НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Факультет електроніки

Кафедра мікроелектроніки

До захисту допущено:

В.о. завідувача кафедри

_____ Дмитро ТАТАРЧУК

«___»_____20__ р.

Дипломна робота

на здобуття ступеня бакалавра

за освітньо-професійною програмою «Мікро- та наноелектроніка»

спеціальності 153 «Мікро- та наносистемна техніка»

на тему: «Квантові алгоритми пошуку об'єктів в неупорядкованому списку**»**

Виконала:
студентка IV курсу, групи ДП-91
Кольчик Ольга Андріївна _____

Керівник: професор, доктор фізико-математичних наук
Королюк Дмитро Володимирович _____

Консультант з нормоконтролю: ст.викл.каф.МЕ, к.т.н.,
Королевич Любомир Миколайович _____

Консультант з інформаційних питань: доц.каф.МЕ, к.т.н., доц.,
Діденко Юрій Віталійович _____

Рецензент: Рецензент: професор кафедри ЕПС, д.т.н., професор
Мельник Ігор Віталійович _____

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.

Студентка _____

Київ – 2023 року

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Факультет електроніки
Кафедра мікроелектроніки

Рівень вищої освіти – перший (бакалаврський)

Спеціальність – 153 «Мікро- та наносистемна техніка»

Освітньо-професійна програма «Мікро- та наноелектроніка»

ЗАТВЕРДЖУЮ
В.о. завідувача кафедри
_____ Дмитро ТАТАРЧУК
«___»_____20__ р.

ЗАВДАННЯ
на дипломну роботу студенту
Кольчик Ользі Андріївні

1. Тема роботи «Квантові алгоритми пошуку об'єктів в неупорядкованому списку», керівник роботи професор, доктор фізико-математичних наук Королюк Дмитро Володимирович, затверджені наказом по університету від «___»_____ 20__ р. №_____

2. Термін подання студентом роботи _____

3. Вихідні дані до роботи

_____

4. Зміст роботи

_____

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо)

_____

6. Консультанти розділів роботи*

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання _____

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів роботи	Відмітка про виконання
	Пошук літератури, ознайомлення з основними поняттями за темою «Квантові обчислення»	04.04.2023 – 07.05.2023	
	Вивчення квантових алгорітмів та їх застосування	08.05.2023 – 23.04.2023	
	Дослідження квантових обчислень приконденсованому стані	08.05.2023 – 23.04.2023	

Студент Ольга Кольчик

Керівник Дмитро Королюк

* Якщо визначені консультанти. Консультантом не може бути зазначено керівника дипломної роботи.

РЕФЕРАТ

Роботу викладено на 51 сторінку, вона містить 2 розділи, 1 таблицю, 11 рисунків, та 22 джерел.

Мета роботи – вивчення основних принципів і можливостей квантових обчислень та їх застосування в мікро і наносистемній техніці.

Об’єкт дослідження – квантові алгоритми пошуку об'єктів в неупорядкованому списку.

Предмет роботи – вивчення основних принципів квантових обчислень та алгоритмів на квантових комп’ютерах.

В першому розділі роботи наведені основні принципи та поняття квантової теорії інформації.

У другому розділі наведені квантові алгоритми, які застосовуються у квантових комп’ютерах, зокрема алгоритми факторизації, пошуку в неупорядкованому списку, розглянуті коди корекції помилок.

Ключові слова: квантові обчислення, квантові алгоритми, квантова теорія інформації, пошук об'єктів у неупорядкованому списку, алгоритми факторизації, коди корекції помилок, квантові комп'ютери.

ABSTRACT

The abstract is presented in 51 page and includes 2 sections, 1 table, 11 figures, and 22 references.

The objective of the study is to explore the fundamental principles and capabilities of quantum computing and their application in micro and nanosystems engineering.

The research object is quantum algorithms for searching objects in an unordered list.

The subject of the study is the understanding of the basic principles of quantum computing and algorithms on quantum computers.

The first section of the paper provides an overview of the fundamental principles and concepts of quantum information theory.

The second section presents quantum algorithms used in quantum computers, including factorization algorithms, searching in an unordered list, and error correction codes.

Keywords: quantum computing, quantum algorithms, quantum information theory, object search in an unordered list, factorization algorithms, error correction codes, quantum computers.

ЗМІСТ

ВСТУП

За останні десятиліття квантові обчислення стали предметом інтенсивних досліджень в галузі інформаційних технологій. Квантова теорія інформації – це наукова галузь, яка з'явилася на зламі 80-х років, на перетині класичної теорії інформації, теорії обчислень та нерелятивістської квантової механіки. Це нове поле досліджень було викликане зростаючим впливом квантово-механічних ефектів на роботу електронних пристроїв, що ставали все меншими, і потребувало боротьби з цим впливом або навіть використання його на користь.

Проте набагато важливішим фактором є принципова обмеженість можливостей класичних комп'ютерів у вирішенні певних класів задач. Використання комп'ютера, що працює на основі принципів квантової механіки, обіцяє у таких випадках експоненційне по обсягу задачі прискорення обчислень.

Квантова теорія інформації існує вже близько 20 років [1, 2]. Історія квантових обчислень розпочалася у 1981 році, коли Річард Фейнман запропонував ідею використання квантових систем для симуляції складних фізичних процесів [3].

Це дало поштовх до ідеї створення універсального обчислювального пристрою на основі квантової фізичної системи [4] та розробки комп'ютерів, що використовують певний набір математичних аксіом, заснованих на фізичних законах [5]. Це призвело до ідеї універсального квантового обчислювального пристрою на основі фізичної системи та створення комп'ютерів, які використовують певний набір математичних аксіом на основі певного набору фізичних законів.

Проте, перші експерименти з квантовими обчисленнями відбулися лише у 1990-х роках [1, 2], коли вчені змогли створити перший квантовий комп'ютер на кілька кубітів. Кількість кубітів – базових одиниць квантової інформації, які використовуються для зберігання та обробки даних - відтоді збільшується, що дозволяє досягати все більших можливостей квантових обчислень.

Однією з найвідоміших задач, яку здатний розв'язувати квантовий комп'ютер, є факторизація великих чисел [2], що є основою шифрування більшості сучасних систем безпеки. Здатність квантового комп'ютера до розв'язування цієї задачі за допомогою квантового алгоритму Шора [6] може загрожувати безпеці інтернет-транзакцій та інших критичних систем.

Одним зі способів застосування квантових обчислень є моделювання властивостей складних молекул, наприклад, молекул, які можна використовувати для створення нових неорганічних світлодіодів для екранів. Такі обчислення можуть бути складними та трудомісткими, вимагають проведення експериментів та значних витрат часу та коштів. Застосування квантових комп'ютерів дозволяє скоротити витрати, оскільки експерименти можна проводити віртуально.

Проте, існують певні виклики, пов'язані з практичним застосуванням квантових обчислень. Зокрема, квантові комп'ютери потребують спеціального апаратного забезпечення, що вимагає значних інвестицій у дослідження та розробку. Крім того, важливо вирішити проблему шуму та помилок, які виникають під час квантових обчислень і можуть вплинути на точність результатів.

Як висновок, дослідження у цій області є надзвичайно важливим для подальшого розвитку технології. Тому необхідно проводити детальні дослідження у галузі квантових вишукань та знайти рішення для вирішення викликів, пов'язаних із їх практичним застосуванням, адже надалі дослідження у цій області можуть привести до нових можливостей у галузі криптографії, медицини, економіки та багатьох інших галузях.

РОЗДІЛ 1. ОСНОВИ КВАНТОВОЇ ТЕОРІЇ ІНФОРМАЦІЇ

1.1. Основні принципи квантової механіки

Принципи квантової механіки є простими, але вони суперечать інтуїтивному розумінню. Одна з задач квантових обчислень та інформації – це розробка інструментів, які допоможуть покращити інтуїтивне розуміння квантової механіки та зроблять її закони більш доступними людському розуму.

Тим не менш, для побудови схеми квантових обчислень у нерелятивістській квантовій механіці в класичній ймовірнісній інтерпретації не потрібно вводити додаткові постулати. Достатньо розглядати системи з кінцевою кількістю ступенів свободи. Відповідні принципи нерелятивістської квантової механіки можна сформулювати наступним чином:

1. Стан ізольованої системи подається залежним від часу вектором $|\psi(t)\rangle$ у деякому гільбертовому просторі. Якщо система має скінчену кількість ступенів свободи, то простір буде кінцево-вимірним векторним простором над полем комплексних чисел, при чому фізичні стани системи будуть представлені нормованими векторами в тому просторі з умовою нормування $\langle\psi|\psi\rangle=1$.

Фізичний зміст такого опису полягає наступному: якщо система може перебувати в двох різних станах $|a\rangle$ і $|b\rangle$, то вона може перебувати і в будь-якій лінійній комбінації цих станів $c_1|a\rangle + c_2|b\rangle$ з комплексними коефіцієнтами c_1, c_2 та умовою нормування $|c_1|^2 + |c_2|^2 =1$. Простішими словами, квантова механіка являє собою лінійну теорію.

2. Фізичні величини, які спостерігаються, подаються операторами відповідного гільбертового простору, а для системи з кінцевою кількістю ступенів свободи відповідно матрицями кінцевого розміру в обраному базисі.

3. Вектор стану еволюціонує з часом відповідно до лінійного диференціального рівняння – рівняння Шрьодінгера:

$$\hbar \frac{d}{dt}|\psi(t)\rangle = \mathcal{H}|\psi(t)\rangle, \qquad (1.1)$$

де $\mathcal{H}$ – оператор Гамільтона для даної системи. Внаслідок цього вектор стану еволюціонує за кінцевий час за рівнянням:

$$|\psi(\mathrm{t})\rangle = U(t)|\psi(0)\rangle, \qquad \text{де } U(t) = \exp\left(-\frac{i}{\hbar}\int \mathcal{H}dt\right) - \qquad (1.2)$$

деякий визначаємий гамільтоніан оператору еволюції. Гамільтоніан - це оператор енергії системи, який визначає її динаміку. Еволюція стану системи в часі описується за допомогою дії оператора еволюції на квантовий стан.

Головна властивість оператора еволюції - його унітарність Застосування оператора еволюції та його спряженого оператора в довільному порядку до стану системи дає початковий стан системи: $U^{+}U = UU^{+} = 1$.

