $e^{i2\pi\phi}$). Ако применимо исти оператор још једном, почетну фазу ћемо квадрирати. Уз претпоставку да оператор можемо да применимо довољно пута, могли бисмо да конструишемо свих $n$ стања квантне Фуријеове трансофрмације. Пошто је квантна Фуријеова трансформација реверзибилна, ми можемо да сазнамо колика је та фаза $\phi$.
Да бисмо решили овај проблем, потребна су нам два регистра кубита, први који ће имати $q$ кубита и други који ће имати довољно кубита да представи стање $|u\rangle$. У првом регистру су на почетку сви кубити постављени да буду у стању $|0\rangle$, након чега ће сваки кубит проћи кроз Адамарову капију. Када прођу кроз Адамарову капију сваки од тих кубита ће бити контролни кубит за једну од контролисано $U^{2^p}, 0 \leqslant p \leqslant q-1$ капија које делују на други регистар. По дефиницији сопственог вектора капија неће уопште деловати на сопствени вектор $|u\rangle$, али ће зато деловати на $|1\rangle$ компоненту контролног кубита, померајући му фазу. Ово својство се лако доказује.

$$\frac{1}{\sqrt{2}}(|0\rangle|u\rangle + |1\rangle U^{2^q}|u\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle e^{i2\pi 2^q})|u\rangle$$

На крају овог процеса, стање првог регистра ће бити:

$$\frac{1}{\sqrt{2^q}}(|0\rangle + e^{i2\pi 2^{q-1}\phi}|1\rangle) \otimes (|0\rangle + e^{i2\pi 2^{q-2}\phi}|1\rangle) \otimes ... \otimes (|0\rangle + e^{i2\pi 2^0\phi}|1\rangle) =$$

$$= \frac{1}{\sqrt{2^q}} \sum_{k=0}^{2^q-1} e^{i1\pi k\phi}|k\rangle$$

Овај последњи израз подсећа на квантну Фуријеову трансформацију, па ако је применимо на први регистар и потом извршимо мерење над њим, добићемо нешто што је поприлично добра апроксимација фазе $\phi$.

$$\frac{1}{\sqrt{2^q}} \sum_{k=0}^{2^q-1} e^{i1\pi k\phi}|k\rangle \otimes |u\rangle = |\tilde{\phi_0}\rangle \otimes |u\rangle$$

Посматрајмо идеалан случај: фаза $\phi$ се може тачно приказати са $q$ кубита ($\phi = [0.\phi_1\phi_2...\phi_q]$). То значи да можемо да преформулишемо стање првог регистра регистра као:

$$\frac{1}{\sqrt{2^q}}(|0\rangle + e^{i2\pi[0.\phi_1]}|1\rangle) \otimes (|0\rangle + e^{i2\pi[0.\phi_1\phi_2]}|1\rangle) \otimes ... \otimes (|0\rangle + e^{i2\pi[0.\phi_1\phi_2...\phi_q]}|1\rangle)$$

Ово стање нам је познато: ово је стање које добијемо после примене квантне Фуријеове трансформације на вектор $|\phi_1\phi_2...\phi_q\rangle$, што значи да можемо измерити вредност $\phi$ потпуно тачно
Међутим, шта ће се десити када не гледамо овај случај? Испоставља се да и тада можемо

добити поприлично прецизну апроксимацију $\phi$ са великом вероватноћом. Ако желимо да прикажемо $\phi$ са прецизношћу од $n$ цифара и ако нам је тражена вероватноћа да погодимо фазу $1-\epsilon$, број кубита $q$ које први регистар мора имати је:

$$q = n + \lceil \log(\ 2 + \frac{2}{\epsilon}\ ) \rceil$$

Где $\lceil x \rceil$ представља најближи цео број броју $x$ који је већи или једнак њему. Ово тврђење је детално доказано у раду број 7.
Сад када знамо како функционише алгоритам налажења фазе, вратимо се на наш почетни проблем, налажење поретка насумично изабраног броја по модулу $N$. Посматраћемо следећи унитарни оператор:

$$U\left|y\right\rangle \equiv \left|xy \mod N\right\rangle$$

Подразумеваћемо да ако је $y > N$, овај оператор не чини ништа, односно да се оператор нетривијално понаша само кад је $0 \leqslant y \leqslant N-1$ Сада нам је потребно на нађемо сопствени вектор оператор $U$. Срећом, постоји их доста, један од њих је:

$$\left|u_s\right\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{\frac{-i2\pi sk}{r}} \left|x^k \mod N\right\rangle, \quad 0 \leqslant s \leqslant r-1$$

