Izvođenje Shorovog algoritma za faktorizaciju cijelih brojeva na kvantnim računalima iz porodice IBM Q Experience

Blažević, Marko

Master's thesis / Diplomski rad

2022

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Science / Sveučilište u Zagrebu, Prirodoslovno-matematički fakultet**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:217:066959

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2025-02-15**

Repository / Repozitorij:

Repository of the Faculty of Science - University of Zagreb

SVEUČILIŠTE U ZAGREBU
PRIRODOSLOVNO-MATEMATIČKI FAKULTET
FIZIČKI ODSJEK

Marko Blažević

Izvođenje Shorovog algoritma za faktorizaciju cijelih brojeva na kvantnim računalima iz porodice IBM Q Experience

Diplomski rad

Zagreb, 2022.

SVEUČILIŠTE U ZAGREBU
PRIRODOSLOVNO-MATEMATIČKI FAKULTET
FIZIČKI ODSJEK

INTEGRIRANI PREDDIPLOMSKI I DIPLOMSKI SVEUČILIŠNI STUDIJ
FIZIKA; SMJER NASTAVNIČKI

Marko Blažević

Diplomski rad

Izvođenje Shorovog algoritma za faktorizaciju cijelih brojeva na kvantnim računalima iz porodice IBM Q Experience

Voditelj diplomskog rada: izv.prof.dr.sc. Saša Ilijić

Ocjena diplomskog rada: _____

Povjerenstvo: 1. _____

2. _____

3. _____

Datum polaganja: _____

Zagreb, 2022.

Predivnoj osobi koja me vodila kroz ovaj rad, osobi koja je omogućila da ovaj rad pišem kao maksimalno motiviran, veseo i ohrabren student, osobi koja je vjerovala u mene i svakim našim susretom izazvala povećanje moje razine plemenitosti kao i motivacije za prelijepu znanost koju zovemo fizika, želim uputiti jednu od najzahvalnijih zahvala koju ću ikada uputiti:
Hvala profesore Ilijić.
Neizmjerno mi je drago što ste baš Vi bili moj mentor i obećajem da ću Vas od ovog trenutka — *2. Ožujka 2022. godine u 06:25 sati* pokušati svojim budućim postupcima učiniti ponosnim mentorom.
Prijateljima iz djetinjstva *(Toti, Cmeci, Juri, Antoniju, Dejanu, Coli, Kikiju, Anti, Tomici)*, prijateljima srednjoškolskih epiteta *(Rronu, Kruni, Tiću, Dodigu, Kodži, Deliću, Mikiću, Magudu, Kovi, Huziju)*, prijateljima domskih epiteta (*Jubyu, Mati, Šokretu)*, pulenima *(Ragužu, Histrijanu, Malom Ivanu)*, prijateljima s PMF-a *(Katarini, Janu)*, princezi *Mariji* i princu *Mariju* želim zahvaliti na nezamjenjivo pozitivnom utjecaju na moju psihologiju čije se djelovanje može prepoznati u ovom radu. Poznavanje svakog pojedinca navedenog u ovom paragrafu izravan je primjer sreće koju ovaj svemir pruža.
Specijalne zahvale u kontekstu povećanja mog razumijevanja fizike upućujem Filipu Požaru i Luki Bakraču. Vi ste nešto najljepše što PMF fizika može pružiti i vašu pomoć u spektru fizike nikada neću zaboraviti.
Zahvaljujem se profesorici Janji Pišković zbog koje sam zavolio fiziku kao 13-godišnji dječak.
Upućujem zahvale svojoj prekrasnoj, velikobrojnoj obitelji koja je puna ljubavi i koja mi je u nevjerojatnim količinama pomagala kroz razdoblje studiranja.
Tri osobe zaslužuju od mene zahvalu iz najdubljeg dijela srca — moja tetka s prezimenom Neureiter, majka Ivana i otac Mato. Ovaj rad posvećujem upravo njima.

Sažetak

Američka tvrtka IBM omogućila je 2016. godine da kvantna računala budu javno dostupna. Koristeći grafičko korisničko sučelje IBM Quantum Composer moguće je implementirati jednostavne kvantne algoritme. Slavni Shorov algoritam iz 1994. godine za faktorizaciju cijelih brojeva najbolje pokazuje moć kvantnih računala. U ovom radu opisane su osnove kvantne informacije i algoritama. Dana su svojstva i detaljno su opisana kvantna vrata koja se najčešće koriste pri kreiranju kvantnih krugova. Diplomski rad analizira matematičku razradu djelovanja kvantnog Fourierovog transformata na sustav n kvantnih bitova. Također, dat je kvantni krug koji implementira kvantnu Fourierovu transformaciju. Prikazna je procedura faktorizacije brojeva 15, 21, i 35 Shorovim algoritmom. Koristeći IBM Quantum Composer implementirani su kvantni krugovi za kvantnu Fourierovu transformaciju kao i Shorov algoritam za faktorizaciju broja 15.

Ključne riječi: Kvantni bit, Shorov algoritam, kvantna vrata, kvantni Fourierov transformat, *IBM Quantum Composer*

Diploma thesis title

Abstract

In the year of 2016 American company IBM made quantum computers publicly available. Using the graphical user interface IBM Quantum Composer it is possible to implement various quantum algorithms. The famous Shor's algorithm from the year of 1994 used for the integer factorisation is the foremost way of showing how powerful quantum computers are. In this work, the basics of quantum information and algorithms are described. The properties, as well as a brief description of the quantum gates most frequently used in creating quantum circuits are given. The thesis analyses the mathematical examination of applying quantum Fourier transform on a system of quantum bits. Also, a quantum circuit which implements quantum Fourier transform is given. The procedure of factoring the numbers 15,21, and 31 using Shor's algorithm is presented. Quantum circuits for the quantum Fourier transform, as well as Shor's algorithm for factoring the number 15, were implemented using IBM quantum composer.

Keywords: Quantum bit, Shor's algorithm, quantum gate, IBM Quantum Composer, quantum Fourier transform

Sadržaj

1 Uvod

Još 1980. godine pojavljuje se ideja o kvantnim računalima koju je potaknuo ruski matematičar Yuri Manin u svojoj knjizi *Computable and Uncomputable* [2]. Godinu dana kasnije nobelovac Richard Feynman govori o nemogućnosti simuliranja evolucije kvantno-mehaničkog sustava na klasičnom računalu i predlaže model kvantnog računala [3]. U devedesetim godinama prošlog stoljeća pojavili su se kvantni algoritmi od kojih se ističu algoritam Deutscha i Jozse, Simonov, Groverov i Shorov [6]. Shorov algoritam pokazao je da kvantno računalo može i do eksponencijalno puta brže izvesti specifične operacije u odnosu na klasično. Kvantno ubrzanje procesuiranja može se primijetiti i na procesorima sa samo nekoliko kvantnih bitova. Smatra se da je nadmoć kvantnih računala nad klasičnim najbolje vidljiva pri efikasnosti Shorovog algoritma koji predstavlja prijetnju RSA kriptosustavu. Faktorizacija cijelih brojeva smatra se teškim zadatkom za klasično računalo dok kvantno računalo rješava isti problem u polinomnom vremenu. Budući da je Shorov algoritam predstavljen 1994. godine [1], očekivalo bi se da je do sada, 28 godina kasnije, u velikoj upotrebi i da su brojevi koji se sastoje od puno znamenaka faktorizirani koristeći kvantno računalo. Međutim, izvođenje samog algoritma nije protočno jer stanje sustava kvantnih bitova naveliko opstruira dekoherencija. Dekoherencija je glavni razlog pojave šuma pri izvođenju ne samo Shorovog nego općenito svih algoritama na kvantnim procesorima. Problem dekoherencije je Peter Shor uvidio i već 1995. godine objavljuje rad *"Scheme for reducing decoherence in quantum computer memory"* [5]. Problem šuma i nezadovoljavajućih pouzdanosti rezultata mjerenja danas predstavljaju jedan od najvećih problema u svijetu kvantnih računala. Budući da su čestice koje treba zadržati u stanju superpozicije toliko osjetljive na turbulentni okoliš, konstruiranje kvantnog procesora izrazito je zahtjevno. Naime, u korist izbjegavanja dekoherencije kvantno računalo se održava na temperaturama bliskim apsolutnoj nuli — oko 15 milikelvina. Iznimno teška izrada procesora s velikim brojem kvantnih bitova predstavlja prepreku za faktorizaciju većih cijelih brojeva koristeći Shorov algoritam i razlog je zašto 28 godina nakon objave algoritma niti jedan troznamenkasti broj nije faktoriziran. Shorov algoritam oslanja se na kvantnu Fourierovu transformaciju čiji je cilj odrediti period dane funkcije. Osim kvantne Fourierove transformacije, svrhu u Shorovom algoritmu pronalazi i modularna eks-

ponencijacija. Implementacija navedenih operacija kao i još nekih drugih ostvaruje se djelovanjem kvantnih vrata na određene kvantne bitove. Budući da je kvantna mehanika unitarna sva kvantna vrata su unitarna pa tako i reverzibilna. Kvantna vrata matematički se opisuju matrično. Koristeći takav zapis matematički je moguće odrediti stanje kvantnog sustava u bilo kojem trenutku kvantnog kruga. Stanje neposredno prije mjerenja moguće je simulirati i kreirati graf ovisnosti vjerojatnosti o određenom stanju. Vjerojatnosti dobivene računalnom simulacijom zgodno je usporediti s dobivenim rezultatima i zaključiti jesu li rezultati vjerodostojni. Upravo to donosimo u ovom radu koristeći *IBM Quantum Composer*.

2 Kvantna informacija i kvantni algoritmi

2.1 Kvantni bit

Osnovna jedinica informacije u klasičnom računarstvu je bit. Klasični bit uvijek je u jednom od dva točno određena stanja — 0 ili 1. Kvantno mehanička generalizacija bita naziva se kvantni bit (engl. *qubit*) i osnovna je jedinica kvantne informacije. Za razliku od klasičnog bita, kvantni bit ima kvantno-mehaničko svojstvo da se nalazi u superpoziciji dvaju stanja koja najčešće obilježavamo s $|0\rangle$ i $|1\rangle$. Ta se stanja često prikazuju vektorima

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \qquad |1\rangle \begin{bmatrix} 0 \\ 1 \end{bmatrix}. \tag{2.1}$$

Stanje superpozicije kvantnog bita matematički se može opisati kao linearna kombinacija tih dvaju stanja:

$$\psi = \alpha|0\rangle + \beta|1\rangle, \tag{2.2}$$

gdje su α i β kompleksni brojevi. Mjerenjem kvantnog bita može se ustanoviti je li on u stanju $|0\rangle$ s vjerojatnošću $|\alpha|^2$, ili je on u stanju $|1\rangle$ s vjerojatnošću $|\beta|^2$. Vrijedi da je $|\alpha|^2 + |\beta|^2 = 1$ tj. ukupna vjerojatnost mora biti jedan. Stanje kvantnog bita je jedinični vektor u dvodimenzionalnom kompleksnom vektorskom kojeg zovemo Hilbertovim prostorom [6]. Tijekom mjerenja u bazi $\{|0\rangle, |1\rangle\}$, stanje će kolabirati ili u $|0\rangle$ ili u $|1\rangle$. Mjerenje u toj bazi zove se z-mjerenje. Postoji beskonačno mnogo baza od kojih se često koriste $\{|0\rangle, |1\rangle\}$, $\{|+\rangle, |-\rangle\}$ i $\{|R\rangle, |L\rangle\}$ gdje je:

$$|+\rangle = \frac{1}{\sqrt{2}}\Big(|0\rangle + |1\rangle\Big) \tag{2.3}$$

$$|-\rangle = \frac{1}{\sqrt{2}}\Big(|0\rangle - |1\rangle\Big) \tag{2.4}$$

$$|R\rangle = \frac{1}{\sqrt{2}}\Big(|0\rangle + i|1\rangle\Big) \tag{2.5}$$

$$|L\rangle = \frac{1}{\sqrt{2}}\Big(|0\rangle - i|1\rangle\Big) \tag{2.6}$$

Procesor u kvantnom računalu sadrži više od jednog kvantnog bita. Iz tog razloga potrebno je matematički opisati sustav od više kvantnih bitova što se postiže tenzorskim produktom $\otimes$. Stanje sustava $|\psi\rangle$ od tri kvantna bita koja se nalaze u stanjima

$|\Upsilon_i\rangle = \alpha_i|0\rangle + \beta_i|1\rangle$ za $i = 1, 2, 3$ matematički se opisuje kao

$$|\psi\rangle = |\Upsilon_1\rangle \otimes |\Upsilon_2\rangle \otimes |\Upsilon_2\rangle \tag{2.7}$$

$$\begin{aligned} &= \alpha_1\alpha_2\alpha_3|000\rangle + \alpha_1\alpha_2\beta_3|001\rangle + \alpha_1\beta_2\alpha_3|010\rangle + \alpha_1\beta_2\beta_3|011\rangle \\ &+ \beta_1\alpha_2\alpha_3|100\rangle + \beta_1\alpha_2\alpha_3|101\rangle + \beta_1\beta_2\alpha_3|110\rangle + \beta_1\beta_2\beta_3|111\rangle \end{aligned} \tag{2.8}$$

Izraz (2.7) često se skraćuje kao $|\Upsilon_1\Upsilon_2\Upsilon_3\rangle$ i na taj način opisuje stanje sustava od tri kvantna bita. Mjerenje stanja $|\Upsilon_1\Upsilon_2\Upsilon_3\rangle$ može rezultirati s bilo kojim od osam (2^3) navedenih stanja iz (2.8). Iz prethodnog se može primijetiti da broj vektora baze raste s brojem kvantnih bitova n kao 2^n [8].

2.2 Blochova sfera

Budući da za stanje kvantnog bita $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ vrijedi $|\alpha|^2 + |\beta|^2 = 1$, ili drugim riječima, budući da je stanje kvantnog bita normirano, $|\psi\rangle$ se može zapisati kao

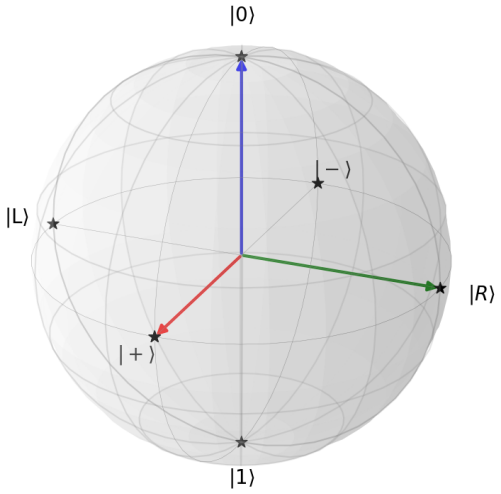
$$|\psi\rangle = e^{i\beta}\left(\cos\frac{\vartheta}{2}|0\rangle + e^{i\varphi}\sin\frac{\vartheta}{2}|1\rangle\right) \tag{2.9}$$

, gdje $e^{i\beta}$ predstavlja globalni fazni faktor, a kutovi $\varphi \in [0, 2\pi]$ i $\vartheta \in [0, \pi]$ u izrazu (2.9) definiraju točku na jediničnoj sferi koja nosi naziv *Blochova sfera* a prikazana je na slici 2.1. Iz (2.9) slijedi da ϑ određuje vjerojatnost mjerenja $|0\rangle$ odnosno $|1\rangle$,

$$P\big(|0\rangle\big) = |\langle 0|\psi\rangle|^2 = \cos^2\frac{\vartheta}{2} \qquad P\big(|1\rangle\big) = |\langle 1|\psi\rangle|^2 = \sin^2\frac{\vartheta}{2} \tag{2.10}$$

Globalni fazni faktor $e^{i\beta}$ ne utječe na stanje $|\psi\rangle$. Naime, u Eulerovom zapisu kompleksnog broja $z = r^{i\vartheta}$, faza utječe na rotaciju u kompleksnoj ravnini, ali ne i na amplitudu kompleksnog broja. Neutralnost globalnog faznog faktor može se pokazati računajući vjerojatnost ishoda mjerenja. Neka su $|\psi\rangle$ i $|\phi\rangle$

$$|\psi\rangle = e^{i\beta}\left(\lambda|0\rangle + \mu|1\rangle\right), \qquad |\phi\rangle = \gamma|0\rangle + \delta|1\rangle. \tag{2.11}$$



Slika 2.1: Prikaz stanja $|0\rangle$,$|1\rangle$,$|+\rangle$,$|-\rangle$,$|R\rangle$ i $|L\rangle$ na Blochovoj sferi.

