

# МАТЕМАТИЧКА ГИМНАЗИЈА

МАТУРСКИ РАД  
ИЗ ФИЗИКЕ

## Квантна телепортација

Ученик  
Лазар БРАЈОВИЋ, IVд

Ментор  
др Александра ГОЧАНИН

Београд, 25. мај 2023.



# Садржај

<b>1</b>	<b>Увод</b>	<b>1</b>
<b>2</b>	<b>Квантни битови - кубити</b>	<b>5</b>
2.1	Основна својства кубита . . . . .	5
2.2	Блохова сфера . . . . .	6
2.3	Вишеструки кубити . . . . .	8
2.4	Квантна замршеност . . . . .	9
<b>3</b>	<b>Квантне логичке капије</b>	<b>10</b>
3.1	Логичке капије са једним кубитом . . . . .	10
3.2	Логичке капије са више кубита . . . . .	12
3.2.1	Белова стања . . . . .	13
3.3	Идентитети са логичким капијама . . . . .	14
<b>4</b>	<b>Qiskit</b>	<b>17</b>
4.1	Увод у Qiskit . . . . .	17
4.2	Представљање кубита . . . . .	17
4.3	Представљање квантних логичких капија . . . . .	20
<b>5</b>	<b>Квантна телепортација</b>	<b>22</b>
5.1	Протокол квантне телепортације . . . . .	22
5.2	Теорија . . . . .	25
5.3	Симулација квантне телепортације . . . . .	26
5.4	Примена . . . . .	29
<b>6</b>	<b>Закључак</b>	<b>32</b>
	<b>Белешке</b>	<b>32</b>
	<b>Литература</b>	<b>35</b>



# 1

## Увод

Квантна информатика проучава обраду и пренос података уз помоћ квантно механичких система. Попут других једноставних, али добро осмишљених идеја, требало је доста времена пре него што је неко покушао да обрађује податке на овај начин. Да бисмо разумели зашто, потребно је да се вратимо у прошлост и видимо које су то све области допринеле основним идејама квантне информатике – квантна механика, теорија информације, рачунарске науке, криптографија.

Прича креће почетком 20. века, када се спремаола револуција у свету науке. Теорија физике у то време (сада проглашена *класичном физиком*), је предвиђала апсурдне ствари, попут постојања ултраљубичасте катастрофе (проблем са бесконачним енергијама) или спиралног кретања електрона ка језгру атома. Криза је завршена 20 година касније и као резултат је настала модерна теорија квантне механике. И од тада, она је саставни део науке, примењујемо је када говоримо о структури атома, нуклеарној фузији, суперпроводницима, структури ДНК, па чак и основним честицама природе.

Али, шта је тачно квантна механика? Квантна механика је математички оквир или скуп правила за конструкцију физичке теорије. На пример, квантна електродинамика, која невероватно прецизно описује интеракцију атома и светлости, проистекла је из оквира квантне механике, али садржи посебна правила, неодређена квантном механиком. Правила квантне механике су веома једноставна, али их и највећи експерти сматрају неинтуитивним. Сама квантна информатика произилази баш из жеље да физичари боље разумеју квантну механику. Дакле сам циљ квантне информатике јесте да направи технологију која ће изоштрити нашу интуицију и перцепцију квантне механике.

На пример, почетком 1980-их, порасло је интересовање о томе да ли можемо квантним ефектима да направимо сигнал бржи од светлости - што се сматрало великим не, по *Ајнштајновој<sup>1</sup> теорији релативности*. Проблем је сведен на питање, да ли се може клонирати непознато квантно стање. Али, клони-

рање које са класичном информацијом можемо лако постићи, није могуће у квантној механици. То је постало познато као *no-cloning theorem*<sup>2</sup>, и допринело је многобројним резултатима у квантној информатици. Због тога сада имамо увид у концепте који нам помажу да разумемо како би такви уређаји за кломирање радили. А такве концепте, користимо у даљем разумевању квантне механике.

Хајде сада да се окренемо ка још једном интелектуалном тријумфу 20. века - рачунарској науци. Основе произилазе још из давне историје (око 1750. године пре нове ере), када су у Вавилону користили глинене таблице за прве алгоритаме. Модерне основе је поставио чувени математичар Alan Turing<sup>3</sup>, у свом раду из 1936. Он је први изнео идеју о рачунару који можемо да програмирамо, моделу за израчунавање, сада познатом као *Тјурингова машина*<sup>4</sup>. Тјуринг је показао да постоји *Универзална Тјурингова машина*<sup>5</sup>, која може да симулира сваку другу. Шта више, тврдио је да за сваки алгоритам који врши неки хардвер (на пример, модеран рачунар), постоји еквивалентан алгоритам, који може да се изврши на Универзалној машини. Ово је постало познато као *Church-Turing thesis*<sup>6</sup>. И баш ова теза је темељ за развој рачунарске науке.

Недуго после Тјуринговог рада је направљен први компјутер са електричним компонентама. John von Neumann<sup>7</sup> је смислио једноставан теоријски модел за састављање компоненти неопходних за Универзалну Тјурингову машину. Даљи развој хардвера је омогућен конструкцијом првих транзистора 1947. године. Напредак је био толико невероватан, да је 1965. Gordon Moore<sup>8</sup>, поставио *Муров закон*, који каже да ће се снага компјутера дуплирати за исту цену, сваке две године.

Шта ће се десити када Муров закон не буде важио? Једно од решења пружа квантно израчунавање, које се заснива на коришћењу квантне механике за израчунавања, уместо класичне физике. Квантни компјутери пружају неопходну предност у брзини, у односу на класичне рачунаре. Ово је омогућило и ефикасно време решавања проблема. Ефикасни алгоритми су они који решавају проблем у полиномијалном времену (неефикасни би решавали у експоненцијалном). Овиме долазимо до јаче верзије Чурч-Тјурингове тезе: *Сваки алгоритамски процес се може ефикасно симулисати са вероватношћом Тјуринговом машином.*

1985. године David Deutsch<sup>9</sup> покушава да направи уређај који може ефикасно да симулира произвољан физички систем. Пошто су закони физике, квантно механички, Дајч је морао да разматра само уређаје чији се принципи заснивају на квантној механици. Такви уређаји, који су квантно аналогни Тјуринговој машини, су допринели до данашње концепције квантног компјутера.

Окренимо се сада ка теорији информације. Отприлике у исто време (1940-их), када се рачунарска наука брзо развијала, дошло је и до револуције у нашем схватању комуникације.

1948. Claude Shannon<sup>10</sup> је објавио невероватан рад, којем износи основе модерне теорије информације и комуникације. Вероватно кључан корак у Шеноновом раду је математичко дефинисање концепта информације. Рад се заснива на два кључна питања у вези са преносом информације преко комуникационог канала. Прво, шта су ресурси који су потребни да пошаљемо информацију? На пример, телефонске компаније морају да знају колико информације могу да пренесу преко одговарајућег кабла. Друго, да ли информација може да се пренесе тако да је заштићена од шума у комуникационом каналу?

На ова питања Шенон одговара доказивањем две основне теореме у теорији информације. Прва је позната као *noiseless channel coding theorem* и квантификује физичке ресурсе неопходне за складиштење информације из информационог извора. Друга је позната као *noisy channel coding theorem* и квантификује колико поуздане информације можемо пренети кроз комуникациони канал. Такође да бисмо постигли поуздан пренос, Шенон показује да постоје кодови који служе за ту заштиту, познати као *error-correcting* кодови. Друга теорема даје и горњу границу коју можемо постићи коришћењем ових кодова, али нажалост не и то како се постиже. До данас су научници развили доста класа таквих кодова, који су бољи него у Шеноновом раду, али ниједан није постигао ту границу.

Квантна теорија информације се слично развијала. 1995. Benjamin Schumacher<sup>11</sup> је смислио теорему аналогну са *noiseless channel coding theorem*, а у процесу је дефинисао и *квантни бит*, односно *кубити*, као физички ресурс. Насупрот овој, у квантној информатици и даље нема теореме аналогне са *noisy channel coding theorem*. Али ипак су смишљени квантни *error-correcting* кодови, који омогућавају комуникацију преко квантног канала.

А шта са преносом класичне информације преко квантног канала? Неколико изненађења се појавило у овој области. Најпознатије је када су 1992. Charles Bennett<sup>12</sup> и Stephen Wiesner<sup>13</sup> објаснили како се два бита информације могу пренети помоћу једног кубита, а као резултат је проистекао *superdense coding*<sup>14</sup>.

Још занимљивији су резултати у умреженом квантном израчунавању. Замислимо два умрежена компјутера, која решавају неки проблем. Колико комуникације између њих је потребно да би решили проблем? Недавно је показано да квантни компјутери захтевају експоненцијално мање комуникације од класичних компјутера да би решили одређене проблеме. Један од већих задатака за будућност квантне информатике је баш проналазак проблема у стварном свету, које можемо лакше решити умреженим квантним израчунавањем.

Споменимо још и стару уметност и науку познату као криптографија. Опште речено криптографија је проблем вршења комуникације или израчунавања које укључује две или више страна, које можда не верују једна другој.

Најпознатији криптографски проблем је пренос тајне поруке. Претпоставимо да двоје људи хоће тајно да комуницирају. Ово постижемо криптографским протоколом, који се разликује у зависности од система. Најбитније је направити разлику између криптосистема са приватним и јавним кључем.

Начин на који криптосистем са приватним кључем функционише јесте да две особе које комуницирају имају заједнички приватан кључ. Помоћу њега једна особа шифрује поруку, а да би је друга особа дешифровала, мора да зна приватан кључ. Али долазимо до питања како се расподељују приватни кључеви? Можда неко трећи прислушкује разговор о расподели кључева и пресреће један и користи га за даље дешифровање.

