Kvantno ispravljanje pogrešaka

Žilić, Frane

Sveučilište u Splitu
Prirodoslovno – matematički fakultet

Kvantno ispravljanje pogrešaka

Završni rad

Frane Žilić

Split, rujan 2023.

Temeljna dokumentacijska kartica

Sveučilište u Splitu
Prirodoslovno – matematički fakultet
Odjel za fiziku
Ruđera Boškovića 33, 21000 Split, Hrvatska

Završni rad

Kvantno ispravljanje pogrešaka

Frane Žilić

Sveučilišni prijediplomski studij Fizika

Sažetak:

Rad služi kao uvod u područje kvantnog programiranja i ispravljanja pogrešaka u kvantnim računalima. Budući da je riječ o tehnologiji koja se brzo razvija i mnogo obećava, ovaj rad nastoji zadovoljiti interes za njom. Prvi dio opisuje qbitove kao osnovnu jedinicu za pohranjivanje podataka u kvantnom računarstvu te razvija matematički formalizam potreban za rad s njima. Nakon kratkog pregleda nekoliko fizikalnih realizacija qbita, uvode se kvantna vrata kojima se qbitom manipulira. Slijedi opis svojstava kvantnih sustava važnih za kvantno računarstvo. Kako je prevladavanje pogrešaka jedna od ozbiljnijih prepreka u razvoju kvantnih računala, rad se posebno bavi tom temom. Opisuju se osnovne vrste kvantnih pogrešaka te kodovi za njihovo ispravljanje. Razvija se stabilizacijski formalizam bitan za baratanje programima za ispravljanje pogrešaka. Napokon se konstruiraju neki složeniji kodovi koji mogu ispraviti pogreške u kvantnim sustavima: Shorov i Steaneov kod.

Ključne riječi: kvantno programiranje, qbit, kvantna vrata, kvantno ispravljanje pogrešaka, Shorov kod, Steaneov kod, zaštićeni qbit

Rad sadrži: 33 stranice, 1 sliku, 2 tablice, 12 literaturnih navoda. Izvornik je na hrvatskom jeziku.

Mentor: prof. dr. sc. Leandra Vranješ Markić

Ocjenjivači: prof. dr. sc. Leandra Vranješ Markić,
izv. prof. dr. sc. Petar Stipanović,
doc. dr. sc. Ivana Weber

Rad prihvaćen: 25. 9. 2023.

Rad je pohranjen u Knjižnici Prirodoslovno – matematičkog fakulteta, Sveučilišta u Splitu.

Basic documentation card

University of Split
Faculty of Science
Department of Physics
Ruđera Boškovića 33, 21000 Split, Croatia

Bachelor thesis

Quantum Error Correction

Frane Žilić

University undergraduate study Physics

Abstract:

The paper is written as an introduction to quantum computing and quantum error correction. Recent advances have aroused much interest in the field, which this paper aims to satisfy. Firstly, the qbit is introduced as the elementary unit of data in quantum computing, along with the necessary mathematical formalism. After a short overview of qbit modalities, quantum gates used to manipulate them are described. Some properties of quantum systems important to quantum computing are detailed. Since overcoming errors is one of the main obstacles to development of quantum computing, the paper is focused on this topic. Elementary quantum errors are described along with their correction codes. Stabilizer formalism important for work with error correction programs is developed. Finally, a couple of complex quantum error correction codes are constructed: Shor's code and Steane's code.

Keywords: quantum programming, qbit, quantum gates, quantum error correction, Shor code, Steane code, protected qbit

Thesis consists of: 33 pages, 1 figures, 2 tables, 12 references. Original language: Croatian.

Supervisor: Prof. Dr. Leandra Vranješ Markić

Reviewers: Prof. Dr. Leandra Vranješ Markić,
Asoc. Prof. Dr. Petar Stipanović,
Assist. Prof. Dr. Ivana Weber

Thesis accepted: Sep. 25, 2023

Thesis is deposited in the library of the Faculty of Science, University of Split.

Sadržaj

1 Uvod

Posljednjih nekoliko godina sve se više u medijskom prostoru spominje pojam kvantnog računala. Kako popularno-znanstveni tako i širi mediji donose obećanja o brojnim inovacijama koje bi nam ti uređaji u bliskoj budućnosti trebali priuštiti: otkrića novih lijekova i revolucionarnih materijala, poboljšanu umjetnu inteligenciju, rješenja dosad neprobojnih matematičkih i fizikalnih problema, ubrzane i poboljšane modele predviđanja financijskih tržišta itd. Slušamo obećanja o skoroj "kvantnoj revoluciji" i "kvantnoj nadmoći" (eng. *quantum supremacy*) nad klasičnim analognim računalima. [1] Državne institucije i privatne tvrtke sve više ulažu u razvoj kvantnih tehnologija: IBM, Google, HP, Intel i Huawei samo su neka od najzvučnijih imena koja su uložila znatna sredstva u razvoj kvantnih računala.
Iako je popularni i investitorski interes za ovu tehnologiju novijeg datuma, osnove kvantnog računanja položene su prije gotovo pola stoljeća. Prve teorijske spekulacije o mogućem korištenju kvantnih sustava za komputaciju počele su krajem 70-ih i početkom 80-ih godina prošlog stoljeća u radovima Paula Benioffa, Yurija Manina i Richarda Feynmana. [2] Slijedila su dva desetljeća pokušaja pronalaska adekvatnih fizikalnih realizacija takvog sustava i intenzivnog razvoja algoritama za tada još čisto teoretska kvantna računala. Pogotovo je značajan doprinos Petera Shora, koji je razvio algoritam pomoću kojeg bi kvantna računala mogla dešifrirati najčešće korištene protokole za enkripciju. Napokon, neki su programi i eksperimentalno provedeni. Prvo funkcionalno kvantno računalo nastalo je 2007. godine, a 2016. IBM je za javnost otvorio svoj program Quantum Experience, te tako široj javnosti omogućio pristup eksperimentima s kvantnim računalima. IBM i Google razvili su svoje kvantne programske jezike zasnovane na klasičnim jezicima Python i C++. [3]
Usprkos velikom napretku kvantne tehnologije u relativno kratkom vremenu, praktično korisna kvantna računala još uvijek nisu na obzoru. Korisno kvantno računalo trebalo bi imati broj qbitova (kvantna ekvivalenta bitu) reda veličine nekoliko milijuna. Trenutno najnaprednija kvantna računala imaju ih tek oko 500. [1] Jedna od glavnih prepreka u razvoju kvantnih računala je implementacija kvantnog ispravljanja pogrešaka. U svakom komputacijskom sustavu može doći do greške, bilo zbog interferencije sustava s okolinom, bilo zbog kvara. U klasičnom računalu zasnovanom na bitovima može doći samo do jedne vrste greške: nula se može pretvoriti u jedinicu ili jedinica u nulu. Kvantna računala mnogo su osjetljivija na greške upravo zbog istih kvantnih svojstava koja im (u teoriji) omogućavaju da nadiđu kapacitete klasičnih računala. Današnja kvantna računala zato moraju veliki dio svog kapaciteta posvetiti ispravljanju pogrešaka, što ih bitno ograničava. Razvoj učinkovitijih algoritama za kvantno ispravljanje pogrešaka i kvantnih sustava otpornih na greške bit će ključan korak u daljnjem razvoju ove tehnologije. [3] Prvi dio ovog rada uvest će osnovne koncepte i pojmove kvantnog računanja, uz pretpostavku čitateljeva poznavanja osnova kvantne mehanike. Drugi dio razvit će neke trenutno dostupne algoritme za kvantno ispravljanje pogrešaka.

2 Osnove kvantnog računanja

Kvantno računalo uređaj je koji koristi svojstva kvantne mehanike za komputaciju. [2] U ovom poglavlju, uvode se najvažnija svojstva kvantnih fizikalnih sustava koja kvantna računala koriste. Uvodi se pojam qbita kao osnovne jedinica informacije u kvantnom programiranju, ekvivalentne bitu u klasičnom programiranju. [3] Qbit se opisuje u matematičkom formalizmu kvantne mehanike te se navodi nekoliko primjera njegovih fizikalnih realizacija (modaliteta). Nakon toga slijedi opis kvantnih vrata koja na qbitove mogu djelovati te pomoću kojih se izgrađuju kvantni programi. Navode se neka jedinstvena svojstva kvantnih sustava koja bitno utječu na kvantno računanje. Naposljetku su navedeni DiVincenzovi kriteriji koji definiraju zahtjeve za funkcionalno kvantno računalo.

2.1 Qbit

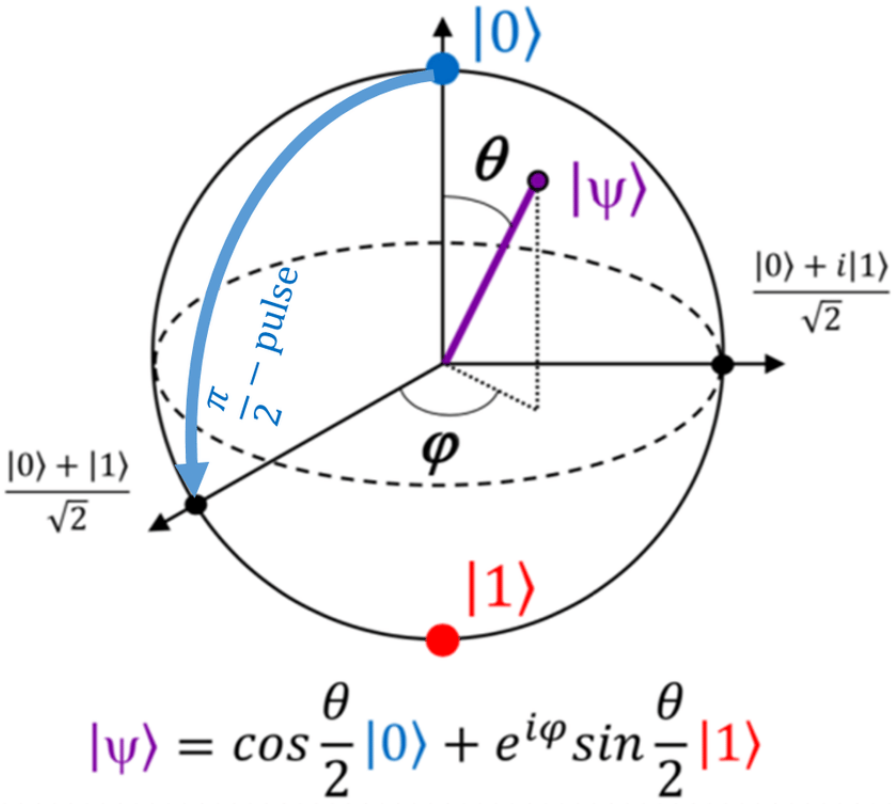
Klasični digitalni bit može se naći u dvama stanjima: 1 i 0. Kombinacijom velikog broja bitova informacije se pohranjuju u binarnom jeziku, a izvršavanjem matematičkih operacija na njima grade se programi. U kvantnom računanju, podatci se pohranjuju u qbitovima.
Qbit ili kvantni bit definira se kao kvantni sustav s dva svojstvena stanja reprezentiran u dvodimenzionalnom Hilbertovom prostoru. Ova dva stanja označavaju se u Diracovoj bra-ket notaciji kao $|0\rangle$ i $|1\rangle$ te čine ortonormiranu bazu $\{|0\rangle, |1\rangle\}$ koja je poznata kao komputacijska baza (eng. *computational basis*). U ovoj se bazi vektor stanja koji opisuje sustav qbita može pisati kao:

$$|\Psi\rangle = a\,|0\rangle + b\,|1\rangle = \begin{bmatrix} a \\ b \end{bmatrix}, \tag{2.1}$$

gdje su a i b amplitude vjerojatnosti, to jest kompleksni brojevi koji opisuju vjerojatnost da se qbit $|\Psi\rangle$ nađe u odgovarajućem stanju. Kod mjerenja smjera vektora stanja qbita vjerojatnost ishoda "0" jednaka je $|a|^2$, a vjerojatnost ishoda "1" je $|b|^2$, pri čemu mora biti zadovoljen uvjet normiranosti $|a|^2 + |b|^2 = 1$. [3] U matričnom obliku vektori baze dani su kao:

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \text{ i } |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}. \tag{2.2}$$

Dakle, qbit se nalazi u superpoziciji stanja 0 i 1. Mjerenjem qbita dobit će se rezultat koji odgovara jednom od tih stanja, no za razliku od klasičnog bita rezultat tog mjerenja bit će probabilističke prirode. Upravo ovo svojstvo qbita omogućava primjene kvantnih računala na načine koji nisu mogući u klasičnom računarstvu. [4]



Slika 1: *Blochova sfera. Vektor stanja qbita može se nacrtati kao vektor unutar sfere čiji polovi odgovaraju vektorima komputacijske baze (slika preuzeta iz [6])*

Vektor stanja qbita često se reprezentira pomoću Blochove sfere (slika 1). Riječ je o sferi radijusa 1 sa središtem u ishodištu koordinatnog sustava, takvoj da je stanje $|0\rangle$ na sjevernom, a $|1\rangle$ na južnom polu. Vektor $|\Psi\rangle$ polazi iz ishodišta te završava na površini sfere. Svaka moguća superpozicija dvaju osnovnih stanja koja čini $|\Psi\rangle$ može se prikazati kao vektor u ovoj sferi.
U sfernom koordinatnom sustavu Blochove sfere, vektor stanja qbita može se izraziti preko kuta otklona od z-osi θ i azimutalnog kuta ϕ projekcije na xy os [3]:

$$|\Psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle = \begin{bmatrix} \cos\left(\frac{\theta}{2}\right) \\ e^{i\phi}\sin\left(\frac{\theta}{2}\right) \end{bmatrix}. \tag{2.3}$$

2.1.1 Rotacije qbita

Paulijeve matrice su hermitske, unitarne, kompleksne matrice dimenzije 2×2 oblika:

$$\sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \tag{2.4}$$

Ove matrice mogu zarotirati vektor stanja qbita za 180° u Blochovoj reprezentaciji. Ove se operacije zovu vrata te će o njima biti više riječi kasnije. Operator rotacije $\hat{R}$ općenito je dan

jednadžbom:

$$\hat{R} = e^{-i\frac{\theta}{2}(\hat{n}\cdot\vec{\sigma})} = \cos(\frac{\theta}{2}) - i(\hat{n}\cdot\vec{\sigma})\sin(\frac{\theta}{2}), \tag{2.5}$$

gdje je $\hat{n}$ jedinični vektor u smjeru osi rotacije, θ kut rotacije i $\vec{\sigma}$ vektor čije su Kartezijeve komponente u matričnom zapisu odgovarajuće Paulijeve matrice. [3]

2.1.2 Projektivna mjerenja

Mjerenja stanja qbita ključni su dio kvantnog računarstava. Mjerenja se najčešće obavljaju na kraju izvršavanja programa, no ponekad se vrše i unutar programa radi ispravljanja greški ili primjene "if" izjava. Da bi se kvantni programi mogli opisati, potrebno je koristiti matematički formalizam kvantnih mjerenja. [3]
Mjerenja neke opservable M u kvantnoj mehanici opisana su djelovanjem povezanog operatora $\hat{M}$ na vektor stanja sustava $|\phi\rangle$. Mogući ishodi mjerenja dani su svojstvenim vrijednostima m operatora koja se dobivaju djelovanjem na povezane svojstvene vektore operatora:

$$\hat{M}|m\rangle = m|m\rangle. \tag{2.6}$$

Da bi se operator mogao primijeniti na neki sustav, vektor stanja tog sustave mora biti moguće napisati u bazi koju čine svojstveni vektori operatora $\hat{M}$. Vjerojatnost da će rezultat mjerenja opservable biti jednak m iznosi:

$$p(m) = \frac{|\langle m|\phi\rangle|^2}{\langle\phi|\phi\rangle}. \tag{2.7}$$

Dakle, vjerojatnost da će se qbit s normiranim vektorom stanja $|\psi\rangle = a|0\rangle + b|1\rangle$ naći u stanju $|0\rangle$ iznosi:

$$p(0) = |\langle 0|\psi\rangle|^2 = |a|^2. \tag{2.8}$$

Zbroj vjerojatnosti svih mogućih ishoda mjerenja mora biti jednak jedinici, $\sum_m p(m) = 1$. Nakon mjerenja, ako je izmjerena svojstvena vrijednost m, sustav će se naći u odgovarajućem svojstvenom stanju $|m\rangle$. [5] Zato mjerenjem qbita dolazi do "uništenja" njegovog stanja, za razliku od klasičnog digitalnog bita koji se može mjeriti bez promjene stanja. [2]
Prosječna vrijednost mjerenja dana je izrazom:

$$\langle\hat{M}\rangle = \frac{\langle\phi|\hat{M}|\phi\rangle}{\langle\phi|\phi\rangle} = \sum_m mp(m), \tag{2.9}$$

te se pomoću nje definira standardna devijacija mjerene vrijednosti [5]:

$$\sigma_M^2 = \Delta M^2 = \langle M^2\rangle - \langle M\rangle^2. \tag{2.10}$$

U kvantnom računarstvu posebno su važna projektivna mjerenja. Riječ je o mjerenjima

opisanim operatorima projekcije, koji su hermitski i jednaki svom kvadratu: $\hat{P}^2 = \hat{P}$.
U komputacijskoj bazi mogu se definirati operatori projekcije $\hat{P}_0$ i $\hat{P}_1$:

$$\hat{P}_0 = |0\rangle \langle 0| \ , \hat{P}_1 = |1\rangle \langle 1| \, , \tag{2.11}$$

za koje se lako pokaže da zadovoljavaju uvjete projektivnosti. Nadalje, $\hat{P}_0$ i $\hat{P}_1$ čine potpuni skup komutirajućih operatora:

$$\hat{P}_0\hat{P}_0 + \hat{P}_1\hat{P}_1 = |0\rangle \langle 0|0\rangle \langle 0| + |1\rangle \langle 1|1\rangle \langle 1| = |0\rangle \langle 0| + |1\rangle \langle 1| = \hat{I}. \tag{2.12}$$

Djelovanjem na vektor stanja qbita, ovi operatori vraćaju $|0\rangle$, to jest $|1\rangle$ komponentu vektora. Njihova srednja vrijednost kod djelovanja na vektor stanja, određena jednadžbom (2.9), daje vjerojatnost da će se qbit naći u stanju $|0\rangle$, to jest $|1\rangle$. [3]

2.1.3 Qdit

Na kraju uvoda u pojam qbita, valja još spomenuti i tzv. qdit kao alternativnu osnovnu jedinicu kvantne komputacije. Dok qbit informacije sprema pomoću superpozicije dvaju kvantnih stanja, qdit koristi superpoziciju $d > 2$ stanja. Povećanje broja stanja dopušta pohranjivanje većeg broja informacije u manje čestica, što povećava efikasnost i smanjuje broj interakcija među nositeljima podataka. Dva qdita dimenzije $d = 32$ sadrže istu količinu podataka kao 20 qbitova. Qditovi su trenutačno u veoma ranoj fazi laboratorijskog istraživanja, te još nisu proizvedeni primjerci koji bi mogli imati praktičnu primjenu. [3]

2.2 Modaliteti qbita

Klasični digitalni bit danas se fizikalno realizira kao poluvodički tranzistor. Ta je tehnologija rezultat višedesetljetnog razvoja i istraživanja. Kako je kvantno računanje u relativno ranoj fazi razvoja, još uvijek ne postoji standardizirani fizikalni model, tzv. modalitet (eng. *modality*), qbita.
Qbit se može fizikalno realizirati bilo kojim kvantnim sustavom s dva svojstvena stanja, te se trenutačno razmatra i istražuje niz mogućih modaliteta. Da bi modalitet qbita bio praktično primjenjiv, mora ga biti moguće skalirati na nekoliko tisuća primjeraka, tako da se u sustavu mogu implementirati složeni programi zajedno s nužnim mehanizmima za ispravljanje greški. Tijekom vremena qbit interagira s okolinom pri čemu dolazi do dekoherencije - gubitka informacija. Svaki modalitet qbita mora biti što je moguće otporniji na takve interakcije, sa što je moguće dužim vremenom koherencije. Modalitet treba omogućiti i sparivanje (eng. *coupling*) među qbitovima koje je nužno za izvršavanje kvantnih algoritama. Ako sparivanje nije moguće, potrebno je koristiti tzv. SWAP operacije (kvantna vrata koja zamjenjuju stanja

qbitova u dvoqbitnom sustavu) za izmjenjivanje stanja među qbitovima, što bitno smanjuje moguću duljinu programa prije dekoherencije. [3]
Većina danas dostupnih kvantnih procesora ima 50-100 qbitova. Uz to su osjetljivi na kvantne greške i podložni dekoherenciji, zbog čega su njihove primjene veoma ograničene. [2] Slijedi pregled nekoliko obećavajućih modaliteta qbita za koje postoji mogućnost skaliranja i usavršavanja u bliskoj budućnosti.

2.2.1 Qbit zarobljenog iona

Qbit zarobljenog iona nastaje tako da se atomi nekog elementa, najčešće iterbija i kalcija [3], ioniziraju laserom te zarobe u električnom potencijalu. Na taj način poredani niz iona čini niz qbita čija se stanja mogu mjeriti i manipulirati laserom ili primjenom radiofrekvencijskih pulsova.
Dvije se različite vrste qbita mogu realizirati pomoću zarobljenih iona: optički qbitovi i hiperfini qbitovi. Kod optičkog qbita, dva osnovna stanja $|0\rangle$ i $|1\rangle$ dana su osnovnim i prvim pobuđenim energetskim stanjem iona. Kod hiperfinog qbita, $|0\rangle$ i $|1\rangle$ predstavljaju dva različita osnovna stanja iona. [2] "Hiperfina" osnovna stanja javljaju se kao posljedica interakcije magnetskog polja elektrona i nuklearnog spina. Do sparivanja qbita u ovom modalitetu dolazi uslijed međusobnog odbijanja iona Coulombovom silom ili pomoću lasera. Budući da je samo stanje $|1\rangle$ fluorescentno, stanja qbita mogu se mjeriti praćenjem fluorescencije što omogućuje laku implementaciju mjerenja.
Poteškoće kod modaliteta zarobljenog iona stvara teškoća sparivanja qbitova i korištenje velikog broja lasera. Izvori buke su zagrijavanje iona, nestabilnosti polja lasera i vibracije iz okoliša. [3] Prednost im je veoma dobro vrijeme koherencije i odlično implementirane operacije vrata na malom broju qbitova. Za sad je moguće konstruirati sustave od 20-30 takvih qbitova. [7]