Це забезпечує збереження норми вектора стану та існування оберненого оператора $U^{-1} = U^{+1}$.

Крім того, унітарність оператора еволюції дозволяє зворотно відновити початковий стан системи: $|\psi(0)\rangle = U^{+}\psi(\mathrm{t})\rangle$. Таким чином, еволюція в ізольованій системі є унітарною та оборотною.

4. Постулат вимірювання стверджує наявність взаємодії, відомої як спостереження або вимірювання, при якому квантова система припиняє бути ізольованою і вступає взаємодію з макроскопічною (класичною) системою, яка називається вимірювальним пристроєм і має кілька (скажімо, k) розрізняючих станів.

В результаті такої взаємодії пристрій переходить випадковим чином в один з можливих станів з номером $i = 1\ldots k$, а система переходить до відповідного власного стану $|\psi_i\rangle$. Ймовірність переходу до даного стану P_i залежить лише від конструкції пристрою (тобто вимірюваної величини) та стану системи $|\psi\rangle$ у момент вимірювання. Початковий стан системи незворотно розривається, а єдиним інформаційним відомим елементом, який можна виміряти, є (випадковий) номер стану, в який перейшов пристрій (і, відповідно, система).

Математично можна сформалізувати цей постулат наступним чином. Нехай стан системи описується вектором стану у деякому гільбертовому просторі H.

Спостерігаємою O, ми визначаємо колекцію підпросторів $E_1, E_2, \ldots, E_k \subseteq H$, які повністю розбивають H і не перетинаються між собою:

$$E_1 \times E_2 \times \cdots \times E_k = H, \qquad E_i \perp E_j \text{ для } i,j = 1 \ldots k, i \neq j. \tag{1.3}$$

Любий вектор стану |ψ⟩ може бути представлений як лінійна комбінація (суперпозиція) компонент, що належать кожному з підпросторів Ei.

Основні принципи квантової механіки включають поняття стану, суперпозиції та вимірювання. Суперпозиція стверджує, що два або більше квантових станів можна скласти разом, і результат буде новим квантовим станом. Квантовий комп'ютер використовує цю властивість, щоб обробляти велику кількість операцій паралельно.

Любий вектор стану $|\psi\rangle$ може бути представлений як лінійна комбінація (суперпозиція) компонент, що належать кожному з підпросторів E_i:

$$|\psi\rangle = \sum_{i=1}^{k} \alpha_i \left|\psi_{E_i}\right\rangle, \tag{1.4}$$

де α_i - довільні комплексні коефіцієнти з умовою нормування $\sum_{i=1}^{k} |\alpha_i|^2 = 1$. Тоді результат спостереження вектора стану $|\psi\rangle$ через спостережуваний оператор O буде таким:

A) Буде випадково обраним один з підпросторів E_i з ймовірністю $|\alpha_i|^2$;

B) Початковий вектор стану $|\psi\rangle$ звузиться до нормованого $|\psi E_i\rangle$;

C) Єдиною отриманою інформацією буде номер обраного підпростору i.

Таким чином, при повторному вимірюванні ми завжди отримуємо практично той же результат, оскільки вектор стану знаходиться в E_i. Можемо зробити висновок, що операція вимірювання також перетворює квантову систему, але оператор перетворення (зазвичай називається проектором) не є ні унітарним, ні оборотним.

Зрозуміло, що описана схема має свої обмеження. Вона придатна лише для систем з дискретним спектром і працює з чистими станами, ігноруючи формалізм матриці щільності. Релятивістські аспекти квантової механіки не розглядаються, а питання про симетрію хвильової функції системи тотожних

частинок залишаються поза обговоренням. Зокрема, вимога симетризації повної хвильової функції залишається актуальною для дискретних ступенів свободи. Не зважаючи на ці обмеження, важливо підкреслити, що описана схема досить задовольняє потребам опису основних ідей квантової теорії інформації.

1.2. Поняття квантових бітів (qubits), їх структура та використання в квантових обчисленнях. Однокубітні операції

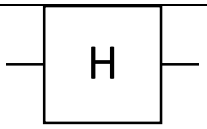
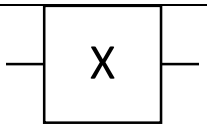
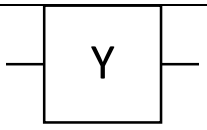
Як відомо, у класичних комп'ютерах одиницею зберігання інформації є біт - система, яка має два стани, зазвичай позначені як 0 і 1. За аналогією, ми можемо визначити квантовий біт, або коротко q-біт, як квантову систему, яка має два стани, позначені відповідно як $|0\rangle$ і $|1\rangle$. Однак, на відміну від класичного випадку в квантовій механіці ці два стани можуть взаємодіяти один з одним, так що найбільш загальний стан квантового біта може бути записаний як вектор, який являє собою суперпозицію цих станів[2]:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{pmatrix}\alpha\\ \beta\end{pmatrix}, \tag{1.5}$$

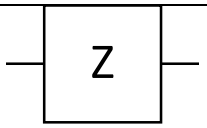
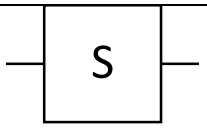
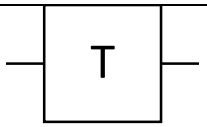
де α і β є комплексними числами і виконується умова нормування

$|\alpha|^2 + |\beta|^2 = 1$. Операції над кубітами обов’язково повинні зберігати цю норму. Їх також можно описати унітарними матрицями розмірністю 2x2. У табл. 1.1 наведено перелік основних гейтів:

Таблиця № 1.1 – Перелік універсальних квантових гейтів

Назва елемента	*Графічне зображення*	*Унітарна матриця*
Адамара		$\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$
Паулі-X		$\begin{bmatrix}1 & 1\\ 1 & 0\end{bmatrix}$
Паулі-Y		$\begin{bmatrix}0 & -i\\ i & 0\end{bmatrix}$

Продовження таблиці № 1.1:

Назва елемента	*Графічне зображення*	*Унітарна матриця*
Паулі-Z		$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
Фазовий		$\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$
π/8		$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$

Основні властивості квантових ланцюгів: час рухається зліва направо; проводки представляють кубіти, а символ '/' може використовуватись для позначення групи кубітів.

Крім того, рівняння 2.1, записане у традиційній нотації квантової механіки "станів", введеної Діраком, можна переписати в термінах матричної алгебри, оскільки наші вектори станів представлені двовимірним простором:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \qquad |\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}. \tag{1.6}$$

Фізичні реалізації подібної системи з двома квантовими станами можуть бути різноманітними: електрон або кубіт зі спіном 1/2, що орієнтований вздовж або проти напрямку магнітного поля; атом з двома різними енергетичними станами; фотон з горизонтальною або вертикальною поляризацією і т.д.

Оскільки квантовий біт може перебувати у стані суперпозиції з нескінченною кількістю можливих варіантів, на перший погляд може здатися, що ми можемо закодувати нескінченну кількість класичної інформації у стані одного квантового біта. Проте, це не так.

По-перше, при "створенні" суперпозицій ми фактично працюємо не з дискретними, а з неперервними величинами, і саме точність процедури підготовки заданого стану визначає кількість збереженої інформації. Аналогічно

в класичній електроніці ми зберігаємо інформацію не у вигляді логічних рівнянь, а у вигляді довільної напруги на електричному елементі. Точність задання, утримання та вимірювання цієї напруги визначають кількість збереженої інформації.

По-друге, у квантовому випадку те, що записано, просто не вдасться відтворити точно. Фактично, розмірність простору станів нашої системи дорівнює двом, і відповідно до постулату вимірювання ми можемо побудувати виміряну величину, яка має не більше ніж два стани (у просторі розмірністю N неможливо умістити більше ніж N ортогональних підпросторів) і отримати два можливих результати внаслідок вимірювання з певною ймовірністю. Таким чином, у випадку одного квантового біта немає жодної переваги порівняно з класичним випадком.

Справді, можна показати, що для одного квантового біта існує спостерігаєма $B = \{E_0, E_1\}$, де E_0 і E_1 є підпросторами, спряженими з базисними векторами $|0\rangle$ та $|1\rangle$ відповідно. Наприклад, іншим можливим базисом може бути $O = \{E_0', E_1'\}$, де E_0' і E_1' задаються векторам

$$|0\rangle' = \frac{1}{2}(|0\rangle + |1\rangle) \text{ та } |1\rangle' = \frac{1}{2}(|0\rangle - |1\rangle), \tag{1.7}$$

Якщо фізичний стан нашого q-біта закодовано у формі вертикальної або горизонтальної поляризації фотона, то ми можемо виміряти поляризацію фотона у проекції на вісь, повернуту під кутом 45 градусів до вертикалі. У разі, коли стани $|0\rangle$ та $|1\rangle$ реалізуються у вигляді станів електрона з визначеною проекцією спіна на вісь Z, ми можемо виміряти проекцію спіна на ортогональну ось X або Y.

У класичній обчислювальній системі з одним бітом можна виконувати перетворення $\{0, 1\} \rightarrow \{0, 1\}$. Легко перевірити, що існує чотири таких перетворення:

1. Тотожне (жодних змін).

2. Інверсія (заміна 0 на 1 і навпаки).

3. Встановлення біта в 0.

4. Встановлення біта в 1.

У квантовій системі можливостей перетворень одного квантового біта значно більше, вони являють собою простір унітарних матриць розміром 2×2. Наведемо квантові аналоги класичним перетворенням:

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad NOT = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Set0 = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, \; Set1 = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}. \quad (1.8)$$

Проте операції встановлення біта в певний стан у квантовій системі є незворотними (попередній стан втрачається), тому відповідні оператори не є унітарними і не можуть бути операторами "еволюції". Ці дії можна виконувати лише за допомогою класичних засобів.