Računajući vjerojatnost P kao

$$\begin{aligned} P_{|\psi\rangle\to|\phi\rangle} &= |\langle\phi|\psi\rangle|^2 \\ &= |\gamma^*\lambda e^{i\beta} + \delta^*\mu e^{i\beta}|^2 \\ &= |e^{i\beta}\left(\gamma^*\lambda + \delta^*\mu\right)|^2 \\ &= |\gamma^*\lambda + \delta^*\mu|^2 \end{aligned} \tag{2.12}$$

može se zaključiti da nema utjecaja globalnog faznog faktora na vjerojatnost $P_{|\psi\rangle\to|\phi\rangle}$.

Točke na površini Blochove sfere mogu se izraziti preko Kartezijevih koordinata kao

$$\left(x, y, z\right) = \left(\sin\vartheta\cos\varphi, \sin\vartheta\sin\varphi, cos\vartheta\right) \tag{2.13}$$

Koordinate takve točke koje označavaju normirano stanje dane su s vektorom $\vec{r}$ koji se matematički može opisati kao

$$\vec{r} = \begin{pmatrix} \sin\vartheta\cos\varphi \\ \sin\vartheta\sin\varphi \\ \cos\vartheta \end{pmatrix} \tag{2.14}$$

U tablici 2.1 navedene su odgovarajuće vrijednosti φ, ϑ i $\vec{r}$ za stanja $|0\rangle$, $|1\rangle$, $|+\rangle$,$|-\rangle$,$|R\rangle$, i $|L\rangle$. Blochova sfera, prikazana na slici 2.1 vizualizira stanje samo jednog kvantnog bita [9].

Stanje	ϑ	φ	$\vec{r}$
$\|0\rangle$	$\vartheta = 0$	$\varphi =$ proizvoljan	$\vec{r}_{\|0\rangle} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$
$\|1\rangle$	$\vartheta = \pi$	$\varphi =$ proizvoljan	$\vec{r}_{\|1\rangle} = \begin{pmatrix} 0 \\ 0 \\ -1 \end{pmatrix}$
$\|+\rangle$	$\vartheta = \frac{\pi}{2}$	$\varphi = 0$	$\vec{r}_{\|+\rangle} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$
$\|-\rangle$	$\vartheta = \frac{\pi}{2}$	$\varphi = \pi$	$\vec{r}_{\|-\rangle} = \begin{pmatrix} -1 \\ 0 \\ 0 \end{pmatrix}$
$\|i\rangle$	$\vartheta = \frac{\pi}{2}$	$\varphi = \frac{\pi}{2}$	$\vec{r}_{\|i\rangle} = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$
$\|-i\rangle$	$\vartheta = \frac{\pi}{2}$	$\varphi = \frac{3\pi}{2}$	$\vec{r}_{\|-i\rangle} = \begin{pmatrix} 0 \\ -1 \\ 0 \end{pmatrix}$

Tablica 2.1: Blochovi vektori za stanja $|0\rangle$,$|1\rangle$,$|+\rangle$,$|-\rangle$,$|R\rangle$, $|L\rangle$ i odgovarajući kutovi ϑ i φ.

2.3 Spregnuta stanja

Stanja poput (2.7) koja je moguće prikazati tenzorskim produktom zovu se separabilna stanja. U slučaju kada se sistem kvantnih bitova ne može prikazati tenzorskim produktom takvo stanje naziva se spregnutim (engl. *entangled state*). Spregnutost ima veliki značaj u području kvantne informacije. Naime, bez postojanja spregnutih stanja kvantna računala ne bi bila moćnija od klasičnih [11]. Pojava spregnutosti pri definiranju 2^n dimenzionalnog kompleksnog vektorskog prostora omogućuje provođenje kvantnih računa koristeći n fizikalnih kvantnih bitova.

- Neka su (Q_1, Q_2, Q_3) tri kvantna bita, a odgovarajući Hilbertovi prostori $\mathcal{H}_1^{(2)}$,$\mathcal{H}_2^{(2)}$,$\mathcal{H}_3^{(2)}$.
- Koristeći tenzorske produkte 2^n dimenzionalni Hilbertov prostor moguće je zapisati kao

$$\mathcal{H}^{2^3} = \mathcal{H}_1^{(2)} \otimes \mathcal{H}_2^{(2)} \otimes \mathcal{H}_3^{(2)} \tag{2.15}$$

Naizgled, definiran je 2^n dimenzionalni Hilbertov prostor bez spregnutih stanja. Međutim, greška je pretpostaviti da u (2.15) ne postoje spregnuta stanja. Primjerice, stanje

$$|GHZ\rangle = \frac{|000\rangle + |111\rangle}{\sqrt{2}} \in \mathcal{H}^{2^3} \tag{2.16}$$

je *Greenberger-Horne-Zeilinger* stanje ili skraćeno *GHZ* stanje koje predstavlja specifičan oblik spregnutog kvantnog stanja koje uključuje tri podsustava - u ovom slučaju kvantna bita. Dakle, spregnutost se pojavljuje kao posljedica korištenja tenzorskih produkata u definiciji (2.15). Tenzorski produkt dozvoljava $\mathcal{H}^{2^3}$ da sadrži superpozicije stanja poput $|000\rangle$ i $|111\rangle$. Ispada da je većina takvih stanja spregnuto. Neka stanja više su spregnuta od drugih, a postoje i stanja koja su maksimalno spregnuta i zovu se Bellova stanja. Bellova stanja dvaju kvantnih bitova matematički se opisuju kao

$$|\psi^{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \tag{2.17}$$

$$|\psi^{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \tag{2.18}$$

$$|\psi^{10}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \tag{2.19}$$

$$|\psi^{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \tag{2.20}$$

Spregnuto stanje potpuni je opis vezanog sistema. Ništa više nije moguće znati o sustavu. U maksimalno spregnutim stanjima (2.17)-(2.20) ništa nije poznato o individualnim stanjima kvantnih bitova [10].

2.4 Kvantna vrata

Kvantni bit ili sustav kvantnih bitova može promijeniti svoje stanje prolazeći kroz jednu ili više unitarnih transformacija. Unitarna transformacija opisana je unitarnom matricom koja mora zadovoljavati

$$U^\dagger U = UU^\dagger = I \tag{2.21}$$

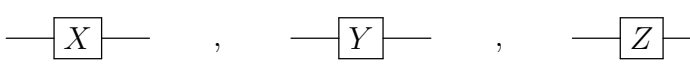
gdje bodež † označava kompleksno-konjugirani član, a I jediničnu matricu. Analogno klasičnim logičkim vratima poput NOT i AND, takve unitarne transformacije koje se koriste za transformacije kvantnih bitova zovu se vrata. Sva kvantna vrata su unitarne transformacije i mogu se opisati unitarnim matricama. Iz jednadžbe (2.21) slijedi da je broj ulaznih kvantnih bitova jednak broju izlaznih [8]. Iz unitarnosti slijedi svojstvo svih kvantnih vrata - reverzibilnost. Naime, za svaku unitarnu transformaciju U mora postojati odgovarajuća transformacija $U^\dagger$ koja će istu transformaciju izvesti u suprotnom smjeru. Drugim riječima, reverzibilnost znači da se ulazni podaci mogu rekonstruirati iz izlaznih. Klasična logička vrata ne moraju biti reverzibilna. Primjer nereverzibilnih vrata su vrata AND čiji će izlaz biti 1 ako i samo ako su obje ulazne jedinice 1. Naime, ako je izlaz logičke operacije AND 1 ulaz se može rekonstruirati međutim ako je izlaz 0 nije moguće znati samo na osnovu izlaza da li je ulaz bio 00, 01 ili 10 što logičku operaciju AND čini nereverzibilnom. Ograničenje svojstvom reverzibilnosti ne čini kvantna vrata manje moćnijim od klasičnih [13].

2.4.1 Paulijeva vrata

Kvanta vrata mogu se podijeliti na ona koja djeluju na samo jedan kvantni bit (engl. *single qubit gate*) i na ona koja djeluju na više kvantnih bitova. Kvantna vrata koja se mogu matematički opisati Paulijevim matricama zovu se Paulijeva vrata, a to su X, Y i Z vrata koja predstavljaju rotacije oko osi x, y i z na Blochovoj sferi za π radijana. Preciznije, X vrata mijenjaju stanje kvantnog bita iz $|0\rangle$ u $|1\rangle$ ili obratno. Z vrata ne mijenjaju stanje $|0\rangle$ dok stanju $|1\rangle$ mijenjaju predznak. Analogno zamijeni $|0\rangle$ i $|1\rangle$ stanja kod X vrata - Z vrata mijenjaju stanja $|+\rangle$ i $|-\rangle$, što znači da u bazi $\{|+\rangle, |-\rangle\}$ imaju istu ulogu kao X vrata u $\{|0\rangle, |1\rangle\}$ bazi. Y vrata mijenjaju i stanje i fazu kvantnog bita npr. $|0\rangle \to i|1\rangle$. Matrični zapis Paulijevih vrata je

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{2.22}$$

Simboli Paulijevih X, Y i Z vrata koji se koriste u shematskim prikazima kvantnih logičkih krugova su:



(2.23)

Slika 2.2: Oznake kvantnih vrata u *IBM Quantum Composer*-u, redom s lijeva na desno: X, Y i Z vrata. Slike su preuzete s [15].

Također, na slici (2.2) prikazane su oznake istih vrata koje se koriste u *IBM Quantum Composer*-u gdje se koristi različita oznaka za X ili NOT gate.

2.4.2 Hadamardova vrata

Zbrajanjem X i Z vrata dobiva se izraz za Hadamardova vrata. Hadamardova vrata mijenjaju bazu iz $\{|0\rangle, |1\rangle\}$ u $\{|+\rangle/|-\rangle\}$ i obratno. Na početku kvantnog algoritma Hadamardova vrata koriste se kako bi se ostvarila superpozicija. Matrični zapis Hadamardovih vrata je

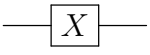
$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{2.24}$$

Djelovanje Hadamardovih vrata na stanja $|0\rangle$ i $|1\rangle$ rezultira s:

$$H|0\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = |+\rangle = \frac{1}{\sqrt{2}} \Big(|0\rangle + |1\rangle \Big) \tag{2.25}$$

$$H|1\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = |-\rangle = \frac{1}{\sqrt{2}} \Big(|0\rangle - |1\rangle \Big) \tag{2.26}$$

Može se primijetiti da su rezultati te dvije operacije $|+\rangle$ odnosno $|-\rangle$, što dokazuje tvrdnju da Hadamardova vrata mijenjaju bazu iz $\{|0\rangle, |1\rangle\}$ u $\{|+\rangle, |-\rangle\}$. Uobičajena oznaka Hadamardovih vrata je kvadrat sa slovom H u sredini:



(2.27)

Oznaka koja se koristi u kreiranju kvantnih krugova koristeći *IBM Quantum Composer* prikazana je na slici (2.3). Vrijedi napomenuti da H^2 ne mijenja stanje kvantnog bita jer se množenjem matrice (2.24) sa samim sobom dobiva jedinična matrica I. Jediničnom matricom I definirana su kvantna vrata I čiji je zadatak osigurati da

Slika 2.3: Oznaka za Hadamardova vrata u *IBM Quantum Experience*. Slika je preuzeta s [15].

Slika 2.4: Oznake kvantnih vrata u IBM Quantum Experience-u, redom s lijeva na desno: RX, RY i RZ vrata. Slike su preuzete s [15].

stanje kvantnog bita ostaje nepromijenjeno za jednu jedinicu kvantnog kruga.

$$H^2 = \left(\frac{1}{\sqrt{2}}\right)^2 \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I \tag{2.28}$$

2.4.3 Rotacija jednog kvantnog bita oko x,y i z osi

Postoje vrata koja rotiraju kvantni bit za proizvoljni kut θ oko x, y osi odnosno za proizvoljni kut φ oko z osi gdje se za vrijednosti θ i ϕ koriste radijani. To su vrata RX, RY i RZ. Matrični zapis tih vrata je

$$RX(\theta) = e^{\left(-i\frac{\theta}{2}X\right)} = \begin{pmatrix} \cos\frac{\theta}{2} & -i\sin\frac{\theta}{2} \\ -i\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix}, \tag{2.29}$$

$$RY(\theta) = e^{\left(-i\frac{\theta}{2}Y\right)} = \begin{pmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix}, \tag{2.30}$$

$$RZ(\varphi) = e^{\left(-i\frac{\varphi}{2}Z\right)} = \begin{pmatrix} e^{\left(-i\frac{\varphi}{2}\right)} & 0 \\ 0 & e^{\left(i\frac{\varphi}{2}\right)} \end{pmatrix}, \tag{2.31}$$

a oznake istih u *IBM Quantum Composer*-u prikazane su na slici (2.4). Preko izraza (2.31) definiraju se vrata T i S. Naime, T vrata su ekvivalentna RZ vratima za

Slika 2.5: Oznake kvantnih vrata unutar platforme *IBM Quantum Experience*, redom s lijeva na desno: U i P vrata. Slike su preuzete s [15].

$\varphi = \frac{\pi}{4}$, dok su S vrata ekvivalentna RZ vratima za $\varphi = \frac{\pi}{2}$. Može se zaključiti da vrata S djeluju fazom i na stanje $|1\rangle$. Koriste se još P i U vrata. P vrata djeluju fazom $e^{i\theta}$ na stanje $|1\rangle$. Posljedica djelovanja P vrata je rotacija kvantnog bita oko z osi što je slučaj i sa RZ vratima, ali postoji bitna razlika između P i RZ vrata: $P(\lambda) = e^{i\lambda/2}RZ(\lambda)$. Pomoću P vrata može se doći do drugih kao što su T, S i Z. Općenitiji slučaj P vrata su U vrata koja osim proizvoljnog kuta λ omogućuju djelovanje proizvoljnim kutovima θ i φ. Osobitost U vrata leži u tome što se pomoću tri proizvoljna kuta može konstruirati bilo koja vrata koja djeluju na samo jedan kvantni bit. Matrični zapisi U i P vrata dani su u (2.32), a njihove oznake u *IBM Quantum Experience* prikazani su na slici (2.5) [9].

$$P(\lambda) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\lambda} \end{pmatrix} \qquad U(\theta, \phi, \lambda) = \begin{pmatrix} \cos(\theta) & -e^{i\lambda}\sin(\theta) \\ e^{i\phi}\sin(\theta) & e^{i(\phi+\lambda)}\cos(\theta) \end{pmatrix} \tag{2.32}$$

Vrijedi napomenuti da postoji opcija upravljanih U i P vrata koja bi u tom slučaju funkcionirala prema istom načelu kao i $CNOT$ vrata.