2.2.2 Supravodljivi qbit

Pri niskim temperaturama dolazi do sparivanja elektrona u Cooperove parove. [8] Pojava ovog fenomena u supravodičima koristi se kao jedan modalitet qbitova. Na qbit se pričvršćuje mikrovalni trag te se pomoću mikrovalnih valova točno određene frekvencije i vremena djelovanja na qbit mogu provoditi unitarne operacije. Sustav mora biti ohlađen na temperaturu ispod 10 mK i zaštićen od magnetskih polja i ostalih oblika dekoherencije. Postoji više vrsta supravodljivih qbitova.
Niz tvrtki i istraživačkih organizacija, uključujući Google i IBM, koristi kvantna računala sa supravodljivim qbitovima. [2] Prednost je velika brzina vrata te visoka razina kontrole i mogućnosti skaliranja sustava (za sada oko 100 qbitova). Mane su im niska temperatura koju sustavu treba održavati i nepoželjne izmjene signala među qbitovima. [7]

2.2.3 Spinski qbit

Osim orbitalne kutne količine gibanja, elementarne čestice posjeduju i intrinsičnu kutnu količinu gibanja koja nije povezana s prostornim stupnjevima slobode. Ovaj element kutne količine gibanja zove se spin. Stern-Gerlachov eksperiment pokazao je da će se snop atoma srebra prolazeći kroz nehomogeno magnetsko polje razdvojiti na dvije različite komponente. Pomoću ovakvog i sličnih eksperimenta utvrđeno je da elektroni imaju dva karakteristična smjera spina istog iznosa: spin gore $|\uparrow\rangle$ i spin dolje $|\downarrow\rangle$. [5]
Dvije spinske orijentacije elektrona mogu se koristiti kao dva osnovna stanja komputacijske baze spinskog qbita. Prednost ove vrste qbita jest što se mogu konstruirati pomoću kvantnih točaka (eng. *quantum dots*) u silikonskim poluvodičkim uređajima. Barijera među susjednim točkama može se mijenjati variranjem napona pomoću električnih krugova. Temperatura rada sustava je oko 1K, što je bitno toplije od supravodljivih qbita. Riječ je o već poznatim i dobro istraženim tehnologijama i materijalima pomoću kojih se spinski qbit može lako implementirati i skalirati u odnosu na druge modalitete. [3]
Međutim, teško je ovom metodom proizvesti stabilne qbitove s kojima se može lako komunicirati. [2]

2.2.4 Topološki qbit

Topološki qbit temelji se na svojstvima anyona, dvodimenzionalne kvazičestice koja nije ni bozon ni fermion. Ispreplitanjem staza anyona u 4D vremenprostoru teoretski je moguće stvoriti sustav qbita otporan na dekoherenciju; zahvaljujući ispreplitanju, topologija sustava će usprkos malim perturbacijama ostati nepromijenjena što omogućava dulje vrijeme koherencije. Ovim modalitetom mogli bi se realizirati veliki sustavi sustavi zaštićeni od pogrešaka.
Riječ je o novoj tehnologiji koja još nije praktično implementirana, no teoretski je obećavajuća. još uvijek nisu pronađeni materijali ili sustavi u kojima bi topološki qbit mogao zaživjeti. [2][7]

2.3 Kvantna vrata

Princip rada kvantnog računala zasniva se na kvantnim krugovima (eng. *quantum circuit*), slično kao što se rad klasičnog računala zasniva na digitalnim krugovima. Izvršavanje programa započinje pripremanjem određenog broja qbitova u potrebna početna stanja. Nakon toga se nad qbitovima pomoću kvantnih vrata vrše operacije koje treba riješiti primjenom kvantne mehanike. Naposljetku se qbitovi mjere projekcijom na skup klasičnih bitova pomoću komputacijske baze. Za razliku od klasičnog računala, ishod izvršavanja programa svaki put može biti različit zbog probabilističke prirode kvantnih sustava. Program se zato izvršava više puta te se gleda distribucija njegovih rezultata.
Kvantni krug konstruiran na ovaj način rješava zadani problem primjenom niza operatora

preko kvantnih vrata. [3] Kako je vremenska i prostorna evolucija kvantnih sustava opisana unitarnim transformacijama [5], ovi operatori moraju biti unitarni; svaki kvantni krug odgovara hermitskom, unitarnom operatoru U_{qc}:

$$U_{qc}U_{qc}^{\dagger} = U_{qc}^{\dagger}U_{qc} = 1. \tag{2.13}$$

Gornja jednadžba sugerira da operator kvantnog kruga mora imati inverz. Zato su kvantni krugovi reverzibilni, to jest moguće ih je izvršiti unatrag. Zbog unitarnosti su kvantni krugovi također aciklički (nemaju petlje ni povratne krugove) te imaju isti broj ulaznih i izlaznih podataka.
Svi kvantni krugovi svode se na niz primjena unitarnih operacija koje zovemo kvantna vrata. Pregledu kvantnih programa zato mora prethoditi opis kvantnih vrata i njihovih svojstava. [3]

2.3.1 Not vrata

Not vrata, također poznata kao bit-flip vrata ili Paulijeva X-vrata, mijenjaju qbit iz stanja $|0\rangle$ u $|1\rangle$ i obrnuto. U matričnom obliku dana su kao

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \tag{2.14}$$

te na qbit djeluju na sljedeći način:

$$X|0\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |1\rangle \ , X|1\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0\rangle . \tag{2.15}$$

2.3.2 Vrata identiteta

Ova vrata ostavljaju stanja $|0\rangle$ i $|1\rangle$ nepromijenjena te se predstavljaju jediničnim operatorom:

$$I = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}. \tag{2.16}$$

Jasno se vidi da djelovanjem na stanja baze neće doći do bilo kakve promjene.

2.3.3 Hadamardova vrata

Hadamardova vrata rotiraju qbit za kut π oko osi dijagonalne na xy ravninu u Blochovoj reprezentaciji. Uslijed ove rotacije z-os i x-os zamijene mjesta. Dana su slijedećom

jednadžbom:

$$H = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \langle 0| + \frac{|0\rangle - |1\rangle}{\sqrt{2}} \langle 1| \,, \tag{2.17}$$

što se u matričnoj reprezentaciji može napisati kao

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}. \tag{2.18}$$

Djelovanjem na osnovna stanja H-vrata daju vektore takozvane polarne baze:

$$H|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \langle 0|0\rangle + \frac{|0\rangle - |1\rangle}{\sqrt{2}} \langle 1|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |+\rangle \tag{2.19}$$

$$H|1\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \langle 0|1\rangle + \frac{|0\rangle - |1\rangle}{\sqrt{2}} \langle 1|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |-\rangle \,. \tag{2.20}$$

U matričnoj reprezentaciji $|+\rangle$ i $|-\rangle$ postaju:

$$|+\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} \,,\; |-\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix}. \tag{2.21}$$

Kompaktno se djelovanje H-vrata može zapisati kao:

$$H|x\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{2\pi i \frac{x}{2}} |1\rangle) \tag{2.22}$$

$$H|x\rangle = \frac{1}{\sqrt{2}} \sum_{y=0}^{1} (-1)^{x \cdot y} |y\rangle \,. \tag{2.23}$$

Uzastopnom primjenom dvaju H-vrata sustav se vraća u početno stanje.

2.3.4 Paulijeva Y-vrata

Paulijeva Y-vrata rotiraju qbit oko osi y za kut π. U matričnoj reprezentaciji imaju oblik

$$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \tag{2.24}$$

a djelovanjem na vektore baze daju:

$$Y|0\rangle = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ i \end{bmatrix} = i|1\rangle \;,\; Y|1\rangle = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} -i \\ 0 \end{bmatrix} = -i|0\rangle \,. \tag{2.25}$$

2.3.5 Paulijeva Z-vrata

Paulijeva Z-vrata rotiraju qbit oko osi z za kut π. Kako ne mijenjaju stanje $|0\rangle$, a $|1\rangle$ "preokreću" u $-|1\rangle$, zovu se i vrata faznog okreta (eng. *phase flip gate*). [3] U matričnoj reprezentaciji imaju oblik

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \tag{2.26}$$

a djelovanjem na vektore baze daju:

$$Z|0\rangle = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0\rangle \ , Z|1\rangle = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ -1 \end{bmatrix} = -|1\rangle . \tag{2.27}$$

2.3.6 S vrata

S vrata, poznata još kao Z90 vrata ili fazna vrata, rotiraju qbit za kut $\pi/2$ oko z-osi. U matričnoj reprezentaciji imaju oblik

$$S = \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{i\pi}{2}} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}, \tag{2.28}$$

a djelovanjem na vektore baze daju:

$$S|0\rangle = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0\rangle \ , S|1\rangle = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = i \begin{bmatrix} 0 \\ 1 \end{bmatrix} = i|1\rangle . \tag{2.29}$$

2.3.7 S† vrata

S† vrata su hermitski konjugat vrata S. U matričnoj reprezentaciji imaju oblik

$$S^\dagger = \begin{bmatrix} 1 & 0 \\ 0 & e^{-\frac{i\pi}{2}} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -i \end{bmatrix}, \tag{2.30}$$

a djelovanjem na vektore baze daju:

$$S^\dagger|0\rangle = \begin{bmatrix} 1 & 0 \\ 0 & -i \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0\rangle \ , S|1\rangle = \begin{bmatrix} 1 & 0 \\ 0 & -i \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = -i \begin{bmatrix} 0 \\ 1 \end{bmatrix} = -i|1\rangle . \tag{2.31}$$

Vrata S i S† rotiraju qbit između x i y baze, gdje su x i y svojstvena stanja operatora X i Y, te čine dva moguća korijena vrata Z. [3]

2.3.8 Proizvoljna rotacija qbita

Za rotaciju qbita za proizvoljni kut oko x, y ili z-osi koriste se R vrata, koja su u matričnoj reprezentaciji definirana kao:

$$R_x(\theta) = \begin{bmatrix} \cos(\theta/2) & -i\sin(\theta/2) \\ -i\sin(\theta/2) & \cos(\theta/2) \end{bmatrix}, R_y(\theta) = \begin{bmatrix} \cos(\theta/2) & -\sin(\theta/2) \\ \sin(\theta/2) & \cos(\theta/2) \end{bmatrix} \\ R_z(\phi) = \begin{bmatrix} e^{-\frac{i\phi}{2}} & 0 \\ 0 & e^{-\frac{i\phi}{2}}. \end{bmatrix} \tag{2.32}$$

Preko Paulijevih matrica mogu se zapisati kao

$$R_x(\theta) = \cos(\frac{\theta}{2})I - i\sin(\frac{\theta}{2})X = e^{-i\frac{\theta}{2}X} \tag{2.33}$$

$$R_y(\theta) = \cos(\frac{\theta}{2})I - i\sin(\frac{\theta}{2})Y = e^{-i\frac{\theta}{2}Y} \tag{2.34}$$

$$R_z(\phi) = \cos(\frac{\phi}{2})I - i\sin(\frac{\phi}{2}) = Ze^{-i\frac{\phi}{2}Z}. \tag{2.35}$$

Kao posebni slučaj R_z vrata kad je kut $\theta = \pm\frac{\pi}{4}$ definiraju se vrata T i $T^\dagger$, t.j. drugi korijen vrata S.