Једно од првих открића у квантној информатици је да квантна механика може да се искористи за расподелу приватних кључева. Ова процедура је позната као *квантна криптографија*. Основна идеја је квантно механички принцип да посматрање нарушава стање система. Односно, ако постоји неко трећи ко прислушкује, појавиће се сметња у комуникационом каналу који прве две особе користе за расподелу кључева. Затим они могу само да почну испочетка. Прве квантне криптографске идеје је предложио Стивен Визнер касних 1960-их, али нису биле прихваћене. 1984. Чарлс Бенет и Gilles Brassard<sup>15</sup>, надограђују Визнеров рад и предлажу овај квантно механички протокол за расподелу кључева.

Начин на који криптосистеми са јавним кључем раде је следећи. Једна особа *објави* јавни кључ, који сада сви могу да користе за шифровање порука. Неко други шифрује поруку и пошаље је првој особи. Зашто нико други не може да прочита поруку? Порука је шифрована на одређен начин тако да је веома тешко (не и немогуће) да се дешифрује само уз помоћ јавног кључа. Прва особа има и посебан тајни кључ, са којим лако дешифрује поруку. Расподела кључева је решена тиме што никоје две особе не морају да деле тајни кључ.

Средином 1970-их су овакав криптосистем предложили Whitfield Diffie<sup>16</sup>, Martin Hellman<sup>17</sup> и Ralph Merkle<sup>18</sup>. Нешто касније Ronald Rivest<sup>19</sup>, Adi Shamir<sup>20</sup> и Leonard Adleman<sup>21</sup> су развили RSA криптосистем - најпознатији криптосистем са јавним кључем. Сигурност код ових криптосистема је тежина у дешифровању уз помоћ само јавног кључа. Испоставља се да је дешифровање RSA тешко и за најјаче класичне компјутере, док Шоров алгоритам на квантном компјутеру лако може да дешифрује RSA. Слично, и други криптосистеми са јавним кључем се могу лако дешифровати на квантном компјутеру, ако би нам били познати одговарајући алгоритми. Ова практична примена квантних компјутера у разбијању криптографских шифри је проузроковала доста интересовања у области квантне информатике.



## 2

# Квантни битови - кубити

## 2.1 Основна својства кубита

Бит је, у класичној теорији, основна јединица информације. Може да узима две вредности - 0 или 1, које су јединствено одређене, и помоћу њих можемо да представимо било коју информацију. Можемо да их меримо и читамо без утицаја на остатак система. Слично, у квантној теорији информације, основна јединица мере је квантни бит - кубит. За разлику од битова, кубити могу да представљају и системе који се могу наћи у стањима 0 или 1, али и у њиховој суперпозицији. Један од начина да прикажемо ово је користећи Диракову<sup>22</sup> нотацију. Стања 0 и 1 су представљена кет векторима, који су математички вектори колоне:  $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$  и  $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ . Пошто су ова два стања из ортонормираног базиса, помоћу њих можемо представити било који дводимензиони (2D) вектор. Дакле, уводимо кубит, математички, као линеарну комбинацију ових стања:

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

Овде су  $\alpha$  и  $\beta$  амплитуде кет вектора, које су неки комплексни бројеви сразмерни вероватноћи да се кубит нађе у одговарајућем стању. Мерењем кубита не можемо добити информације о тим бројевима, али можемо добити коначно стање  $|0\rangle$  или  $|1\rangle$ . Вероватноћа да ћемо добити стање  $|0\rangle$  је  $|\alpha|^2$ , а да ћемо добити стање  $|1\rangle$  је  $|\beta|^2$ . Закључујемо да онда мора да важи  $|\alpha|^2 + |\beta|^2 = 1$ . Након мерења кубита, он се више не налази у суперпозицији стања, већ мора да буде или у стању  $|0\rangle$  или у стању  $|1\rangle$ .

Насупрот кет векторима, имамо и бра векторе, који су математички вектори врсте:  $\langle 0| = (1 \ 0)$  и  $\langle 1| = (0 \ 1)$ . Односно у општем случају:

$$\langle \phi| = \alpha^* \langle 0| + \beta^* \langle 1| = (\alpha^* \ \beta^*).$$

Где су  $\alpha^*$  и  $\beta^*$  комплексни коњугати амплитудама кет вектора. Можемо да уведемо и скаларни производ кубита, “бракет”, као:

$$\langle \psi | \phi \rangle = (\alpha^* \quad \beta^*) \begin{pmatrix} \gamma \\ \delta \end{pmatrix} = \alpha^* \gamma + \beta^* \delta.$$

Приметимо да онда важи да је производ нормалних стања 0, а једнаких 1. На овај начин можемо мерити вероватноћу да се кубит  $|\psi\rangle$  нађе у стању  $|0\rangle$ , као  $|\langle \psi | 0 \rangle|^2$ . Такође можемо увести и оператор, “кетбра”, као матрицу:

$$|\psi\rangle \langle \phi| = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} (\gamma^* \quad \delta^*) = \begin{pmatrix} \alpha\gamma^* & \alpha\delta^* \\ \beta\gamma^* & \beta\delta^* \end{pmatrix}.$$

Као што је већ споменуто стања  $|0\rangle$  и  $|1\rangle$  чине ортонормирани базис, али можемо бирати и друге базе, при чему резултат мерења увек зависи од изабране базе. Један такав је базис који чине стања  $|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$  и  $|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$ . Такође, још једна разлика у односу на битове јесте да при читању једног кубита можемо да утичемо на остале кубите у систему, а не можемо га копирати, што ће се показати врло битним. Ово је још познато као *no-cloning theorem*.

## 2.2 Блохова сфера

Показали смо да сваки кубит можемо представити као:

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

Покажимо сада да сваки кубит можемо представити и у облику:

$$|\psi\rangle = e^{i\delta} \left( \cos \frac{\theta}{2} |0\rangle + e^{i\phi} \sin \frac{\theta}{2} |1\rangle \right),$$

при чему је  $\delta$  глобална фазна разлика, која се не представља на Блоховој<sup>23</sup> сфери јер физички није опсервабилна, односно не може се измерити и не утиче на вероватноће тј. резултате мерења.

Знамо да су  $\alpha$  и  $\beta$  комплексни бројеви, па их у поларним координатама представљамо као  $\alpha = r_1 e^{i\phi_1}$  и  $\beta = r_2 e^{i\phi_2}$ . Након извлачења заједничке фазе  $\delta = \phi_1$ , добијамо  $|\psi\rangle = e^{i\delta} (r_1 |0\rangle + r_2 e^{i(\phi_2 - \phi_1)} |1\rangle)$ . Приметимо да  $r_2 e^{i(\phi_2 - \phi_1)}$  можемо представити као  $a + ib$ , где су  $a, b$  реални бројеви. Затим знамо да је  $|e^{i\delta}|^2 (|r_1|^2 + |a + bi|^2) = 1$ , односно  $|r_1|^2 + |a|^2 + |b|^2 = 1$ .

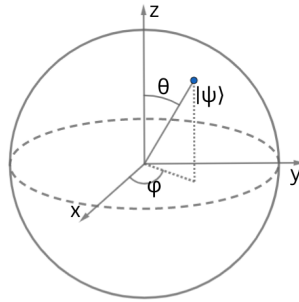
Дакле сваком стању  $|\psi\rangle$  можемо придружити тачку на сфери, користећи

сферне координате:

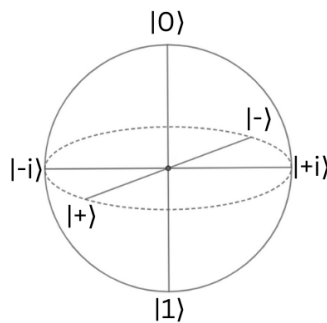
$$\begin{aligned}x &= a = \sin \frac{\theta}{2} \cos \phi, \\y &= b = \sin \frac{\theta}{2} \sin \phi, \\z &= r_1 = \cos \frac{\theta}{2}.\end{aligned}$$

При чему за  $\theta = 0^\circ$  добијамо стање  $|0\rangle$ , а за  $\theta = 180^\circ$  добијамо стање  $|1\rangle$ .

Закључујемо да сваки кубит  $|\psi\rangle = e^{i\delta}(\cos \frac{\theta}{2} |0\rangle + e^{i\phi} \sin \frac{\theta}{2} |1\rangle)$  можемо представити на јединичној Блоховој сфери, при чему стањима  $|0\rangle$  и  $|1\rangle$  одговарају северни и јужни пол сфере. Приметимо да су ова стања ортогонална, а на сфери им одговарају дијаметрално супротне тачке. Исто ће важити и за било која два ортогонална стања.



**Слика 2.1.** Представљање кубита  $|\psi\rangle$  на Блоховој сфери, у зависности од углова  $\theta$  и  $\varphi$



**Слика 2.2.** Карактеристични кубити на Блоховој сфери:  $|0\rangle$ ,  $|1\rangle$ ,  $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ ,  $|-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$ ,  $|+i\rangle = \frac{|0\rangle+i|1\rangle}{\sqrt{2}}$ ,  $|-i\rangle = \frac{|0\rangle-i|1\rangle}{\sqrt{2}}$

### 2.3 Вишеструки кубити

Видели смо да кубит након мерења може да буде у два стања, и да сваки кубит има две комплексне амплитуде. Слично, када посматрамо два кубита, резултат њиховог мерења могу бити стања  $|00\rangle$ ,  $|01\rangle$ ,  $|10\rangle$  и  $|11\rangle$ .

Дакле, систем се пре мерења налази у њиховој суперпозицији:

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

Као и до сада, правило мерења је исто, односно вероватноћа да добијемо одговарајуће стање једнака је квадрату одговарајуће амплитуде. Самим тим важи:  $|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$ . На исти начин приказујемо и системе сачињене од произвољног броја појединачних кубита.