2.4.4 Kvantna vrata koja uključuju više kvantnih bitova

Upravljana X vrata (CX) ili upravljana NOT vrata $(CNOT)$ djeluju na dva kvantna bita gdje je jedan upravljani, a drugi ciljni. Naime, na ciljni kvantni bit djelovati će se s operacijom NOT samo u slučaju kada je drugi kvantni bit - upravljani u stanju $|1\rangle$. Dakle, ako je upravljani kvantni bit u stanju $|0\rangle$ ciljnom kvantnom bitu uključenom u $CNOT$ vrata neće se promijeniti stanje. Matrični zapis $CNOT$ vrata je

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}_{q_1,q_0} \qquad \text{ili} \qquad \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}_{q_0,q_1} \tag{2.33}$$

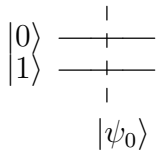
u gdje je prvi po redu navedeni kvantni bit u indeksu upravljani [9]. Moguća je i situacija kada je upravljani kvantni bit u stanju superpozicije. U tom slučaju $CNOT$ vrata kreirat će spregnuto stanje. Drugim riječima, slijed Hadamardovih vrata popraćenih s $CNOT$ vratima rezultira spregnutim stanjem. Postoje i kontrolirana $CNOT$ vrata - CCX ili $CCNOT$ vrata koja se nazivaju *Toffolijeva vrata* i djeluju operacijom NOT samo u slučaju u kojem su oba upravljana kvantna bita u stanju $|1\rangle$. Matrični zapis Toffolijevih vrata je

$$CCX = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}_{q_2,q_1,q_0} \quad \text{ili} \quad \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}_{q_0,q_1,q_2}, \tag{2.34}$$

gdje također kao i u (2.33) prvi navedeni kvantni bit u indeksu predstavlja upravljani. Naime, pri implementaciji kvantnog algoritma imamo slobodu birati koji će od n kvantnih bitova biti ciljni. Bitno je napomenuti da postoje različite konvencije oko značajnosti kvantnih bitova u slijedu $q_0, q_1, q_2, ...q_n$. U konvenciji koja će se koristiti u ovome radu najznačajniji kvantni bit onaj je čiji indeks ima najveću vrijednost. Takva konvencija na engleskom jeziku zove se *little endian convention*. Redoslijed značajnosti kvantnih bitova može se usporediti s analognom situacijom klasičnih bitova gdje nije jednako da li je najznačajniji bit prvi s desna ili s lijeva. Ako se primjerice binarni zapis brojeva 1011 želi prikazati u decimalnom zapisu rezultat će se razlikovati ovisno o tome koji bit se uzme kao najznačajniji. Konkretno, u sljedećem kvantnom krugu (2.35) stanje $|\psi_0\rangle$ jednako je $|01\rangle$ vodeći se po konvenciji koja se koristi u većini udžbenika. Međutim, po konvenciji koja se koristi na platformi *IBM Quantum Experience* stanje $|\psi_0\rangle$ raspisalo bi se kao $|10\rangle$. Isprekidane, vertikalne linije uobičajeno je koristiti pri promatranju kvantnog stanja u određenom trenutku

Slika 2.6: Oznake kvantnih vrata u IBM Quantum Experience-u, redom s lijeva na desno: $CNOT$, CCX i $SWAP$ vrata. $CNOT$ i CCX vrata prikazana su za slučaj onzačen u (2.33) odnosno (2.34) s indeksima q_0q_1 odnosno $q_0q_1q_2$. U oznakama za obrnuti slučaj $CNOT$ i CCX vrata (q_1q_0) odnosno $q_0q_1q_2$ zamijenjeni su upravljani i ciljni kvantni bit. Slike su preuzete s [15].

kvantnog kruga:



(2.35)

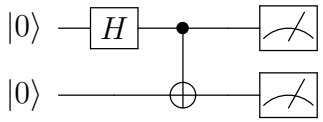
Vrata koja služe kako bi se izmijenila stanja dvaju kvantnih bitova zovu se $SWAP$, a matrični zapis istih je:

$$SWAP = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \tag{2.36}$$

Oznake kvantnih vrata $CNOT, CCX$ i $SWAP$ koje se koriste u *IBM Quantum Composer*-u prikazane su na slici 2.6.

2.4.5 Prikaz kvantnog logičkog kruga

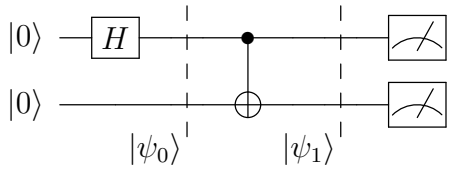
Jednostavni kvantni logički krug može se prikazati shemom poput



(2.37)

Krug je kreiran koristeći Hadamardova vrata primijenjena na ulazni kvantni bit u stanju $|0\rangle$ nakon čega slijede upravljana NOT vrata odnosno $CNOT$ vrata. Primjena tih vrata rezultira spregnutim stanjem dvaju kvantnih bitova. Posljednja tj. najdesnija kvantna vrata su vrata koja označuju mjerenje. Može se promatrati kako određena kvantna vrata u krugu (2.37) djeluju na stanje pojedinog kvantnog bita. Neka je $|\psi_0\rangle$ stanje sustava nakon djelovanja Hadamardovih vrata, a $|\psi_1\rangle$ stanje sustava nakon

$CNOT$ vrata.



(2.38)

Djelovanje Hadamardovih vrata na $|0\rangle$ već je pokazano u (2.25). Drugi kvantni bit $|0\rangle$ ostaje nepromijenjen. Matrični i vektorski zapis stanja $|\psi_0\rangle$ može se dobiti sljedećim postupkom

1. Djelovanje Hadamardovih vrata na stanje $|0\rangle \rightarrow H\,|0\rangle$

$$H\,|0\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \tag{2.39}$$

2. Odrediti tenzorski produkt $H|0\rangle \otimes |0\rangle$

$$|\psi_0\rangle = H|0\rangle \otimes |0\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} \tag{2.40}$$

3. Dobivenu matricu zapisati kao zbroj ket vektora s koeficijentima a, b, c, d

$$|\psi\rangle = a\,|00\rangle + b\,|01\rangle + c\,|10\rangle + d\,|11\rangle \tag{2.41}$$

4. Odrediti keoficijente a, b, c, d te izmnožiti ih s odgovarajućim ket vektorima.

$$\begin{aligned} a = \langle 00|\psi_0\rangle = \frac{1}{\sqrt{2}}, \quad b = \langle 01|\psi_0\rangle = 0, \\ c = \langle 00|\psi_0\rangle = \frac{1}{\sqrt{2}}, \quad d = \langle 00|\psi_0\rangle = 0 \end{aligned} \tag{2.42}$$

$$|\psi\rangle = \frac{1}{\sqrt{2}}|00\rangle + 0|01\rangle + \frac{1}{\sqrt{2}}|10\rangle + 0|11\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |10\rangle\right) \tag{2.43}$$

5. Konačno:

$$|\psi_0\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |10\rangle\right). \tag{2.44}$$

Navedeni postupak matematički opisuje djelovanje Hadamardovih kvantnih vrata za kvantni krug (2.38). Nadalje, stanje $|\psi_1\rangle$ dobije se djelovanjem matrice (2.33) za

slučaj $q_1 q_0$ na (2.40)

$$|\psi_1\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}_{q_1,q_0} \cdot \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} \tag{2.45}$$

Budući da se u postupku (2.40-2.44) koristila klasična konvencija, a ne onakva kakva se koristi u *IBM Quantum Experience* pomoću koje su definirane matrice (2.33) potrebno je koristiti suprotan slučaj - matricu s indeksom $(q_1 q_0)$ iz (2.33). Dobivena matrica iz (2.45) može se raspisati kao što je to učinjeno u (2.41). Lako se pokaže da su koeficijenti $a, d = 1$ dok su $b, c = 0$, iz čega slijedi da se (2.45) može zapisati kao

$$|\psi_1\rangle = \frac{1}{\sqrt{2}} \left(|00\rangle + |11\rangle\right). \tag{2.46}$$

Slično kao (2.46) mogu se dobiti i ostala maksimalno spregnuta stanja (2.17-2.20). Naime, postoje četiri ulazne kombinacije početnih stanja kvantnih bitova i svaka će rezultirati različitim izrazom za spregnuto stanje nakon prolaska kroz krug (2.38).

3 Kvantni Fourierov transformat

Diskretni Fourierov transformat može se opisati kao transformacija vektora kompleksnog skupa brojeva s N članova $x_0, x_1, ..., x_{N-1}$ u vektor kompleksnog skupa brojeva $y_o, y_1, ..., y_{N-1}$ zadovoljavajući sljedeću jednadžbu [6]

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{2\pi ijk/N} x_j. \tag{3.1}$$

Analogon za diskretni Fourierov transformat koji se koristi u kvantnim algoritmima je kvantni Fourierov transformat. Za razliku od diskretnog Fourierovog transformata, kvantni Fourierov transformat (engl. *Quantum Fourier Transform*) ili skraćeno QFT na ortonormiranu bazu $|0\rangle, ..., |N-1\rangle$ definira se kao linearni operator s operacijom na stanja baze opisanom u (3.2)

$$|j\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi ijk/N} |k\rangle. \tag{3.2}$$

U (3.2) N se definira kao 2^n gdje je n broj kvantnih bitova tj. stanja baze na koji djelujemo kvantnim Fourierovim transformatom. Djelovanje kvantnog Fourierovog transformata za slučaj samo jednog kvantnog bita za $j = |\tilde{0}\rangle$ i $j = |\tilde{1}\rangle$ gdje $|\tilde{j}\rangle$ predstavlja član u Fourierovoj bazi matematički je opisano s

$$|\tilde{0}\rangle = \frac{1}{\sqrt{2}} \sum_{k=0}^{1} e^{\frac{2\pi i 0k}{2}} |k\rangle = \frac{1}{\sqrt{2}} \sum_{k=0}^{1} |k\rangle = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) = |+\rangle \tag{3.3}$$

$$\begin{aligned} |\tilde{1}\rangle &= \frac{1}{\sqrt{2}} \sum_{k=0}^{1} e^{\frac{2\pi i 1k}{2}} |k\rangle = \frac{1}{\sqrt{2}} \left(e^{\frac{2\pi i 1 \cdot 0}{2}} |0\rangle + e^{\frac{2\pi i 1 \cdot 1}{2}} |1\rangle \right) \\ &= \frac{1}{\sqrt{2}} (|0\rangle + (-1)|1\rangle) = \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) = |-\rangle \end{aligned} \tag{3.4}$$

U slučaju u kojem je broj kvantnih bitova n veći, raspisivanjem kvantnog Fourierovog transformata može se doći do drugog načina zapisivanja - u obliku produkata koji se često koristi. U notaciji gdje je $|k\rangle$ zapisan kao npr. $|k\rangle = |5\rangle$ broj 5 može se zapisati u binarnom zapisu kao $|101\rangle$. Shodno tome k se može binarno zapisati kao $2^{n-1}k_1 + 2^{n-2}k_2 + ... + 2^0 k_n$, odnosno općenitije kao $\sum_{l=1}^{n} k_l 2^{n-l}$. Budući da se broj

$|k\rangle$ zapisao binarno granica sumacije više ne može biti $2^n - 1$. Primjerice, ako je $2^n = 8 = N$, tj. ako je $N - 1 = 7$, nije moguće razviti sumu jer u raspisu broja $|k\rangle$ su samo nule i jedinice. Naime, ako se $|k\rangle$ zapiše binarno sumacija se raspisuje na način kao što je pokazano u (3.5)

$$\sum_{k=0}^{N-1} = \sum_{k_1=0}^{1} \sum_{k_2=0}^{1} \sum_{k_3=0}^{1} ... \sum_{k_n=0}^{1} . \tag{3.5}$$

Koristeći (3.5) i općeniti zapis binarnog broja dolazi se do

$$|\tilde{j}\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{\frac{2\pi i j \sum_{l=1}^{n} k_l 2^{n-l}}{2^n}} |k\rangle \tag{3.6}$$

$$= \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i j \sum_{l=1}^{n} k_l 2^{-l}} |k\rangle \tag{3.7}$$

$$= \frac{1}{\sqrt{N}} \sum_{k_1=0}^{1} ... \sum_{k_n=0}^{1} e^{2\pi i j \left(\sum_{l=1}^{n} k_l 2^{-l}\right)} |k_1 ... k_n\rangle \tag{3.8}$$

$$= \frac{1}{\sqrt{N}} \sum_{k_1=0}^{1} ... \sum_{k_n=0}^{1} \prod_{l=1}^{n} e^{2\pi i j k_l 2^{-l}} |k_l\rangle. \tag{3.9}$$

Direktno iz izraza (3.9) se teško zaključuje o utjecaju na stanje kvantnog bita. Iz tog razloga korisno je raspisati produkte i doći do izraza

$$|\tilde{j}\rangle = \frac{1}{\sqrt{N}} \left[\left(|0\rangle + e^{\frac{2\pi i j}{2^1}} |1\rangle \right) \otimes \left(|0\rangle + e^{\frac{2\pi i j}{2^2}} |1\rangle \right) \otimes ... \otimes \left(|0\rangle + e^{\frac{2\pi i j}{2^n}} |1\rangle \right) \right]. \tag{3.10}$$

Također, takav zapis od koristi je pri kreiranju algoritma za kvantni Fourierov transformat. Operacija kvantne Fourierove transformacije ukratko se može opisati kao prelazak iz baze $|j\rangle = |j_1 j_2 ... j_n\rangle = |j_1\rangle \otimes |j_2\rangle \otimes ... \otimes |j_n\rangle$ u bazu $|\tilde{j}\rangle$ koja je opisana izrazom (3.10). U izrazu (3.11) prikazani su prijelazi odgovarajućih članova iz baze

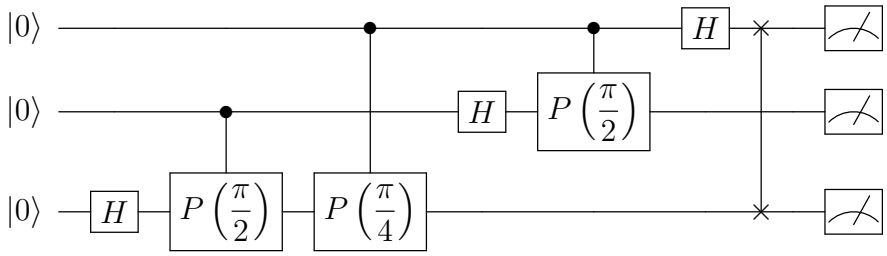
$|j\rangle$ u bazu $|\tilde{j}\rangle$ gdje je faktor $\frac{1}{\sqrt{N}}$ izostavljen zbog jednostavnosti

$$\begin{aligned}
|j_1\rangle &\longrightarrow \left(|0\rangle + e^{\frac{2\pi i j}{2^1}}|1\rangle\right) \\
|j_2\rangle &\longrightarrow \left(|0\rangle + e^{\frac{2\pi i j}{2^2}}|1\rangle\right) \\
&\vdots \\
|j_n\rangle &\longrightarrow \left(|0\rangle + e^{\frac{2\pi i j}{2^n}}|1\rangle\right)
\end{aligned} \tag{3.11}$$

Rezultati kvantne Fourierove transformacije sada su puno jasniji i lakše se može uvidjeti utjecaj na pojedini kvantni bit. Naime, izraz pojedinog člana u (3.10) sličan je rezultantnom izrazu nakon djelovanja Hadamardovih vrata na $|0\rangle$, a razlika leži u faktoru $e^{\frac{2\pi i j}{2^n}}$ ispred $|1\rangle$ koji predstavlja određenu fazu [6]. Od velikog je značaja primijetiti da su faze različite za pojedine članove u izrazu (3.10). Za potrebe kreiranja kvantnog kruga koji opisuje kvantnu Fourierovu transformaciju često se definiraju vrata R_k čiji je matrični zapis

$$R_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i}{2^k}} \end{pmatrix}. \tag{3.12}$$

Vodeći se zapisom (3.10), koristeći unitarne transformacije R_k koje su analogon P vratima, i Hadamardova vrata H može se kreirati kvantni krug koji opisuje kvantnu Fourierovu transformaciju:



(3.13)

Budući da su sva vrata u takvog sklopu unitarna zaključuje se da je kvantna Fourierova transformacija unitarna. Usporedbe radi, brza Fourierova transformacija koja je najbrži algoritam za računanje diskretne Fourierove transformacije na 2^n elemenata zahtjeva eksponencijalno puta više operacija da izračuna Fourierov transfor-

mat na klasičnom računalu, nego da implementira kvantni Fourierov transformat na kvantnom računalu.