Оператор NOT співпадає з матрицею Паулі σ_x, а так само з усіма іншими операторами групи SU(2). Оператори цієї групи можуть фізично реалізуватись за допомогою ядерного магнітного резонансу, тобто керованого еволюцією системи зі спіном 1/2 в поєднанні постійного та змінного магнітних полів [5]. Зокрема, оператор NOT є просто оператором обертання спіну на 180°. Варто зазначити, що при цьому фактично реалізується перетворення $|1\rangle \rightarrow |0\rangle, |0\rangle \rightarrow -|1\rangle$,але незначний фазовий множник можна виправити. Крім того, згадаємо оператор обертання спіну на 90° A і оператор Адамара H, які часто зустрічаються в обчисленнях:

$$A = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}, \quad H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \quad (1.9)$$

Цікавим прикладом також є "квадратний корінь з NOT", оператор, який при подвійному застосуванні, фактично дає оператор інверсії.

$$\sqrt{NOT} = \frac{1}{4}\begin{pmatrix} 1-i & 1+i \\ 1+i & 1-i \end{pmatrix}. \quad (1.10)$$

Фізично це той самий оператор повороту спіна на 90° з додатковим фазовим зсувом компоненті

1.3.Квантові регістри

Очевидно, що для практичних обчислень потрібно мати більше одного квантового біта. Такий набір квантових бітів, упорядкованих в регістрі, називається квантовим регістром і складається з n квантових бітів. Біти в регістрі можуть бути ізольованими або взаємодіяти між собою відповідно до необхідного закону еволюції. Звичайно, базисні стани квантового регістра позначаються упорядкованими рядками з нулів і одиниць, так що у регістрі з двох бітів базисні стани будуть $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$. Кількість базисних станів у регістрі з n бітів дорівнює 2^n, що так само відповідає загальній кількості станів у класичному бітовому регістрі такої ж довжини. Найбільш загальним вектором станів n-бітового квантового регістра є

$$|\psi\rangle = \sum_{i=0}^{2^n-1} a_i|i\rangle\,, \tag{1.11}$$

де в позначенні базисних векторів $|i\rangle$ мається на увазі двійковий запис цього числа.

Стан квантового регістра, який складається з двох кубітів, що знаходиться у визначених станах $|\varphi_1\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$ та $|\varphi_2\rangle = \beta_0|0\rangle + \beta_1|1\rangle$, визначається їх тензорним добутком:

$$|\psi\rangle = |\varphi_1\rangle \otimes |\varphi_2\rangle = \left(\sum_{i=0}^{1} \alpha_i|i\rangle\right) \otimes \left(\sum_{j=0}^{1} \beta_j|j\rangle\right) \tag{1.12}$$

Якщо A і B є унітарними перетвореннями, то їхнє незалежне застосування до $|\psi\rangle = |\varphi_1\rangle \otimes |\varphi_2\rangle$, а також їх спільна дія на цей стан , буде визначатися 4x4 матрицею прямого добутку:

$$C = A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B \\ a_{21}B & a_{22}B \end{pmatrix}$$
$$\text{як } (A \otimes B)(|\varphi_1\rangle \otimes |\varphi_2\rangle) = (A|\varphi_1\rangle \otimes B|\varphi_2\rangle) \tag{1.13}$$

Один з основних принципів об'єднання квантових бітів у квантовий регістр полягає у тому, щоб дозволити їм бути взаємозалежними. Основна властивість квантових механічних систем полягає в тому, що їхні стани не обмежуються

визначеними станами підсистем. Далеко не всі стани двобітового квантового регістра можна виразити як прямі добутки станів окремих бітів. Приклад такого стану:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \quad (1.14)$$

При вимірюванні такого стану в стандартній базі результати $|00\rangle$ і $|11\rangle$ будуть спостерігатися з ймовірністю 50%, тоді як результати $|01\rangle$ і $|10\rangle$ ніколи не будуть спостерігатися. Це можна перевірити простим експериментом, який переконує нас, що не існує таких α_i, β_i, при яких виконується рівняння (3.2) (рівняння для $\alpha_i\beta_i$ суперечливі).

Таким чином, суцільний регістр перебуває в певному квантовому стані, в той час як його підсистеми перебувають в окремих станах, які не знаходяться взаємодії, інакше рівняння (3.2) було б виконане. Такий "заплутаний", взаємозалежний стан системи в англомовних джерелах описується терміном "entanglement", який не має точного еквівалента. Стани підсистем в подібних випадках слід описувати більш загальною мовою матриць щільності.

1.4. Квантові схеми та їхні приклади

Як відомо, еволюція квантової системи описується за допомогою унітарних операторів. Однак для системи з n квантових бітів оператори такого типу представляють собою $2^n \times 2^n$-матриці, що можуть бути важкими для розуміння звичайною людиною. Більш природнім способом подання еволюції квантової системи є набір послідовних перетворень, кожне з яких впливає на невелику кількість, приблизно 2-3 окремих бітів. В результаті еволюція квантової системи може бути аналогічною роботі звичайної логічної схеми. Відповідні окремі перетворення називають квантовими логічними елементами (квантові ворота), а сукупність цих елементів утворює квантову схему. Основна відмінність квантових логічнх елементів від класичних полягає в тому, що вони мають бути унітарними, тобто і оберненими.

Простими класичними логічними елементами є І (AND), АБО (OR), ВИКЛЮЧНЕ АБО (XOR). Вони відображають дві вхідні біти в один біт результату і, отже, не можуть бути зворотними і, відповідно, не можуть бути реалізовані в квантово-механічному контексті. Однак можна виправити положення для функції XOR - як відомо, вона є зворотньою в тому сенсі, що за її результатом і одним зі змінних можна відновити другий: якщо c = a $\oplus$ b, то b = a $\oplus$ c і a = b $\oplus$ c. Тому для перетворення функції XOR в оборотний унітарний оператор достатньо зберегти на виході один з її аргументів і визначити її наступним чином:

$$Cnot|a,b\rangle = |a, a \oplus b\rangle. \tag{1.15}$$

У квантовому варіанті ця функція зазвичай називається контрольованим NOT (CNOT), оскільки її ефект залежить від наступного: якщо перший (контрольований) біт перебуває у стані $|0\rangle$, то другий (цільовий або управляємий) біт зберігає свій стан; в іншому випадку цільовий біт інвертується. У матричній нотації і нотації станів це перетворення виглядає наступним чином, де індекси у C_{12} вказують на управляючий і цільовий біти:

$$C_{12} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \text{ або } \begin{matrix} |00\rangle \to |00\rangle \\ |01\rangle \to |01\rangle \\ |10\rangle \to |11\rangle \\ |11\rangle \to |10\rangle \end{matrix}. \tag{1.16}$$

Оскільки класичні логічні функції AND і OR не є оборотними (у тому сенсі, що XOR), у квантовому варіанті їх можна виконати не менш як на трьох кубітах, фактично зберігаючи на виході стани обох вхідних. Наприклад, функцію AND можна перетворити на дворівневий контрольований NOT (controlled-controlled-NOT), який визначається таким чином: цільовий біт інвертується тоді і тільки тоді, коли обидва контрольованих біти перебувають у стані $|1\rangle$.

Перетворення «контрольованого NOT» відіграє дуже важливу роль у системі квантової логіки. Ідеї, закладені в його конструкцію, а також властивості цього квантового аналога логічної операції XOR, мають широкі сфери застосування:

1. "Керовані оператори" – універсальний спосіб конструювання простих та часто використовуваних унітарних операторів у квантових обчисленнях: якщо управляючий біт перебуває в стані $|0\rangle$, до цільового біту застосовується оператор A, інакше до нього застосовується оператор B;

2. Збереження вхідних аргументів на виході - універсальний спосіб оборотного виконання функцій. Якщо у нас є аргумент $|x\rangle$, довжиною n бітів, і ми хочемо побудувати оператор (квантову схему) F, обчислюючу функцію $f(x)$, ми використовуємо у якості робочих змінних ще m біт, схема може виглядати наступним чином:

$$F|\, x, 0, 0^m\rangle \rightarrow\ |x, f(x), 0^m\rangle. \tag{1.17}$$

Для збереження оборотності, необхідно повернути вхідні дані і робочий простір до початкового стану.

3. Унітарність приводить до того, що квантова інформація не може бути втрачена. Для збереження оборотності звернемо увагу на вхідний нульовий біта, який перетворюється на значення функції $f(x)$. Цей біт не може бути просто знищений, потрібна конструкція, яка зберігатиме його початкове значення $|0\rangle$ і кінцеве значення $|f(x)\rangle$. Це можна зробити, якщо схема F працює наступним чином:

$$F|x, b\rangle \rightarrow\ |x, b\ \oplus\ f(x)\rangle. \tag{1.18}$$

При значенні $b\ =\ 0$ отримується схема, яка є оборотною. Таким чином, виключне АБО перезаписує дані без їх знищення.

4. Універсальність визначається здатністю одного або декількох операторів (гейтів) скласти таку схему, яка здійснює будь-яке унітарне перетворення. Сам по собі оператор "controlled-not" не є універсальним, але може стати таким, якщо до нього додати вирази загального вигляду, що діють на один q-біт[9]:

$$V(\theta, \varphi) = \begin{pmatrix} Cos\left(\frac{\theta}{2}\right) & -ie^{-i\varphi}\left(\frac{\theta}{2}\right) \\ -ie^{i\varphi}Sin\left(\frac{\theta}{2}\right) & Cos\left(\frac{\theta}{2}\right) \end{pmatrix} \tag{1.19}$$

Цей оператор походить з техніки ядерного магнітного резонансу і має конкретну форму, яка може бути обрана з класу ірраціональних чисел, таких як θ і φ (де φ вибирається з діапазону [0, 2π], а θ - з діапазону [0, π]). Практично всі двобітові оператори є універсальними [9], тому controlled-NOT є своєрідним винятком в цьому сенсі.

5. Обмін квантових станів. Для будь-яких |φ⟩ та |ψ⟩ має місце рівність

$$C_{12}C_{21}C_{22}|\varphi\rangle|\psi\rangle = |\psi\rangle|\varphi\rangle, \qquad (1.20)$$

при чому ці стани можуть бути реалізовані на фізично різних системах (наприклад, електронах та фотонах). Сутність цієї формули полягає в тому, що вона представляє собою квантовий варіант відомого серед програмістів завдання: як обміняти значення змінних a і b без використання додаткової пам'яті? Дуже просто:

$a := a \oplus b$;

$b := a \oplus b$; Тепер b містить початкове значення a;

$a := a \oplus b$; Тепер a містить початкове значення b.