Приметимо да сем мерења свих кубита система, можемо мерити појединачне подскупове. На пример ако имамо систем од три кубита и стање  $|\psi\rangle = \alpha_{000}|000\rangle + \alpha_{001}|001\rangle + \alpha_{010}|010\rangle + \alpha_{011}|011\rangle + \alpha_{100}|100\rangle + \alpha_{101}|101\rangle + \alpha_{110}|110\rangle + \alpha_{111}|111\rangle$ , и меримо само први кубит, добијамо стање  $|0\rangle$  са вероватноћом  $|\alpha_{000}|^2 + |\alpha_{001}|^2 + |\alpha_{010}|^2 + |\alpha_{011}|^2$ . Након мерења долазимо у стање:

$$|\psi\rangle = \frac{\alpha_{000}|000\rangle + \alpha_{001}|001\rangle + \alpha_{010}|010\rangle + \alpha_{011}|011\rangle}{\sqrt{|\alpha_{000}|^2 + |\alpha_{001}|^2 + |\alpha_{010}|^2 + |\alpha_{011}|^2}}.$$

Такође, ако посматрамо два раздвојена кубита  $|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$  и  $|\phi\rangle = \begin{pmatrix} \gamma \\ \delta \end{pmatrix}$ , њихово продукт стање можемо да добијемо ако применимо Декартов производ:

$$|\phi\psi\rangle = |\phi\rangle \otimes |\psi\rangle = \begin{pmatrix} \gamma \\ \delta \end{pmatrix} \otimes \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \gamma\alpha \\ \gamma\beta \\ \delta\alpha \\ \delta\beta \end{pmatrix} = \gamma\alpha|00\rangle + \gamma\beta|01\rangle + \delta\alpha|10\rangle + \delta\beta|11\rangle.$$

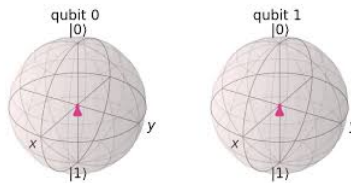
Аналогно, користећи Декартов производ, представљамо продукт стање било ког броја кубита. Приметимо да за  $n$  кубита морамо да пратимо  $2^n$  амплитуда. Ово је разлог зашто су квантни системи са великим бројем кубита тешки за симулацију. Модеран компјутер би могао да симулира квантно стање са око 20 кубита, али симулација са, на пример, 100 кубита је тешка и за најбоље суперкомпјутере.

## 2.4 Квантна замршеност

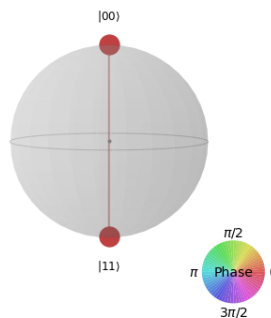
Уведимо сада *квантна замршена стања*<sup>24</sup>, као стања која не могу бити представљена као продукт стања кубита који чине то квантно замршено стање. Дакле, не можемо их посматрати као засебне кубите, већ као једну нераздвојну целину. Оваква стања могу да настану кроз доста различитих интеракција, али исто тако замршеност може да се прекине кроз неки вид интеракције са околином, на пример, извршавањем мерења. Односно, иако су кубити у суперпозицији, мерење једног кубита нарушава ту суперпозицију и даје нам информације о осталим.

Чак иако би честице биле удаљене светлосним годинама, мерење једне би нарушило суперпозицију и имало тренутан утицај на другу. Ово је познато као *spooky action at a distance*<sup>25</sup>, и продрмало је цео свет физике током 20. века.

Такође, важно је истаћи да је резултат мерења насумичан, као и да операције над кубитима не утичу на саме статистике мерења. Баш због овога не постоји начин да се оваква стања искористе за комуникацију. Одатле и назив *no - communication theorem*<sup>26</sup>.



**Слика 2.3.** Пошто квантна замршена стања нису продукт стања, не можемо их представити са тачкама на Блоховој сфери



**Слика 2.4.** Један од начина за приказ квантних замршених стања је Q - сфера, на којој су амплитуде представљене куглицама на њеној поврчини, где је полупречник куглице пропорционалан величини амплитуде, а боја одговара фази амплитуде

# 3

## Квантне логичке капије

Квантни рачунари се састоје од квантних кола, која се састоје од квантних логичких капија. Улога ових капија је манипулисање информацијом, тако што се над једним или више улазних кубита врши одређена операција, и они се преводе у ново стање. Логичке капије представљамо унитарним матрицама.

Да бисмо разумели шта су унитарне матрице, прво уводимо адјунговани оператор. Ако је  $\langle\psi|$  дуални вектор вектора  $|\psi\rangle$ , шта је дуални вектор вектора  $A|\psi\rangle$ ? Његов дуални вектор ће бити  $\langle\psi|A^\dagger$ . Оператор  $A^\dagger$  зовео адјунговани оператор и њему одговара матрица која је транспонована и коњугована.

Унитарни оператор је оператор чији је инверз једнак адјунгованом, односно  $U^{-1} = U^\dagger$ .

На пример, ако имамо логичку капију  $U = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$  и кубит  $|\psi\rangle = a|0\rangle + b|1\rangle$ , изаlazно стање добијамо на следећи начин:

$$U|\psi\rangle = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} a\alpha & b\beta \\ a\gamma & b\delta \end{pmatrix} = |\psi'\rangle.$$

### 3.1 Логичке капије са једним кубитом

Квантне логичке капије над једним кубитом представљамо унитарним матрицама  $2 \times 2$ . Постоји бесконачно много оваквих капија, али у овом раду ћемо навести само неке карактеристичне.

Прво уводимо три Паулијеве<sup>27</sup> матрице, од којих је прва Паулијева  $X$  матрица. Она је аналогна са класичном NOT капијом, односно уместо резултата  $|0\rangle$  добијамо  $|1\rangle$ , односно мења амплитуде стања  $|0\rangle$  и  $|1\rangle$ . Дата је на следећи начин:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = |0\rangle\langle 1| + |1\rangle\langle 0|.$$

Следеће, имамо  $Y$  и  $Z$  капије, које су представљене Паулијевим  $Y$  и  $Z$  матрицама:

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = -i|0\rangle\langle 1| + i|1\rangle\langle 0|,$$

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

Дакле  $Z$  капија од кубита у стању  $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$  прави кубит у стању  $|\psi'\rangle = \alpha|0\rangle - \beta|1\rangle$ , а  $Y$  капија прави кубит у стању  $|\psi''\rangle = -i\beta|0\rangle + i\alpha|1\rangle$ .

Следеће уводимо веома значајну Адамарову<sup>28</sup> логичку капију. Она, полазећи од стања  $|0\rangle$ , даје стање  $|+\rangle$ , а од стања  $|1\rangle$ , даје стање  $|-\rangle$ . Дакле, у општем случају, од кубита  $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$  добијамо кубит  $|\psi'\rangle = \alpha|+\rangle + \beta|-\rangle = \frac{\alpha+\beta}{\sqrt{2}}|0\rangle + \frac{\alpha-\beta}{\sqrt{2}}|1\rangle$ . Адамарову капију приказујемо матрицом:

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

Приметимо још да је Адамарова матрица уједно и сама себи инверзна, односно њеном поновном применом кубит враћамо у почетно стање. Такође приметимо да на Блоховој сфери она одговара ротацији за  $90^\circ$  око  $y$ -осе и осној рефлексiji у односу на  $xy$ -раван.

Уведимо и  $P$  капију. Ова капија зависи од параметра  $\phi$ , и представља ротацију за  $\phi$  око  $z$ -осе. Дата је као матрица:

$$P(\phi) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix}.$$

Приметимо да је  $Z$  капија специјалан случај  $P$  капије, односно  $P$  капија са параметром  $\phi = \pi$ .

Још неки специјални случаји  $P$  капије су  $I$  капија, односно идентичка капија,  $S$  капија, која је  $P$  капија са параметром  $\phi = \frac{\pi}{2}$  и  $T$  капија, која је  $P$  капија са параметром  $\phi = \frac{\pi}{4}$ . У матричном облику су:

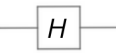



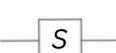
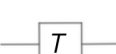
$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad S = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{2}} \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{pmatrix}.$$

Можемо да уведемо и најопштенију квантну капију са параметрима:

$$U(\theta, \phi, \lambda) = \begin{pmatrix} \cos \frac{\theta}{2} & -e^{i\lambda} \sin \frac{\theta}{2} \\ e^{i\phi} \sin \frac{\theta}{2} & e^{i(\phi+\lambda)} \cos \frac{\theta}{2} \end{pmatrix}.$$

Приметимо да је онда:

$$U\left(\frac{\pi}{2}, 0, \pi\right) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = H, \quad U(0, 0, \lambda) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\lambda} \end{pmatrix} = P(\lambda).$$

Hadamard		$1/\sqrt{2} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
Pauli-X		$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
Pauli-Y		$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$
Pauli-Z		$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
Phase		$\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$
T( $\pi/8$ )		$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$

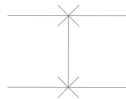
Слика 3.1. Приказ неколико квантних логичких капија и њима одговарајућих матрица

## 3.2 Логичке капије са више кубита

Операције над више кубита такође представљамо унитарним матрицама, али димензије зависе од броја кубита. У општем случају операцију над  $n$  кубита представљамо матрицом димензије  $2^n \times 2^n$ .