4 Shorov algoritam

4.1 Uvod i cilj Shorovog algoritma

Peter Shor je 1994. godine pokazao da postoji algoritam koji bi koristeći kvantno računalo mogao faktorizirati broj N koji ima barem dva različita prosta faktora koristeći broj koraka koji raste polinomno s količinom unosa $\log_2 N$ [4]. Vremenska kompleksnost tj. količina računalnog vremena potrebna za izvođenje određenog algoritma uobičajeno se označava s velikom O notacijom primjerice $O(n)$, $O(n^\alpha)$, itd. gdje je n broj bitova koji se koristi za opis unosa, a α konstanta za koju vrijedi $\alpha > 1$. Vremenska kompleksnost $O(n)$ opisuje da se dani algoritam izvodi linearno u vremenu dok $O(n^\alpha)$ opisuje polinomni vremenski algoritam. Drugim riječima, vremenska kompleksnost algoritma $O(n^\alpha)$ raste polinomno s brojem bitova potrebnim za opis unosa. Budući da je cilj Shorovog algoritma faktorizirati velike brojeve - za koje je potrebno velik broj bitova, bitno je da vremenska kompleksnost raste što sporije s povećanjem broja bitova pri unosu. Konkretno, broj računalnih koraka $O(n)$ u Shorovom algoritmu za faktoriziranje broja N zadovoljava

$$O(N) \in O\left((log_2 N)^3 \, log_2 log_2 N\right) \tag{4.1}$$

za $N \to \infty$. 4.1 predstavlja vremensku kompleksnost nešto bržu od $O(n^3)$. Usporedbe radi, vremenska kompleksnost izvođenja istog procesa na klasičnom računalu bila bi $O(\mathrm{e}^{\left(\mathrm{cn}^{1/3}(\log \mathrm{n})^{2/3}\right)}$ gdje je c konstanta. Dakle, klasično, vremenska kompleksnost izvođenja istog algoritma raste brže nego polinomna, tj. onakva kakva se ostvaruje pri izvođenju Shorovog algoritma na kvantnim računalima.
Shorov algoritam bazira se na sljedećim činjenicama [7]:

- Faktorizacija broja N ekvivalentna je pronalasku perioda dane funkcije.
- Pronalazak tog perioda može biti ubrzan pomoću kvantnog algoritma.

Reformulacija faktorizacije kao problem pronalaska perioda bazirana je na rezultatima teorije brojeva bez kvantno-mehaničkih svojstava i procesa. Međutim, za provedbu cijelog algoritma na kvantnom računalu koristi se kvantni Fourierov transformat opisan u cjelini 3. Neka je $N \in \mathbb{N}$ neparan broj s minimalno dva različita prosta faktora. Cilj algoritma je pronaći djelitelj broja N.

a	0	1	2	3	4	5	6	7	8	9
$x = a(\text{mod } 4)$	0	1	2	3	0	1	2	3	0	1

Tablica 4.1: Vrijednosti funkcije $a(\text{mod } 4)$ za vrijednosti a od 0 do 9.

r	0	1	2	3	4	5	6	7	8	9
$x = 13^r(\text{mod } 15)$	1	13	4	7	1	13	4	7	1	13

Tablica 4.2: Vrijednosti funkcije $13^r(\text{mod } 15)$ za vrijednosti r od 0 do 9.

4.2 Modularna aritmetika

Neka su $x, a \in \mathbb{N}$ i neka je $\frac{x-a}{N}$ prirodni broj. U tom slučaju x i a su kongruentni u odnosu na N. Primjerice, neka je $x = 43$, $a = 27$ i $N = 4$. Tada je $\frac{43-27}{4} = 4$ iz čega se može zaključiti da su brojevi 43 i 27 kongruentni u odnosu na 4. Matematički se kongruencija opisuje kao $x = a(\text{mod } N)$ tj. u maloprije navedenom slučaju $43 = 27(\text{mod } N)$. Nadalje, da brojevi x, a imaju isti ostatak nakon dijeljenja s brojem 4 može se dobiti preko jednostavne formule $x(\text{mod } N)$ odnosno $a(\text{mod } N)$. Konkretno, $43(\text{mod } N) = 2$ i $27(\text{mod } N) = 2$. Modularna aritmetika je aritmetika kongruencija. U modularnoj aritmetici definira se niz brojeva $a_N = (0, 1, 2, ..., N-1, 0, 1, 2, ...)$ koji za primjer gdje je $N = 12$ može poprimiti vrijednosti $a_{12} = (0, 1, 2, ..., 11, 0, 1, 2, ...)$. Dakle, u trenutku kada niz a_N dostigne vrijednost N, niz kreće iznova, počevši od 0. Primjer takvog niza su sati, kutovi $\theta \in [0, 2\pi]$, itd. Očito je da su takvi nizovi periodični. U tablici 4.2 dan je primjer periodičnog ponašanja funkcije $x = a \pmod N$ za $N = 4$. Iz tablice 4.2 može se lako zaključiti da se kongruencija dvaju brojeva x, a u odnosu na treći N može zapisati kao

$$x = a(\text{mod } N) \qquad \longrightarrow \qquad x = Nk + a \qquad \text{za } k \in \mathbb{Z}. \tag{4.2}$$

Međutim, u Shorovom algoritmu cilj je odrediti stupanj funkcije $a^r \text{mod } N$ gdje je stupanj označen s r. Stupanj je onaj r koji odgovara članu niza $a_n = (0, 1, 2, ..., N-1, 0, 1, 2, ...)$ koji dolazi po prvi puta nakon $N-1$. Drugim riječima, stupanj r je član niza pri kojem niz dostigne vrijednost N po prvi put. Može se primijetiti da r iznosom odgovara periodu. Oblik funkcije opisan s $a^r \text{mod } N$ zove se modularna eksponencijacija i jedna je od ključnih stvari u Shorovom algoritmu. Primjer periodičnog ponašanja takve funkcije dan je u tablici 4.2.

4.3 Procedura

Procedura Shorovog algoritma [7] za dani broj N sastoji se od tri koraka:

1. Odaberi broj a, $(1 < a < N)$ takav da je najveći zajednički djelitelj (*engl. greatest common divisor*, skraćeno gcd) brojevima a, N broj 1

2. Pronađi stupanj r funckije $a^r (\text{mod } N)$.

3. Ako je r paran onda je $a^{r/2} (\text{mod } N) = x$.
   Ako je $x + 1 \neq 0 (\text{mod } N)$ onda su faktori broja N brojevi p i $q$odnosno $N = pq$:

$$\{p, q\} = \{\text{gcd}(x + 1, N), \text{gcd}(x - 1, N)\} \tag{4.3}$$

   Inače: Odaberi drugi a i ponovi korake $1.$ do $3.$

Prvi korak jednostavan je i jasan - potrebno je proizvoljno odabrati broj a između 1 i N takav da zadovoljava $\text{gcd}(a, N) = 1$. U drugom koraku potrebno je pronaći stupanj r kao što je učinjeno u tablici 4.2. Nakon što je pronađen stupanj razmatra se da li je paran ili ne. Ako stupanj funkcije nije paran potrebno je vratiti se na korak $1.$ i odabrati novi a. U slučaju da je r paran određuje se vrijednost $x = a^{r/2} (\text{mod } N)$. Potom, provjerava se da li dobiveni x zadovoljava $x + 1 \neq 0 (\text{mod } N)$. Ako je i taj kriterij zadovoljen slijedi da je barem jedan netrivijalni faktor broja $N = pq$ dan s

$$\{p, q\} = \Big\{\text{gcd}\left(x + 1, N\right), \text{gcd}\left(x - 1, N\right)\Big\}, \tag{4.4}$$

a u protivnom potrebno je odabrati novi a i proći kroz sve korake algoritma ispočetka. Konkretni primjeri za faktorizaciju brojeva $N = 15, 21, 35$ koristeći ovakvu proceduru algoritma dani su u nastavku.

Procedura algoritma za $N = 15$

1. Neka je $a = 13$

2. Stupanj r za $a = 13$ već je pronađen u tablici 4.2 i iznosi 4.

3. Je li r paran ? - Broj 4 je paran.
   Računa se x:

$$x = 13^{r/2} (\text{mod } 15)$$
$$x = 13^2 (\text{mod } 15)$$
$$x = 4$$

   Je li $x + 1 \neq 0 (\text{mod } N)$?

$$x + 1 = 5 \neq 0 (\text{mod } N)$$

   Zaključuje se da je i taj uvjet ispunjen.
   Slijedi da je

$$\{p, q\} = \left\{ \text{gcd}\,(5, 15)\,, \text{gcd}\,(3, 15) \right\}$$
$$\{p, q\} = \{5, 3\}$$

   Zaključuje se da su faktori broja $N = 15$ brojevi 3 i 5.

Procedura za $N = 21$

1. Neka je $a = 8$

2. Pomoću sljedeće tablice može se odrediti stupanj r

r	0	1	2	3	4	5	6	7	8	9
$x = 8^r (\text{mod } 21)$	1	8	1	8	1	8	1	8	1	8

   Iz tablice vidi se da je $r = 2$

3. Je li r paran ? - Broj 2 je paran.
   Računa se x:

$$x = 8^{r/2} (\text{mod } 21)$$
$$x = 8^1 (\text{mod } 21)$$
$$x = 8$$

   Je li $x + 1 \neq 0 (\text{mod } N)$?

$$x + 1 = 9 \neq 0 (\text{mod } 21)$$

   Zaključuje se da je i taj uvjet ispunjen.
   Slijedi da je

$$\{p, q\} = \left\{ \text{gcd}\,(9, 21)\,, \text{gcd}\,(7, 21) \right\}$$
$$\{p, q\} = \{3, 7\}$$

   Zaključuje se da su faktori broja $N = 21$ brojevi 3 i 7.

Procedura za $N = 35$

1. Neka je $a = 4$

2. Pomoću sljedeće tablice može se odrediti stupanj r

r	0	1	2	3	4	5	6	7	8	9
$x = 4^r (\text{mod } 35)$	1	4	16	29	11	9	1	4	16	29

   Iz tablice vidi se da je $r = 6$

3. Je li r paran ? - Broj 6 je paran.
   Računa se x:

$$x = 4^{6/2} (\text{mod } 35)$$
$$x = 4^3 (\text{mod } 35)$$
$$x = 29$$

   Je li $x + 1 \neq 0 (\text{mod } N)$?

$$x + 1 = 30 \neq 0 (\text{mod } 35)$$

   Zaključuje se da je i taj uvjet ispunjen.
   Slijedi da je

$$\{p, q\} = \left\{ \text{gcd}\,(30, 35)\,, \text{gcd}\,(28, 35) \right\}$$
$$\{p, q\} = \{5, 7\}$$

   Zaključuje se da su faktori broja $N = 35$ brojevi 5 i 7.

5 Implementacija Shorovog algoritma

5.1 IBM Quantum Composer

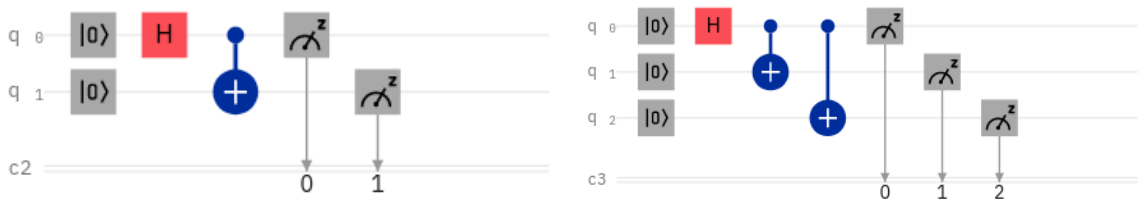
Američka tvrtka *International Bussines Machines,* skraćeno IBM omogućila je 2016. godine javnu dostupnost kvantnih računala. Usluzi je moguće pristupiti putem poveznice `https://quantum-computing.ibm.com/`. Na toj poveznici moguće je odabrati opciju *IBM Quantum Composer*. *IBM Quantum Composer* je grafičko korisničko sučelje koje omogućuje izvođenje kvantnih algoritama jednostavnim povlačenjem i ispuštanjem ikona koje predstavljaju određena kvantna vrata. Također, postoji i mogućnost korištenja *IBM Quantum Lab*-a koji omogućuje implementiranje kvantnih algoritama putem programskog koda. U 2021. godini, ime *IBM Quantum Experience* je umirovljeno, a do tog trenutka predstavljalo je kombinaciju *IBM Quantum Composer*-a i *IBM Quantum Lab*-a. Skup kvantnih vrata s kojima je moguće manevrirati unutar sučelja moguće je podijeliti na nekoliko skupina:

- Klasična vrata:$\{X, I, CX, CCX, SWAP\}$
- Fazna vrata:$\{S, S^\dagger, T, T^\dagger, Z, RZ, P(\lambda)\}$
- Kvantna vrata:$\{U(\lambda, \varphi, \vartheta), SX, SXdg, Y, RX, RY, RXX, RYY\}$
- Hadamardova vrata:$\{H\}$
- Neunitarne operacije:
  Mjerenje, operacija ako (engl. *if*), upravljani modifikator vrata, barijera, $|0\rangle$

Analogon jednostavnog kvantnog kruga (2.37) koji rezultira spregnutim stanjem, kao i kvantni krug koji rezultira GHZ stanjem u *IBM Quantum Composer*u prikazani su na (5.1).