при чему је $r$ поредак који тражимо. Лако се доказује да је $\left|u_s\right\rangle$ сопствени вектор.

$$U\left|u_s\right\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} e^{\frac{-i2\pi sk}{r}} \left|x^{k+1} \mod N\right\rangle =$$

$$= e^{\frac{i2\pi s}{r}} \left|u_s\right\rangle$$

Одавде се види да је сопствена вредност оператора $e^{\frac{i2\pi s}{r}}$. Под претпоставком да смо узели довољан број кубита да можемо да прецизно одредимо $\frac{s}{r}$ са великом вероватноћом, на први регистар применимо инверзну квантну Фуријеову трансформацију и после тога га измеримо, добићемо број јако приближан $\frac{s}{r}$. Уз промену сопствених вектора $\left|u_s\right\rangle$, добијаћемо више вредности $\frac{s}{r}$ за различито $s$, након чега ћемо применити Еуклидов алгоритам и пронаћи $\frac{1}{r}$, чиме је проблем налажења поретка решен.

## 3.4 Ефикасност Шоровог алгоритма

Ефикасност било ког алгоритма се дефинише његовом **временском комплексношћу**, односно временом које је потребно да се изврши за велике бројеве. За одређивање временске комплексности користи се **нотација великог** $O$, која се посвећује броју битова које су потребне највећем регистру или подалгоритму самог алгоритима.
Пошто је квантним рачунарима за чување $N$ стања потребно $n = \log_2 N$ кубита, а очекивано време извршења алгоритма проналажења фазе је реда $O(n^3)$, очекивано време извршавања Шоровог алгоритма је $O((log_2 N)^3)$. Ово време се сврстава у полилогаритаско време и заиста

показује ефикасност Шоровог алгоритма у поређењу са другим алгоритмима за факторизацију бројева. Поређења ради, очекивано време извршавања најефикаснијег бинарног алгоритма за решавање факторизације бројева је реда $O(e^{1.9(\log N)^{1/3}(\log\log N)^{2/3}})$, што се сврстава у субекспоненцијално време извршавања. То значи да је време извршавање брже од експоненцијалног алгоритма, али ипак много спорије од полиномског логаритма, а неупоредиво спорије од полилогаритамског алгоритма као што је Шоров алгоритам.

# 4 Примене

Током овог рада смо се детаљно посветили описивању и објашњењу рада квантних рачунара и вероватно најпозантијег алгоритма насталог за њих, Шоровог алгоритма. Ипак, пред нама је остало много питања, понајвише оних која се тичу сврхе и примене самог алгоритма и наравно, сврхе и примене ових дивних машина. На крају ћемо одговорити на једно од тренутно најчешћих питања: "Зашто се квантни рачунари још увек не примењују?"

## 4.1 Примена Шоровог алгоритма

Када је настао 1994. године, Шоров алгоритам је за циљ имао да ефикасно реши проблем који је постојао још у Старој Грчкој, а није успео да се ефикасно реши ни помоћу бинарног рачунара: факторизацију бројева. Овај проблем је толико тежак за решавање да је на њему заснован цео један криптосистем који је још увек популаран: **RSA криптосистем**. Следи кратка прича о овом криптосистему и објашњењу зашто му Шоров алгоритам представља потенцијалну опасност.
**RSA (Ривест-Шамир-Едлман) криптосистем**[1] настао 1977. је систем који информацију криптује на принципу **јавног кључа**, доступног свима и **приватног кључа**, доступног само оном који жели приступити информацији. Особи која жели да приступи информацији мора да поседује оба кључа. У пар корака ћемо приказати како оба кључа настају.

1. Главни корак: изабрати два велика и приближно једнака проста броја $p$ и $q$.