Приметимо да као што у обичним рачунарима премештамо информације, некада ћемо их премештати и у квантним компјутерима. Код одређених имплементација то можемо урадити физички, али бољи приступ је само променом стања између два кубита. За то користимо SWAP капију (Слика 3.2):

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



Слика 3.2. SWAP капија



Најзначајнија квантна логичка капија над два кубита је контролисана NOT капија (CNOT капија), која у зависности од стања првог кубита, или врши  $X$  капију на другом, или примењује јединичну операцију. У матричном облику је можемо представити на следећи начин:

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

Дакле CNOT капија мења амплитуде  $|01\rangle$  и  $|11\rangle$  посматраног кубита:

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

Посматрајмо сада два кубита, један у стању  $|0\rangle$ , а други у стању  $|+\rangle$ . Показали смо да такав систем представљамо помоћу Декартовог производа:  $|0\rangle \otimes |+\rangle = |0+\rangle$ . Приметимо да је:

$$|0+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |01\rangle).$$

Применимо сада CNOT капију на овај систем:

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

На овај начин добијамо квантно стање које зовемо *Белово стање*<sup>29</sup>.

### 3.2.1 Белова стања

Белова стања су специфична квантна стања од два кубита, која представљају најједноставнију, али и максималну квантну замршеност. Она су суперпозиција продукт стања  $|00\rangle$ ,  $|01\rangle$ ,  $|10\rangle$  и  $|11\rangle$  дакле представљају се као њихова линеарна комбинација и има их четири:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle),$$

$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle),$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle),$$

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle).$$

Ова стања чине максимално замршен базис у простору стања два кубита, познат као *Белов базис*. Приметимо и да због ефекта квантне замршености, мерењем једног кубита тачно одређујемо стање другог. Такође, вероватноћа са којом ће први кубит завршити у стању  $|0\rangle$  једнака је вероватноћи да заврши у стању  $|1\rangle$ , односно једнака је  $(\frac{1}{\sqrt{2}})^2 = \frac{1}{2}$ . Оваква стања имају велику примену у експерименталној физици, поготово у супергустом кодирању, квантној криптографији и у протоколу квантне телепортације, што ћемо имати прилику да видимо у наставку рада.

### 3.3 Идентитети са логичким капијама

Навешћемо неколико идентитета, помоћу којих можемо више капија заменити са једном, и самим тим упростити наше квантно логичко коло:

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

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

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

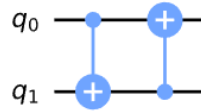
$$ZYZ = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = -Y,$$

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

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

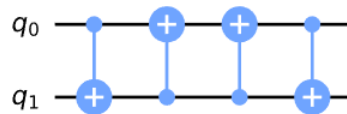
$$HZH = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{2}\begin{pmatrix}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

Покушајмо да SWAP капију представимо преко CNOT капија. Најпре посматрајмо систем са два кубита  $q_0$  у стању  $|1\rangle$  и кубит  $q_1$  у стању  $|0\rangle$ . Применимо сада CNOT капију контролисану кубитом  $q_0$  на кубит  $q_1$ , а затим обрнуто (Слика 3.3).



Слика 3.3

На овакав начин постижемо да је кубит  $q_0$  у стању  $|0\rangle$  и кубит  $q_1$  у стању  $|1\rangle$ . Сада посматрајмо добијено стање и вратимо га у почетно применом истих CNOT капија, али обрнутим редоследом (Слика 3.4).

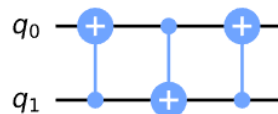


Слика 3.4

Приметимо сада да прва CNOT капија једног процеса не утиче на почетно стање кубита у другом. Односно када, на пример, пребацујемо  $|1\rangle$  из  $q_1$  у  $q_0$ , прва капија коју примењујемо је CNOT контролисана са  $q_1$  на  $q_0$ , али ако бисмо ову капију применили у процесу у ком почетно  $|1\rangle$  није на  $q_1$ , ова капија не би имала никакав ефекат.

Приметимо и да последња CNOT капија једног процеса не утиче на коначно стање кубита у другом. Односно када, на пример, пребацујемо  $|1\rangle$  из  $q_0$  у  $q_1$ , последња капија коју примењујемо је CNOT контролисана са  $q_1$  на  $q_0$ , али ако бисмо ову капију применили у процесу у ком на крају  $|1\rangle$  није на  $q_1$ , ова капија не би имала никакав ефекат.

Дакле можемо спојити ова два процеса додавањем једне CNOT капије (Слика 3.5).



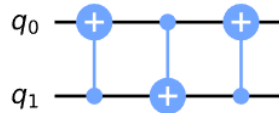
Слика 3.5

На овај процес можемо да гледамо као да мења  $|1\rangle$  из  $q_0$  у  $q_1$ , али са бескорисном CNOT капијом на почетку, или као да мења  $|1\rangle$  из  $q_1$  у  $q_0$ , али са бескорисном CNOT капијом на крају.

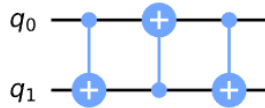
Такође примена ових капија на стање  $|00\rangle$  нема ефекат (CNOT капија нема ефекат када су контролни кубити  $|0\rangle$ ), а нема ефекат ни на стање  $|11\rangle$  (због

прве капије, друга неће имати ефекат, а трећа поништава прву).

Како овај процес ради за сва стања мерног базиса, мора да ради и на свим осталим стањима, односно SWAP капију можемо представити помоћу три CNOT капије на претходно описан начин (Слика 3.6).



Слика 3.6

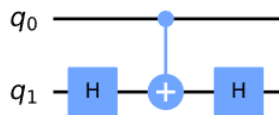


Слика 3.7. Напоменимо да и променом редоследа CNOT капија такође добијамо SWAP капију.

Споменимо још Controlled-Z капију над два кубита. Видели смо да CNOT капија примењује X капију на други кубит, ако је први - контролни - кубит у стању  $|1\rangle$ . На сличан начин дефинишемо Controlled-Z капију, која примењује Z капију на други кубит, ако је први у стању  $|1\rangle$ .

Пошто знамо да Адамарова капија преводи стања  $|0\rangle$  и  $|1\rangle$  у стања  $|+\rangle$  и  $|-\rangle$ , а знамо и да Z капија има исти ефекат на  $|+\rangle$  и  $|-\rangle$ , као X капија на  $|0\rangle$  и  $|1\rangle$  закључујемо  $HZH = X$  и  $HXH = Z$ . Приметимо да смо ово већ показали само множењем матрица.

Исти принцип можемо да искористимо са CNOT капијом, односно да бисмо добили Controlled-Z капију, све што треба да урадимо је да применимо Адамарову капију на други кубит пре и после примењивања CNOT капије.



Слика 3.8. Представљање Controlled-Z капије уз помоћ Адамарових капија и CNOT капије

# 4

## Qiskit

### 4.1 Увод у Qiskit

Qiskit је софтвер, који се налази између квантних алгоритама и физичког квантног уређаја. Он служи да преведе обичне програмске језике, попут Python-а, у језик који квантни рачунари разумеју. Садржи многобројне алате, помоћу којих можемо да правимо и управљамо квантним програмима, а затим да их симулирамо. Основна верзија користи Python као програмски језик и опремљена је са великом колекцијом готових квантних алгоритама. Најбитније, свима је доступан и пружа приступ креирању експеримената и апликација, које можемо покренути чак и на правом квантном компјутеру или их симулирати.

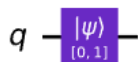
### 4.2 Представљање кубита

За почетак морамо да укључимо све потребне функције из одређених библиотека:

```
from qiskit import QuantumCircuit, assemble, Aer
from qiskit.visualization import plot_histogram, plot_bloch_vector
from math import sqrt, pi
```

У Qiskit-у користимо објекат QuantumCircuit да бисмо направили жељено квантно коло. У суштини, то је скуп логичких капија и кубита на које их примењујемо. На почетку се свим кубитима квантног кола додељује почетно стање  $|0\rangle$ . Ми можемо да га променимо:

```
qc = QuantumCircuit(1) # Pravimo kvanтно kolo sa jednim kubitom
početno_stanje = [0,1] # Definišemo početnu vrednost, npr. stanje 1
qc.initialize(početno_stanje, 0) # Dodeljujemo tu početnu vrednost nultom kubitom
qc.draw() # prikaz
```



Користимо Qiskit-симулатор, да бисмо видели крајње стање нашег кубита:

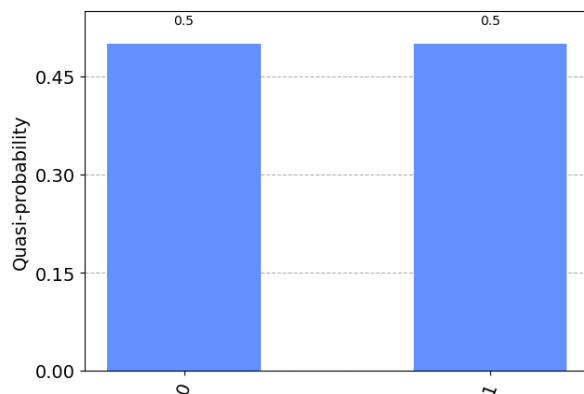
```
sim = Aer.get_backend('aer_simulator') # Pravimo Qiskit-simulator
qc = QuantumCircuit(1)
početno_stanje = [1/sqrt(2), 1j/sqrt(2)]
qc.initialize(početno_stanje, 0)
qc.save_statevector() # Čuvamo stanje
rezultat1 = sim.run(qc).result() # Izvršavamo simulaciju i vraćamo rezultat
krajnje_stanje = rezultat1.get_statevector() # Iz rezultata dobijamo krajnje stanje sistema
print(krajnje_stanje) # Prikaz stanja
```

```
Statevector([0.70710678+0.j , 0. +0.70710678j],
            dims=(2,))
```

Приметимо да Qiskit користи  $j$  да би представио  $i$  у комплексним бројевима. Такође,  $dims$  враћа појединачне димензије кубита из система.