5.1.1 QASM, Simulator i Qiskit

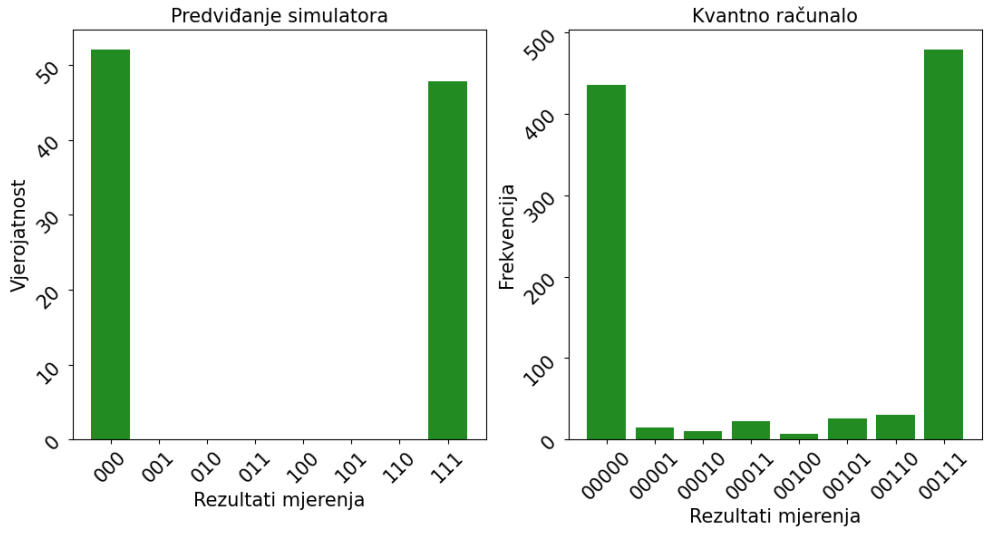
Unutar grafičkog sučelja postoji opcija unošenja programskog koda koristeći jezik *Open Quantum Assembly Language,* skraćeno QASM. Kod se generira sukladno implementiranju određenih kvantnih vrata u *IBM Quantum Composer*-u. Primjer QASM programskog koda za kvantni krug koji rezultira spregnutim stanjem na slici 5.1 (lijevo) je



Slika 5.1: Kvantni krug (2.37) koji rezultira spregnutim stanjem (2.46) (lijevo) i kvantni krug koji rezultira GHZ stanjem (desno) u *IBM Quantum Experience*. Slike su preuzete direktno iz *IBM Quantum Composer*-a.

```
OPENQASM 2.0;
include "qelib1.inc";
qreg q[2];
creg c[2];
reset q[0];
reset q[1];
h q[0];
cx q[0],q[1];
measure q[0] -> c[0];
measure q[1] -> c[1];
```

Uz QASM i sučelje za povlačenje i ispuštanje ikona koja predstavljaju kvantna vrata moguće je uživati i u simulaciji koja rezultira grafom na kojem su prikazane vjerojatnosti rezultantnih stanja. Taj graf se ažurira shodno implementiranju kvantnih vrata. Primjer takvog grafa za implementirano GHZ stanje prikazan je na slici (5.2). Međutim, taj graf je simulacija - matematički izračun računala koji govori kakve bi rezultate trebali dobiti. Naime, za prave rezultate potrebno je pokrenuti algoritam na stvarnom kvantnom procesoru. Procesuiranje algoritma na pravom kvantnom procesoru može izazvati određene greške izazvane šumom koji je rezultat dekoherencije i neposluha kvantnih vrata (engl. *gate infidelity*). Neposluh kvantnih vrata rezultat je postojanja razlike između dostupnih kvantnih vrata u *IBM Quantum Composer*-u i pravih, fizikalno implementiranih kvantnih vrata [8]. S druge strane, dekoherencija je proces gdje kvantno računalo gubi kvantno-mehanička svojstva i počinje se ponašati sve sličnije klasičnom objektu. Dekoherencija zajedno s neposluhom kvantnih vrata predstavlja prepreku u dobivanju savršeno točnih rezultata koristeći kvantno računalo. Na slici 5.2 prikazana je usporedba simulatora i rezultata dobive-

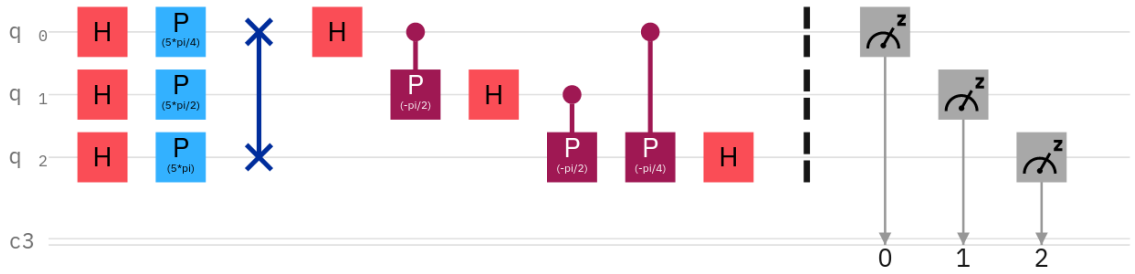


Slika 5.2: Usporedba vjerojatnosti rezultantnih kvantnih stanja predviđena računalnom simulacijom (lijevo) i dobivenih rezultata (desno) korištenjem stvarnog kvantnog procesora.

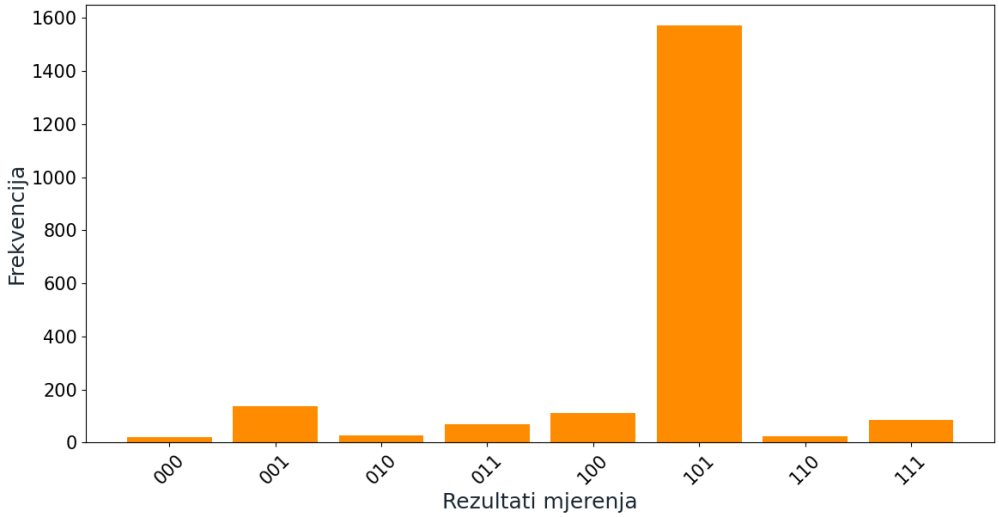
nih pokretanjem programa na pravom računalu. Promatrajući sliku može se zaključiti da se simulacija savršeno ne preklapa s dobivenim rezultatima. Razliku je najlakše uočiti uviđajući da su na rezultatima dobivenih izvođenjem algoritma na pravom kvantnom računalu osim $|000\rangle$ i $|111\rangle$ stanja, zabilježena i druga stanja koja nisu predviđena simulacijom. Drugi dio bivšeg *IBM Quantum Experience*-a je *IBM Quantum Lab* unutar kojeg je moguće kreirati kvantne programe putem biblioteke *Qiskit*. Qiskit je razvijen s ciljem kreiranja programskog koda koji će omogućiti izvođenje programa na IBM-ovim procesorima ili simulatorima. Pomoću Qiskit-a je moguće pokretati kvantne programe bez grafičkog sučelja što je od velike važnosti jer grafička sučelja postaju sve nepraktičnija s porastom broja iskorištenih kvantnih bitova.

5.2 Implementacija Shorovog algoritma u grafičkom sučelju IBM Quantum Composer-a

Kvantni krug prikazan na (3.13) nije od praktične koristi jer su svi kvantni bitovi u jednakim superpozicijama $|0\rangle$ i $|1\rangle$ pa će rezultat biti potpuno nasumičan. Kvantni Fourierov transformat može se koristiti i u suprotnom smjeru. Primjerice, stvaranjem stanja $|\tilde{5}\rangle$ i djelovanjem inverznog kvantnog Fourierovog transformata na to stanje može se pokazati da će rezultat pokretanja algoritma na kvantnom računalu biti $|5\rangle$.

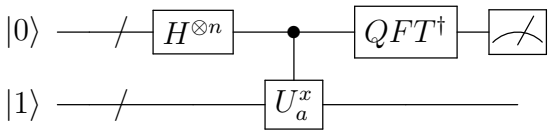


Slika 5.3: Kvantni krug za izvođenje kvantnog Fourierovog transformata za tri kvantna bita u IBM Quantum Composer-u. Slika je preuzeta izravno iz *IBM Quantum Composer*-a.

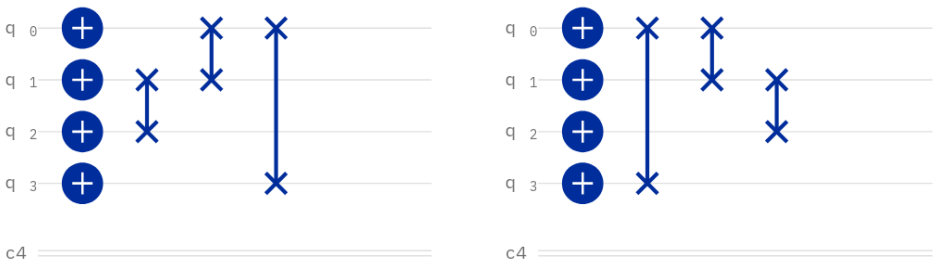


Slika 5.4: Rezultati dobiveni izvođenjem kruga 5.3 na kvantnom računalu.

Kvantni krug koji to i dokazuje prikazan je na slici 5.3. Dobiveni rezultati nakon pokretanja tog algoritma na kvantnom računalu prikazani su na slici 5.4. Ovakav oblik kvantnog Fourierovog transformata koristi se pri izvođenju Shorovog algoritma. Često se cijeli kvantni krug prikazan na slici 5.3 bez Hadamardovih i P vrata, dakle počevši sa $SWAP$ vratima, označuje kao operator s oznakom $QFT^{\dagger}$. Operator $QFT^{\dagger}$ može djelovati na proizvoljni broj n kvantnih bitova, a kao takav se koristi u znanstvenim radovima pri opisu raznih algoritama. Primjer kvantnog kruga u kojem je iskorišten operator $QFT^{\dagger}$ je:



(5.5)

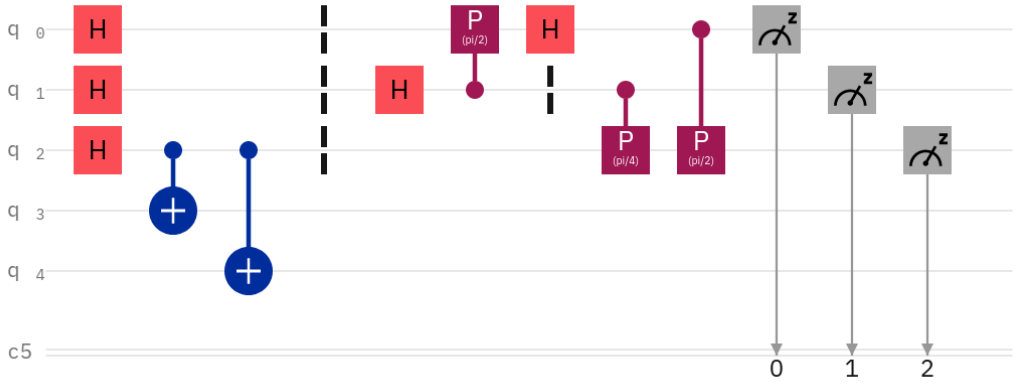


Slika 5.5: Kvantni krug koji mapira $|x\rangle$ u $|7^x \text{mod} 15\rangle$ (lijevo) odnosno u $|13^x \text{mod} 15\}$ (desno). Slike su preuzete direktno iz *IBM Quantum Composer*-a.

Krug (5.5) upravo prikazuje proceduru određivanja perioda koja je srž Shorovog algoritma. Prvi, gornji registar sastoji se od n kvantnih bitova i zove se upravljani. Drugi, donji registar zove se radni registar i sastoji se od m kvantnih bitova [16]. Broj bitova potrebnih za upravljani registar je $n = 2[log_2 N]$ dok je za radni registar potrebno $m = [log_2 N]$ kvantnih bitova [18]. Procedura kvantnog algoritma prikazanom na (5.5) može se ukratko opisati u nekoliko koraka:

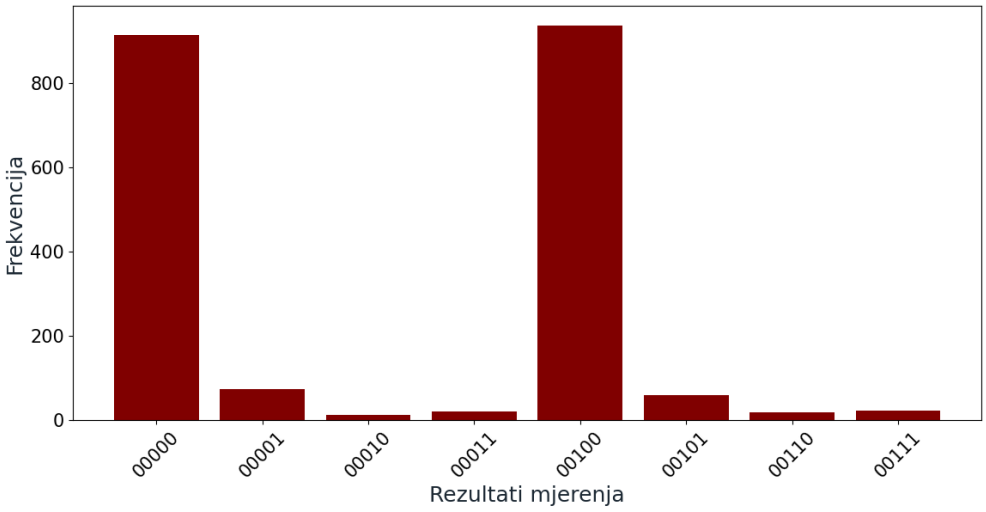
1. Djelovanje Hadamardovih vrata na n kvantnih bitova u upravljanom registru
2. Modularna eksponencijacija
3. Inverzni kvantni Fouerierov transformat
4. Mjerenje upravljanog registra

Korake $1.$ i $4.$ jednostavno je implementirati. Naime, potrebno je djelovati Hadamardovim vratima na početku, odnosno operacijom mjerenja na kraju algoritima samo na upravljani registar. Najsloženiji dio pri implementaciji Shorovog algoritma predstavlja korak 2. - modularna eksponencijacija. Naime, za svaku kombinaciju N i a potrebno je koristiti specifični algoritam. Raznovrsni algoritmi za modularnu eksponencijaciju mogu se naći u radovima [14] i [17]. Dva primjera iz [14] prikazana su na slici 5.5. To su primjeri najjednostavnijih algoritama koji se mogu iskoristiti za faktoriziranje broja $N = 15$. Međutim, algoritmi za faktorizaciju većih brojeva znatno su kompliciraniji, a neki od njih mogu se pronaći u [14]. Budući da je implementacija koraka 3. - kvantna Fourierova transformacija već pokazana, sada je vrijeme ujediniti pojedine korake 1.-4. i konstruirati krug za izvođenje Shorovog algoritma za faktorizaciju cijelog broja $N = 15$ s $a = 11$ na kvantnom računalu koristeći *IBM Quantum*



Slika 5.6: Optimizirani Shorov algoritam za $N = 15$ i $a = 11$. Slika je preuzeta direktno iz *IBM Quantum Composer*-a.