6. Можливість реалізації. Операцію XOR було успішно реалізовано в експериментах з переносом поляризації в області електронно-ядерної резонансної спектроскопії ще у 1956 році [5]. Перенос поляризації фактично описувався схемою $|a, b\rangle \rightarrow |a \oplus b, a\rangle$, і авторів на першому етапі цікавив саме перенос стану поляризації |a⟩ на систему |b⟩, при цьому відбулася реалізація логічної функції, що було необхідним, але не викликало на той час інтересу у дослідників, які займалися поляризацією.

1.5. Теорема про некопійованість квантового стану

Копіювання довільного квантового стану |α⟩ є неможливим. Для того, щоб створити копію стану $|\alpha\rangle$, потрібно знайти лінійний і унітарний оператор U, який діє на пару станів $|\alpha\rangle$ та $|0\rangle$ і задовольняє умову $U(|\alpha\rangle|0\rangle) = |\alpha\rangle|\alpha\rangle$. Оскільки копіювання має працювати на будь-якому стані, ми виберемо інший вектор стану |β⟩, що буде скопійований: | $U(|\beta\rangle|0\rangle) = |\beta\rangle|\beta\rangle$. Нарешті, ми утворюємо третій

вектор, який є лінійною комбінацією двох попередніх: $|\gamma\rangle = \frac{|\alpha\rangle + |\beta\rangle}{\sqrt{2}}$. Спроба скопіювати його стан за допомогою лінійності оператора U дає нам наступне[5]:

$$|U(|\gamma\rangle|0\rangle) = \frac{1}{\sqrt{2}}(|\alpha\rangle|\alpha\rangle + |\beta\rangle|\beta\rangle) \neq |\gamma\rangle|\gamma\rangle. \quad (1.21)$$

Звичайно, що оператор може копіювати деякі стани, які є ортогональними один одному, наприклад, оператор controlled-NOT успішно копіює стани $|0\rangle$ і $|1\rangle$, але не $\frac{|0\rangle \pm |1\rangle}{\sqrt{2}}$ [10].

1.6. Квантовий паралелізм та його використання в квантових алгоритмах

Відмінність від класичного квантового регістра полягає у тому, що він може перебувати у стані суперпозиції, включаючи всі його 2^n станів.

Якщо ми тепер застосуємо до такого "універсального" стану будь-який "корисний" унітарний оператор U, перетворивши будь-який базисний стан у потрібну нам функцію від цього стану, ми отримаємо у регістрі суперпозицію значень цієї функції на всіх можливих вхідних даних. Таким чином, за один цикл роботи квантового комп'ютера ми виконуємо одночасно 2^n обчислень – експоненційно більше, ніж у випадку класичної обчислювальної роботи. Цей феномен зазвичай називають квантовим паралелізмом.

Таля того, щоб отримати інформацію із отриманого результату, необхідно виміряти кінцевий стан квантового реєстру. Зрозуміло, що ми можемо побудувати спостереження, яке має 2^n станів, і застосувати його до нашого стану, в якому закодовані всі результати обчислень, і отримати з певною ймовірністю один із 2^n результатів.

Однак це буде всього лише один стан класичного реєстру з n бітами. Квантова суперпозиція буде розпадатися, залишаючи в ній інформацію в обмеженому обсязі. Ситуація може трохи поліпшитися, якщо повторити цикл роботи комп'ютера декілька разів і отримати розподіл ймовірностей кінцевого результату вимірювань.

Можна прийти до висновку, що використовувати експоненційне прискорення обчислень можна тільки тоді, коли один результат вимірювань містить деяку загальну, інтегральну характеристику всіх значень обчислюваної функції, тобто виявляє певну періодичність, симетрію або групову структуру. Саме в таких випадках вдається побудувати практично корисні квантові алгоритми.

Варто зазначити, що можлива реалізація квантового комп'ютера, що працює лише з базовими станами $|0\rangle$ і $|1\rangle$, була запропонована у ранніх роботах Фейнмана. Функціонально він представляє собою копію класичного комп'ютера. Запропонований Фейнманом пристрій називається квантовим симулятором і не може надати жодної переваги порівняно з класичним комп'ютером, але є важливим етапом в розвитку квантових технологій [7].

РОЗДІЛ 2. КВАНТОВІ АЛГОРИТМИ

Квантові комп'ютери відкривають нові можливості для розв'язання складних обчислювальних задач, які на класичних комп'ютерах потребували би величезних ресурсів. Вони використовують особливі квантові алгоритми, які надають значний швидкісний приріст порівняно з класичними алгоритмами. Зокрема, алгоритм Шора дозволяє швидко факторизувати числа і знаходити дискретні логарифми, алгоритм Гровера забезпечує швидке пошукове рішення. Ці прогресивні алгоритми дають змогу ефективно вирішувати проблеми, які раніше були недосяжними для класичних комп'ютерів. В результаті, квантові комп'ютери відкривають нові перспективи в наукових дослідженнях, оптимізації та розв'язанні складних обчислювальних завдань. На рис.2.1. наведено можливі застосування наявних квантових алгоритмів та їх взаємодії:

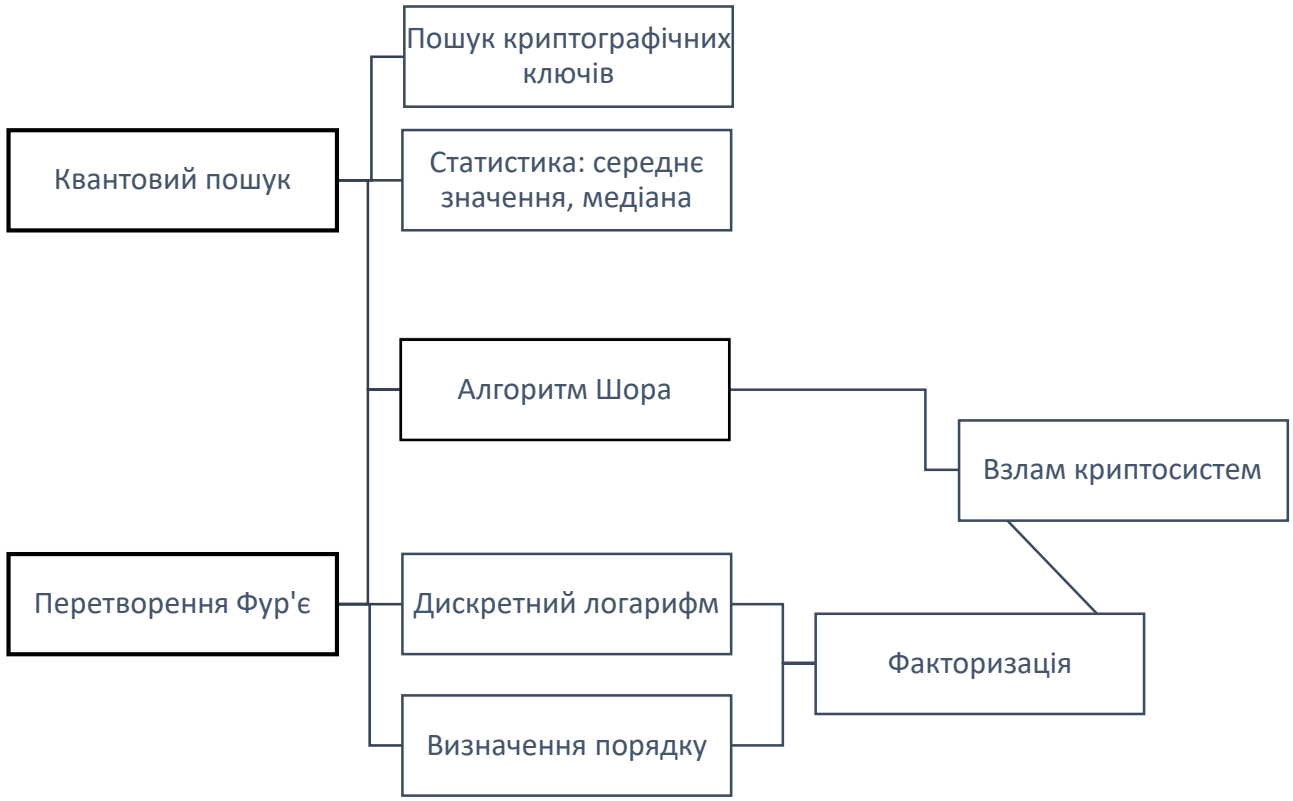


Рисунок № 2.1 – Головні квантові алгоритми та їх зв’язки

Чому відомо так мало квантових алгоритмів, які перевершують свої класичні аналоги? Відповідь полягає в тому, що розробка ефективних квантових алгоритмів виявляється складною задачею. Це пояснюється, принаймні, двома причинами. По-перше, проектування алгоритмів, будь то класичних чи квантових, є складним завданням! Історія алгоритмів показує, що для розробки наближено оптимальних алгоритмів, навіть для на перший погляд простих задач, таких як множення двох чисел, потрібна значна винахідливість. Знаходження ефективних квантових алгоритмів ускладнюється додатковим обмеженням: ми хочемо, щоб наші квантові алгоритми були кращими за найкращі відомі класичні алгоритми. Другою причиною складності пошуку ефективних квантових алгоритмів є те, що наші інтуїції набагато краще пристосовані до класичного світу, ніж до квантового. Якщо ми думаємо про проблеми, використовуючи нашу вроджену інтуїцію, то алгоритми, які ми придумуємо, будуть класичними алгоритмами. Для створення ефективних квантових алгоритмів потрібні спеціальні інсайти і прийоми.

Тому не всі алгоритми є обчислювально ефективними, проте всі вони представляють собою цікаві та незвичайні способи використання принципів квантової механіки.

2.1. Моделювання фізичних систем

Найпростішим і природним застосуванням квантового комп'ютера, тобто квантової системи з керованою еволюцією, є моделювання інших квантових систем. Для моделювання вектора стану квантової системи з розмірністю простору станів 2n необхідний класичний комп'ютер з приблизно таким же розміром пам'яті, але достатньо квантового регістру розміром n. Для моделювання операцій такої системи в цьому випадку потрібно перемножати унітарні матриці розміром 2n × 2n, так що як класичний, так і квантовий комп'ютери можуть бути неефективними –квантова схема в принципі може бути експоненційно великою. Однак було показано, що широкий клас систем

(наприклад, багаточастинкові системи з локальними взаємодіями) може бути моделюваний ефективно.