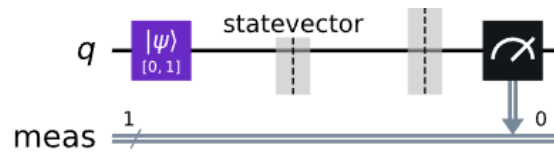
Подсетимо се да вероватноћа да кубит  $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$  заврши у стању  $|0\rangle$  је  $|\alpha|^2$ , а у стању  $|1\rangle$  је  $|\beta|^2$ . Ево и како то приказујемо:

```
rezultat2 = sim.run(qc).result().get_counts()
plot_histogram(rezultat2)
```



Ако при додељивању почетне вредности, није испуњен услов  $|\alpha|^2 + |\beta|^2 = 1$ , Qiskit ће избацити грешку. Ако је услов испуњен, онда мерење вршимо на следећи начин:

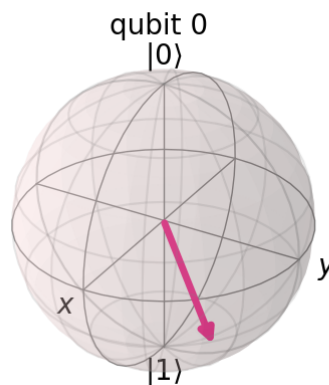
```
qc.measure_all()
qc.draw()
```



Приметимо да можемо да приказујемо кубите и на Блоховој сфери:

```
from qiskit.quantum_info import random_statevector
from qiskit.visualization import plot_bloch_multivector, array_to_latex # Još neke funkcije
psi = random_statevector(2) # Možemo i napraviti kubit u proizvoljnom stanju
display(array_to_latex(psi, prefix="|\psi\rangle")) # Za lep prikaz
plot_bloch_multivector(psi) # Prikaz na Blohovoj sferi
```

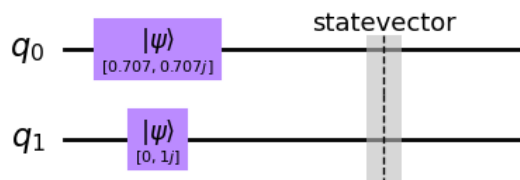
$$|\psi\rangle = [0.1115997404 - 0.5130124387i \quad 0.7606657042 - 0.3817740459i]$$



Прикажимо сада један пример са квантним колом са 2 кубита, нпр.  $|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{i}{\sqrt{2}}|1\rangle$  и  $|\phi\rangle = 0|0\rangle + i|1\rangle$ . У поглављу **2.3** смо показали да ће њихово заједничко стање бити  $|\phi\psi\rangle = 0 \cdot \frac{1}{\sqrt{2}}|00\rangle + 0 \cdot \frac{i}{\sqrt{2}}|01\rangle + i \cdot \frac{1}{\sqrt{2}}|10\rangle + i \cdot \frac{i}{\sqrt{2}}|11\rangle = 0|00\rangle + 0|01\rangle + \frac{i}{\sqrt{2}}|10\rangle - \frac{1}{\sqrt{2}}|11\rangle$ . Проверимо то сада симулацијом у Qiskit-у:

```
qc = QuantumCircuit(2)
početno_stanje1 = [1/sqrt(2), 1j/sqrt(2)]
početno_stanje2 = [0, 1.j]
qc.initialize(početno_stanje1, 0) # Dodela početnog stanja nultom kubit
qc.initialize(početno_stanje2, 1) # Dodela početnog stanja prvom kubit
qc.save_statevector()
result = sim.run(qc).result()
krajnje_stanje = result.get_statevector() # Stanje sistema
print(krajnje_stanje)
qc.draw()
```

```
Statevector([ 0.          +0.j          ,  0.          +0.j          ,
              0.          +0.70710678j, -0.70710678+0.j          ],
            dims=(2, 2))
```



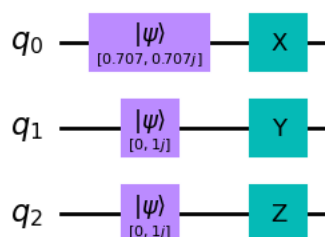
### 4.3 Представљање квантних логичких капија

Подсетимо се Паулијеве  $X$ ,  $Y$  и  $Z$  капије, којима одговарају матрице:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

У Qiskit-у их користимо на следећи начин:

```
qc = QuantumCircuit(3)
početno_stanje1 = [1/sqrt(2), 1j/sqrt(2)]
početno_stanje2 = [0, 1.j]
početno_stanje3 = [0, 1.j]
qc.initialize(početno_stanje1, 0)
qc.initialize(početno_stanje2, 1)
qc.initialize(početno_stanje3, 2)
qc.x(0) # Primenimo X kapiju na multi kubit
qc.y(1) # Primenimo Y kapiju na prvi kubit
qc.z(2) # Primenimo Z kapiju na drugi kubit
qc.draw()
```



Присетимо се и Адамарове капије која на стања  $|0\rangle$  и  $|1\rangle$  делује на следећи начин:  $H|0\rangle = |+\rangle$  и  $H|1\rangle = |-\rangle$ . Такође у поглављу **2.1** смо споменули да мерење можемо да вршимо и у другим базама, које морају бити ортонормиране. Једну од њих чине баш стања  $|+\rangle$  и  $|-\rangle$ , и тај базис се назива  $X$ -базисом, због тога што су  $|+\rangle$  и  $|-\rangle$  својствена стања оператора  $X$ .



Пошто Qiskit дозвољава само мерење у  $Z$ -базису, морамо сами да направимо функцију за мерење у  $X$ -базису:

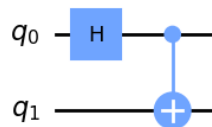
```
def merenje_xbasis(qc, qubit, cbit):
    # Merimo kubit u X-bazisu i skladištimo rezultat kao klasičan bit
    qc.h(qubit) # Vidimo primenu Adamarove kapije
    qc.measure(qubit, cbit)
    return qc
# U glavnom kodu pozivamo metodu:
početno_stanje = [1/sqrt(2), -1/sqrt(2)]
qc = QuantumCircuit(1,1) # Kvantno kolo sa jednim kubitom i jednim klasičnim bitom
qc.initialize(početno_stanje, 0)
merenje_xbasis(qc, 0, 0)
```

Такође можемо да користимо и  $P, S, T$  и  $U$  капије:

```
qc = QuantumCircuit(1)
qc.p(pi/4, 0) # P kapija sa parametrom
qc.s(0) # S kapija
qc.t(0) # T kapija
qc.u(pi/2, 0, pi, 0) # U kapija sa parametrima
```

Посматрајмо сада следећи код:

```
qc = QuantumCircuit(2)
qc.h(0)
# Primenjujemo CNOT kapiju:
qc.cx(0,1)
qc.draw()
```



```
qc.save_statevector()
result = sim.run(qc).result()
# Za pregledan prikaz
final_state = result.get_statevector()
array_to_latex(final_state, prefix="\\text{Statevector = }")
```

$$\text{Statevector} = \left[ \frac{\sqrt{2}}{2} \quad 0 \quad 0 \quad \frac{\sqrt{2}}{2} \right]$$

У поглављу **3.2** смо показали да на овакав начин добијемо *Белово стање*  $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ , што смо и добили овом симулацијом у Qiskit-у.

# 5

## Квантна телепортација

Нека Ана жели да Болету пошаље квантну информацију. Специфично, нека жели да му пошаље кубит у стању  $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ . Ово се своди на преношење информација о амплитудама ( $\alpha$  и  $\beta$ ) кубита, од Ане до Болета.

У поглављу **2.1** смо споменули да у квантној механици постоји теорема, позната као *no-cloning theorem*, која каже да не можемо да направимо идентичну копију непознатог квантног стања. Дакле, због ове теореме, Ана не може само да направи копију  $|\psi\rangle$  и да је пошаље Болету.

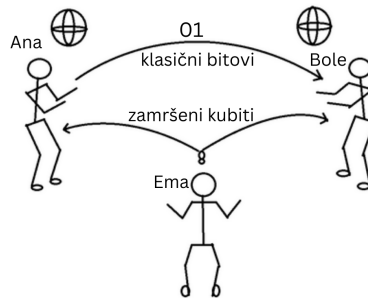
Али, користећи предности замршеног пара кубита и два класична бита, Ана може успешно да пошаље стање  $|\psi\rangle$  Болету. Овај процес се назива *квантним телепортацијом*, јер на крају, Боле има стање  $|\psi\rangle$ , док га Ана више нема.

### 5.1 Протокол квантне телепортације

Да би Ана послала Болету кубит, за почетак мора неко трећи (Ема) да сваком од њих уручи по један кубит из замршеног пара кубита. Затим ће Ана да изврши неке операције на њеним кубитима, па да их измери и пошаље два класична бита Болету. На основу информација тих битова, Боле ће применити неке операције на свом кубиту и добиће кубит у стању  $|\psi\rangle$ .