2.3.9 Fizikalna vrata

Sva dosad nabrojena kvantna vrata su jednoqbitna (eng. *single-qbit*) vrata, to jest vrata koja djeluju na jedan qbit. Sva takva vrata možemo izvesti iz fizikalnih vrata ili U-vrata koja su fizikalno implementirana u kvantnim uređajima.
Općeniti oblik unitarnih jednoqbitnih operacija opisuju U_3 vrata definirana kao [3]:

$$U_3 = (\theta, \phi, \lambda) = \begin{bmatrix} \cos(\frac{\theta}{2}) & -e^{i\lambda}\sin(\frac{\theta}{2}) \\ e^{i\phi}\sin(\frac{\theta}{2}) & e^{i\lambda+i\phi}\cos(\frac{\theta}{2}) \end{bmatrix}, \tag{2.36}$$

gdje su θ i ϕ kutovi rotacije u Blochovoj sferi, a $e^{i\lambda}$ globalna faza. Djelovanjem na qbit, U_3 vrata ga dovode u proizvoljnu superpoziciju određenu kutovima rotacije.
Ostala se U-vrata mogu izvesti iz vrata U_3:

$$U_2(\phi, \lambda) = U_3(\frac{\pi}{2}, \phi, \lambda) = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & -e^{i\lambda} \\ e^{i\phi} & e^{i(\phi+\lambda)} \end{bmatrix}, \tag{2.37}$$

$$U_1(\lambda) = U_3(0, 0, \lambda) = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 0 \\ 0 & e^{i\lambda} \end{bmatrix}. \tag{2.38}$$

NOT vrata zapisana preko U-vrata glase $X = U_3(\pi, 0, \pi)$, Hadamardova vrata glase $H = U_2(0, \pi)$, Y vrata $Y = U_3(\pi, \frac{\pi}{2}, \frac{\pi}{2})$, a Z vrata $Z = U_1(\pi)$. Koristeći rotaciju U_1, S i S† vrata mogu se zapisati kao $S = U_1(\pi/2)$ i $S^\dagger = U_1(-\pi/2)$. Proizvoljne rotacije izvedene iz U vrata imaju oblik

$$R_x(\theta) = U_3(\theta, -\frac{\pi}{2}, \frac{\pi}{2}) \, , \, R_y(\theta) = U_3(\theta, 0, 0) \, , \, R_z(\phi) = e^{-i\frac{\phi}{2}} U_1(\phi). \tag{2.39}$$

2.3.10 Reset vrata

Reset vrata postavljaju qbit u stanje $|0\rangle$ bez obzira na njegovo prethodno stanje. Pomoću njih se qbit može resetirati i usred operacije. [3]

2.4 Sustavi više qbitova i multiqbitna vrata

Pošto smo opisali jedan qbit i osnovne operacije koje se na njemu mogu obavljati, valja prijeći na opis sustava više qbitova i vrata koja djeluju na njih.
Kako svaki qbit ima dva ortonormirana bazna stanja, sustav od n qbitova ima 2^n ortonormiranih baznih stanja u komputacijskoj bazi. Ovakav se sustav označava sa $|x_1 x_2 ... x_n\rangle$, gdje je svaki x_i jednak 0 ili 1. Svakom od ovih stanja odgovara amplituda vjerojatnosti a_x, pri čemu kao i za sustav jednog qbita vektor stanja mora biti normaliziran:

$$|\psi\rangle = \sum_{x \in \{0,1\}^n} a_x |x\rangle \, , \, \sum_{x \in \{0,1\}^n} |a_x|^2 = 1. \tag{2.40}$$

Matematički se sustav više qbitova opisuje tenzorskim produktom. Ako su $|\psi_1\rangle = a_1 |0\rangle + b_1 |1\rangle$ i $|\psi_2\rangle = a_2 |0\rangle + b_2 |1\rangle$ vektori stanja dvaju qbitova, tada je sustav sastavljen od ova dva qbita dan sa:

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle = a_1 a_2 |00\rangle + a_1 b_2 |01\rangle + a_2 b_1 |10\rangle + a_2 b_2 |11\rangle \, , \tag{2.41}$$

pri čemu zbog uvjeta normiranosti mora vrijediti $|a_1 b_1|^2 + |a_1 b_2|^2 + |a_2 b_1|^2 + |a_2 b_2|^2 = 1$. U matričnoj reprezentaciji četiri svojstvena stanja ovog sustava su:

$$\begin{aligned} |00\rangle &= \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \, , \, |01\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} \\ |10\rangle &= \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} \, , \, |11\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} \end{aligned} \tag{2.42}$$

Vjerojatnost mjerenja jednog od svojstvenih stanja i dalje je jednaka $P_1 = |\langle x_i x_j|\psi\rangle|^2$. Osim mjerenja cijelog sustava, moguće je mjeriti svaki qbit pojedinačno. Takvim parcijalnim mjerenjem mijenja se stanje samo mjerenog qbita dok ostali ostaju u istom stanju. Na primjer, vjerojatnost da će prvi qbit u sustavu dva qbita biti u stanju 0 iznosi:

$$p_1(0) = P(00) + P(01) = |a_1 a_2|^2 + |a_1 b_2|^2, \tag{2.43}$$

te je novonastali vektor stanja potrebno nanovo normalizirati [3]:

$$|\psi\rangle = \frac{a_1 a_2 |00\rangle + a_1 b_2 |01\rangle}{\sqrt{|a_1 a_2|^2 + |a_1 b_2|^2}}. \tag{2.44}$$

Sada možemo opisati kvantna vrata koja djeluju na sustave više qbitova.

2.4.1 SWAP vrata

SWAP vrata zamijenjuju (eng. *swap*) stanja qbitova u sustavu dva qbita (npr. $|01\rangle \rightarrow |10\rangle$). U matričnom se obliku zapisuju:

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}. \tag{2.45}$$

Ova se vrata mogu implementirati primjenom triju CNOT vrata (odjeljak 2.3.1). Korijen iz SWAP vrata, $\sqrt{\text{SWAP}}$, obavlja polovicu akcije SWAP vrata. U matričnom obliku glasi:

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & \frac{1+i}{2} & \frac{1-i}{2} & 0 \\ 0 & \frac{1-i}{2} & \frac{1+i}{2} & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}. \tag{2.46}$$

Kombinacijom $\sqrt{\text{SWAP}}$ vrata s rotacijskim vratima mogu se implementirati bilo koja druga vrata. [3]

2.4.2 Kontrolirana U vrata

Kontrolirana U vrata u matričnom zapisu glase:

$$C(U) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & u_{00} & u_{01} \\ 0 & 0 & u_{10} & u_{11} \end{bmatrix}, \tag{2.47}$$

gdje je $U = \begin{bmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{bmatrix}$ jedna od Paulijevih matrica. Djelovanje U vrata na sustav općenito ima oblik:

$$\begin{aligned} |00\rangle &\rightarrow |00\rangle \\ |01\rangle &\rightarrow |01\rangle \\ |10\rangle &\rightarrow |1\rangle \otimes \mathrm{U}\,|0\rangle \\ |11\rangle &\rightarrow |1\rangle \otimes \mathrm{U}\,|1\rangle\,, \end{aligned} \tag{2.48}$$

gdje lijevi qbit služi kao kontrolni qbit, a desni qbit je meta djelovanja vrata.
Kontrolirana NOT (CNOT) ili cX vrata djeluju X-vratima na ciljani qbit ako je kontrolni qbit u stanju $|1\rangle$. Inače se ciljani qbit ne mijenja, a kontrolni qbit u svakom slučaju ostaje nepromijenjen. U matričnom se obliku cX vrata zapisuju kao:

$$\mathrm{CNOT} = cX = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}. \tag{2.49}$$

cY i cZ (CPHASE) vrata djeluju slično kao cX vrata, samo što umjesto Paulijevih X-vrata koriste Y-, to jest Z-vrata.
Postoje još kontrolirana Hadamardova (cH) vrata, kontrolirana Rz vrata, kontrolirana U_3 i U_1 vrata... Sva ova vrata djeluju svojim pripadnim unitarnim operatorima na ciljani qbit ako je kontrolni qbit u stanju $|1\rangle$, a inače ga ostavljaju nepromijenjenog. [3]

2.4.3 Produžena vrata

Produžena vrata (eng. *extended gates*) djeluju na tri qbita. Toffolijeva ili CCNOT vrata imaju dva kontrolna qbita i jedan ciljani qbit. Ona primjenjuju NOT vrata na ciljani qbit ako su oba kontrolna qbita u stanju $|1\rangle$. Fredkinova ili CSWAP vrata imaju jedan kontrolni i dva ciljana qbita; ako je kontrolni bit $|1\rangle$, primijenit će na dva ciljana bita SWAP vrata. Deutchova (D(θ)) vrata provode rotaciju $R_x(\theta)$ nad ciljanim qbitom ako to dopuste dva kontrolna qbita. [3]

2.4.4 Univerzalnost kvantnih vrata

Univerzalna vrata su skup vrata čijom se uzastopnom primjenom mogu izvesti sve moguće operacije na sustav. U klasičnom računanju skup univerzalnih vrata čine NOT, OR i AND vrata. [2] Koja su vrata univerzalna u kvantnom računanju?
Univerzalnost kvantnih vrata zahtijevala bi da se pomoću njih može izvesti rotacija R(θ). Kako kut θ može poprimiti proizvoljnu vrijednost na kontinuiranom spektru, čini se da bio bilo

nemoguće svaku rotaciju svesti na konačan broj vrata. Zato se univerzalnost kvantnih vrata definira aproksimacijom zvanom Solvay-Kitajev teorem. Ovaj teorem kaže da će skup od G kvantnih vrata biti univerzalan ako vrijedi

$$\forall U \ , \forall \epsilon > 0 \ , \exists g_1, g_2 ... g_n \in G : ||U - U_{g_1}, U_{g_2} ... U_{g_n}|| \leq \epsilon, \tag{2.50}$$

to jest da će za svaki univerzalni operator U razlika između U i niza operatora iz G biti manja od nekog proizvoljno malog broja ϵ. Najčešće korišteni set univerzalnih kvantnih vrata čine tzv. Cliffordova grupa (H-vrata, CNOT vrata, fazna vrata) i T vrata. [3] Univerzalni skup također daju Toffoli vrata zajedno s H-vratima. [2]
Odabir pravog skupa univerzalnih vrata važan je jer kvantna računala koja koriste samo određene operacije neće biti odviše korisna. Može se dokazati da se kvantni krugovi koji unitarno evoluiraju koristeći samo operacije iz Cliffordove grupe, te mjerenja i pripremu qbitova u komputacijskoj bazi, mogu efektivno simulirati na klasičnim računalima. Ova se tvrdnja zove Gottesman-Knill teorem. Za nadmoć kvantnog računala nad klasičnim nužno je koristiti kompleksnija vrata. [9]

2.5 Svojstva kvantnih sustava u računarstvu

Iako se bitovi u klasičnim digitalnim računalima danas realiziraju preko poluvodičkih tranzistora koji u radu koriste kvantni fenomen tuneliranja, sama klasična računala nisu kvantni sustavi. Kvantna računala pak podatke pohranjuju u kvantnim sustavima, to jest qbitovima. Zbog zakona kvantne mehanike kod kvantnog računarstva dolazi do izražaja niz važnih svojstava koja nisu prisutna u klasičnim računalima. Neka od njih otežavaju rad kvantnih računala, dok neka omogućavaju nove načine pohranjivanja i prijenosa podataka. [2] Ovdje se opisuju neka svojstva ključna za rad kvantnih računala.