2.2. Факторизація великих чисел

Факторизація (розклад на множники) великих чисел (100 і більше десяткових цифр) є одним з актуальних завдань сучасної теорії чисел і криптоаналізу. Це завдання є обчислювально складним, оскільки обчислювальна складність всіх відомих класичних алгоритмів для його розв'язання експоненційно зростає з розміром задачі. Допустимо, нам потрібно розкласти на множники число N, що має двійкове представлення з n розрядами. Очевидний спосіб - спробувати поділити N на всі цілі числа (або на всі прості числа, що не перевищують кореня з N), що призводить до приблизно $2^{n/2}$ варіантів.

Існують ефективні алгоритми, такі як "квадратичне решето" і "решето числового поля", які розв'язують це завдання для задачі розкладання з порядком $exp(cn^{1/3})$, де c - константа порядку одиниці. Ці алгоритми здатні факторизувати число з 100 десятковими цифрами за тиждень, але для чисел з 200 цифрами потрібні мільйони років. Досі не відомо, чи існує класичний алгоритм факторизації з поліноміальною складністю від n.

Задача факторизації тісно пов'язана з так званою задачею про дискретний логарифм. Задане число N і цілі числа a, b < N. Ціле число x < N називається дискретним логарифмом b за основою a і модулем N, якщо воно є розв'язком рівняння a^x = b mod N. Вважається, що обчислювальна складність дискретного логарифмування приблизно така ж, як у факторизації.

На таких задачах базуються практично всі широко застосовувані алгоритми шифрування з відкритим ключем, такі як RSA і El Gamal, які дозволяють забезпечити недоступність інформації — конфіденційність через відкритий канал. Алгоритм "Рукопожаття" настільки простий, що його можна описати кількома рядками. Абоненти A і B бажають встановити спільний секрет через

канал, всі повідомлення по якому можуть переглядати сторонні спостерігачі. Можна застосувати шифрування, але як передати пароль? Абоненти A і B

- вибирають велике просте число N і число e, яке менше N
- абоненти випадковим чином вибирають числа A і B, які менші за N
- абонент A обчислює e^{A} mod N і передає його абоненту B
- абонент B обчислює e^{B} mod N і передає його абоненту A.

Тепер і a, і b можуть незалежно вирахувати число

$$X = (e^{B})^{A} mod\ N = \ (e^{A})^{B} mod N, \qquad (2.1)$$

воно і буде служити паролем. Споглядач, який бачив все, за розумний час не зможе знайти A і B.

Алгоритм RSA (названий за іменами авторів: Рівера, Шамира, Адлемана) породив цілий клас методів шифрування, для яких придумали назву шифрування з відкритим ключем. Всі ці методи уступають два класи, один використовується тільки для шифрування даних, другий – тільки для розшифрування. Користувач згідно з алгоритмом створює таку пару ключів, після чого ключ для шифрування (публічний ключ) розповсюджується всім, а ключ для розшифрування (приватний ключ) зберігається у себе. В результаті він отримує конфіденційний поштовий знак – лист, який може зашифрувати відкритим ключем і кинути його в поштову скриньку, але тільки власник може отримати (та розшифрувати) лист. Цей алгоритм підходить і для передачі паролів по відкритому каналу: кожна сторона просто створює власну пару ключів і власний "поштовий знак". З погляду шифрування, відомі методи шифрування з відкритим ключем досить складні, тому зручніше передати паролі для більш простого методу шифрування, ніж шифрувати весь потік даних. А що стосується листів, тут методи, описані вище, використовуються безпосередньо, оскільки час шифрування не має великого значення.

Справді, в цих методах також виникає конструкція цифрового підпису. Якщо зберегти в таємниці ключ для шифрування і поширити публічний ключ для розшифрування, то тільки автор зможе зашифрувати повідомлення, а

розшифрувати його і перевірити його може будь-яка відповідальна сторона. З усіх відомих сьогодні алгоритмів шифрування з відкритим ключем, кожен ключ представляє собою пару більших цілих чисел, а розбиття шифру (знаходження по відкритому ключу приватного і навпаки) вимагає розв'язання задачі факторизації (у деяких випадках – задачі знаходження дискретного логарифма).

В 1994 році Пітером Шором був розроблений квантовий алгоритм[6], який дозволяє вирішувати задачу факторизації та задачу дискретного логарифму за поліноміальний час[12]. Цей історичний результат базується на використанні квантового паралелізму та властивостей пошуку періоду функції. Нехай нам потрібно розкласти на множники деяке число N. Ми обираємо довільне a < N і розглядаємо функцію

$$f_N(x) = a^x mod\ N. \tag{2.2}$$

Якщо функція є періодичною з деяким періодом r, це означає, що значення функції повторюються через кожні r обчислень. Якщо N є простим числом, то r = N - 1, але цей випадок легко вирішується класичними методами, існують швидкі алгоритми для перевірки простоти числа. В загальному випадку, коли N не є простим числом, для знаходження періоду r необхідні квантові алгоритми, які дозволяють вирішити цю задачу ефективно. В загальному випадку:

$$f_N(x + r) + f_N(x), \qquad \text{і відповідно } a^r = 1 mod N. \tag{2.3}$$

Якщо відомий період r (дискретний логарифм одиниці по основі a), то розкладання числа N на множники можна знайти класичними методами. Зокрема, якщо r є парним і маємо рівність a^r - 1 = 0 (mod N), то це означає, що N має нетривіальний множник.

$$\left(a^{\frac{r}{2}} - 1\right)\left(a^{\frac{r}{2}} + 1\right) = 0 mod N. \tag{2.4}$$

Якщо в добутку з лівої частини рівності відомого періоду r спостерігаються лише дільники N, то ці дільники повинні мати загальні дільники з N, які можуть бути знайдені класичним алгоритмом, таким як алгоритм Евкліда для пошуку найбільшого спільного дільника. Якщо r є непарним або добуток у лівій частині

рівності дорівнює нулю, алгоритм не вдається, і нам потрібно вибрати інше значення a.

Квантовий алгоритм Пітера Шора призначений для швидкого пошуку періоду r в задачі дискретного логарифма і має поліноміальну складність. Для вирішення цієї задачі використовується квантовий комп'ютер з двома квантовими реєстрами довжини n, де M = 2^n > N і M ≈ N^2. Алгоритм має наступну структуру:

7. Спочатку переведемо обидва регістри в стан $|0\rangle$. Далі застосуємо перетворення Адамара (H-перетворення) до кожного біта другого регістра в окремості. Це перетворення змінює стан $|0\rangle$ на $1/\sqrt{2}$ ($|0\rangle + |1\rangle$), де кожен стан має однакову амплітуду:

$$H|0\rangle \dots H|0\rangle = \frac{1}{2^{\frac{N}{2}}}(|0\rangle + |1\rangle)^N = \frac{1}{\sqrt{M}}\sum_{x=0}^{M-1}|x\rangle. \quad (2.5)$$

8. Якщо ми застосуємо оператор k до наших квантових регістрів, які обчислюють функцію f_N(x), ми отримаємо новий стан, який містить суперпозицію усіх можливих значень функції f_N(x) для заданого x. Це стане основою для подальшого застосування алгоритму Шора для пошуку періоду функції. Варто зауважити, що існує швидкий класичний алгоритм для обчислення функції f_N(x), за певних умов. Після застосування оператора k до наших регістрів, вони перейдуть в новий стан:

$$\frac{1}{\sqrt{M}}\sum_{x=0}^{M-1}|x\rangle\, f_N(\mathrm{x})\rangle. \quad (2.6)$$

9. Якщо ми виміряємо стан вихідного регістра, то отримаємо значення функції f_N(k) для певного випадкового k. Проте, стан вихідного регістра після вимірювання зменшиться до $|f_N(\mathrm{k})\rangle$. Отримане значення не є цікавим для нас, але важливим є стан вихідного регістра після цього вимірювання. Цей стан буде відповідати лінійній комбінації станів, які сумісні з виміряним значенням на виході, тобто збережуть значення x, для яких

f_N (x) = f_N (k), тобто x = k, k + r, k + 2r, ..., де r - період функції f_N (x).

10. Для виявлення періодичності, яка виникає в вихідному класичному регістрі, застосовується квантове перетворення Фур'є.

$$U|x\rangle = \frac{1}{M}\sum_{k=0}^{M-1} e^{\frac{i2\pi kx}{M}}|k\rangle \ . \qquad (2.7)$$

Далі виміряємо результат. Під час застосування перетворення Фур'є, період r перетворюється на M/r, де M - загальна кількість можливих станів. З високою ймовірністю ми виміряємо число, близьке до jM/r, де j = 1, 2, і так далі. Потім, за допомогою класичних методів (розкладання у неперервну дріб, наприклад), ми вилучаємо з цього числа r, яке становить основу для подальшого алгоритму.

Алгоритм Шора вважається ефективним з середньою складністю порядку log^3(N). Ця ефективність базується не лише на експоненційно великій кількості задіяних станів, але і на особливому використанні інформації під час зведення "скрученого" (entangled) стану |x⟩|f_N(x)⟩.

2.3. Квантова телепортація

Нехай, нам необхідно передати з пункту А до пункту Б, від Аліси до Боба (звичайні персонажі з статті про теорію інформації), один квантовий біт у стані $|\varphi\rangle$. Зокрема, ми хочемо передати повну інформацію про цей стан, матеріальна система, на якій реалізований цей біт, нам не потрібна. Якщо існує класичний алгоритм побудови стану $|\varphi\rangle$, можна передати до пункту б цей алгоритм і відновити потрібний стан на місці. У протилежному випадку, здається, єдиним виходом є переміщення стану в область, ізольовану від зовнішнього середовища, і таким чином фізичне переміщення його до пункту б. Можна також обмінюватись нашим станом з довільним станом якої-небудь системи, наприклад, фотона, і фізично відправити його в більш транспортабельну систему. Такий обмін станами можливий за допомогою управляючої функції. Іншого виходу, здається, немає, оскільки повністю знати довільний стан $|\varphi\rangle$ неможливо – перше вимірювання його руйнує, а з нього неможливо зробити копію. Однак, у 1993 році було відкрито спосіб передаі з пункту А до пункту Б

повної інформації про стан $|\varphi\rangle$, при цьому передається лише класична інформація[13]! Описана конструкція базується на використанні парадоксу Ейнштейна-Подольського-Розена.