2. Израчунати $n = pq$. Број $n$ ће бити један од делова јавног кључа

3. Израчунати Кармајклову функцију[2] од $n$ ($\lambda(n)$). У општем случају Кармајклова функција за број $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$ је дефинисана као

$$\lambda(n) = (\lambda(p_1^{\alpha_1})\lambda(p_2^{\alpha_2})..., \lambda(p_k^{\alpha_k}))$$

   где НЗС представља најмањи заједнички садржалац свих ових бројева. За степен простог броја $p^\alpha$ $\lambda(p^\alpha)$ једнако:

$$\lambda(p^\alpha) = p^{\alpha-1}(p-1)$$

   У нашем случају $\lambda(n)$ ће изгледати овако:

$$\lambda(n) = (p-1, q-1)$$

4. Изабрати природан број $(1 < e < n)$ такав да је НЗД$(e, n)$=1. Ово ће бити други део јавног кључа.

[1] Ron Rivest (1947-)-амерички криптограф
Adi Shamir (1952-)-израелски криптограф
Leonard Adleman (1945-)-амерички информатичар
[2] Robert Carmichael (1879-1967.)-амерички математичар

5. Одабрати природан број $d$ такав да је:

$$ed \equiv 1 \mod \lambda(n)$$

број $d$ се назива модуларни мултипликативни инверз.

Јавни кључ су бројеви $(e, n)$, док приватни кључ чине бројеви $(d, n)$.
Посмтрајмо како ово функционише у практичном случају: особа А хоће да пошаље особи Б неки број $m$, са намером да је нико други не прочита осим особе Б. Особа А ће енкриптовати $m$, користећи функцију $c(m)$:

$$c(m) = m^e \mod n$$

Затим ће $c, n$ и $e$ бити послати у јавност. Особа Б ће користити свој приватни кључ, прецизније $d$ да би декриптовала $c$ и добила $m$:

$$c(m) = c^d \mod n$$

Односно, ако се овај израз напише другачије:

$$(m^e)^d \equiv m \mod n$$

Ово својство се може доказати помоћу мале Фермаове теореме[3].

Главни проблем за бинарне рачунаре представља факторизација броја $n$ после чега ниједан од следећих корака није претерано проблематичан јер постоје алгоритми који их ефикасно решавају. Због величине бројева који се факторизују и чињенице да је временска комплексност најбржег бинарног алгоритма реда $O(e^{1.9(\log N)^{1/3}(\log\log N)^{2/3}})$ за природни број $N$, разбијање енкрипције је толико споро да је неисплативо. Исто се не може рећи за Шоров алгоритам, који са временском комплексношћу реда $O((\log N)^3)$ овај проблем решава много брже и ипак показује да ће ова енкрипција убрзо морати бити замењена.

Како је овај алгоритам успео да ефикасно реши проблем који је био дуго неисплатив или чак немогућ на бинарним рачунарима, убрзо је постало јасно да су квантни рачунари способнији уређаји од бинарних. О термину квантне надмоћи и потенцијалној примени квантних рачунара биће речи у следећем потпоглављу.

## 4.2 Појам квантне надмоћи и потенцијална примена квантних рачунара

Појам квантне надмоћи (енг. *quantum supremacy*) је први увео Џон Прескил[4] и представља тренутак када ће квантни рачунар успети да победи најбржи бинарни суперкомпјутер у решавању неког проблема, без обзира на то да ли је решавање тог проблема корисно на неки начин или не. Углавном се односи на рачунарску комплексност, али и на велико убрзавање класичних алгоритама које је на квантним рачунарима могуће. Један од алгоритама који

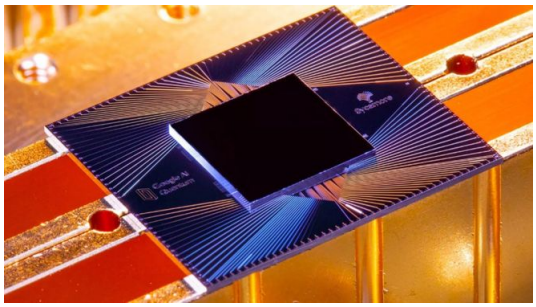
[3]Pierre de Fermat (1601-1665.)-француски математичар
[4]John Preskill(1953-)-амерички теорерски физичар

достижу велико убрзање уз помоћ квантних рачунара је Шоров алгоритам. Уз њега постоје још два начина помоћу којих је могуће показати квантну надмоћ, а то су: бозон семплинг (енг. *boson sampling*) и узроковање излазне дистрибуције насумичних квантних кола.