Покушајмо да опишемо протокол и да видимо како бисмо направили симулацију у Qiskit-у. За почетак, хајде да укључимо све потребне функције:

```
# Dohvatamo neophodne funkcije, neke ćemo koristiti tek u sledećim poglavlјima
import numpy as np
from qiskit import QuantumCircuit, QuantumRegister, ClassicalRegister
from qiskit import IBMQ, Aer, transpile, assemble
from qiskit.visualization import plot_distribution, plot_bloch_multivector, array_to_latex
from qiskit.extensions import Initialize
from qiskit.quantum_info import random_statevector
from qiskit.result import utils
```



Слика 5.1. Процес квантне телепортације

Затим правимо квантно коло:

```
# Protokol koristi ukupno tri kubita i dva klasična bita
qr = QuantumRegister(3, name="q") # Pravimo kvantni registar za tri kubita
crZ = ClassicalRegister(1, name="crZ") # Jedan klasičan registar za prvi bit
crX = ClassicalRegister(1, name="crX") # Jedan klasičan registar za drugi bit
kvantna_teleportacija = QuantumCircuit(qr, crz, crx) # Pravimo kvantno kolo sa ova tri registra
```

Сада, Ема прави замршени пар кубита и даје Ани и Болету по један кубит из пара. Замршен пар кубита, који Ема прави је специјални замршен пар - *Белов пар*. Дакле на језику квантних кола, да бисмо направили Белов пар од два кубита, морамо један да пребацимо у  $X$ -базис. То радимо тако што применимо Адамарову капију на њему. Затим примењујемо  $CNOT$  капију на други кубит, контролисан кубитом који је сада у  $X$ -базису.

```
def belov_par(qc, a, b):
    # Pravimo Belov par kubita
    qc.h(a) # Prebacujemo jedan kubit u stanje +
    qc.cx(a,b) # CNOT na kubit b, kontrolisan kubitom a
```

Надаље ћемо, без умањења општости, претпоставити да Ана има кубит  $q_0 = |\psi\rangle$  и кубит  $q_1$ , а Боле кубит  $q_2$ . Следећи корак би био да Ана изврши неку операцију над њеним кубитима.

Ана ће применити  $CNOT$  капију на кубит  $q_1$  контролисан кубитом  $q_0$ . Затим ће да примени Адамарову капију на кубит  $q_0$ :

```
def ana_kapije(qc, q0, q1):
    qc.cx(q0, q1) # Primenjujemo CNOT kapiju na q1, kontrolisan kubitom q0
    qc.h(q0) # Primenjujemo Admarovu kapiju na q0
```

Ана затим мора да измери њене кубите и да пошаље информацију о резултатима мерења Болету као два класична бита:

```
def merenje_i_slanje(qc, q0, q1):
    qc.barrier() # Odvajamo korake u protokolu
    qc.measure(q0,0) # Merenje kubita q0
    qc.measure(q1,1) # Merenje kubita q1
```

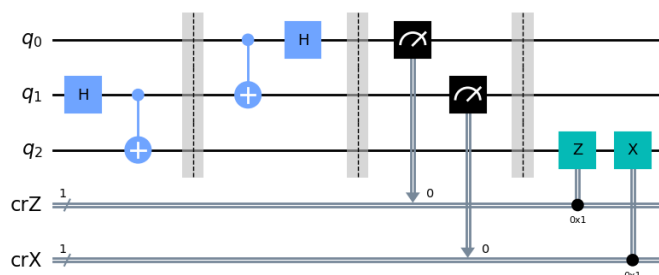
Након тога Боле, који има кубит  $q_2$ , примењује одговарајуће капије у зависности од тога које вредности битова добије:

00 → Не ради ништа  
 01 → Примењује  $X$  капију  
 10 → Примењује  $Z$  капију  
 11 → Примењује  $ZX$  капију

```
def bole_kapije(qc, q2, crZ, crX):
    # Koristimo c_if da bismo uradili nešto sa kubitom, ako klasičan bit ispunjava neki uslov
    qc.z(q2).c_if(crZ, 1) # Primenujemo Z kapiju ako je prvi registar u stanju 1
    qc.x(q2).c_if(crX, 1) # Primenujemo X kapiju ako je drugi registar u stanju 1
```

Сада би Боле требало да је успешно реконструисао стање кубита  $q_0$ . Дакле наше коло би изгледало отприлике овако:

```
qr = QuantumRegister(3, name="q") # Pravimo kvantni registar za tri kubita
crZ = ClassicalRegister(1, name="crZ") # Jedan klasičan registar za prvi bit
crX = ClassicalRegister(1, name="crX") # Jedan klasičan registar za drugi bit
kvantna_teleportacija = QuantumCircuit(qr, crZ, crX) # Pravimo kvantno kolo sa ova tri registra
# Prvi korak
belov_par(kvantna_teleportacija, 1, 2) # Ema pravi Belov par od prvog i drugog kubita
# Drugi korak
kvantna_teleportacija.barrier() # Odvajamo korake
ana_kapije(kvantna_teleportacija, 0, 1) # Ana primenuje kapije nad njenim kubitima
# Treći korak
merenje_i_slanje(kvantna_teleportacija, 0, 1) # Ana šalje klasične bitove Boletu
# Četvrti korak
kvantna_teleportacija.barrier() # Odvajamo korake
bole_kapije(kvantna_teleportacija, 2, crZ, crX) # Boles primenuje kapije nad njegovim kubitom
kvantna_teleportacija.draw()
```



## 5.2 Теорија

У поглављу **5.1** смо показали протокол квантне телепортације и његову имплементацију у Qiskit-у. У овом поглављу ћемо се упознати са самом теоријом иза протокола.

Сама квантна телепортација почиње чињеницом да Ана жели да пошаље произвољан кубит у стању  $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$  Болету, при чему, она наравно не зна стање њеног кубита. Онда Ема прави Белов пар замршених кубита за Ану и Болета.

У поглављу **3.2** смо показали да Белов пар представљамо на следећи начин:

$$|e\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

Пошто и Ана и Боле поседују по један кубит из тог замршеног пара, означимо га овако:

$$|e\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A |0\rangle_B + |1\rangle_A |1\rangle_B).$$

Онда имамо систем од три кубита, у ком Ана има прва два кубита, а Боле трећи:

$$\begin{aligned} |\psi\rangle \otimes |e\rangle &= \frac{1}{\sqrt{2}}(\alpha|0\rangle \otimes (|00\rangle + |11\rangle) + \beta|1\rangle \otimes (|00\rangle + |11\rangle)) = \\ &= \frac{1}{\sqrt{2}}(\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle). \end{aligned}$$

У следећем кораку, Ана примењује *CNOT* капију на други кубит, контролисан првим, а онда и Адамарову капију на први кубит. Стање система након тих операција ће бити:

$$\begin{aligned} (H \otimes I \otimes I)(CNOT \otimes I)(|\psi\rangle \otimes |e\rangle) &= \\ &= (H \otimes I \otimes I)(CNOT \otimes I)\left(\frac{1}{\sqrt{2}}(\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle)\right) = \\ &= (H \otimes I \otimes I)\left(\frac{1}{\sqrt{2}}(\alpha|000\rangle + \alpha|011\rangle + \beta|110\rangle + \beta|101\rangle)\right) = \\ &= \frac{1}{2}(\alpha(|000\rangle + |011\rangle + |100\rangle + |111\rangle) + \beta(|010\rangle + |001\rangle - |110\rangle - |101\rangle)). \end{aligned}$$

Ово на другачији начин можемо записати као:

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

Ана онда мери своја два кубита и информацију о резултатима мерења као класичне битове шаље Болету. Она мерењем својих кубита сигурно добија стања  $|00\rangle$ ,  $|01\rangle$ ,  $|10\rangle$  или  $|11\rangle$  и то свако са истом вероватноћом.

На основу њеног мерења, због нарушавања суперпозиције, стање кубита који је код Болета постаје:

$$\begin{aligned} |00\rangle &\longrightarrow (\alpha |0\rangle + \beta |1\rangle), \\ |01\rangle &\longrightarrow (\alpha |1\rangle + \beta |0\rangle), \\ |10\rangle &\longrightarrow (\alpha |0\rangle - \beta |1\rangle), \\ |11\rangle &\longrightarrow (\alpha |1\rangle - \beta |0\rangle). \end{aligned}$$

Дакле Боле, након што добије битове од Ане, може да добије оригинално стање  $|\psi\rangle$ , тако што ће применити одговарајуће капије на свој кубит, који је некада био део замршеног пара. И то на следећи начин:

Има битове 00, следи има стање  $\alpha |0\rangle + \beta |1\rangle$ , дакле примењује капију  $I$   
 Има битове 01, следи има стање  $\alpha |1\rangle + \beta |0\rangle$ , дакле примењује капију  $X$   
 Има битове 10, следи има стање  $\alpha |0\rangle - \beta |1\rangle$ , дакле примењује капију  $Z$   
 Има битове 11, следи има стање  $\alpha |1\rangle - \beta |0\rangle$ , дакле примењује капију  $ZX$

Након овог корака Боле је успешно реконструисао стање које је Ана имала.

### 5.3 Симулација квантне телепортације

Након поглавља 5.1 и 5.2 би требало да разумемо шта се дешава у квантној телепортацији и како у Qiskit-у правимо коло које врши квантну телепортацију. Хајде сада да симулирамо протокол.