2.5.1 Kvantno ispreplitanje

Ako su dva kvantna sustava u superpoziciji takvoj da se ne mogu separirati, kaže se da su oni isprepleteni (eng. *entangled*). Isprepleteni se sustavi ne mogu opisati svaki zasebno - mjerenje jednog automatski će odrediti stanje drugog, bez obzira na njihovu udaljenost. [2] Oni se također zovu EPR (Einstein Podolsky Rosen) parovi, po članku u kojem su ih navedena trojica prvi opisali. [10] Isprepleteni qbitovi primjenjuju se u kvantnom računanju, pogotovo u kvantnoj komunikaciji.
Na primjer, ako na sustav dva qbita djelujemo H vratima, a onda CNOT vratima, dobit ćemo

jedno od četiri takozvana Bellova stanja:

$$\begin{aligned}
|00\rangle &\to \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = |\phi^+\rangle \\
|01\rangle &\to \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) = |\phi^-\rangle \\
|10\rangle &\to \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) = |\psi^+\rangle \\
|11\rangle &\to \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) = |\psi^-\rangle
\end{aligned} \tag{2.51}$$

Ova se stanja ne mogu izraziti preko stanja pojedinačnih qbitova, stoga čine EPR par. [3]

2.5.2 Teorem o nemogućnosti kloniranja

Teorem o nemogućnosti kloniranja (eng. *no-cloning theorem*) kaže da nije moguće napraviti kopiju qbita u proizvoljnom nepoznatom stanju. Recimo da qbit može biti u stanju $|\phi\rangle$ ili $|\psi\rangle$, te da njegovo stanje želimo klonirati na qbit $|0\rangle$ pomoću operatora kloniranja C. Očekuje se da će nakon kloniranja oba qbita biti u istom stanju:

$$\begin{aligned}
|\phi\rangle \otimes |0\rangle &\to |\phi\rangle \otimes |\phi\rangle \\
|\psi\rangle \otimes |0\rangle &\to |\psi\rangle \otimes |\psi\rangle
\end{aligned} \tag{2.52}$$

Međutim, iz ovoga proizlazi:

$$\begin{aligned}
\langle\phi|\psi\rangle = \langle\phi|\psi\rangle \langle 0|0\rangle = (\langle\phi| \otimes \langle 0|)C^\dagger C(|\psi\rangle \otimes |0\rangle) \\
= (\langle\phi| \otimes \langle\phi|)(|\psi\rangle \otimes |\psi\rangle) = \langle\phi|\psi\rangle \langle\phi|\psi\rangle = \langle\phi|\psi\rangle^2,
\end{aligned} \tag{2.53}$$

što je moguće samo kad su stanja $|\psi\rangle$ i $|\phi\rangle$ ortonormirana, što općenito nije slučaj. [3] U klasičnim računalima ispravljanje pogrešaka može se implementirati kloniranjem stanja bitova te mjerenjem velikog broja tako nastalih identičnih sustava. No-cloning teorem onemogućava korištenje ove metode za kvantno ispravljanje pogrešaka, jer se qbit može kopirati samo uz uništenje originala. [2]

2.5.3 Supergusto kodiranje

Supergusto kodiranje omogućava da se pomoću jednog qbita pošalju dva klasična bita informacija, pod uvjetom da pošiljatelj i primatelj imaju po isprepleteni qbit. Recimo da neki izvor isprepletе dva qbita u Bellovom stanju $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, te da Alice dobije qbit A, a Bob qbit B[1]. Alice primjenom X i/ili Z vrata preoblikuje svoj qbit u jedan od četiri moguća

[1] Alice i Bob su fiktivni par koji se često koristi za ilustraciju sigurnosnih protokola u kriptografiji.

oblika poruke koju želi poslati (00, 01, 10, 11), čime se isprepleteno stanje mijenja u jedno od Bellovih stanja (ili ne mijenja ako Alice šalje signal 00). Alice pošalje svoj qbit Bobu koji sada ima dva isprepletena qbita. Bob izvornu poruku može dekodirati prvo primjenom CNOT vrata na qbit B pa primjenom H vrata na qbit A, te naposljetku Z mjerenjem oba qbita.
Na primjer, ako Alice želi poslati poruku $|10\rangle$, na svoj će qbit primijeniti Z-vrata, zbog čega će se isprepleteno stanje promijeniti u $|\phi^-\rangle$:

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

Alice sada šalje qbit Bobu. Da bi dekodirao poruku, Bob djeluje CNOT vratima na qbit B, s qbitom A kao kontrolnim:

$$|\phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \rightarrow \frac{1}{\sqrt{2}}(|00\rangle - |10\rangle),$$

a onda djeluje Hadamardovim vratima na qbit A:

$$\frac{1}{\sqrt{2}}(|00\rangle - |10\rangle) \rightarrow \frac{1}{\sqrt{2}}(H|0\rangle|0\rangle - H|1\rangle|0\rangle) = |1\rangle|0\rangle = |10\rangle\,.$$

Naposljetku, Bob izvornu poruku dobiva Z mjerenjem. [3]

2.5.4 GHZ i W stanje

Osim ispreplitanja parova qbitova, može doći i do ispreplitanja većeg broja qbitova, tzv. multipartitnog ispreplitanja. Kao primjeri mogu se navesti GHZ i W stanje. Greenberger-Horne-Zeilinger (GHZ) stanje je isprepleteno kvantno stanje triju qbitova:

$$|\text{GHZ}\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle). \tag{2.54}$$

Ako se izmjeri samo jedan qbit GHZ stanja, sustav će se raspasti u neisprepleteno stanje dvaju qbitova. Isprepletenost ovog sustava doći će do izražaja samo kad se sva tri qbita mjere istovremeno.
W stanje je definirano kao:

$$|\text{W}\rangle = \frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |100\rangle). \tag{2.55}$$

Za razliku od GHZ stanja, mjerenje ili gubitak jednog qbita u W stanju neće dokinuti isprepletenost. Zbog ovog se svojstva W stanje primjenjuje u kvantnoj memoriji. [3]

2.5.5 Globalna faza i fazni povrat

Stanje qbita može se opisati vektorom

$$|\psi\rangle = a\,|0\rangle + b\,|1\rangle\,, \tag{2.56}$$

gdje su a i b kompleksni brojevi koji predstavljaju amplitude vjerojatnosti. Ovi se kompleksni brojevi mogu zapisati u eksponencijalnom obliku:

$$|\psi\rangle = r_1 e^{i\theta_1}\,|0\rangle + r_2 e^{i\theta_2}\,|1\rangle = e^{i\theta_1}(r_1 e\,|0\rangle + r_2 e^{i(\theta_2-\theta_1)}\,|1\rangle). \tag{2.57}$$

Faktor $e^{i\theta_1}$ se zove globalna faza, a faktor $(\theta_2 - \theta_1)$ se zove relativna faza. Očigledno je da će u kvadratu norme $|\,|\psi\rangle\,|^2$ globalna faza nestati, zbog čega ona ne utječe na kvantni program, dok relativna faza utječe.
Proces prebacivanja globalne faze jednog qbita u relativnu fazu drugog zove se fazni povrat (eng. *phase kickback*). Ovaj se proces često koristi u kvantnim programima. [3]

2.6 DiVincenzovi kriteriji za kvantna računala

Prije prelaska na užu tematiku kvantnog ispravljanja pogrešaka, navode se zahtjevi koje kvantno računalo treba ispuniti da bi bilo funkcionalno i korisno. Američki fizičar David DiVincenzo sažeo je u sedam kriterija osnovna svojstva koja se očekuju od kvantnog računala [2][3]:

1. Kvantna računala moraju imati dobro definirane qbitove koji čine sustav koji se može skalirati. Dobro definirani qbit mora imati lako razlučiva osnovna stanja. Mnogo veći tehnički problem predstavlja izgradnja qbita koji se lako može skalirati na veće sustave. Što je qbitova više, to je sve teže ispravljanje pogrešaka za sustav.

2. Qbit treba biti moguće brzo i lako inicijalizirati u osnovno stanje $|0\rangle$.

3. Qbit mora imati dugo vrijeme koherencije, u najmanju ruku dulje od vremena vrata. Zato sustavi kvantnih računala moraju biti izolirani od okoline.

4. Za realizaciju algoritama potreban je minimalni set univerzalnih kvantnih vrata.

5. Mora postojati mogućnost mjerenja qbita. Potrebna su "jaka" mjerenja qbitova koja ih projiciraju u klasične bitove kao i "slaba" mjerenja koja čuvaju qbit.

6. Da bi komunikacija između kvantnih sustava bila moguća, stacionarni qbitovi se pretvaraju u tzv. leteće qbitove. Riječ je o fotonima koji se enkodiraju polarizacijom te šalju optičkim kabelom drugim kvantnim sustavima. Mora biti moguće pretvoriti "stacionarne" qbitove u "leteće" i ponovno dekodirati leteće qbitove u sustavu-primaocu.

7. Mora biti moguća transmisija letećih qbitova među sustavima bez gubitka informacija dekoherencijom.

3 Kvantno ispravljanje pogrešaka

Među glavnim preprekama na putu k funkcionalnom kvantnom računalu ističe se problem kvantnih pogrešaka. Iako su razvijeni brojni kvantni kodovi koji na simulatorima daju dobre rezultate, na stvarnim kvantnim računalima izvršavaju se sa značajnom greškom. Ove pogreške proizlaze dijelom iz dekoherencije zbog interakcija qbitova s okolinom. Kvantna vrata su unitarni operatori koji se ne mogu savršeno fizikalno reprezentirati, što dodatno doprinosi pogreški. [3] Iako su moderna klasična računala veoma otporna na pogreške, brojni su im klasični sustavi ipak podložni. Zato je razvijen niz različitih metoda ispravljanja pogrešaka za klasične računalne sustave. Međutim, zbog fundamentalnih razlika između klasičnih i kvantnih računala, ovi se kodovi ne mogu primijeniti za kvantno ispravljanje pogrešaka. [4]
U ovom poglavlju opisuju se neke metode za ispravljane pogrešaka u kvantnim programima te se uvode osnove teorije kvantnog ispravljanja pogrešaka.

3.1 Klasično ispravljanje pogrešaka

Ispravljanje pogrešaka u kvantnim sustavima djelomično se oslanjaju na klasično ispravljanje. Zato se ovdje ukratko opisuju neki bitni kodovi za ispravljanja pogrešaka u klasičnim računalima.