**Шоров алгоритам** је, као што смо показали, јако ефикасан алгоритам за факторизацију бројева, али и за разбијање RSA криптографије. Добра особина Шоровог алгоритма је да се може користити на бинарним рачунарима, али са доста споријом брзином, с тога је од почетка био један од првих кандидата за показивање квантне надмоћи. У прилог иде и чињеница да се тачност факторизације може показати ефикасно и на бинарном рачунару, јер све што је потребно је да помножимо факторе и проверимо да ли је добијени број онај број чију смо извршили факторизацију. Међутим, главни проблем Шоровог алгоритма су ресурси потребни за извршавање алгоритма за велике бројеве. Са повећањем броја, ресурси постају велики и експеримент је немогуће извести са садашњом технологијом. С тога су се научници фокусирали на преостала два начина показивања квантне надмоћи.

**Бозон семплинг** је рачунаска парадигма која се заснива на идентичним фотонима који су пропуштени кроз оптичку мрежу. Бозон семплинг може да реши одређене проблеме претраге и узимања узорака који се сматрају нерешивим за бинарне рачунаре. Временска комплексност најбољег класичног алгоритма за симулирање бозон семплинга је $O(n2^n + mn^2)$, где је $n$ број фотона, а $m$ број изалазних модова. Претпоставља се да је симулирање 50 фотона немогуће за било који суперрачунар, који тренутно постоји.

**Узроковање излазне дистрибуције насумичних квантних кола** , односно симулирање произвољног квантног кола је проблем којем са порастом кубита временска комплексност расте експоненцијално. Овај проблем је могуће решавати и на бинарним рачунарима јер је симулирање квантних рачунара могуће. Америчка компанија IBM је на свом рачунару успела да симулира квантни систем од 56 кубита и то је највећа симулација до сад. Пошто је овај проблем расте експоненцијално са бројем кубита, с тога ће у будућности број кубита који се могу симулирати бинарним рачунаром доћи до границе. Занимљива чињеница је да ако би постојао рачунар који би симулирао квантни систем од 260 кубита, он би имао већи број битова него што постоји атома у познатом универзуму, према томе то је немогуће.
Ипак, помоћу овог принципа је и показана квантна надмоћ. Компанија Гугл је 23. октобра 2019. објавила да је користећи квантни процесор *Sycamore* са високо квалитетних 54 суперпроводних кубита, од којих је један неактиван, успела да постигне квантну надмоћ. Овај процесор је успео да уради циљано израчунавање за 200 секунди, док би одређеном суперкомпјутеру потребно 10000 година. Ипак, компанија IBM у чијем је власништву тај суперкомпјутер је ово демантовала, тврдећи да је направила побољшан алгоритам који дато израчунавање може да изврши за два и по дана. Још увек је дуг пут до праве квантне надмоћи, али свакако је вредно чекати.



Слика 17: Гуглов Sycamore процесор

Занимљива је и потенцијална примена квантних рачунара. Пошто квантни рачунари немају универзалну архитектуру као што је фон Најманова архитектура код бинарних рачунара, варијације квантних рачунара су много веће. Ипак, постоје два правца у којима се развој квантних рачунара креће: **дигитални** и **аналогни**.

**Аналогни приступ** се углавном односи на примену квантних рачунара где су заиста неопходни и примеренији од бинарних рачунара. Односи се на симулацију квантних система, о чему је Фајнман и писао још давне 1982. године. Овакве симулације су готово немогуће на суперкомпјутерима и оваква имплементација би нам дала многе одговоре на питања из поља физике, али и хемије.

**Дигитални приступ** се углавном односи на примену квантних рачунара при решавању проблема који се њиховом применом могу драстично убрзати. Неке од главних оваквих примена су:

- Квантна криптографија-пошто смо показали да Шоров алгоритам може разбити веома популаран RSA криптосистем, а постоје и други квантни алгоритми који чистом силом могу да разбијају друге криптосистеме, све више ће се покретати питање сигурности података која би, са појавом довољно јаког квантног рачунара, била и те како нарушена. Срећом, постоје криптосистеми за које још увек не постоји алгоритам њиховог разбијања, међу њима има и квантних криптосистема који би потенцијално могли да имају користи од квантних рачунара. Већина тих криптосистема је засновано на законима квантне механике приликом генерисања приватних и јавних кључева, мада постоје и они који се заснивају на директној размени кубита између два рачунара који не верују један другом.