Як відомо, запропонований Ейнштейном, Подольским і Розеном (ЕПР) мислений «експеримент» [11] є далекодіючим висновком у квантовій механіці. Основна ідея полягає у розгляді пар квантових систем з двома дискретними станами, наприклад, спін-1/2 частинок (самі автори розглядали більш важкий неперервний випадок системи двох частинок з нульовим повним імпульсом, і акцент робився на доказі неповноти квантовомеханічного опису дійсності). Розглянемо пару частинок A і B зі спіном 1/2 і позначимо стан з позитивною проекцією спіну на вісь z як $|\uparrow\rangle$ і стан з від'ємною проекцією як $|\downarrow\rangle$. Система з двох частинок спочатку готується у синглетному стані за спіном $\frac{1}{\sqrt{2}}(|\uparrow\rangle\ |\downarrow\rangle$ - $|\downarrow\rangle|\uparrow\rangle)$, а потім частинки розходяться на значну відстань у просторі. Оскільки сумарний кутовий момент системи дорівнює нулю, вимірювання спіну частинки A в проекції на ось x миттєво переводить частинку B у стан, в якому її проекція спіну на цю вісь протилежна тій, яку ми виміряли у A. Точніше казати, змінюється не стан частинки B, а наше знання (інформація) про цей стан. Подібна "передача" інформації не суперечить теорії відносності, оскільки насправді інформація залишається в пункті A, оскільки через теорему про некопійованість станів, ми не можемо передати миттєвий сигнал про B(неможливо встановити, з якого моменту розпочинати вимірювання стану частинки B і повторити вимірювання не вдасться).

Ми можемо зробити спостереження, що кореляція між результатами вимірювань проекцій спінів A та B на різних осях η_A та η_B, пов'язаних з кутами φ_A та φ_B відносно осі z. Теорія [21] передбачає, що ймовірність отримати однаковий результат (обидва "+" або обидва "-") при такому вимірюванні для обох частинок становить P = $sin^2((\varphi_A - \varphi_B)/2)$, де P дорівнює нулю при φA = φB, 100% при $\varphi_A = \varphi_B$ 180◦ та 75% при $\varphi_A - \varphi_B = 120$◦. Результати проведених експериментів [15, 16] підтвердили вірність квантової механіки.

Варто зазначити, що неможливо присвоїти частинкам A та B локальні, тобто незалежні властивості, які б породжували таку високу кореляцію. Таким чином, для φA − φB = 120◦ локальні приховані змінні можуть породити кореляцію не більше ніж 2/3. Проведені експерименти підтверджують правильність квантової механіки. На рис. 2.2. наведено порівняння квантової телепортації з традиційною:

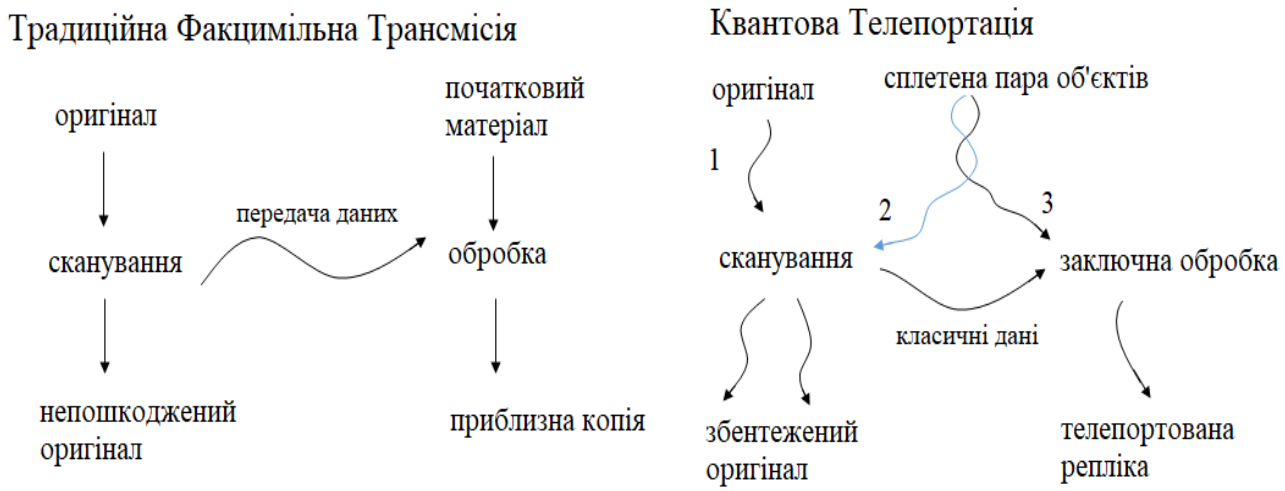


Рисунок № 2.2 – Порівняння квантової телепортації з традиційною факсимільною передачею даних

За зазначеними причинами самі по собі ефекти ЕПР-кореляції непридатні для передачі інформації. Однак, якщо їх поєднати з класичним сигналом, виникає конструкція, яку зазвичай називають квантовою телепортацією[13]. Вона ілюструється на малюнку 2.3.1. Для передачі стану $|\varphi\rangle$ (який ми будемо називати частинкою 1) з пункту А до пункту Б, Алісі та Бобу слід передбачити пару частинок 2 та 3 у стані синглетної ЕПР-кореляції.

$$|\Psi_{23}^{-}\rangle = \frac{1}{\sqrt{2}}(|\uparrow_2\rangle|\downarrow_3\rangle - |\downarrow_2\rangle|\uparrow_3\rangle). \qquad (2.8)$$

Їх слід розділити і частинку 2 передати Алісі, а частинку 3 - Бобу. Можна уявити собі "центр телепортації" C, який виготовляє такі пари і заздалегідь розсилає їх усім бажаючим. Стан частинки 1 можна записати як $|\varphi_1\rangle$ = a$|\uparrow_1\rangle$+b$|\downarrow_1\rangle$, де a і b невідомі комплексні коефіцієнти з $|a|^2+|b|^2 = 1$, а спільний

стан частинок 1, 2, 3 представляє собою декартів добуток незалежних станів $|\varphi_1\rangle|\Psi_{23}^-\rangle$.

На початку передачі, Аліса вимірює стан пари частинок 1 і 2 в так званому базисі Белла, який складається з сінглета $|\Psi_{12}^-\rangle$ і триплета

$$|\Psi_{12}^+\rangle = \frac{1}{\sqrt{2}}(|\uparrow_1\rangle|\downarrow_2\rangle + |\downarrow_1\rangle|\uparrow_2\rangle),$$
$$|\Phi_{12}^\pm\rangle = \frac{1}{\sqrt{2}}(|\uparrow_1\rangle|\uparrow_2\rangle \pm |\downarrow_1\rangle|\downarrow_2\rangle, \quad (2.9)$$

які представляють собою повний базис для системи частинок 1 і 2. Повний стан системи трьох частинок до вимірювання можна переписати як

$$|\Psi_{123}\rangle = \frac{a}{\sqrt{2}}(|\uparrow_1\rangle|\uparrow_2\rangle|\downarrow_3\rangle - |\uparrow_1\rangle|\downarrow_2\rangle|\uparrow_3\rangle) + \frac{b}{\sqrt{2}}(|\downarrow_1\rangle|\uparrow_2\rangle|\downarrow_3\rangle - |\downarrow_1\rangle|\downarrow_2\rangle|\uparrow_3\rangle). \quad (2.10)$$

У цьому виразі стани частинок 1 і 2 можна виразити через базис Белла $|\Psi_{12}{}^\pm\rangle, |\Phi_{12}{}^\pm\rangle$:

$$|\Psi_{123}\rangle = \frac{1}{2}[|\Psi_{12}{}^-\rangle(-a|\uparrow_3\rangle - b|\downarrow_3\rangle) + |\Psi_{12}{}^+\rangle(-a|\uparrow_3\rangle + b|\downarrow_3\rangle)$$
$$+|\Phi_{12}{}^-\rangle(a|\downarrow_3\rangle + b|\uparrow_3\rangle) + |\Phi_{12}{}^+\rangle(a|\downarrow_3\rangle - b|\uparrow_3\rangle)]. \quad (2.11)$$

У момент вимірювання стан системи 1,2,3 колапсує до стану, що відповідає одному з елементів виразу. В результаті вимірювання Аліса отримує один з чотирьох станів пари 1,2 з однаковою ймовірністю 1/4, а частинка 3, яка належить Бобу, відповідно проектується на один з чотирьох чистих станів.

$$|\varphi_3\rangle = -\begin{pmatrix} a \\ b \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix}. \quad (2.12)$$

Ці стани відрізняються фіксованими матричними множниками від початкового стану частинки 1. Тепер Алісі достатньо передати Бобу по класичному каналу (телефону) номер результату свого вимірювання (1,2,3,4), що становить два біти класичної інформації, після чого Боб відтворює із своєї частинки 3 копію стану частинки 1, застосовуючи до частинки 3 один з чотирьох фіксованих унітарних операторів (фактично, це фазовий зсув і обертання на 180° відносно осей z, x, y відповідно). Телепортація здійснена, Боб має копію частинки 1, але жодні квантові об'єкти з А в Б не передавались! Стан частинки 1

незворотно розрушено вимірюванням, у руках у Аліси залишилась один зі станів базису Белла пари 1 і 2, теорема про некопіювання не порушена.

Телепортація можлива за допомогою лінійних операцій, тому вона буде працювати не тільки для чистих, але і для змішаних і зчеплених станів. Наприклад, якщо частинка 1 утворює до телепортації пару з частинкою 0, після телепортації стани частинок 3 і 0 будуть утворювати сінглетну пару. Це також можливо застосувати до систем з $N > 2$ ортогональних станів.

Класичне повідомлення відіграє важливу роль в цій конструкції. Якщо спробувати "вгадати" і вибрати оператор реконструкції випадковим чином, отримається рівномірна суміш всіх можливих станів, абсолютно некорельована з початковим. Таким чином, неможливо передати надсвітловий сигнал таким способом. Телепортація відбувається лише в момент приходу класичного сигналу, тобто вона відбувається всередині світлового конусу і не порушує жодних фізичних законів. Цікаво, що для здійснення телепортації Алісі не потрібно знати місцезнаходження Боба - класичну інформацію можна передати широкомовним способом (по телевізору), а копія відтвориться там, де знаходиться частинка 3.