3.1.1 Parnost

Parnost je kod koji dodaje informacije na kodnu riječ, to jest sustav koji se želi zaštititi, tako da broj jedinica u sustavu bude paran. Na primjer, na 8-bitni sustav 00101000 s dvije jedinice, parnost će dodati nulu. Na sustav s tri jedinice 10011000 će pak dodati jedinicu. Nakon što sustav prođe kroz bučni proces, provjerava se parnost. Ako je broj jedinica neparan, znači da je došlo do preokretanja jednog bita. Međutim, sposobnost detekcije ovog koda ograničena je na samo jednu pogrešku, te je on ne može ispraviti. [3]

3.1.2 Linearni kodovi

Linearni kod enkodira k bitova podataka u n bitova prostora koda. Broj n naziva se duljina bloka, a k duljina poruke. Valja napomenuti da se sve operacije zbrajanja i množenja u ovom odjeljku izvršavaju kao modulo 2[2]. Prostor koda definiran je $n \times k$ generatorskom matricom $\mathscr{G}$ s elementima $\{0, 1\}$ koja preslikava poruke u enkodirani oblik. Na primjer, ponavljački kod štiti bitove tako što ih umnaža tri puta: $\mathscr{G}(0, 1) = (0, 0, 0, 1, 1, 1)$. [3] Generatorska matrica koda

[2]U modulo-2 operacijama, na rezultat zbrajanja ili množenja se djeluje operatorom %2, koji vraća ostatak diobe sa dva.

koji jedan bit ponavlja tri puta glasi:

$$\mathscr{G} = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}. \tag{3.1}$$

Budući da ovaj kod enkodira jedan (k) bit pomoću tri (n) bita, označava se kao [3, 1] linearni kod. Linearnim kodom mogu se konstruirati matrice za provjeru parnosti H. Na primjer, matrica provjere parnosti za ponavljački [3, 1] kod dobiva se tako da se odaberu $3 - 1 = 2$ linearno nezavisna vektora ortogonalna na stupce $\mathscr{G}$:

$$H = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}. \tag{3.2}$$

Pri djelovanju na vektor x s neparnim brojem jedinica, matrica provjere parnosti vraća 0, a djelovanjem na vektor s parnim vraća 1. Dualni kod od linearnog koda C sastoji se od vektora ortogonalnih na svaki vektor od C te se označava sa $C^{\perp}$. Valja primijetiti da je generatorska matrica od $C^{\perp}$ matrica provjere parnosti od C. [4]

3.1.3 Hammingov kod

Hammingovi kodovi su vrsta linearnih kodova koji detektiraju dvobitne i ispravljaju jednobitne pogreške. [3] Neka postoji neki kod s duljinom bloka $n = 2^r - 1$ i duljinom poruke $k = 2^r - r - 1$, gdje je $r \geq 2$ cijeli broj. Matrica provjere parnosti za ovaj kod sastojat će se od r linearno nezavisnih vektora različitih od 0, te će tako definirati Hammingov kod. Kad je $r = 3$, matrica provjere parnosti za [7, 4] kod glasit će:

$$H = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}. \tag{3.3}$$

Ako se dogodi pogreška na j-tom bitu, Hammingova matrica će djelovanjem na sustav vratiti binarnu reprezentaciju rednog broja j. Na taj način H otkriva koji bit treba preokrenuti da bi se ispravila pogreška. [4]

3.2 Osnove Kvantnog ispravljanja pogrešaka

Neka kvantni sustav A u stanju $|\phi_A\rangle$ postoji uz buku iz okoline. Sada se definira kvantni sustav B opisan sa $|\phi_B\rangle$ pripremljen u stanju $|0\rangle$, te se provodi proces enkodiranja E koji preslikava zajedničko stanje od A i B na novo stanje, $|\phi_A\rangle \otimes |\phi_B\rangle \rightarrow |\phi_{AB}^E\rangle = E(|\phi_A\rangle \otimes |\phi_B\rangle)$. Sustav tada prolazi kroz bučni proces $|\phi_{AB}^E\rangle \rightarrow \sum_s e_s |\phi_{AB}^E\rangle$. Da bi se izvorni sustav mogao rekonstruirati, mora postajati operator $E^{\dagger}$ tako da $E^{\dagger} |\phi_{AB}^E\rangle \rightarrow (|\phi_A\rangle \otimes |\phi_B\rangle)$.

Kvantnim ispravljanjem pogrešaka treba pronaći enkodiranje E takvo da će se u procesu najvjerojatnije dogoditi pogreške iz ispravljivog skupa $S = \{e^s\}$. Pritom se pretpostavlja da nema grešaka pri operacijama E i $E^\dagger$, što je moguće samo ako su kvantni krugovi koji ih izvršavaju idealni. [3]
U ispravljanju pogrešaka često se koriste pomoćni (eng. *ancilla*) kvantni sustavi $|\phi_C\rangle$. Riječ je o dodatnim qbitovima pripremljenim u poznata stanja koji se koriste za provođenje ireverzibilnih logičkih operacija. Ako je pomoćni qbit pripremljen u stanju $|0_C\rangle$, nekad je moguće pronaći operator oporavka R koji buku prenosi sa sustava AB na C: $Re^s(|\phi^E_{AB}\rangle \otimes |0_C\rangle) \rightarrow |\phi^E_{AB}\rangle \otimes |S_C\rangle$, za svaki e_s iz C.[4]
Proces ispravljanja kvantnih pogrešaka teče ovako: kod za ispravljanje pogrešaka prvo enkodira sustav s k qbitova u stanjima $\rho_i^{(k)}(0)$ u sustav n qbitova u stanjima $\rho_i^{(n)}(0)$. Tada sustav prolazi kroz bučni proces u vremenu t. Na kraju procesa, n-qbitni $\rho_i^{(n)}(t)$ sustav se dekodira u k-qbitni sustav $\rho_i^{(k)}(t)$. Najjednostavniji primjer enkodiranja je tzv. ponavljački kod, u kom se poruka ponavlja veći broj puta (npr. $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$ se enkodira kao $|\psi\rangle = a\,|000\rangle + b\,|111\rangle$). Dekodiranje se vrši pravilom većine: za onu poruku koja prevladava nakon dekoherencije, pretpostavlja se da je točna (npr. $|010\rangle$ se dekodira kao $|000\rangle$). [3]

3.2.1 Kvantni kod

Kvantnu pogrešku opisuje operator E:

$$|\phi\rangle = E\,|\psi\rangle\,. \tag{3.4}$$

Ako se mogu ispraviti neke proizvoljne greške E_a i E_b, onda se može ispraviti bilo koja njihova linearna kombinacija $E = aE_a + bE_b$. Budući da se mogu razlikovati samo ortogonalna stanja $\langle\psi_i|\psi_j\rangle = 0$; $i \neq j$, stanja koja proizlaze iz djelovanja operatora pogreški, mogu se razlikovati samo ako su ortogonalna:

$$\langle\psi_i|E_a^\dagger E_b|\psi_j\rangle = 0. \tag{3.5}$$

U klasičnom računalu, prisutnost pogreške u bitovima određuje se mjerenjem. Međutim, u kvantnim računalima mjerenje će uništiti stanja $|\psi_i\rangle$ ili $|\psi_j\rangle$. Zato se podatci o $|\psi_i\rangle$ prikupljaju mjerenjem izraza $\langle\psi_i|E_a^\dagger E_b|\psi_i\rangle$, što je moguće samo ako je $\langle\psi_i|E_a^\dagger E_b|\psi_i\rangle$ konstanta po svim baznim stanjima. Ovo je nužni uvjet za kvantni kod:

$$\langle\psi_i|E_a^\dagger E_b|\psi_j\rangle = C_{ij}\delta_{ij}, \tag{3.6}$$

gdje je C_{ij} konstanta koja u sebi objedinjuje zahtjev da greške ne unište ortogonalnost baznih stanja.
Da bi se enkodirao jedan qbit podataka koji onda tvore tzv. logički qbit, zbog ispravljanja pogreška ga je potrebno enkodirati pomoću više fizikalnih qbitova. Neka postoji neki kod za

kvantno ispravljanje pogrešaka sa $2^k = 2$ baznih stanja koji preslikava jedan logički qbit u n fizikalnih qbitova u Hilbertovom prostoru dimenzije 2^n:

$$|0\rangle_L = \sum_i a_i |i\rangle\,,\ |1\rangle_L = \sum_i b_i |i\rangle \tag{3.7}$$

Kod za ispravljanje pogrešaka mora preslikati 2D prostor koji opisuju ova dva isprepletena logička qbita u 2D Hilbertove prostore nužne da se isprave tri vrste pogrešaka (preokretanje bita, preokretanje faze i njihova kombinacija) za svaki od n fizikalnih qbitova. Dakle, Hilbertov prostor mora biti dovoljno velik da sadrži dva seta (jedan za svaki logički qbit) $(3n + 1)$ ortogonalnih 2D potprostora, po jedan za svaku vrstu pogreške po qbitu, te još jedan za potprostor bez grešaka. Ovaj zahtjev definira Hammingovu kvantnu vezu, nejednakost koja određuje minimalni broj qbitova za enkodiranje logičkih qbitova za zaštitu od jedne od prethodno navedenih pogrešaka: $2(3n + 1) \leq 2^n$. Dakle, za enkodiranje $|0\rangle_L$ i $|1\rangle_L$ potrebno je minimalno 5 fizikalnih qbitova. [3]

3.2.2 Kvantne pogreške

Tri vrste pogrešaka u kvantnim sustavima proizlaze iz interakcije sustava s okolinom. Njihov utjecaj na sustav $|\psi\rangle = a|0\rangle + b|1\rangle = \begin{bmatrix} a \\ b \end{bmatrix}$ može se modelirati Paulijevim matricama. Kada nema pogreške u sustavu, koristi se jedinična matrica:

$$\sigma_1 |\psi\rangle = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} a \\ b \end{bmatrix} = a|0\rangle + b|1\rangle\,. \tag{3.8}$$

Amplitudna greška ili greška preokretanja bita (eng. *bit-flip*) zamjeni stanja $|0\rangle$ i $|1\rangle$, što se opisuje Paulijevom X matricom:

$$\sigma_x |\psi\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} b \\ a \end{bmatrix} = b|0\rangle + a|1\rangle\,. \tag{3.9}$$

Fazna greška ili greška preokretanja faze (eng. *phase-flip*) uzrokuje Paulijevu Z rotaciju na qbitu:

$$\sigma_z |\psi\rangle = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} a \\ -b \end{bmatrix} = a|0\rangle - b|1\rangle\,. \tag{3.10}$$

Kod greška preokretanja faze i bita, dvije prethodne greške se događaju istovremeno, što opisuje Paulijeva Y matrica [3]:

$$\sigma_y |\psi\rangle = i \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} -b \\ a \end{bmatrix} = i(a|1\rangle + b|0\rangle). \tag{3.11}$$

3.2.3 Ispravljanje preokretanja bita

Prvi korak u ispravljanju greške preokretanja bita je enkodiranje stanja $|\psi\rangle = a|0\rangle + b|1\rangle$ u $|\psi\rangle = a|000\rangle + b|111\rangle$. Ovo se postiže tako da se na početno stanje oblika

$$|\psi\rangle = (a|0\rangle + b|1\rangle) \otimes |0\rangle \otimes |0\rangle = a|000\rangle + b|100\rangle \tag{3.12}$$

primjene dva CNOT vrata s qbitom q[0] kao kontrolnim i djelovanjem na q[1] te q[2]:

$$\text{CNOT}_{1,2}\text{CNOT}_{1,3}|\psi\rangle = a\text{CNOT}_{1,2}\text{CNOT}_{1,3}|000\rangle + b\text{CNOT}_{1,2}\text{CNOT}_{1,3}|100\rangle \rightarrow a|000\rangle + b|111\rangle\,. \tag{3.13}$$