Composer. Kvantni krug prikazan je na slici 5.6. Motivacija za izradu ovog kvantnog kruga potaknuta je optimizacijom koja je predložena u [18]. Rezultati dobiveni pokretanjem tog kvantnog kruga na kvantnom računalu prikazani su na slici 5.7. Iz grafa na slici 5.7 vidi se da su dobiveni rezultati periodi 00000 i 00100 odnosno brojevi 0 i 4 u decimalnom zapisu. Primjećuje se da su rezultati dobiveni s velikom vjerojatnošću jer su ostali brojevi izmjereni samo nekoliko puta. Rješenje 0 se odbacuje kao trivijalno rješenje. S druge strane rješenje 4 uzima se kao dobro rješenje. Međutim, 4 u ovom slučaju nije period - to je vrijednost koja se često označuje s y a zadovoljava jednadžbu $y = \frac{M}{r}$. Do perioda r moguće je doći dijeljenjem broja 2, podignutim na potenciju ulaznih kvantnih bitova u upravljanom registru $(2^n) = M$ s dobivenim periodom r. U ovom slučaju broj ulaznih kvantnih bitova korišten u upravljanom registru je 3 - to su oni kvantni bitovi na kojima se djeluje Hadamardovim vratima u prvom koraku algoritma. Slijedi da je period za danu situaciju: $\frac{2^3}{4} = 2$. Klasičnim računom funkcije $f(r) = 11^r \text{mod} 15$ može se provjeriti točnost dobivenog perioda. Uvrštavanjem niza brojeva $0, 1, 2, 3, 4, ...$ slijedi niz $1, 11, 1, 11, 1, ...$, iz čega se zaključuje da je 2 traženi period funkcije. Za određivanje faktora broja 15 sada je moguće koristiti klasični dio algoritma opisan u cjelini 4:



Slika 5.7: Rezultati dobiveni izvođenjem kvantnog kruga prikazanom na slici 5.6 na kvantnom računalu s pet kvantnih bitova.

$$
\begin{aligned}
\{p, q\} &= \text{gcd}\{a^{r/2} \pm; N\} \\
\{p, q\} &= \text{gcd}\{a - 1, N\}, \text{gcd}\{a - 1, N\} \\
\{p, q\} &= \text{gcd}\{11 - 1, 15\}, \text{gcd}\{10 - 1, 15\} \\
\{p, q\} &= \{3, 5\}
\end{aligned}
\tag{5.6}
$$

Na krugu prikazanom na slici 5.6 mogu se jasno uočiti pojedini koraci izvođenja algoritma:

1. Djelovanje Hadamardovim vratima na tri kvantna bita u upravljanom registru.
2. Modularna eksponencijacija optimizirana sa samo dvama kvantnim vratima - CX i CCX.
3. Kvantni Fourierov transformat kojeg čine kombinacija Hadamrdovih i P vrata
4. Mjerenje

6 Zaključak

Tema ovog diplomskog rada bio je Shorov algoritam, a glavni cilj bila je implementacija Shorovog algoritma koristeći grafičko sučelje *IBM Quantum Composer*. Shorov algoritam implementiran je kao što je prikazano na slici 5.6. Dobiveni rezultati uspoređeni su s onima koje predviđa simulator. Također, točnost dobivenog rezultata provjerena je klasičnim putem kao što je pokazano u (5.6). Zaključuje se da se rezultati podudaraju s predviđanjima. Rezultati nisu savršeni na što upućuju izmjerena stanja koja nisu predviđena simulatorom i ne predstavljaju dobro rješenje. Ipak, usporedbom tih rezultata s rezultatima koji su dobiveni za isti kvantni krug u radu [8] iz 2020. godine zaključuje se da je kvantna korekcija grešaka znatno napredovala u tom periodu. Pri implementiranju kvantnog kruga korišten je procesor s pet kvantnih bitova. Za faktoriziranje većih brojeva potreban je veći broj ulaznih kvantnih bitova što znatno otežava kreiranje kvantnih krugova koji će rezultirati izvođenjem Shorovog algoritma u *IBM Quantum Composer*-u. Najveći razlog otežavanja implementacije na takav način je dio algoritma koji provodi modularnu eksponencijaciju. Naime, modularna eksponencijacija za malo veće brojeve zahtijevala bi korištenje jako velikog broja kvantnih vrata. Porastom broja ulaznih kvantnih bitova, kvantna Fourierova transformacija postaje također kompliciranija. Rezultat toga bio bi krug koji bi čitatelju bio iznimno nepregledan i nerazumljiv. Iz tog razloga očekuje se sve veća upotreba *Qiskit*-a koji koristi programski jezik *Python*. Korištenje *Qiskit*-a također je javno dostupno u drugom dijelu bivšeg *IBM Quantum Experience*-a, *IBM Quantum Lab*-u. Sljedeći korak mogla bi upravo biti implementacija Shorovog, ili nekog drugog algoritma koristeći *Qiskit*.

7 Metodički dio: Fotoelektrični učinak

7.1 Nastavna priprema: Fotoelektrični učinak

Nastavna priprema koja će biti predstavljena u ovom poglavlju namijenjena je za jedan školski sat u četvrtom razredu opće gimnazije. Nastavna jedinica koja će biti obrađena je *"Fotoelektrični učinak"*. Vrsta nastave za koju je prilagođena ova priprema je istraživački usmjerena nastava. Cilj istraživački usmjerene nastave je učiniti nastavu što je više moguće interaktivnom — teži se k tome da svi učenici

budu uključeni iznošenjem svojih predviđanja, postavljanjem pitanja i donošenjem zaključaka. Nastavna pomagala i sredstva koja bi se koristila pri izvođenju ovog sata su računalo, projektor, elektroskop s metalnom pločicom, plastični štap, živina ultraljubičasta lampa, lampa bijele svjetlosti i kartice s oznakama A,B,C,D. Nastavne metode koje se koriste su metoda razgovora — razredna rasprava, metoda usmenog izlaganja, metoda pisanja i crtanja i konceptualna pitanja s karticama. Nastavnik može očekivati da učenici, po završetku sata usvoje znanja opisana sljedeći predmetnim ishodima. Literatura koja se koristila za izradu ove pripreme je [22] - [25].

Predmetni ishodi:

- FIZ SŠ A.4.3. , D.4.3. Analizira valno-čestičnu prirodu svjetlosti i tvari
  Razrada ishoda:
  1. Matematički opisuje i analizira fotoelektrični učinak
  2. Opisuje kako intenzitet i frekvencija utječu na fotoelektrični učinak
- FIZ SŠ. A.4.9. D.4.9. Rješava fizičke probleme
  Razrada ishoda:
  1. Identificira ciljeve rješavanja problema
  2. Konstruira plan rješavanja problema
  3. Matematički modelira situacije
  4. Zaključuje iz grafičkih prikaza
- FIZ SŠ.ABCD.4.10. Istražuje fizičke pojave
  Razrada ishoda:
  1. Istražuje pojavu uz pomoć računalne simulacije.

Međupredmetni ishodi:

1. uku A.4/5.1. Upravljanje informacijama
2. uku A.4/5.2. Primjena strategija učenja i rješavanje problema
3. uku A.4/5.4. Kritičko mišljenje
4. uku A.4/5.3. Kreativno mišljenje

TIJEK NASTAVNOG SATA

Uvodi dio sata

Sat započinjemo uvodnim pitanjem:

Na koji način solarne ćelije pretvaraju sunčevu energiju u električnu energiju?

Prikupljanjem učeničkih mišljenja i komentiranjem istih nastavnik pokušava dobiti uvid u njihov način razmišljanja.

Opservacijski pokus:

Elektroskop s metalnom pločicom nabije se plastičnim štapom tako da se kazaljka odmakne za određeni kut.

Zašto se kazaljka elektroskopa odmiče?

Ovo pitanje nastavnik postavlja jer želi navesti učenike na razmišljanje o prelasku elektrona sa štapa na elektroskop.
Metalna pločica osvjetljuje se bijelom svjetlošću.

Što ste opazili?

Otklon kazaljke elektroskopa ostao je isti.
Metalna pločica se zatim osvjetljuje živinom ultraljubičastom lampom.

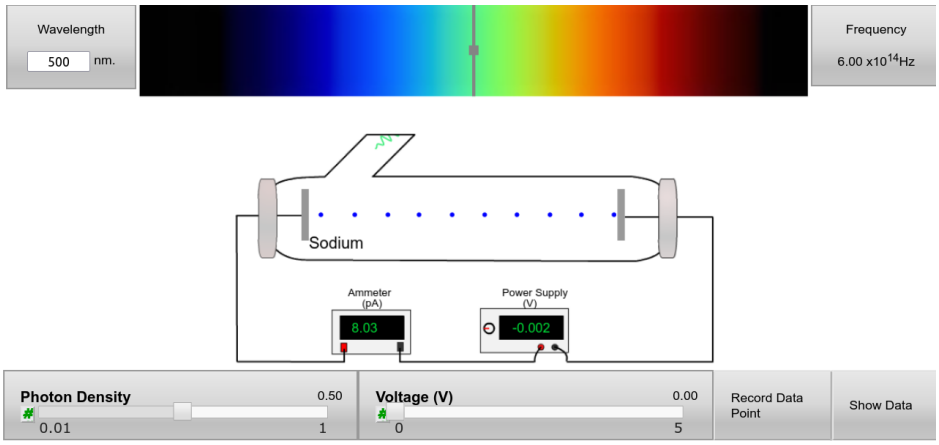
Što ste sada opazili?

Otklon kazaljke elektroskopa se smanjio i cilj nam je da učenici to uoče. Iz tog razloga po potrebi ponavljamo pokus nekoliko puta.

Zašto se kazaljka elektroskopa pomiče u ovom slučaju?

Učenici uočavaju da **osvjetljavanjem metalne pločice ultraljubičastom živinom lampom dolazi do izbijanja elektrona iz metalne pločice**. Uvodimo naziv pojave, fotoelektrični učinak, i opisujemo je kao pojavu pri kojoj elektromagnetsko zračenje izbija elektrone iz materijala. Piše se naslov: ”**Fotoelektrični učinak**”.

Središnji dio sata



Slika 7.1: Prikaz postava na simulaciji koji će se koristiti za istraživanje povezanosti kinetičke energije i frekvencije.

Istraživačko pitanje:

Kako kinetička energija izbijenih elektrona ovisi o frekvenciji, valnoj duljini i intenzitetu upadnog elektromagnetskog zračenja?

- *Možete li predložiti način na koji bi se mogla ispitati ta povezanost?*
- *Što ćemo mjeriti?*
- *Kako ćemo izmjeriti kinetičku energiju?*

Cilj ovih pitanja je da učenici prepoznaju da je potrebno mijenjati frekvenciju i mjeriti kinetičku energiju gdje nailaze na problem.
Opisujemo postav na simulaciji koji je prikazan na 7.1:
Katoda se osvjetljava elektromagnetskim zračenjem koje dolazi iz lampe. Intenzitet zračenja je moguće mijenjati. Katoda igra ulogu metalne pločice iz pokusa izvedenog u uvodnom dijelu. U simulaciji moguće je promijeniti materijal koji će biti osvijetljen. Nasuprot katode nalazi se anoda, a kolektivno se nazivaju fotoćelija. Katoda i anoda su zatvorene u vakuumsku cijev. Katoda je emiter tj. emitira elektrone, dok je anoda kolektor koji apsorbira elektrone emitirane iz katode. Budući da postoji usmjereno gibanje elektrona može se govoriti o struji kroz vakuumsku cijev. Ampermetar kojim je moguće izmjeriti struju i baterija pomoću koje je moguće mijenjati napon u strujnom krugu spojeni su na fotoćeliju. U cilju dolaska do odgovora na pitanje *Kako ćemo mjeriti kinetičku energiju elektrona?* učenike navodimo do točnog odgovora sljedećim pitanjima.

- *Kako bi se izbijeni elektroni gibali u slučaju kada bi katoda bila negativno nabijena, a anoda pozitivno nabijena?*

  - Elektroni će ubrzavati prema anodi.

- *Što se događa s kinetičkom energijom elektrona tijekom putovanja od katode do anode?*

  - Kinetička energija elektrona se povećava.

- *Vrši li električna sila pozitivan ili negativan rad na elektron tijekom putovanja od katode do anode?*

  - Električna sila vrši pozitivan rad jer se energija elektrona povećava ili električna sila vrši pozitivan rad jer je smjer sile jednak pomaku elektrona.

Učeničke pretpostavke provjeravaju se koristeći simulaciju.
Od učenika se traži da nacrtaju stupčasti dijagram energija za sustav samo jednog elektrona na putu od katode do anode u trenutku neposredno nakon izbijanja iz katode koji će se označiti s t_1, a trenutak neposredno prije stizanja do anode označit će se s t_2. Nakon što su učenici pokušali nacrtati stupčasti dijagram energija, komentiraju se predloženi dijagrami, a točan oblik dijagrama koji je prikazan na 7.2 prikazuje se na projektoru. Koristeći stupčasti dijagram, od učenika se traži da napišu jednadžbu energija. Učenici čitaju napisane jednadžbe. Nakon što su učenici dali svoje prijedloge, nastavnik na ploču piše točan oblik jednadžbe do koje je došao uz pomoć učenika.

$$KE_1 + W = KE_2 \tag{7.1}$$

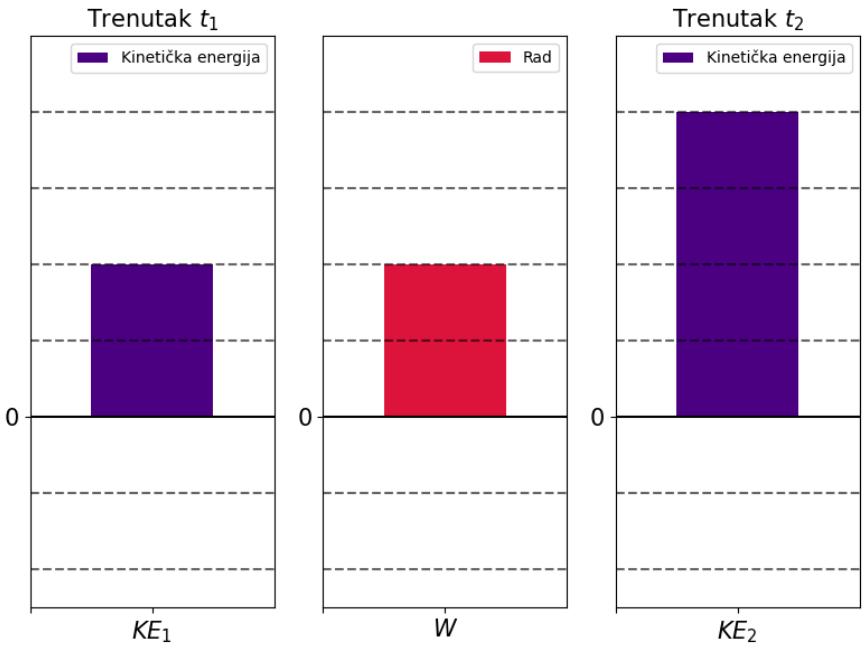
- *Kako bi se izbijeni elektroni gibali u slučaju kada bi katoda bila pozitivno nabijena, a anoda negativno nabijena?*

  - Elektroni pri gibanju od katode do anode usporavaju.

- *Što se događa s kinetičkom energijom elektrona tijekom putovanja od katode do anode?*

  - Kinetička energija elektrona se smanjuje.

- *Vrši li električna sila pozitivan ili negativan rad na elektron tijekom putovanja od katode do anode?*



Slika 7.2: Stupčasti dijagram koji prikazuje raspodjelu energija za sustav samo jednog elektrona na putu od katode do anode za slučaj kada je anoda pozitivno nabijena.

- Električna sila vrši negativan rad jer se energija elektrona smanjuje ili električna sila vrši negativan rad jer je smjer sile suprotan pomaku elektrona.

Od učenika se ponovno traži da nacrtaju stupčasti dijagram. Točan oblik stupčastog dijagrama prikazan je na 7.3.
Prisjećamo se formule za rad električne sile.

$$W = eU \tag{7.2}$$

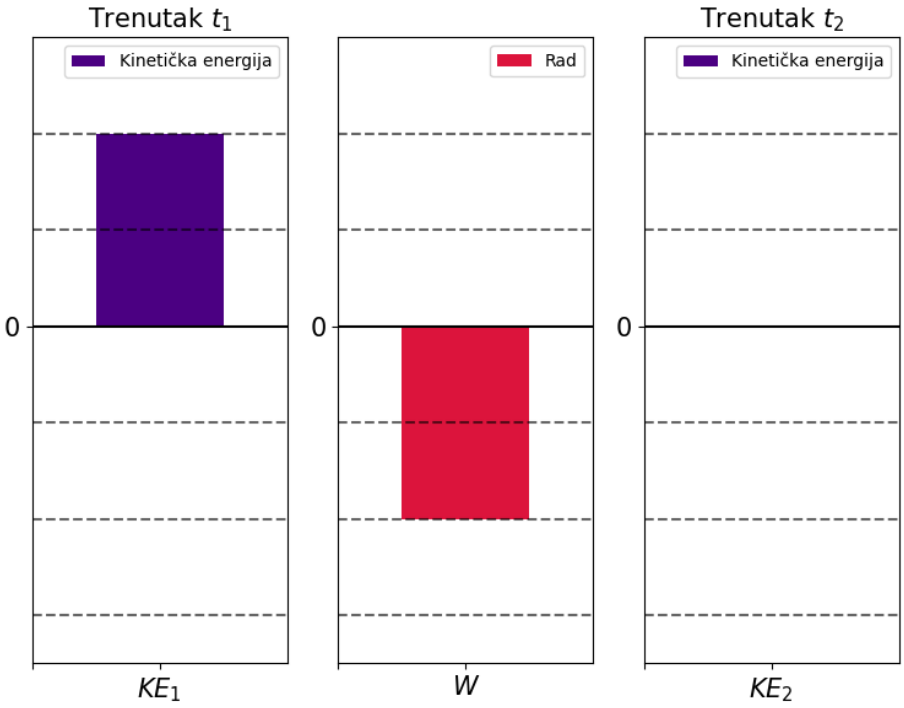
gdje je e naboj elektrona, a U napon.
Iz stupčastog dijagrama zaključuje se da je KE_2 jednaka 0. Vodeći se time jednadžba (2) poprima oblik:

$$KE_1 = eU \tag{7.3}$$

U jednadžbi (4) napon U se zove **zaustavni napon**. To je najmanji napon pri kojem elektroni ne uspiju doći do anode.