За почетак направимо *капију*, која преводи стање  $|0\rangle$  у произвољно стање  $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$ .

```
psi = random_statevector(2) # psi postaje proizvoljan vektor dimenzije 2
psi_kapija = Initialize(psi)
psi_kapija.label = "psi"
```

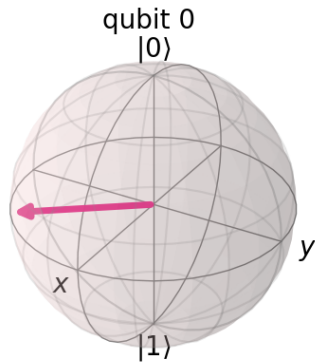
Можемо да прикажемо стање  $|\psi\rangle$ :

```
display(array_to_latex(psi, prefix="|\psi\rangle =")) # Prikaz vektora
plot_bloch_multivector(psi) # Prikaz stanja na Blohovej sferi
```

Хајде онда мало да изменимо квантно коло из поглавља 5.1:

```
qr = QuantumRegister(3, name="q") # Pravimo kvanтни registar za tri kubita
crZ = ClassicalRegister(1, name="crZ") # Jedan klasičan registar za prvi bit
crX = ClassicalRegister(1, name="crX") # Jedan klasičan registar za drugi bit
kvantna_teleportacija = QuantumCircuit(qr, crZ, crX) # Pravimo kvanтно коло sa ova tri registra
kvantna_teleportacija.append(psi_kapija, [0]) # Nultom kubitu dodeljujemo vrednost psi
kvantna_teleportacija.barrier()
```

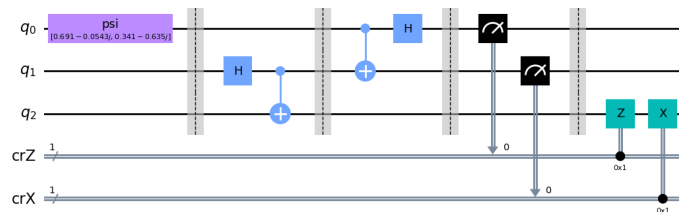
$$|\psi\rangle = [0.6911322565 - 0.0542760022i \quad 0.3405798121 - 0.6351344041i]$$



```

belov_par(kvantna_teleportacija, 1, 2) # Ema pravi Belov par od prvog i drugog kubita
kvantna_teleportacija.barrier()
ana_kapije(kvantna_teleportacija, 0, 1) # Ana primenjuje kapije nad njenim kubitima
merenje_i_slanje(kvantna_teleportacija, 0, 1) # Ana šalje klasične bitove Boletu
kvantna_teleportacija.barrier()
bole_kapije(kvantna_teleportacija, 2, crZ, crX) # Boles primenjuje kapije nad njegovim kubitom
kvantna_teleportacija.draw()

```

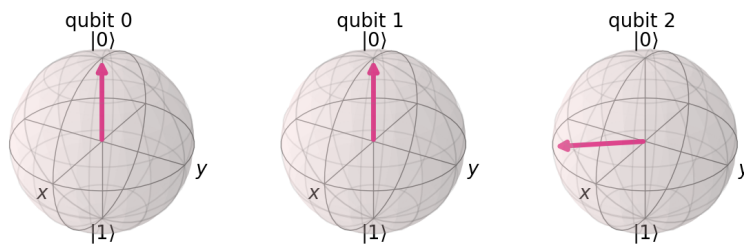


Искористимо сада Qiskit-симулатор да проверимо да смо у ствари *телепортовали* наш кубит.

```

sim = Aer.get_backend('aer_simulator')
kvantna_teleportacija.save_statevector()
krajnje_stanje = sim.run(kvantna_teleportacija).result().get_statevector()
plot_bloch_multivector(krajnje_stanje)

```



Приметимо да је стање  $|q_2\rangle$  исто као стање  $|\psi\rangle$ , док су стања  $|q_0\rangle$  и  $|q_1\rangle$  измерена, па су самим тим, или  $|0\rangle$ , или  $|1\rangle$ . Дакле успешно смо *телепортовали* произвољно стање  $|\psi\rangle$  од кубита  $q_0$  до кубита  $q_2$ .

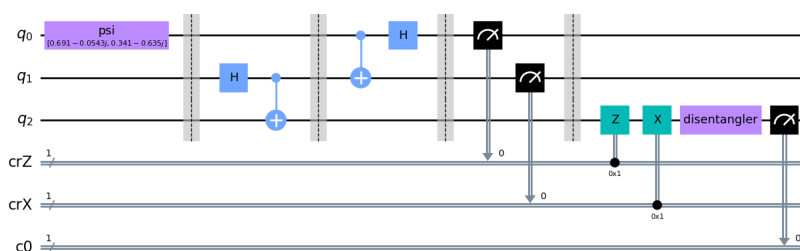
Пошто на правом квантном рачунару не бисмо могли да приказујемо вектор произвољног стања, односно, ако бисмо хтели да проверимо да ли *телепортација* ради, морали бисмо то да урадимо на мало другачији начин.

Како за сваку квантну капију постоји њима инверзна, онда и за нашу *psi* капију, постоји њој инверзна:

```
inverzna_psi_kapija = psi_kapija.gates_to_uncompute()
```

Дакле она преводи кубит из стања  $|\psi\rangle$  у стање  $|0\rangle$ . Значи да бисмо проверили да ли се стање  $q_0$  *телепортовало* у  $|q_2\rangle$ , морамо да применимо инверзну *psi* капију на  $|q_2\rangle$ . Очекујемо да ћемо онда са сигурношћу измерити  $|0\rangle$ .

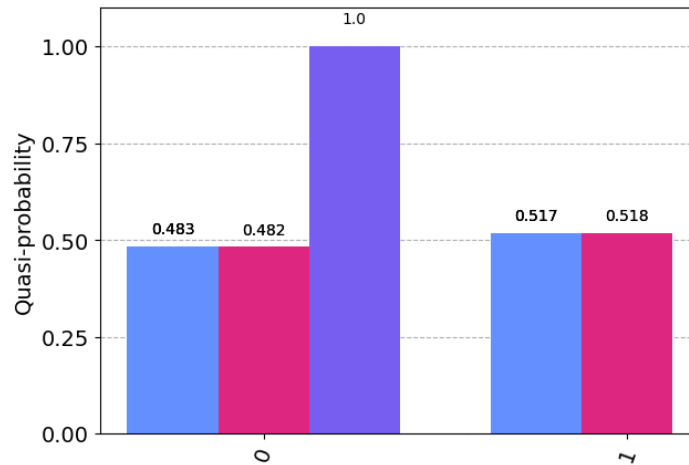
```
qr = QuantumRegister(3, name="q") # Pravimo kvantni registar za tri kubita
crZ = ClassicalRegister(1, name="crZ") # Jedan klasičan registar za prvi bit
crX = ClassicalRegister(1, name="crX") # Jedan klasičan registar za drugi bit
kvantna_teleportacija = QuantumCircuit(qr, crZ, crX) # Pravimo kvantno kolo sa ova tri registra
kvantna_teleportacija.append(psi_kapija, [0]) # Nultom kubitu dodeljujemo vrednost psi
kvantna_teleportacija.barrier()
belov_par(kvantna_teleportacija, 1, 2) # Ema pravi Belov par od prvog i drugog kubita
kvantna_teleportacija.barrier()
ana_kapije(kvantna_teleportacija, 0, 1) # Ana primenjuje kapije nad njenim kubitima
merenje_i_slanje(kvantna_teleportacija, 0, 1) # Ana šalje kubit Boletu
kvantna_teleportacija.barrier()
bole_kapije(kvantna_teleportacija, 2, crZ, crX) # Bole primenjuje kapije nad njegovim kubitom
kvantna_teleportacija.append(inverzna_psi_kapija, [2]) # Drugi kubit prebacujemo u stanje 0
cr_result = ClassicalRegister(1)
kvantna_teleportacija.add_register(cr_result)
kvantna_teleportacija.measure(2,2)
kvantna_teleportacija.draw()
```



Извршимо сада симулацију:

```
t_kvantna_teleportacija = transpile(kvantna_teleportacija, sim)
t_kvantna_teleportacija.save_statevector()
counts = sim.run(t_kvantna_teleportacija).result().get_counts()
qubit_counts = [utils.marginal_counts(counts, [qubit]) for qubit in range(3)]
plot_distribution(qubit_counts)
```





**Слика 5.2.** Вероватноће да се кубити  $q_0$ ,  $q_1$  и  $q_2$  нађу у стањима  $|0\rangle$  и  $|1\rangle$ . Плавом бојом је приказана вероватноћа за кубит  $q_0$ , розе бојом за кубит  $q_1$ , а љубичастом за кубит  $q_2$

Приметимо да ће вероватноћа да се кубит  $q_2$  нађе у стању  $|0\rangle$  бити 1. Ово је и био очекиван резултат, дакле показали смо да је протокол квантне телепортације успео.

## 5.4 Примена

Видели смо да је квантна телепортација процес којим преносимо квантну информацију са једне локације на другу. Са гледишта класичног преноса информација, квантна телепортација је револуционарна, јер пружа комплетан и сигуран пренос информације. Такође, веома је значајна и за квантну технологију, јер служи као незаменљив темељ. Квантне мреже, *port-based* телепортација и телепортација квантних капија, се изводе баш из основа квантне телепортације. Сам протокол телепортације је успешно изведен у доста лабораторија широм света, али сада ћемо се осврнути на неколико експеримената који су највише допринели развоју квантне технологије.

За почетак споменимо да су Asher Peres<sup>30</sup> и William Wootters<sup>31</sup>, 1993. године објавили *Teleporting an Unknown Quantum State via Dual Classical and Einstein-Podolsky-Rosen Channels*, први научни рад који је истраживао концепте квантне телепортације. Неколико година касније, 1997. су Anton Zeilinger<sup>32</sup> и Dirk Bouwmeester<sup>33</sup>, уз помоћ замршеног пара фотона, реализовали први експеримент који проверава протокол квантне телепортације.

Споменимо и да се тачност телепортације мери као преклапање између идеално телепортованог стања и измерене матрице густине, која је генерали-

зација вектора стања и таласне функције. Да би се протокол сматрао квантном телепортацијом ова тачност мора да превазилази класичну границу која износи  $\frac{2}{3}$ .

2004. Rupert Ursin<sup>34</sup> и његове колеге са Института за Експерименталну Физику у Бечу, су извршили експеримент квантне телепортације преко Дунава на дужини од  $600m$ . Користећи кабал од оптичких влакна дужине од  $800m$ , који је био постављен у канализационим цевима испод реке, и микроталаса послатих изнад воде, успешно су пренели и реконструисали поларизацију почетног фотона. Након 28 сати извођења експеримента, тачност је била у границама од 0.84 до 0.90 што је доста изнад класичне границе. Ово је веома значајан експеримент јер нас приближава имплементацији *quantum repeater*-а, који служи за расподелу замршених кубита у квантној мрежи.