Kad prolazi kroz bučni proces, postoje četiri moguća ishoda ili sindroma: odsustvo pogreške ($|\psi\rangle = a|000\rangle + b|111\rangle$), preokretanje prvog bita ($|\psi_1\rangle = a|100\rangle + b|011\rangle$), preokretanje drugog bita ($|\psi_2\rangle = a|010\rangle + b|101\rangle$) i preokretanje trećeg bita ($|\psi_3\rangle = a|001\rangle + b|110\rangle$). Potrebno je odrediti sindrom sustava bez mjerenja koje bi uništilo njegovo stanje. To se može postići pohranjivanjem sindroma u pomoćne qbitove.
Uvode se dva pomoćna qbita u stanju $|0\rangle$. Sada se qbitovi s porukom ($|\psi\rangle$ iz 3.13) isprepliću s pomoćnim qbitovima primjenom četiriju CNOT vrata. Prva dva CNOT vrata koriste drugi, to jest treći, qbit poruke kao kontrolni, a prvi pomoćni qbit kao metu. Druga dva CNOT vrata koriste prvi, to jest treći, qbit poruke kao kontrolni, a drugi pomoćni qbit kao metu. Na primjer, za preokretanje prvog qbita:

$$\begin{aligned}
&\text{CNOT}_{2,4}\text{CNOT}_{3,4}\text{CNOT}_{1,5}\text{CNOT}_{3,5}(a|100\rangle + b|011\rangle) \otimes |0\rangle \otimes |0\rangle \\
&\quad = \text{CNOT}_{2,4}\text{CNOT}_{3,4}\text{CNOT}_{1,5}\text{CNOT}_{3,5}(a|10000\rangle + b|01100\rangle) \\
&\quad \rightarrow (a|10001\rangle + b|01101\rangle) = (a|100\rangle + b|011\rangle) \otimes |0\rangle \otimes |1\rangle
\end{aligned} \tag{3.14}$$

Prvi (najmanje važni) pomoćni qbit postavljen je na 1 ako su drugi ili treći qbit preokrenuti. Drugi (najvažniji) pomoćni qbit postavljen je na 1 ako su prvi ili treći qbit preokrenuti. Dakle, veza pomoćnih qbitova s porukom izgledat će ovako:

$$\begin{aligned}
|\psi\rangle &\leftrightarrow |00\rangle \\
|\psi_1\rangle &\leftrightarrow |01\rangle \\
|\psi_2\rangle &\leftrightarrow |10\rangle \\
|\psi_3\rangle &\leftrightarrow |11\rangle
\end{aligned} \tag{3.15}$$

Pošto je ustanovljena veza između greške i stanja pomoćnih qbitova, greška se može ispraviti bez mjerenja. Ispravak se vrši djelovanjem kombinacije CNOT ili CCNOT vrata s pomoćnim qbitovima kao kontrolnim. [3] Na primjer, za preokretanje prvog qbita:

$$\text{CNOT}_{5,1}(a|10001\rangle + b|01101\rangle) \rightarrow a|00001\rangle + b|11101\rangle = a|000\rangle + b|111\rangle \otimes |0\rangle \otimes |1\rangle \tag{3.16}$$

3.2.4 Ispravljanje preokretanja faze

Pogreška preokretanja faze može se ispraviti na isti način kao preokretanje bita, ako se sustav $|\psi\rangle = a|0\rangle + b|1\rangle$ prvo prebaci u polarnu bazu $\{|+\rangle, |-\rangle\}$ pomoću Hadamardovih vrata:

$$H|0\rangle = |+\rangle, H|1\rangle = |-\rangle, H|+\rangle = |0\rangle, H|-\rangle = |1\rangle. \tag{3.17}$$

U ovoj bazi operator preokretanja faze Z djeluje kao operator preokretanja bita: $Z(a|+\rangle + b|-\rangle) = a|-\rangle + b|+\rangle$. U novoj bazi sustav se enkodira na isti način kao za preokretanje bita. Nakon prolaska kroz bučni proces, ponovno postoje četiri sindroma: odsustvo pogreške ($|\psi\rangle = a|+++\rangle + b|---\rangle$), preokretanje prvog bita ($|\psi_1\rangle = a|-++\rangle + b|+--\rangle$), preokretanje drugog bita ($|\psi_2\rangle = a|+-+\rangle + b|-+-\rangle$) i preokretanje trećeg bita ($|\psi_3\rangle = a|++-\rangle + b|--+\rangle$). [4] Povratak u izvornu baza provodi se Hadamardovom konjugacijom:

$$HXH = Z, HZH = X. \tag{3.18}$$

Budući da je pogreška preokretanja faze opisana operatorom Z, ako se sada na sustav primijeni H, ovaj će se po (3.18) vratiti u komputacijsku bazu. Tada se detekcija pogrešaka i ispravak vrši na analogan način kao u primjeru za preokretanje bita. [3]

3.3 Stabilizacijski formalizam

Prije prelaska na složenije kodove za ispravljanje pogrešaka, treba uvesti stabilizacijski formalizam. Kaže se da je stanje $|\psi\rangle$ stabilizirano operatorom S ako vrijedi $S|\psi\rangle = |\psi\rangle$, to jest ako je $|\psi\rangle$ svojstveni vektor operatora S svojstvene vrijednosti 1. Skup svih takvih operatora zove se stabilizator ili stabilizatorska grupa.

Svaka kodna riječ $|\psi\rangle$ može se opisati jedinstvenom stabilizatorskom grupom. Na primjer, stabilizator troqbitnog ponavljačkog koda $a|0\rangle + b|1\rangle \rightarrow a|000\rangle + b|111\rangle$ glasi $\mathscr{S} = \{I, Z_1Z_2, Z_1Z_3, Z_2Z_3\}$. Ovaj je zapis veoma koristan kod kompleksnih kodova za ispravljanja pogrešaka.

Neka je $\mathscr{G}_n$ grupa koju čini n-terostruki produkt Paulijevih operatora s fazom p koja poprima vrijednosti $p \in \{\pm i, \pm 1\}$. Stabilizator $\mathscr{S}$ se formalno definira kao abelska podgrupa od $\mathscr{G}_n$ koja ne sadrži operator $-I$. Stabilizator se može kraće zapisati preko svojih generatora, to jest elementa stabilizatorske grupe iz kojih se mogu izvesti svi ostali elementi iste. Na primjer, $\mathscr{S} = \{I, Z_1Z_2, Z_1Z_3, Z_2Z_3\}$ se preko svojih generatora može zapisati kao $\mathscr{S} =< Z_1Z_2, Z_2Z_3 >$. [2]

Neka je Q kvantni kod koji se sastoji od n-qbitnih kvantnih riječi $|\psi_i\rangle$. Neka postoje operatori M_i koji detektiraju pogreške na kodnim riječima, te koji su generatori nekog stabilizatora $\mathscr{S}$. Svojstvena vrijednost generatora bit će 1 ako djeluju na neizmijenjene kodne riječi od Q, a -1 ako je došlo do pogreške. Pogreške $E = \{E_1, E_2, ..., E_e\}$ na kodnim riječima također su

podgrupa od $\mathscr{G}_n$, te su njihovi operatori tenzorski produkti Paulijevih matrica.
U sustavima više qbitova, stabilizacijska stanja se definiraju kao potprostori unutar šire Hilbertovog prostora. Na primjer, za dvoqbitni sustav potreban je četverodimenzionalni Hilbertov prostor, no ako se sustav može opisati dvama ZZ operatorima, za njegovu reprezentaciju su potrebna samo dva ortogonalna stanja:

$$|0\rangle_L \equiv \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \quad |1\rangle_L \equiv \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \tag{3.19}$$

Na taj način se višeqbitni sustav može opisati jednim logičkim qbitom. [3]
Stabilizacijskim formalizmom mogu se opisati i unitarni operatori, to jest kvantna vrata. Neka na kod Q stabiliziran sa $\mathscr{S}$ djeluje unitarni operator U. Ako je $|\psi_i\rangle$ stanje od Q, a g_i element iz $\mathscr{S}$, vrijedi:

$$U|\psi_i\rangle = Ug_i|\psi_i\rangle = Ug_iU^\dagger U|\psi_i\rangle\,. \tag{3.20}$$

Dakle, $Ug_iU^\dagger$ je stabilizator od $U|\psi_i\rangle$. Za primjer se može promotriti djelovanje Hadamardovih vrata na Z operator: $HZH^\dagger = X$. Primjenom H vrata na stanje koje stabilizira Z (npr. $|0\rangle$), dobiva se neko stanje koje stabilizira X (u ovom slučaju $|+\rangle$). Ako je dan n-qbitni sustav sa generatorima stabilizatora $< Z_1, Z_2, ..., Z_n >$, H vrata ga transformiraju u sustav sa generatorima $< X_1, X_2, ..., X_n >$. [4]

3.4 Shorov kod

Shorov kod može ispraviti proizvoljnu pogrešku (preokretanje bita, faze ili oboje) za jedan qbit. Ova metoda prvo enkodira qbit za oporavak od preokretanja faze: $|0\rangle \rightarrow |+++\rangle$, $|1\rangle \rightarrow |---\rangle$. Nakon toga se svaki od ovih qbitova enkodira za oporavak od preokretanja bita, tako da vrijedi: $|+\rangle \rightarrow \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$, $|-\rangle \rightarrow \frac{1}{\sqrt{2}}(|000\rangle - |111\rangle)$. Dakle, Shorov kod jedan qbit štiti od pogreške pomoću sustava od 9 qbitova:

$$\begin{aligned} |0\rangle \rightarrow |0\rangle_L \rightarrow \frac{(|000\rangle + |111\rangle \otimes)(|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle)}{2\sqrt{2}} \\ |1\rangle \rightarrow |1\rangle_L \rightarrow \frac{(|000\rangle - |111\rangle \otimes)(|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle)}{2\sqrt{2}} \end{aligned} \tag{3.21}$$

Ovaj način enkodiranja pomoću hijerarhije razina zove se ulančavanje (eng. *concatenation*): izvorni se qbit enkodira u tri qbita, nakon čega se svaki od njih enkodira u dodatna tri, čime nastaju tri bloka od po tri qbita. [4]
Logički operatori $\overline{X}$ i $\overline{Z}$ za ovako Shorov enkodirani qbit glase:

$$\begin{aligned} \overline{X} &= Z_1Z_2Z_3Z_4Z_5Z_6Z_7Z_8Z_9 \\ \overline{Z} &= X_1X_2X_3X_4X_5X_6X_7X_8X_9 \end{aligned} \tag{3.22}$$

Kako izgleda stabilizator za sustav od 9 qbitova? Grupu $\mathscr{G}$ koja stabilizira taj sustav generira skup osam operatora $M_1, M_2, ..., M_8$ definiranih kao u tablici 1. Stabilizatori su poredani tako da M_1 i M_2 djeluju na prvi blok, M_3 i M_4 djeluju na drugi blok, a M_5 i M_6 na treći. M_7 pak djeluje na prva dva bloka, a M_8 na prvi i treći.
Nadalje, stabilizatori se dijele na dvije klase: prvih šest sadrži par σ_z operatora, a zadnja dva po šest σ_x. Logički qbitovi $|0\rangle_L$ i $|1\rangle_L$ su svojstveni vektori operatora M_i, te se može pokazati da su im svojstvene vrijednosti kod djelovanja na stanje bez pogreške jednake +1:

$$\begin{aligned} M_i |0\rangle_L &\to |0\rangle_L \\ M_i |1\rangle_L &\to |1\rangle_L \end{aligned} \tag{3.23}$$

Operator greške

$$E_x^{(0)} = X_0 \otimes I_1 \otimes I_2 \otimes I_3 \otimes I_4 \otimes I_5 \otimes I_6 \otimes I_7 \otimes I_8 \tag{3.24}$$