„Zaustavni napon omogućuje određivanje kinetičke energije koju je elektron imao pri izbijanju iz katode."

Ovisnost kinetičke energije izbijenih elektrona o frekvenciji ispitat će se mjerenjem valne duljine, frekvencije i zaustavnog napona sa simulacije. Cilj je namjestiti takav



Slika 7.3: Stupčasti dijagram koji prikazuje raspodjelu energija za sustav samo jednog elektrona na putu od katode do anode za slučaj kada je anoda negativno nabijena.

napon da se elektroni zaustave točno na anodi. Izmjerene vrijednosti unose se u tablicu. Podatke iz simulacije upisujemo u tablicu 7.1. Koristeći te podatke crtamo graf koji je prikazan na slici 7.4.

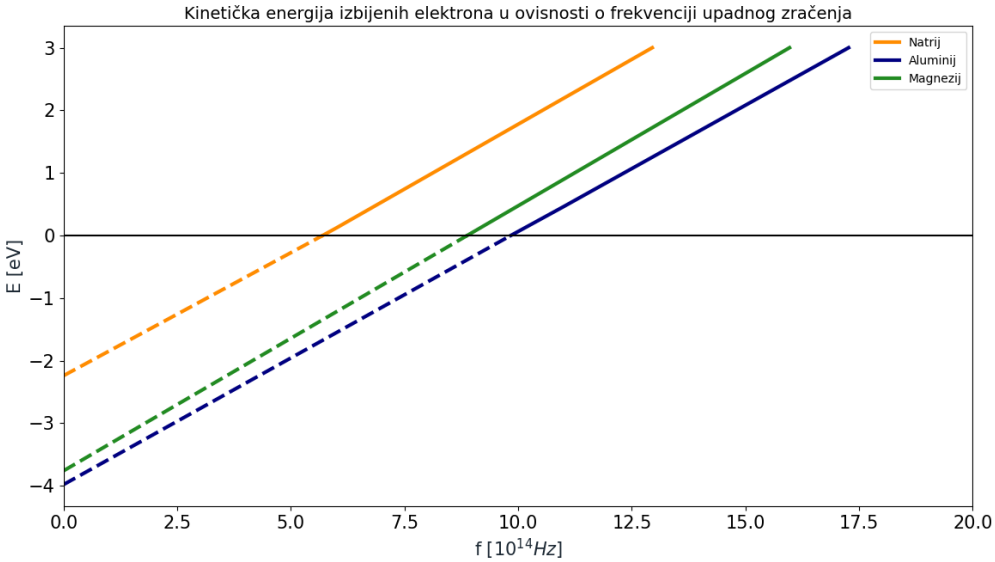
λ [nm]	f [Hz]	U_z [eV]	KE [eV]

Tablica 7.1: Tablica u koju zajedno s učenicima upisujemo podatke očitane sa simulacije. Koristeći podatke iz ove tablice, nacrtati ćemo graf ovisnosti kinetičke energije izbijenih elektrona o frekvenciji upadnog elektromagnetskog zračenja.

U korist određivanja jednadžbe koja matematički opisuje poveznicu između kinetičke energije izbijenih elektrona i frekvencije upadnog elektromagnetskog zračenja postavljamo učenicima sljedeća pitanja.

- *U kakvoj su ovisnosti kinetička energija izbijenih elektrona i frekvencija upadnog zračenja ?*

  - Kinetička energija izbijenih elektrona linearno raste s frekvencijom upadnog zračenja.



Slika 7.4: Graf ovisnosti kinetičke energije izbijenih elektrona o frekvenciji za natrij, aluminij, i magnezij.

- *Kako znamo da je ovisnost linearna, a ne proporcionalna?*

  - Iz razloga što graf ne kreće iz ishodišta.

- *Kako glasi općeniti oblik jednadžbe koja opisuje linearnu ovisnost?*

  $y = ax + b$

- *Koristeći tu jednadžbu, kako bi glasila jednadžba za ovisnost kinetičke energije izbijenih elektrona o frekvenciji upadnog elektromagnetskog zračenja?*

$$KE = hf + \phi \tag{7.4}$$

  gdje je h Planckova konstanta, a ϕ izlazni rad materijala.

Minimalna energija koja je potrebna da bi elektron bio izbijen iz metala zove se **izlazni rad**. Izlazni rad svojstvo je svakog materijala.

- *U kakvoj su ovisnosti kinetička energija izbijenih elektrona i valna duljina upadnog zračenja ?*

  - Kinetička energija izbijenih elektrona linearno se smanjuje s povećanjem valne duljine upadnog zračenja.

- *Kako bi glasila jednadžba za ovisnost kinetičke energije izbijenih elektrona o valnoj duljini upadnog elektromagnetskog zračenja?*

$$KE = h\frac{c}{\lambda} + b \tag{7.5}$$

Došli smo do jednadžbi koje opisuju ovisnost kinetičke energije o frekvenciji i valnoj duljini upadnog elektromagnetskog zračenja. Koristeći isti graf može se ispitati ovisnost kinetičke energije izbijenih elektrona o različitim vrstama materijala.

- *Što se može zaključiti iz grafa uspoređujući pravce za različite materijale, u ovom slučaju natrija, magnezija i aluminija?*

  - Pravci sijeku os apscisu u različitim točkama.

- *Što predstavljaju točke u kojima pravci sijeku os apscisu?*

  - Točka u kojoj pravac siječe os apscisu predstavlja frekvenciju upadnog zračenja pri kojoj počinju izbijati elektroni iz materijala tj. pri kojoj se počinje događati fotoelektrični učinak.

Frekvencija upadnog elektromagnetskog zračenja ispod koje nema fotoelektričnog učinka na materijalu zove se **granična frekvencija**.

- *Što predstavljaju točke u kojima zamišljeni produžeci pravaca sijeku os ordinatu?*

  - Točka u kojoj pravac siječe os ordinatu predstavlja energiju koja je potrebna da bi elektron bio izbijen iz metala. Ta energija odgovara izlaznom radu materijala.

- *Razlikuje li se vrijednost kinetičke energije izbijenih elektrona pri nekoj frekvenciji f za dva različita materijala?*

  - Iz grafa se može vidjeti da za neku frekvenciju f dva različita materijala nemaju istu vrijednost na ordinati. Drugim riječima, kinetička energija izbijenih elektrona razlikuje se ovisno o materijalu za istu frekvenciju upadnog zračenja.

Preostaje još ispitati ovisnost kinetičke energije izbijenih elektrona o intenzitetu upadnog elektromagnetskog zračenja. Ta ovisnost ispitat će se pomoću računalne simulacije, a prije vraćanja na simulaciju pita se učenike za pretpostavke. Odabere se

frekvencija ispod granične i drži se konstantnom kao i sve ostale varijable osim intenziteta upadnog zračenja.

- *Što primjećujete ?*

  - Nema fotoelektričnog učinka kakav god intenzitet odabrali.

Odabere se frekvencija iznad granične i drži se konstantnom kao i sve ostale varijable osim intenziteta upadnog zračenja.

- *Što sada primjećujete, što je različito od slučaja kada je bio odabran manji intenzitet?*

  - Broj izbijenih elektrona je veći kada je intenzitet upadnog zračenja veći.

- *Mijenja li se kinetička energija izbijenih elektrona povećanjem intenziteta upadnog zračenja ?*

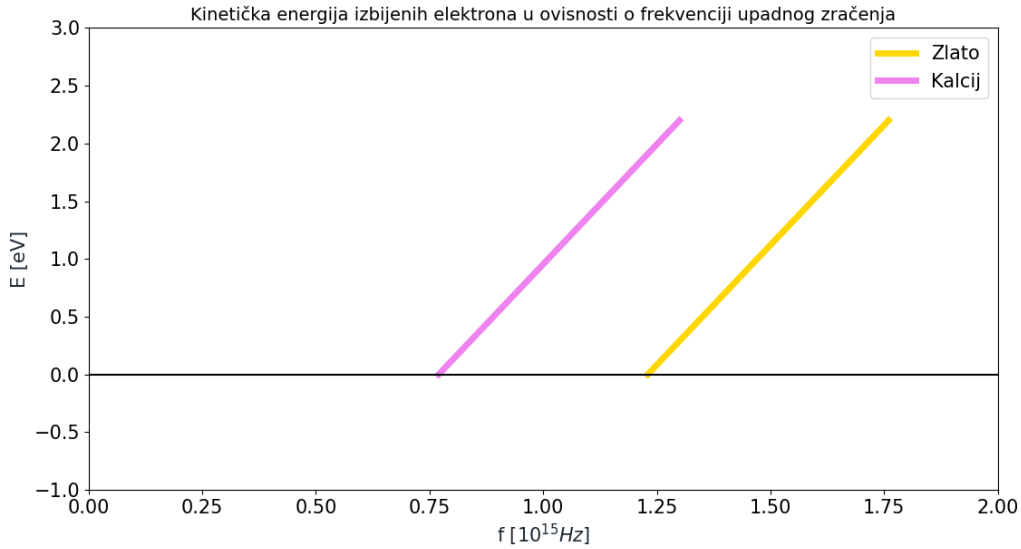
  - Kinetička energija elektrona se ne mijenja povećanjem intenziteta.

Konačno, zaključujemo da

- Kinetička energija izbijenih elektrona raste linearno s povećanjem frekvencije upadnog elektromagnetskog zračenja.
- Kinetička energija izbijenih elektrona smanjuje se linearno s povećanjem valne duljine upadnog elektromagnetskog zračenja.
- Kinetička energija izbijenih elektrona ne ovisi o intenzitetu upadnog elektromagnetskog zračenja.

Završni dio sata

Uvodno pitanje se ponovno diskutira s učenicima. Solarna ćelija se bazira na fotoelektričnom učinku, a elektroni koji se izbijaju uslijed upadnog sunčevog zračenja stvaraju struju. Naime, postoje materijali koji imaju takav izlazni rad da i frekvencija elektromagnetskog zračenja koje dolazi sa Sunca može rezultirati fotoelektričnim učinkom.
Završni dio sata sastoji se još od postavljanja konceptualnih pitanja. Učenici odgovaraju na pitanja prikazana na projektoru karticama koje na sebi imaju oznake A,B,C,D. Odgovori se diskutiraju i obrazlažu u razredu.



Slika 7.5: Ovisnost kinetičke energije izbijenih elektrona o frekvenciji upadnog zračenja za zlato i kalcij.

1. Koristeći graf odredi kod kojih materijala će doći do izbijanja elektrona ako upadno elektromagnetsko zračenje ima frekvenciju $10^{15}\ Hz$.

   A) Kod kalcija

   B) Kod zlata

   C) I kod kalcija i kod zlata

   D) Ni kod jednog materijala

   Točan odgovor je a) jer je dana frekvencija veća samo od granične frekvencije kalcija. Granična frekvencija odgovara točki u kojoj pravac siječe os apscisu.

2. Što će se dogoditi ako se poveća intenzitet upadnog zračenja koje izaziva foto-električni učinak na metalu?

   A) Smanjit će se broj izbijenih elektrona.

   B) Povećat će se kinetička energija izbijenih elektrona.

   C) Smanjit će se granična frekvencija metala.

   D) Povećat će se broj izbijenih elektrona.

Točan odgovor je d) jer intenzitet ne utječe na kinetičku energiju elektrona, već samo na broj izbijenih elektrona tako da broj izbijenih elektrona raste s povećanjem intenziteta upadnog zračenja.

3. Koja tvrdnja vrijedi za graničnu frekvenciju?

   A) Ona je na grafu ovisnosti kinetičke energije izbijenih elektrona o frekvenciji upadnog zračenja predstavljena točkom u kojoj pravac siječe os ordinatu.

   B) To je najveća frekvencija pri kojoj se događa fotoelektrični učinak.

   C) Ona je na grafu ovisnosti kinetičke energije izbijenih elektrona o frekvenciji upadnog zračenja predstavljena točkom u kojoj pravac siječe os apscisu.

   Točna tvrdnja je c). Tvrdnja a) je kriva jer točka u kojoj pravac siječe os ordinatu odgovara izlaznom radu. Tvrdnja b) je kriva jer granična frekvencija je najmanja, a ne najveća frekvencija pri kojoj se događa fotoelektrični učinak.

4. Što će se dogoditi ako smanjimo valnu duljinu upadnog elektromagnetskog zračenja?

   A) Smanjit će se frekvencija upadnog elektromagnetskog zračenja.

   B) Smanjit će se kinetička energija izbijenih elektrona.

   C) Povećat će se broj izbijenih elektrona.

   D) Povećat će se kinetička energija izbijenih elektrona.

   Točan odgovor je d). Tvrdnja a) je kriva je frekvencija upadnog elektromagnetskog zračenja će se povećati ako smanjimo valnu duljinu upadnog elektromagnetskog zračenja. Tvrdnja b) je kriva jer se u tom slučaju kinetička energija izbijenih elektrona povećava. Tvrdnja c) je kriva jer valna duljina ne utječe na broj izbijenih elektrona.

Dodaci

Dodatak A Osnovni koncepti u kvantnoj mehanici

A.1 Hilbertov prostor

A.1.1 Vektorski prostori

Ako je sustav zatvoren na neku operaciju, primjerice zbrajanja, onda je zbroj dva proizvoljna elementa iz tog sustava i dalje u tom sustavu što se matematički može opisati na sljedeći način

$$\text{za svaki } x \in V \text{ i svaki } y \in V \text{ vrijedi } x + y \in V$$

Neprazni skup V koji je zatvoren s obzirom na operacije:

$$(\mathrm{x}, \mathrm{y}) \mapsto \mathrm{x} + \mathrm{y} \text{ iz } V \times V \text{ u } V \text{ zvanom zbrajanje,}$$
$$(\lambda, \mathrm{x}) \mapsto \lambda \mathrm{x} \text{ iz } \mathbb{F} \times V \text{ u } V \text{ zvanom množenje,}$$

tako da $x, y, z \in V$ i $\alpha, \beta \in \mathbb{F}$ zadovoljavaju sjedećih 8 svojstava zove se vektorski prostor V .

1. $x + y = y + x$
2. $(x + y) + z = (x + z) + y$
3. za svaki $x, y \in V$ postoji $z \in V$ takav da je $x + z = y$
4. za svaki $x \in V$ postoji suprotni element $-x \in V$ takav da je $x + (-x) = 0$
5. $\alpha(\beta x) = (\alpha\beta)x$
6. $(\alpha + \beta)x = \alpha x + \beta x$
7. $\alpha(x + y) = \alpha x + \alpha y$

8. $1x = x$

Elementi u V zovu se vektori. Ako je $\mathbb{F} = \mathbb{R}$ onda V zovemo realni vektorski prostor, a ako je $\mathbb{F} = \mathbb{C}$ onda V zovemo kompleksni vektorski prostor [19].