Були проведені перші експерименти з практичною реалізацією квантової телепортації окремих фотонів [14]. Передавалися стани поляризації фотона в напрямку ±45° до осей квантування, а також їх лінійна комбінація - стан кругової поляризації. Як джерело ЕПР-пар використовувалася параметрична конверсія в нелінійному кристалі, при якій ультрафіолетовий фотон розпадався на пару фотонів червоного кольору з ортогональними станами поляризації. Наразі невідомо будь-який спосіб виконати повне вимірювання в базисі Белла. Експериментатори змогли подолати цю складність, виконуючи вимірювання в проекції на один з векторів базису Белла (сінглетний), що разом дозволяє здійснити телепортацію в 25% випадків.

2.4. Пошук в неупорядкованому списку

Одиним з прикладів ефективного квантового алгоритму є алгоритм пошуку інформації в неупорядкованій базі даних, іноді його називають універсальним алгоритмом перебору. У 1997 році був запропонований швидкий алгоритм для вирішення наступної простої задачі: дано неупорядкований набір з N предметів, треба знайти номер предмета, який співпадає з даним зразком[18,19]. Не складно довести, що класичний метод послідовного порівняння зразка з усіма предметами в середньому потребує N/2 порівнянь. Запропонований вченими квантово-механічний алгоритм потребує порядку $\sqrt{N}$ операцій. Він працює наступним чином.

Ми повинні якось виділити потрібний елемент за номером j з усіх інших, непотрібних. Передбачимо, що нами для цієї цілі побудований унітарний оператор порівняння S, який виділяє потрібний елемент наступним чином: він діє як тотожний на непотрібні елементи і змінює фазу у потрібного.

$$S|i\rangle = |i\rangle \text{ при } i \neq j \text{ та } S|j\rangle = -|j\rangle\,. \qquad (2.13)$$

Нехай ми маємо достатньо довгий квантовий регістра, кількість станів якого перевищує N. Ми переводимо його в "універсальний" стан, в якому всі можливі стани регістра присутні з рівними амплітудами. Позначимо амплітуду виділеного стану як a, а звичайного як b. Визначимо стан регістра як пару цих амплітуд, можна описати початковий стан як

$$|a,b\rangle = a|j\rangle + b\sum_{i\neq j}|i\rangle\,. \qquad (2.14)$$

Згідно з умовою нормування a^2 + (N-1)b^2 = 1. У початковому стані a = b = $1/\sqrt{N}$. Застосуємо до цього стану таке складне перетворення U_G: спочатку перетворення S, потім перетворення Фур'є, зміна знаку для всіх компонент, крім $|0\rangle$, та зворотне перетворення Фур'є. Перетворення призводить до наступного результату:

$$U_{G|a,b\rangle} = \left|\frac{2N-2}{N}b + \frac{N-2}{N}a, \frac{N-2}{N}b - \frac{2}{N}a\right|. \qquad (2.15)$$

Коефіцієнт при виділеному елементі став декілька більшим, ніж при інших. Фактично від бувся певний поворот у просторі станів у напрямку чистого стану $|j\rangle$. Далі ми просто застосовуємо перетворення U_G m разів, де $m \simeq (\pi/4)\sqrt{N}$. При цьому початковий стан наближається до чистого стану $|j\rangle$. Залишається лише його виміряти.

Іноді цей метод порівнюють з приготуванням пирога у печі: квантовий стан "поміщають у квантову піч", а відповідь повільно "випікається" до готовності. Якщо витягти його занадто рано, він буде сирий і неточний; якщо пізно, – він спалиться і розсиплеться. Доведено, що цей метод є оптимальним — жоден квантовий алгоритм не може працювати швидше, ніж у квадраті від кореня з N. Варто зауважити, що прискорення в цьому випадку не є експоненціальним, тому для теорії обчислень цей метод не вносить нічого нового.

Однак практична користь даного методу велика. Це справді універсальний алгоритм перебору. Існує безліч задач, в яких знайти розв'язок не легко, але перевірити, що розв'язок правильний, досить просто. Яскравим прикладом є підбір пароля до зашифрованих даних. При такій задачі можна в крайньому випадку застосувати повний перебір методом Гровера — перевірку правильності розв'язку можна вставити в алгоритм порівнянь S.

2.5. Квантова корекція помилок

Алгоритми факторизації і пошуку, описані вище, вимагають для практично корисної реалізації значної кількості квантових бітів і мільйонів квантових логічних переходів (моделювання фізичних систем може бути корисним для комп'ютерів навіть розміром декількох біт). Однак абсолютно точна реалізація операторів еволюції (квантових переходів) і абсолютна ізоляція системи від оточуючого середовища (що гарантує унітарність еволюції та збереження когерентності станів) є неможливими. Відповідно, можуть виникати два типи помилок - зворотні помилки, пов'язані з неточністю реалізації операторів еволюції, і незворотні помилки, тобто втрати когерентності, спричинені

паразитним взаємодією з макроскопічним оточенням або спонтанним випромінюванням. Як ми вже бачили, відмінність квантових комп'ютерів від класичних полягає в тому, що квантова система є системою з неперервним простором станів, і через це навіть дрібні помилки можуть накопичуватися і в кінці кінців порушувати роботу комп'ютера. Відповідно до цього, донедавна вважалося, що масштабні квантові обчислення можуть бути практично неможливими.

Положення в корені змінилося у 1996 році з появою роботи Петера Шора [6], яка включала пропозиції щодо використання квантових кодів для корекції помилок. Ця конструкція насамперед надає нову можливість – вона дозволяє перетворити квантовий комп'ютер у "правильний" класичний стан обчислення, не вимірюючи його стану та не порушуючи його когерентності в незворотний спосіб. Оскільки відсутня необхідність вимірювання, також відсутня залежність від нього та втрата когерентності. Це досягається в принципі таким же шляхом, як і в класичних кодах корекції помилок: до кожного інформаційного біта додається декілька додаткових, вони утворюють оболонку, ансиллу. Група цих фізичних бітів утворює логічний біт, стан якого використовується в обчисленнях, і повна просторова область станів усіх фізичних бітів перестає бути неперервною і розбивається на комірки, різні стани всередині яких не впливають на стан логічного біта і час від часу піддаються корекції. Ймовірність переходу з одної комірки в іншу та відповідно некоректованої помилки може бути зроблена довільно малою.

На прикладі класичних кодів продемонструємо принцип, як така схема може обходитися без вимірювань. Класичний код, стійкий до помилок, може бути побудований наступним чином: з усієї множини n-бітних двійкових чисел обираємо підмножину чисел "настільки різних", що вони залишаються різними навіть після додавання до них (побітною операцією без переносу) будь-якого числа з попередньо визначеної "множини помилок", наприклад, усіх чисел з одним ненульовим бітом. Якщо обрана підмножина чисел замкнена відносно додавання, код називається лінійним. Лінійний код повністю визначається своєю

матрицею перевірки парності H, яка ортогональна до всіх коректних кодових слів: $H \cdot u = 0$. Отже, якщо нам зустрілося неправильне кодове слово $u' = u + e$ з деяким додатковим помилковим внеском e, то

$$H \cdot u' = (H \cdot u) + (H \cdot e) = H \cdot e. \quad (2.16)$$

Якщо з останнього виразу можна відновити e, що можливо для всього класу коригованих помилок, потім ми можемо відняти це e з u', та відновити u. Така операція відновлення не залежить від u. Отже, для корекції помилки не обов'язково знати (вимірювати) повідомлення, яке ми коригуємо.

Конструкції квантових кодів, що коригують помилки, досить складні, і ми не будемо вдаватися в деталі. Взагалі, суть полягає в наступному. Існує певне порогове значення точності на один біт δ_0, таке, що при меншій похибці можливо необмежено довге квантове обчислення (при цьому похибки можуть виникати у всіх бітах). Оцінки δ_0 коливаються в діапазоні від 1/300 до 10^{-6}. В принципі можливі і системи, де стійкість до помилок залежить від "фізичного" рівня, наприклад системи, засновані на аніонних збудженнях[17].

2.6. Системи конденсованої речовини

Системи конденсованої речовини, такі як кристали, суперпровідники, квантові точки та інші матеріали, грають важливу роль у квантових обчисленнях. Вони використовуються для реалізації квантових бітів (кубітів) і забезпечують збереження та маніпулювання квантовою інформацією.

Одним із ключових викликів у квантових обчисленнях є забезпечення довготривалої когерентності кубітів, що є важливим для ефективного виконання квантових операцій. Системи конденсованої речовини дозволяють досягти високої стабільності кубітів і зберегти їх когерентність на тривалий період часу.

Застосування систем конденсованої речовини у квантових обчисленнях включає такі аспекти, як створення квантових гейтів, реалізацію квантових логічних операцій та здійснення квантової інформаційної обробки. Використовуючи властивості матеріалів конденсованої речовини, можна

створити квантові системи зі змінною кількістю кубітів та виконувати складні обчислювальні завдання.

Дослідження та розвиток систем конденсованої речовини у квантових обчисленнях продовжуються, спрямовуючись на покращення квантової когерентності, зменшення помилок та підвищення продуктивності квантових обчислювальних систем. Ці розвитки відкривають нові перспективи для реалізації потужних квантових обчислювальних пристроїв та вирішення складних обчислювальних задач.

Фактично, навіть невелика команда дослідників, використовуючи навіть шумні квантові комп'ютери сьогодення, може мати цінний вплив. Однією з активних областей, що вивчаються фізиками сконденсованих речовин, є динаміка взаємодіючих систем спінов. Два стани квантового біта утворюють природний аналог "верхнього" і "нижнього" спінів, а взаємодії між спінами можна легко перемикати за допомогою контрольних сигналів наших систем.

2.7. Трикубітні коди для корекції помилок у квантових обчисленнях

Одна з найбільших проблем квантових обчислень – це поява помилок. Вони можуть виникати в результаті шумів у квантових системах або взаємодії з навколишнім середовищем. Ці помилки можуть призвести до неточності результатів обчислень, а отже, прямо впливають на обчислення і у випадку великої кількості шумів система взагалі не буде працювати. Але класичні методи не підходять до квантових обчислень, тому що тісно пов'язані з копіюванням певної інформації або її вимірювання (обидві дії неможливі для квантових систем).