- Квантна претрага-прецизније квантна претрага база података уз помоћ Гроверовог[2] алгоритма. Његова временска комплексност је реда $O(\sqrt{N})$ за базу података од $N$ елемената, што је квадратно побољшање у односу на класичне алгоритме који су улавном реда $O(N)$. Како су базе података све присутније и све веће, ово убрзање је и више него повољно.

[2]Lov Grover(1961-)-индијско-амерички информатичар

- Решавање система линерних једначина-алгоритам познатији и као HHL-алгоритам је веома ефикасан алгоритам за решавање ове врсте проблема. Његова комплексност је реда $O((\log N)k^2)$, где $N$ представља број варијабли система, а $k$ представља број случајева у оквиру система у зависности од његових параметара. Овај алгоритам нуди експоненцијално убрзање у односу на најбржи класични алгоритам чија комплексност је реда $O(Nk)$.

Ово су само неке од могућих примена квантних рачунара, треба имати на уму да је ово још увек млада област подобна променама, с тога ће се у блиској будућности појавити још алгоритама и самим тим још могућих области где се квантни рачунари могу применти. О томе како ће та примена тећи и изгледати у реалном свету ћемо морати сачекати неко време.

## 4.3 Зашто квантни рачунари још увек нису у широј примени?

Квантни рачунари, иако на папиру доста супериорнији од бинарних рачунара, имају своје недостатке. Ови недостаци су и главни разлог зашто се квантни рачунари у некој широј примени. Наиме, тренутно највећи проблеми за квантно рачунарство су **декохеренција** и **нежељена бука** код система са више кубита.

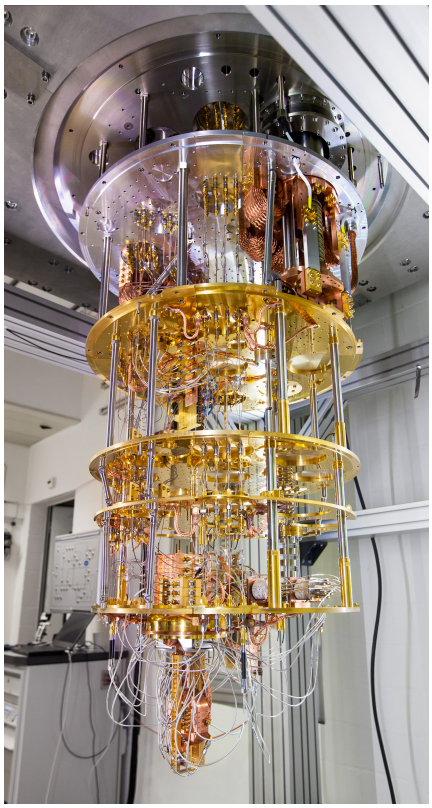
За систем се сматра да је квантно кохерентан ако постоји тачна фаза између његових стања и да не постоји интеракција тих стања са спољашњим светом. Ако овај услов није испуњен, систем је декохерентан. Међутим, декохеренција може настати на још начина, између осталог применом логичке капије на кубите. Декохеренција представља највећи проблем квантног рачунара, највише због медијума од којег се квантни рачунари праве. Испоставља се да се суперпроводници (углавном специјалне врсте керамике са примесама метала, највише бакра) одлично носе са декохеренцијом. Због тога су кубити, капије и кола већине квантних рачунара који тренутно постоје и направљени од овог медијума. Међутим, суперпроводници имају своје недостатке. Суперпроводници су, као што је речено, специјалне врсте керамике које су скупе за производњу и тешке за израду. Поред тога, јако су крте и тешко је од њих направити флексибилну жицу, нешто што нам је потребно при састављању рачунара. Због овога се појављују примесе метала. Још већи проблем су услови у којима квантни рачунари раде. Да не би дошло до интеракције са спољашњим светом, квантни рачунари раде у потпуном вакууму на температури приближној апсолутној нули, што су услови који се могу рекреирати само у посебним лабораторијама и додатно дижу зависност од околних уређаја и самим тим цену целог система.

Још један проблем са којим се квантни рачунарство сусреће је нежељена бука изазвана интеракцијом између самих кубита. Оваква бука може да изазове грешке у калкулацијама које досежу до бројке од чак три посто, што свакако није прихватљиво. Квантни рачунари могу да извршавају квантни алгоритам за исправљање грешака и на тај начин симулирају рачунар код којег је бука занемарљива, са повећањем броја кубита није познато како ће се цео систем понашати са овим алгоритмом.