A.1.2 Skalarni produkt

Neka su $x = (x_1 + x_2 + ... + x_n)$ i $y = (y_1 + y_2 + ... + y_n)$ elementi u V i neka je V kompleksni vektorski prostor. Skalarni produkt elemenata x i y, $(x|y)$ u V zadovoljava sljedeće uvjete

1. $(x|y) = (y|x)^*$ (* simbol za kompleksno konjugirani član)
2. $(\alpha x + \beta y|z) = \alpha(x|z) + \beta(y|z)$
3. $(x|x) \geq 0$
4. $(x|x) = 0$ zahtjeva da je $x = 0$

gdje su $\alpha, \beta \in C$. Vektorski prostor u kojem su zadovoljena pravila 1. - 4. zove se unitarni prostor. Zadnja dva uvjeta od posebnog su značaja jer iz njih slijedi definicija duljine odnosno norma vektora x

$$\| x \| = \sqrt{(x|x)} \tag{A.1}$$

Vektorski prostor u kojem je definirana norma zove se normirani prostor [19].

A.1.3 Potpuni prostor

Niz vektora (x_n) u normiranom prostoru zove se Cauchyjev niz ako za svaki $\varepsilon > 0$ postoji broj M takav da je $\| x_m - x_n \| < \varepsilon$ za sve $m, n > M$. Drugim riječima to je niz u kojem elementi tj. vektori x_m i x_n postaju po volji bliski kako niz evoluira. Iz prethodnog može se lako zaključiti da je svaki niz koji konvergira Cauchyjev. Ako svaki Cauchyjev niz u V konvergira prema nekom elementu iz V onda se takav prostor naziva potpunim. Potpuni prostor koji je normiran zove se Banachov prostor [19].

A.1.4 Definicija Hilbertovog prostora

Unitarni prostor koji je potpun zove se Hilbertov prostor. Primjer takvog prostora je $\mathbb{C}$ - prostor kompleksnih brojeva. Stanje fizičkog sistema u kvantnoj mehanici opisuje se pomoću vektora u Hilbertovom prostoru. Dakle, u kvantnoj mehanici Hilbertov prostor je izraz za prostor stanja. Hilbertov prostor može imati N dimenzija $\mathcal{H}^N$ što uključuje i mogućnost da $N = \infty$ tj. da Hilbertov prostor ima beskonačno dimenzija. Za kvantno računalo s n broj dimenzija N jednak je $N = 2^n$.

A.1.5 Diracova notacija

Diracova ili *bra-ket* notacija koristi se u kvantnoj mehanici za opis elemenata u V. Element $|x\rangle$ je ket, a $\langle y|$ bra vektor. Zajedno oni čine bra-ket $\langle y|x\rangle$ i predstavlja skalarni produkt vektora y i x. Od ovog trenutka pa nadalje u radu će se koristiti ova notacija umjesto prethodno navedene $(x|y)$. Komponente ket vektora se mogu reprezentirati kao stupac, dok se istovremeno komponente bra vektora mogu reprezentirati kao redak pri čemu oboje slijede standardne operacije množenja i zbrajanja matrica. Preciznije, ako je ket vektor $|y\rangle$ opisan stupcem s vrijednostima $(\alpha_1, \alpha_2, ...\alpha_n)$ odgovarajući bra vektor $\langle y|$ opisan je redom s vrijednostima $(\alpha_1^*, \alpha_2^*, ...\alpha_n^*)$ gdje je * oznaka da se radi o kompleksno-konjugiranom članu. Neka je bra vektor $\langle x|$ reprezentiran retkom s komponentama β_n, a ket vektor $|y\rangle$ reprezentiran stupcem s komponentama α_n, onda se skalarni produkt $\langle x|y\rangle$ raspisuje kao

$$\begin{pmatrix} \beta_1^* & \beta_2^* & ... & \beta_n^* \end{pmatrix} \cdot \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix} = \beta_1^*\alpha_1 + \beta_2^*\alpha_2 + ... + \beta_n^*\alpha_n.$$

A.2 Kvantno stanje

U klasičnoj fizici fizičko stanje opisuje se pomoću količine gibanja $\vec{p}(t)$ i položaja $\vec{r}(t)$. U kvantnoj mehanici, stanje ili valna funkcija ψ fizičkog sistema određena je, pri bilo kojem vremenu t vektorom stanja $|\psi(t)\rangle$ u Hilbertovom prostoru $\mathcal{H}$ i sadrži sve potrebne informacije o sistemu [20]. Za razliku od klasične fizike gdje se koriste dvije veličine (x, p) za opisivanje stanja jednodimenzionalne čestice u kvantnoj mehanici

koristi se kompleksna funkcija $\psi(x,t)$. Kvadrat norme valne funkcije je od fizikalnog značaja - on predstavlja gustoću vjerojatnosti položaja ili impulsa. Ukupna vjerojatnost nalaska sistema negdje u prostoru jednaka je 1:

$$\int |\psi(x,t)|^2 d^3r = \int_{-\infty}^{+\infty} dx \int_{-\infty}^{+\infty} dy \int_{-\infty}^{+\infty} |\psi(x,t)|^2 dz \tag{A.2}$$

Valna funkcija koja zadovoljava jednadžbu (A.2) je normalizirana.

A.2.1 Superpozicija

Sistem ne mora biti opisan pomoću samo jedne valne funkcije - može biti opisan dvjema ili više valnih funkcija koje su u stanju superpozicije. Valna funkcija se tako može opisati kao

$$|\psi\rangle = \sum_i \alpha_i |\psi_i\rangle \tag{A.3}$$

gdje su α_i kompleksni brojevi, a odgovarajuća vjerojatnost takve superpozicije jednaka je

$$P = \left| \sum_i \alpha_i |\psi_i\rangle \right|^2 \tag{A.4}$$

Primjer sustava koji je u superpoziciji je

$$|\psi\rangle = \frac{4i}{5}|0\rangle + \frac{3}{5}|1\rangle$$

odgovarajuće vjerojatnosti da je takav sustav u stanju $|0\rangle$ odnosno $|1\rangle$ su

$$P(|0\rangle) = \left|\frac{4i}{5}\right|^2 = \frac{16}{25}$$
$$P(|1\rangle) = \left|\frac{3}{5}\right|^2 = \frac{9}{25}$$

primjetimo da je $\frac{16}{25} + \frac{9}{25} = 1$.

A.2.2 Svojstvene vrijednosti i svojstveni vektori

Operator $\hat{A}$ je matematičko pravilo koje se primjenjuje na ket $|\psi\rangle$ ili bra $\langle\phi|$ i transformira ih u nova stanja $|\psi'\rangle$ odnosno $\langle\phi'|$:

$$\hat{A}|\psi\rangle = |\psi'\rangle \qquad\qquad \langle\phi|\hat{A} = \langle\phi'|$$

Ako se operator $\hat{A}$ nalazi između bra i ket vektora $\langle\phi|\hat{A}|\psi\rangle$ pri evaluiranju tog izraza vrijedi da je svejedno da li prvo $\hat{A}$ djeluje na ket ili na bra:

$$(\langle\phi|\hat{A})|\psi\rangle) = \langle\phi|(\hat{A}|\psi\rangle) \tag{A.5}$$

Vrsta operatora koja ima široku primjenu u kvantnoj mehanici su linearni operatori. Ako je operator $\hat{A}$ takav da komutira s konstantama i da zadovoljava svojstvo distributivnosti. To jest, operator $\hat{A}$ je linearan ako za bilo koja dva vektora $|\psi_1\rangle$ i $|\psi_2\rangle$ i bilo koja dva kompleksna broja a_1 i a_2 zadovoljava [20]

$$\hat{A}(a_1|\psi_1\rangle + a_2|\psi_2\rangle) = a_1\hat{A}|\psi_1\rangle + a_2\hat{A}|\psi_2\rangle \tag{A.6}$$

$$(\langle\psi_1|a_1 + \langle\psi_2|a_2)\hat{A} = a_1\langle\psi_1|\hat{A} + a_2\langle\psi_2|\hat{A} \tag{A.7}$$

Kada linearni operator djeluje na neki vektor $|\psi\rangle$ to može utjecati na smjer vektora. Posebni slučaj kada je linearni operator $\hat{A}$ takav da vektor prije i poslije djelovanja operatora $\hat{A}$ ima isti smjer onda takav vektor nazivamo svojstveni vektor ili svojstveno stanje operatora $\hat{A}$. U jednadžbi

$$\hat{A}|\psi\rangle = a|\psi\rangle$$

svojstveni vektor operatora $\hat{A}$ je $|\psi\rangle$, dok je a kompleksni broj i zove se svojstvena vrijednost operatora $\hat{A}$ [10].

A.2.3 Hermitski operator

Operaciju pri kojoj se matrica M prvo transponira, a onda kompleksno konjugira zovemo hermitska konjugacija i označavamo je s bodežom $[M^T]^* = M^\dagger$. U Matričnom

zapisu hermitska konjugacija matrice M rezultira s

$$[M^T]^* = M^\dagger = \begin{pmatrix} m_{11} & m_{12} & m_{13} \\ m_{21} & m_{22} & m_{23} \\ m_{31} & m_{32} & m_{33} \end{pmatrix}^{[T]^*} = \begin{pmatrix} m_{11} & m_{21} & m_{31} \\ m_{12} & m_{22} & m_{32} \\ m_{13} & m_{23} & m_{33} \end{pmatrix}^* = \begin{pmatrix} m_{11}^* & m_{21}^* & m_{31}^* \\ m_{12}^* & m_{22}^* & m_{32}^* \\ m_{13}^* & m_{23}^* & m_{33}^* \end{pmatrix}$$

Ako ko je $M|A\rangle = |B\rangle$ ne vrijedi i da je $\langle A|M = \langle B|$. Naime, pri prelasku s ket u bra notaciju ili obratno M je potrebno zamijeniti s $M^\dagger$:

Ako je

$$M|A\rangle = |B\rangle$$

onda je

$$\langle A|M^\dagger = \langle B|$$

Linearni operatori koji su jednaki svojim hermitskim konjugatima zovu se hermitski operatori. Drugim riječima ako se matricu M transponira pa kompleksno konjugira rezultat će biti isti kao na početku tj. $M = M^\dagger$. Svakoj fizički mjerljivoj vrijednosti A, zvanoj observabla, odgovara linearni Hermitski operator $\hat{A}$ čiji svojstveni vektori čine kompletnu bazu. Ako vektorski prostor V ima kompletnu bazu, vektori baze mogu kao linearna kombinacija opisati bilo koji vektor u V.

A.2.4 Kvantno sprezanje

Za opisivanje sistema koji se sastoji od više podsistema koristi se tenzorski produkt $\otimes$. Primjerice, ako je jedan podsistem u stanju $|1\rangle$, a drugi u stanju $|0\rangle$ sistem se može opisati kao

$$|10\rangle = |1\rangle \otimes |0\rangle \tag{A.8}$$

Ako stanje $|\psi\rangle_{AB}$ na sistemima A, B ne može biti raspisano preko tenzorskog pro-

dukta kao $|\psi\rangle_{AB} = |\Phi\rangle_A \otimes |\phi\rangle_B$ kažemo da je spregnuto. Neka stanja su više spregnuta od drugih [10], a postoje i stanja koja su maksimalno spregnuta:

$$|\psi^{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \tag{A.9}$$

$$|\psi^{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \tag{A.10}$$

$$|\psi^{10}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \tag{A.11}$$

$$|\psi^{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \tag{A.12}$$

A.3 Vremenska evolucija kvantnog stanja

Kada se neko tijelo mase m počne gibati pod utjecajem neke rezultantne sile F iz početnog položaja $x(t) = x(0)$, koristeći drugi Newtonov zakon možemo odrediti položaj tog tijela u nekom drugom vremenskom trenutku $x(t) = x(t')$. To je slučaj u klasičnoj fizici, međutim u kvantnoj mehanici umjesto položaja tijela $x(t)$ ono što tražimo je kvantno stanje ili valna funkcija $\psi(x,t)$ [21]. Kvantno stanje može se odrediti rješavanjem Schrödingerove jednadžbe koja glasi

$$i\hbar\frac{\partial\psi(x,t)}{\partial t} = \hat{H}\psi(x,t) \tag{A.13}$$

gdje je $\hbar$ reducirana Planckova konstanta $\hbar = \dfrac{h}{2\pi}$, a $\hat{H}$ operator zvan hamiltonijan koji odgovara energiji vektora stanja sistema.

Bibliography

[1] P. Shor, in Proc. 35th Annu. Symp. on the Foundations of Computer Science, edited by S. Goldwasser (IEEE Com- puter Society Press, Los Alamitos, California, 1994).

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

[3] Richard P Feynman. Simulating physics with computers, 1981. International Journal of Theoretical Physics, 21(6/7).

[4] Shor, P. W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Journal on Computing 26, 1484-1509 (1997).

[5] Peter W Shor. Scheme for reducing decoherence in quantum computer memory. Physical Review A, 52(4):R2493, 1995.

[6] Nielsen, M. A., & Chuang, I. L. Quantum Computation and Quantum Information: 10th Anniversary Edition. Cambridge University Press, 2010.

[7] Scherer, W. Mathematics of Quantum Computing : An Introduction. Springer, 2019.

[8] Adedoyin Adetokunbo, et al. Quantum algorithm implementations for beginners. arXiv preprint arXiv:1804.03719, 2018.

[9] Amira Abbas, Abraham Asfaw, et. al Learn Quantum Computation Using Qiskit, 2020. `http://community.qiskit.org/textbook`, 14.02.2022.

[10] Leonard Susskind and Art Friedman The Theoretical Minimum: What You Need to Know to Start Doing Physics. Published by Basic Books, A Member of the Perseus Books Group, 2014.

[11] Guifré Vidal. Efficient classical simulation of slightly entangled quantum computations. Physical review letters, 91(14):147902, 2003.

[12] W. Dür; G. Vidal & J. I. Cirac. ”Three qubits can be entangled in two inequivalent ways”. Phys. Rev. A. 62 (6): 062314. https://arxiv.org/abs/quant-ph/0005115, 2000.

[13] Mehdi Saeedi and Igor L Markov. Synthesis and optimization of reversible circuits - a survey. ACM Computing Surveys (CSUR), 45(2):21, 2013.

[14] Igor L. Markov and Mehdi Saeedi. Constant-Optimized Quantum Circuits for Modular Multiplication and Exponentiation. https://arXiv:1202.6614, 2012.

[15] https://quantum-computing.ibm.com/composer/docs/iqx/operations_glossary, 8.2.2022.

[16] Skosana, U.; Mark, T. : Demonstration of Shor's factoring algorithm for N=21 on IBM quantum processors // Scientific Reports 11, 16599 (2021). https://arxiv.org/abs/2103.13855

[17] Gamel, O.; James, D.F.V : Simplified Factoring Algorithms for Validating Small-Scale Quantum Information Processing Technologies. (2013) https://arxiv.org/abs/1310.6446v2

[18] Vandersypen, et al. Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance. Nature 414, 883-887 (20/27 Dec 2001). https://arxiv.org/abs/quant-ph/0112176

[19] Debnath, L. and Mikusinski, P. Hilbert Spaces with Applications. Elsevier Academic Press, (2005).

[20] Zettili, N. Quantum Mechanics: concepts and applications / Nouredine Zettili. – 2nd ed. (2009).

[21] Griffiths, D.J. and Schroeter, D.F. Introduction to Quantum Mechanics. Cambridge University Press, 3nd ed. (2018).

[22] Poveznica na datum 12. veljače 2022. godine: https://narodne-novine.nn.hr/clanci/sluzbeni/2019_01_10_210.html

[23] Paar, V., Hrlec A., Sambolek, M., Rešetar, K.V. FIZIKA OKO NAS 4 - udžbenik fizike u četvrtom razredu gimnazije. Školska knjiga (2021).

[24] Simulacija fotoelektričnog učinka. Poveznica na simulaciju na datum 12. veljače 2022. godine: https://applets.kcvs.ca/photoelectricEffect/PhotoElectric.html

[25] Poveznica na datum 12. veljače 2022. godine: https://skolazazivot.hr/medupredmetne-teme