će preokrenuti bit prvom qbitu prvog bloka. Za njega se može pokazati da antikomutira s operatorom M_1:

$$M_1 E_x^0 = -E_x^0 M_1, \tag{3.25}$$

što znači da je E_x^0 svojstveni vektor od M_1 sa svojstvenom vrijednosti -1. Iz tablice 1 se vidi da će u slučaju pogreške na prvom qbitu i M_2 vratiti -1. Dakle, po stabilizatorima koji pri mjerenju vraćaju svojstvenu vrijednost -1, određuje se mjesto pogreške koju onda treba ispraviti primjenom odgovarajućih vrata.
Za detekciju preokretanja bita služi prvih šest stabilizatora, a preokretanja faze zadnja dva. Na primjer, ako primjenom stabilizatora $M_1, ..., M_6$ samo M_2 vraća -1, znači da se pogreška preokretanja bita dogodila na drugom qbitu. Pogrešku ispravljamo primjenom operatora X na taj qbit. Nakon toga se na sustav djeluje stabilizatorima M_6 i M_7. Ako oba vrate -1, dogodila se pogreška na prvom bloku, te se ona ispravlja primjenom Z operatora na taj blok. [3]

Tablica 1: *Djelovanje stabilizatora na 9 qbita u Shorovom kodu [3]*

qbitovi→ ↓ operatori	0	1	2	3	4	5	6	7	8
M_1	Z	Z	I	I	I	I	I	I	I
M_2	Z	I	Z	I	I	I	I	I	I
M_3	I	I	I	Z	Z	I	I	I	I
M_4	I	I	I	Z	I	Z	I	I	I
M_5	I	I	I	I	I	I	Z	Z	I
M_6	I	I	I	I	I	I	Z	I	Z
M_7	X	X	X	X	X	X	I	I	I
M_8	X	X	X	I	I	I	X	X	X

3.5 Steaneov kod

Steaneov kod primjer je šire skupine CSS (Calderbank, Shor, Steane) kodova. Neka su C_1 i C_2 neki klasični linearni kodovi koji k_1, to jest k_2 bitova enkodiraju u n bitova, što se označava sa $[n, k_1]$, $[n, k_2]$. Neka također za njih vrijedi $C_2 \subset C_1$, te da C_1 i $C_2^{\perp}$ ispravljaju pogreške na t bitova [4], gdje je $C_2^{\perp}$ ortogonalni kod od C_2. [3] Tada se može konstruirati $[n, k_1 - k_2]$ kvantni kod CSS(C_1, C_2) koji ispravlja pogreške na t qbitova.
Steaneov kod se konstruira pomoću Hammingovog koda za klasično ispravljanje pogrešaka. Matrica provjere parnosti za Hammingov kod glasi:

$$C = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}. \tag{3.26}$$

Uvode se definicije $C \equiv C_1$ i $C^{\perp} \equiv C_2$. Da bi se s ovim kodovima mogao konstruirati CSS kod, mora biti zadovoljen uvjet $C_2 \subset C_1$. Po definiciji (odjeljak 3.1.2), matrica provjere parnosti od $C^{\perp}$ jednaka je transponiranoj matrici generatora od C:

$$H[C_2] = G[C_1]^T = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}. \tag{3.27}$$

Svi redci iz $H[C_2]$ sadržani su u C što znači da je ispunjen uvjet da C_2 mora biti podskup od C_1. Budući da su C_1 i C_2 kodovi tipa [7, 4], to jest [7, 3], Steaneov kod je sedmeroqbitni kod koji ispravlja jedan qbit, [7, 1]. [4]
Hammingov kod (odjeljak 3.1.3) sadrži $2^4 = 16$ kodnih riječi, koje po broju jedinica možemo podijeliti na parne i neparne. Logički qbit $|0_L\rangle$ za Steaneov kod definira se kao superpozicija svih parnih kodnih riječi iz Hammingovog koda:

$$\begin{aligned} |0_L\rangle \rightarrow \frac{1}{\sqrt{8}}[&|0000000\rangle + |0001111\rangle + |0110011\rangle \\ &+ |0111100\rangle + |1010101\rangle + |1011010\rangle \\ &+ |1100110\rangle + |1101001\rangle], \end{aligned} \tag{3.28}$$

a $|1_L\rangle$ kao superpozicija svih neparnih kodnih riječi iz Hammingovog koda:

$$\begin{aligned} |1_L\rangle \rightarrow \frac{1}{\sqrt{8}}[&|0010110\rangle + |0011001\rangle + |0100101\rangle \\ &+ |0101010\rangle + |1000011\rangle + |1001100\rangle \\ &+ |1110000\rangle + |j1111111\rangle]. \end{aligned} \tag{3.29}$$

Da bi se Steaneov kod implementirao, prvo se stanje sustava enkodira primjenom dvaju CNOT vrata te se primjenom H vrata zadnja tri qbita pripreme u jednaka stanja superpozicije:

$$|\psi\rangle_L \rightarrow (a\,|000\rangle + b\,|111\rangle) \otimes |0\rangle \otimes \frac{1}{\sqrt{8}}[(|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle)], \tag{3.30}$$

što se može raspisati kao

$$\begin{aligned} \rightarrow \frac{1}{\sqrt{8}} a(&|0000000\rangle + |0000001\rangle + |0000010\rangle + |0000011\rangle \\ &+ |0000100\rangle + |0000101\rangle\,|0000110\rangle + |0000111\rangle) \\ +\frac{1}{\sqrt{8}} b(&|1110000\rangle + |1110001\rangle + |1110010\rangle + |1110011\rangle \\ &+ |1110100\rangle + |1110101\rangle + |1110110\rangle + |1110111\rangle). \end{aligned} \tag{3.31}$$

Tada se na sustav primjenjuju tri bloka CNOT vrata: prvi blok za kontrolni uzima qbit q[4], a za mete q[1], q[2] i q[3]. Drugi blok za kontrolni uzima qbit q[5], a za mete q[0], q[2] i q[3]. Treći blok za kontrolni uzima qbit q[6], a za mete q[0], q[1] i q[3]. Sustav je najposlije u stanju:

$$\begin{aligned} \frac{1}{\sqrt{8}} a(&|0000000\rangle + |1101001\rangle + |1011010\rangle + |0110011\rangle \\ &+ |0111100\rangle + |1010101\rangle\,|1100110\rangle + |0100111\rangle) \\ +\frac{1}{\sqrt{8}} b(&|1110000\rangle + |0011001\rangle + |0101010\rangle + |1000011\rangle \\ &+ |1001100\rangle + |0100101\rangle + |0010110\rangle + |1111111\rangle). \end{aligned} \tag{3.32}$$

Usporedbom s izrazima za logičke qbitove u Staeneovom kodu, vidi se da je stanje sustava očuvano od greške:

$$|\psi_L\rangle \rightarrow \frac{1}{\sqrt{8}}(a\,|0\rangle_L + b\,|1\rangle_L). \tag{3.33}$$

Primjenom stabilizacijskog formalizma na Steaneov kod, dobivaju se generatori stabilizacijskog koda popisani u tablici 2. Za enkodirana stanja u Steaneeovom kodu vrijedi:

$$\overline{X} \equiv X_1X_2X_3X_4X_5X_6X_7,\ \overline{Z} \equiv Z_1Z_2Z_3Z_4Z_5Z_6Z_7, \tag{3.34}$$

gdje su $\overline{X}$ i $\overline{Z}$ Paulijeva vrata. [3]

Tablica 2: *Djelovanje stabilizatora na 7 qbita u Steaneovom kodu [3]*

qbitovi→ ↓ operatori	0	1	2	3	4	5	6
M_1	I	I	I	X	X	X	X
M_2	I	X	X	I	I	X	X
M_3	X	I	X	I	X	I	X
M_4	I	I	I	Z	Z	Z	Z
M_5	I	Z	Z	I	I	Z	Z
M_6	Z	I	Z	I	Z	I	Z

4 Zaključak

Shorov i Steaneov kod samo su neki od osnovnih kodova za ispravljanje pogrešaka. U razvoju je trenutačno niz različitih shema koje bi trebale pospješiti ovaj proces. Važno je napomenuti da su pogreškama podložni i qbitovi koji se koriste za ispravljanje pogrešaka na drugim qbitovima, kao i mjerenja u procesu ispravljanju pogrešaka. Zato se često paradoksalno događa da povećanje broja qbitova posvećenih ispravljanju pogreški povećava frekvenciju pogrešaka, što predstavlja ozbiljnu prepreku u skaliranju kvantnih računala. Moguće rješenje ovog problema daju takozvani površinski kodovi (eng. *surface codes*). Riječ je o familiji kodova za kvantno ispravljanje pogrešaka koji logički qbit enkodiraju kao isprepleteno stanje $d \times d$ fizičkih qbitova. Nedavna istraživanja Googleovog Quantum AI projekta prvi su puta pomoću ovih kodova postigli da veći, 49-qbitni kod za ispravljanje pogrešaka daje manju frekvenciju grešaka od 17-qbitnog koda. Trenutačno dostupna kvantna računala imaju stopu greške od jedne po tisuću operacija. Procjenjuje se da bi praktično upotrebljiva kvantna računala trebala imati stopu od jedne pogreške na milijun. [12]

Ovakvo se poboljšanje ne može postići samo kodovima za ispravljanje pogrešaka. Klasična računala ne trebaju složene programe za ispravljanje pogrešaka jer su njihovi sustavi veoma otporni na greške. Da bi se kvantna računala usavršila, trebat će razviti qbitove otporne na pogreške. Među nove modele qbitova koji uspijevaju smanjiti frekvenciju pogrešaka broje se $0 - \pi$ qbit, supravodički-poluvodički qbit, itd. [3]

Usprkos velikom napretku u posljednja dva desetljeća, do izgradnje korisnog kvantnog računala još uvijek vodi dug i trnovit put. Velika ulaganja u polje i sve brži napredak ipak bude nadu da će se teoretske blagodati kvantnog računarstva materijalizirati u doglednoj budućnosti.

5 Literatura

[1] M. Brooks, *Quantum computers: what are they good for?*, Nature, 617 S1-S3, 23. 5. 2023.

[2] J. D. Hidary, *Quantum Computing: An Applied Approach*, Springer, 2021.

[3] V. Kasirajan, *Fundamentals of Quantum Computing*, Springer, 2021.

[4] M. A. Nielsen, I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, 2010.

[5] N. Zettili, *Quantum Mechanics*, Wiley, 2022.

[6] A. Beckers, A. Tajalli, J. Sallese, *A Review on Quantum Computing: Qubits, Cryogenic Electronics and Cryogenic MOSFET Physics*, 2019

[7] Bin Cheng, Xiu-Hao Deng, Xiu Gu, Yu He, Guangchong Hu, Peihao Huang, Jun Li, Ben-Chuan Lin, Dawei Lu, Yao Lu, Chudan Qiu, Hui Wang, Tao Xin, Shi Yu, Man-Hong Yung, Junkai Zeng, Song Zhang, Youpeng Zhong, Xinhua Peng, Franco Nori, Dapeng Yu, *Noisy intermediate-scale quantum computers.*, Frontiers of Physics, 18 (2), 2023.

[8] L. N. Cooper, *Bound Electron Pairs in Degenerate Fermi Gas*, Physical Review, 104, 1189-1190, 1956.

[9] S. Aaronson, D. Gottesman, *Improved simulation of stabilizer circuits*. Physical Review, 70 (5), 2004.

[10] A. Einstein, B. Podolsky, N. Rosen, *Can quantum-mechanical description of physical reality be considered complete?*, Phys. Rev., 47:777–780, 1935.

[11] R. Shirey, *Internet Security Glossary, Version 2*, https://datatracker.ietf.org/doc/html/rfc4949, posjećeno 20. 8. 2023.

[12] Google Quantum AI, *Suppressing quantum errors by scaling a surface code logical qubit*, Nauture 614, 676-681, 2023.