Иако квантни рачунари тренутно постоје и постоје компаније од којих је могуће купити квантни рачунар, њихов тренутни однос цене и могућности је неисплатив за већину лабораторија. Да би дошло до неке веће експанзије ових машина, наука и технологија морају још доста да изнапредују.

# 5 Закључак

Кроз овај рад смо се упознали са квантним рачунарима, њиховом основном принципу рада, предностима и недостацима. Упознали смо се и са функционисањем рада вероватно најпознатијег алгоритма који могу да извршавају, Шоровим алгоритмом и схватили да квантни рачунари могу бити надмоћније машине од самих бинарних рачунара. Приказали смо и на који начин квантни рачунари могу показати да су бољи, као и које су могуће примене ових дивних машина. Мени лично је фасцинантно како је у релативно кратком периоду од 39 година када је настао Фајнманов рад "*Simulating physics with computers*" до данас постигнуто. Бинарни рачунари какве их данас познајемо постоје скоро 70 година (са одређеним изменама) и у њих су кроз године инвестирани билиони долара и без обзира на то појавиле су се машине у које је утрошено доста мање времена и новца, а које се могу показати као боља алтернатива. Иако већина тренутних квантних рачунара нема више од 50 кубита[1], иако је највећи број факторизован Шоровим алгоритмом само 12, треба имати на уму да је квантно рачунарство нова област и да се на овоме сигурно неће стати. О томе како ће квантни рачунари утицати на свет у којем живимо, само ће време рећи.



Слика 18: Квантни рачунар са суперпроводним кубитима који је произвела компанија IBM у лабораторији у Цириху

[1] тренутни рекорд у време писања овог рада за број кубита је 72, а у току године компанија D-wave планира да направи рачунар са 5000 кубита и пусти га у продају

Квантни рачунари су област науке која је изазвала моје велико интересовање још од када сам први пут читао о њима пре отприлике седам година. Иако тада нисам имао довољно знање из физике и математике да би их довољно разумео, кроз проучавање и израду овог рада сам стекао знања која су још више продубила моје интересовање ка овим величанственим машинама.

Овом приликом бих желео и да се захвалим свом ментору Игору Салому на помоћи при изради овог рада, али и знању стеченом на часовима менторске наставе, коју сам похађао уз његову дозволу. Желео бих да се захвалим и својим професорима математичких предмета Јелени Николић и Милици Мисојчић, али и професорки физике Катарини Матић за стечена знања из ових поља, али и за мотивацију која ме је водила ка успесима током четири године похађања ове гимназије. Без њих израда овог рада не би била могућа.

# Литература


1. Н.Чалуковић, ***Физика за 4. разред гимназије***, Круг 2014.
2. З.Каделбург, В.Мићић, Ц.Огњановић, ***Анализа са алгебром 2***, Круг 2017.
3. Н.Чалуковић, ***Физика за 4. разред гимназије***, Круг 2014.
4. Н.Лазаревић, Н. Ћирић, М. Ђорић, М. Вељковић, ***Линеарна алгебра и аналитичка геометрија***, Клуб НТ 1995.
5. Н.Алимпић, ***Рачунарство и информатика за 3. разред Математичке гимназије***
6. S. Dasgupta, C. H. Papadimitriou, U. V. Vazirani, ***Algorithms***, 2006.
7. M. Nielsen, I. Chuang, ***Quantum Computation and Quantum Information (10th Anniversary Ed.)***, Cambridge University Press, 2011.
8. U.Vazirani, ***Lecture 9: Shor's algorithm***, 2004, https://people.eecs.berkeley.edu/ vazirani/f04quantum/notes/lec9.pdf Приступљено у мају 2020.
9. R. L. Jaffe, ***Physics 8.05:SUPPLEMENTARY NOTES ON DIRAC NOTATION, QUANTUM STATES, ETC.*** 1996. http://web.mit.edu/8.05/handouts/jaffe1.pdf Приступљено у мају 2020.
10. Wikimedia фондација, ***Википедија, слободна енциклопедија***, www.wikipedia.org Приступљено у мају 2020.
11. Л. Галић, ***Квантни алгоритми***, 2019.