2012. године научници из Цајлингеровог тима су успешно извршили експеримент телепортовања фотона преко раздаљине од  $143km$ , са Канарског острва Ла Палма, до Тенерифа. На Ла Палми је направљен замршен пар фотона, један је послат на Тенерифе, а затим је креиран још један фотон произвољне поларизације. Након операција и мерења фотона на Ла Палми, ласерским пулсом је послата информација  $143km$  даље, где је успешно реконструисана поларизација почетног фотона. Измерена тачност је била 0.863 са стандардном девијацијом од 0.038, што је опет доста изнад класичне границе од 0.67. Овај експеримент се сматра значајним јер је захтевао комбинацију модерних квантних оптичких инструмената, мерних уређаја и синхронизацију између удаљених лабораторија. Такође успешно је превазишао и промене у температури и временске непогоде, попут кише и снега (лабораторије су на надморској висини од  $2400m$ ).

Christopher Monroe<sup>35</sup> и његове колеге су 2004. године успешно извели први експеримент квантне телепортације стања између атома. Ово је веома значајно јер атоме можемо одржавати у истом квантном стању током значајно већег временског интервала (око 1 секунде), него што је случај код фотона. Дакле баш њих можемо користити за меморијске јединице квантне информације, па је овај експеримент од великог значаја за даљи развој квантних компјутера. За овај експеримент су коришћени јони калцијумовог изотопа  $^{40}Ca$ . Помоћу ниске температуре и ласера су добили замршен пар, а затим уз помоћ светлости одређене таласне дужине су извршили мерење. Уз помоћ микроталаса су извршили операцију на последњем јону, који се налазио на раздаљини од  $1m$ , и добили почетно стање првог јона. Тачност овог експеримента је била између 73% и 76%, што је свакако изнад класичне границе.

Најзначајнији експеримент квантне телепортације је био 2016. када је научни тим из Кине успешно пренео информацију из лабораторије у Нгарију, на Тибету (на висини од  $5100m$ ), до *Micius*<sup>36</sup> сателита, чија висина варира од  $500km$  до чак  $1400km$ . Прво су у лабораторији креирали замршене парове

ултра-светлих фотона (да би се смањиле атмосферске турбуленције), а онда су их посебним зрацима слали до сателита, који је сваког дана у поноћ пролазио изнад лабораторије. Да би се показала универзалност протокола, коришћено је 6 различитих базиса. Након 32 дана, послато је неколико милиона фотона, а резултат је био позитиван у 911 случајева. Израчуната је и тачност од 0.80 са стандардном девијацијом од 0.01. Ово је било веома значајно, јер је направљена Земља-сателит квантна комуникациона веза и неопходан корак ка глобалном квантном интернету. Тренунто се у Кини улаже много ресурса и новца за развој квантне комуникационе мреже за националну одбрану, финансије и остале аспекте.

## 6

# Закључак

Кроз овај рад смо имали прилику да се упознамо са неким основама квантне информатике и Qiskit-ом, али и са једним од најзначајнијих квантних протокола за даљи развој квантног рачунарства.

У првом, уводном смо се упознали са историјом и значајем квантне информатике, која проистиче из принципа квантне механике и теорије информације, али да бисмо је заиста разумели потребно је још много тога. Затим смо увели основне јединице информације - кубите, упознали се са њиховим својствима и разумели њихов значај. У трећем делу видимо везу са рачунарским наукама и уводимо квантне логичке капије. Показујемо како вршимо операције над кубитима и долазимо до кључног појма - квантне замршености, вероватно и најбитнијег феномена квантне механике. Након тога сусрећемо се и са софтвером Qiskit који преводи програмске језике на језик који разумеју квантни рачунари. Наравно, овде смо објаснили основе за прављење квантних капија и кола. У последњој целини долазимо до саме квантне телепортације. Након објашњавања протокола и кода који конструише такво коло, прешли смо на теорију која га објашњава. Затим смо извршили и симулацију и извршили проверу. На самом крају, кроз неколико веома значајних експеримената смо схватили колики значај има овај протокол, и за развој квантних рачунара и квантне комуникационе мреже, који представљају будућност квантне информатике.

Овде бих искористио прилику да се захвалим ментору, др Александри Гочанин на уложеном времену и труду за сарадњу и помоћ при писању овог рада. Такође бих се захвалио њој, др Драгољубу Гочанину и др Игору Салому што су ми представили физику на најлепши могући начин и инспирисали ме да је даље истражујем.

# Белешке

1. Albert Einstein (1879-1955) - немачки физичар, сматра се за највећег и најугицајнијег физичара свих времена, најпознатији по својој теорији релативности, а и значајно је допринео развоју квантне механике
2. No-cloning theorem - теорема у физици, која тврди да је немогуће направити независну и идентичну копију произвољног квантног стања, W. K. Wootters, W. H. Zurek, 1982.
3. Alan Turing (1912-1954) - британски математичар, оснивач модерне рачунарске науке
4. Turing machine - математички модел за израчунавање који дефинише апстрактну машину способну за манипулацију над некаквим подацима
5. Universal Turing machine - Тјуриногва машина која може да симулира произвољну Тјурингову машину
6. Church-Turing thesis - теза у области теорије израчунавања, у вези са природом израчунљивих функција, аутори тезе су амерички математичар Alonzo Church (1903-1995) и британски математичар Alan Turing (1912-1954)
7. John von Neumann (1903-1957) - мађарско-амерички математичар, постигао је значајне резултате у неколико области, али је имао највећи допринос у развоју првих рачунара
8. Gordon Moore (1929-2023) - амерички бизнисмен и инжењер, оснивач компаније Intel
9. David Deutsch (1953-) - британски физичар
10. Claude Shannon (1916-2001) - амерички математичар, сматра се оцем теорије информације
11. Benjamin Schumacher - амерички физичар, највећи допринос је постигао у квантној теорији информације
12. Charles Bennett (1943-) - амерички физичар
13. Stephen Wiesner (1942-2021) - америчко-израелски физичар
14. Superdense coding - протокол квантне комуникације, који уместо преноса информације са великим бројем битова, омогућава њен пренос коришћењем мањег броја кубита
15. Gilles Brassard (1955-) - компјутерски научник и професор на Универзитету у Монреалу
16. Whitfield Diffie (1944-) - амерички криптограф
17. Martin Hellman (1945-) - амерички криптограф
18. Ralph Merkle (1952-) - амерички компјутерски научник и математичар

19. Ronald Rivest (1947-) - амерички криптограф
20. Adi Shamir (1952-) - израелски криптограф
21. Leonard Adleman (1945-) - амерички компјутерски научник
22. Paul Dirac (1902-1984) - британски физичар, сматра се једним од оснивача квантне механике и квантне електродинамике
23. Felix Bloch (1905-1983) - швајцарско-амерички физичар, сматра се креатором нуклеарно магнетне резонанце
24. Quantum Entanglement - феномен у физици који се јавља када су две или више честица повезане на одређен начин, тако да се стање једне не може описати без стања осталих, EPR paradox, Albert Einstein, Boris Podolsky, Nathan Rosen, 1935.
25. Spooky action at a distance - феномен у квантној физици, по којем једна честица има информације и утицај на другу, иако се оне налазе на великој удаљености, Albert Einstein
26. No-communication theorem - теорема у физици, која нам говори да је немогуће да током мерења квантно замршеног стања, један посматрач мерењем дела целокупног стања, пренесе ту информацију до другог посматрача
27. Wolfgang Pauli (1900-1958) - аустријски физичар, најпознатији по Паулијевом принципу искључења
28. Jacques Hadamard (1895-1963) - француски математичар
29. John Bell (1928-1990) - физичар из Северне Ирске, најпознатији по Беловој теореми, која је једна од најважнијих теорема квантне механике
30. Asher Peres (1934-2005) - израелски физичар
31. William Wootters (1951-) - амерички физичар
32. Anton Zeilinger (1945-) - аустријски физичар, спровео много истраживања у вези са фундаменталним аспектима квантне замршености
33. Dirk Bouwmeester (1967-) - холандски физичар, значајан допринос развоју квантне оптике
34. Rupert Ursin (1973-) - аустријски физичар
35. Christopher Monroe (1965-) - амерички физичар
36. The Quantum Experiments at Space Scale (QUESS) - Micius - први квантно комуникациони сателит на свету, лансиран 2016 године, име је добио по старом кинеском филозофу и научнику

# Литература

- [1] M. A. Nielsen, I. L. Chuang, Quantum Computation and Quantum Information, Cambridge University Press, 2000.
- [2] Richard Cleve, Quantum Information Processing — A Primer for Beginners, Institute for Quantum Computing & Cheriton School of Computer Science University of Waterloo, 2021.
- [3] P. R. Kaye, R. Laflamme, M. Mosca, An Introduction to Quantum Computing, Oxford University Press, 2007.
- [4] C. P. Williams, Explorations in Quantum Computing, Springer, 2011.
- [5] Qiskit Textbook: <https://learn.qiskit.org/course/ch-algorithms/quantum-teleportation>
- [6] Ma, X.S., Herbst, T., Scheidl, T. et al. Quantum teleportation over 143 kilometres using active feed-forward. Nature 489, 269–273, 2012.
- [7] Ursin, R., Jennewein, T., Aspelmeyer, M. et al. Quantum teleportation across the Danube. Nature 430, 849, 2004.
- [8] [https://quantumoptics.at/images/publications/papers/nature04\\_riebe.pdf](https://quantumoptics.at/images/publications/papers/nature04_riebe.pdf)
- [9] <https://arxiv.org/ftp/arxiv/papers/1707/1707.00934.pdf>