Тому дуже важливо розробляти методи корекції помилок, які б спеціально призначалися для квантових систем. Один з таких методів – використання трикубітових кодів[8]. Трикубітові коди дозволяють виявляти і виправляти помилки, що виникають у квантових системах шляхом додавання додаткових кубітів та застосування логічних операцій до них. Використання трикубітових

кодів дозволяє покращити надійність та стабільність квантових обчислень, мінімізуючи вплив помилок.

Нехай ми передаємо кубіти по каналу, в якому з ймовірністю ρ стан системи $|\psi\rangle$ переходить до стану $X|\psi\rangle$, де $X = \sigma^x$ – оператор класичної зміни біта. Такий канал буде мати класичні помилки.

Аналгічно з класичними системами, де ми кодуємо інформацію про один біт трьома, кодуємо інформацію про стан одного кубіту, трьома кубітами.

$$|0\rangle \longrightarrow |0_L\rangle \equiv |000\rangle, \tag{2.17}$$

$$|1\rangle \longrightarrow |1_L\rangle \equiv |111\rangle, \tag{2.18}$$

де суперпозиції станів 0 та 1 кодуються аналогічними логічними 0 та 1.

На рис. 2.3 наведено схему кодування для виправлення класичних помилок[8].

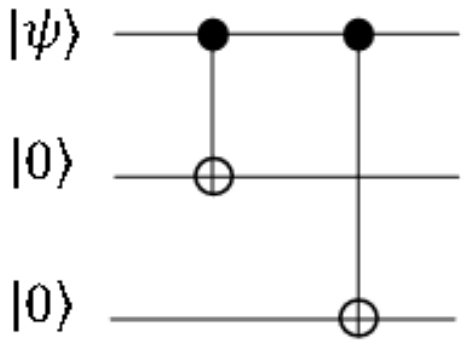


Рисунок № 2.3 – Схема кодування для виправлення класичних помилок[8]

Для того, щоб виправити класичну помилку, по-перше треба її знайти. Для цього ми проводимо вимір, результат якого називається синдромом. Існує всього чотири варіанти таких синдромів, які відповідають наступним проекторам:

$P_0 = |000\rangle\langle 000| + |111\rangle\langle 111|$ - без помилки,

$P_1 = |100\rangle\langle 100| + |011\rangle\langle 011|$ - помилка у першому кубіті,

$P_2 = |010\rangle\langle 010| + |010\rangle\langle 010|$ - у другому кубіті,

$P_3 = |001\rangle\langle 001| + |110\rangle\langle 110|$ - у третьому кубіті.

При знаходженні цих результатів ми не маємо інформації про стани кубітів, які закодовані, оскільки при отриманні цієї інформації дані стани змінюються, і подальше вимірювання не матиме сенсу.

Далі для виправлення помилок ми будемо розглядати синдроми помилок , інвертуючи певні кубіти.

Також трикубітні коди можуть використатися для виправлення фазових помилок. Нехай з вірогідністю P > 0 фазовий оператор помилки Z змінює стан системи з $a|0\rangle + b|1\rangle$ в $a|0\rangle - b|1\rangle$. Нехай маємо басиз $|+\rangle \equiv \frac{|0\rangle+|1\rangle}{2}$, $|-\rangle \equiv \frac{|0\rangle-|1\rangle}{2}$. В цьому базисі оператор фазових помилок працює аналогічно з класичним, але в іншому базисі. Щоб його замінити використовується елемент Адамара. На рис. 2.4 наведено схему кодування фазових помилок[8].

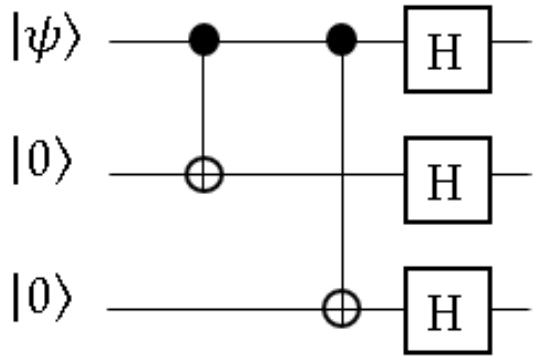


Рисунок № 2.4 – Схема кодування для виправлення фазових помилок[8]

Ефективне використання трикубітових кодів в квантових обчисленнях має велике значення для розвитку цієї галузі та покращення надійності і точності квантових систем. Дослідження та вдосконалення трикубітових кодів є активною галуззю наукових досліджень у сфері квантових обчислень. Шляхи подальшого розвитку трикубітових кодів включають вдосконалення методів декодування, збільшення ефективності корекції помилок і підвищення стійкості до шумів та інших факторів, що впливають на якість квантових систем.

РОЗДІЛ 3. ФІЗИЧНЕ ЗАСТОСУВАННЯ

Завдання практичної реалізації квантового процесора є дуже складним і технічно вимогливим. Зазвичай це пов'язано з точним керуванням окремими атомами. Необхідно врахувати декілька взаємо-несумісних вимог:

1. Квантові біти повинні бути належним чином ізольовані один від одного та від зовнішнього середовища. При цьому становити стійкість повинні не лише базисні стани $|0\rangle$ і $|1\rangle$, але й їх лінійні комбінації типу $|0\rangle + |1\rangle$. Саме тут час втрати когерентності найменший.

2. Для створення логічних переходів необхідно мати можливість вибірково впливати на окремі біти і пари бітів, а також керувати їх взаємодією між собою. Взаємодії цих елементів повинні контролюватися з високою точністю (принаймні, не меншою за критичну, що забезпечує роботу коду, коректує помилки).

3. Для створення логічних переходів необхідно мати можливість готувати необхідні початкові стани і вимірювати кінцеві стани.

Наразі існує декілька більш або менш реальних підходів до проблеми реалізації квантового комп'ютера:

1. Іонні пастки є одними з можливих підходів до реалізації квантових бітів, які представляють стани окремих іонів або атомів, ув'язнених в електромагнітні пастки в глибокому вакуумі. З використанням ультратонкої структури основного стану та спонтанного розпаду в такій пастці можна досягти тривалості життя протягом тисяч років. Переходи між станами одного іона можуть бути реалізовані за допомогою взаємодії з лазерним променем, але двобітові переходи таким шляхом реалізувати неможливо. Замість цього пропонується реалізувати їх шляхом збудження коливальних мод механічного руху системи іонів в цілому (фононів). Підготовка початкового стану можлива за допомогою методів лазерного охолодження, а вимірювання стану системи в цій техніці також відоме. Основною експериментальною проблемою є охолодження системи іонів до основного стану до температури менше мікрокельвіна. Основним джерелом

втрат когерентності є, очевидно, нагрівання системи через взаємодії з шумовою напругою на електродах. Оцінки показують, що за сучасної технологічного рівня можна застосувати порядку 100 переходів до декількох квантових бітів. У довгостроковій перспективі можна сподіватися на збільшення цих величин в декілька разів, але навряд чи більше.

На рис.3.1 наведено зображення алгоритму роботи квантового комп`ютера на основі іонних пасток. Лінійний ланцюг іонів утримується близько до поверхневої електродної пастки (пастка не показана). Лазери з довжинами хвиль 369 та 935 нм (не показані) освітлюють всі іони під час охолодження, ініціалізації та детекції. Флуоресценцію кожного іону зображають через об'єктив з числом апертури 0,6 (оптика детекції) та направляють на окремі канали фотоумножувачів. Два лінійно поляризованих протилежно спрямованих 355 нм раманівських променів вирівнюються на кожен кубіт-іон: глобально-адресуючий промінь, який зв'язується з усіма кубітами (червоний), та окремо-адресуючий промінь, який фокусується на кожному іоні (синій). Акустично-оптичні модулятори (AOM) модулюють частоту та амплітуду кожного з цих променів для генерації однокубітних обертань та XX-гейтів між довільними парами кубіт-іонів.[20]. На рис.3.1 наведено схему апаратної частини. А на рис. 3.2. наведено фотографію іонної пастки[20].

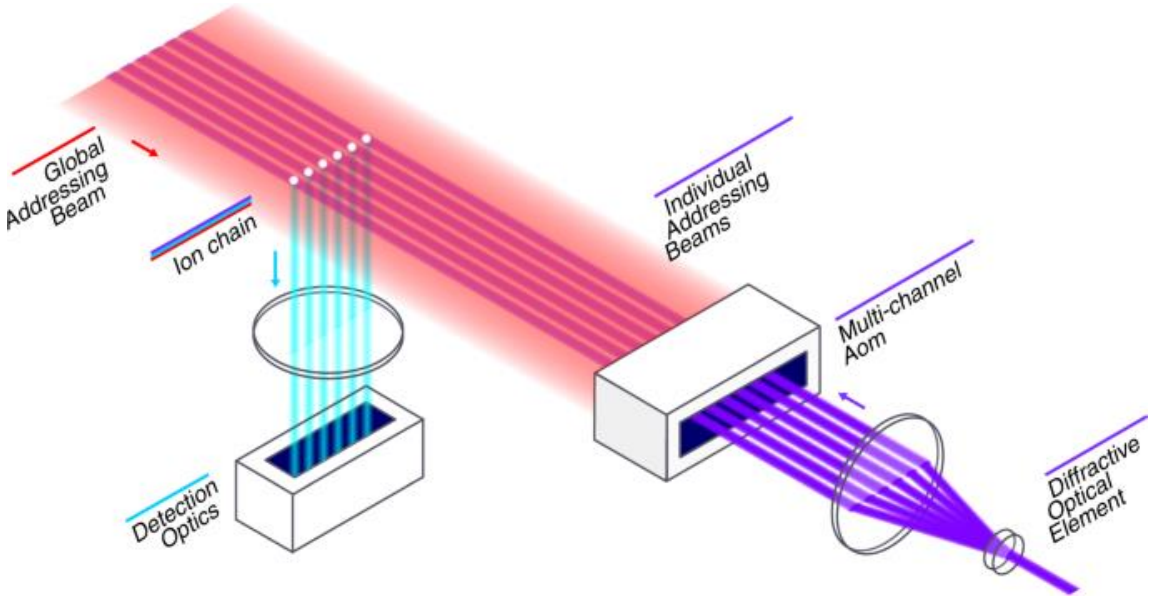


Рисунок № 3.1 – Схема апаратної частини квантового комп`ютера на іонних пастках[20].

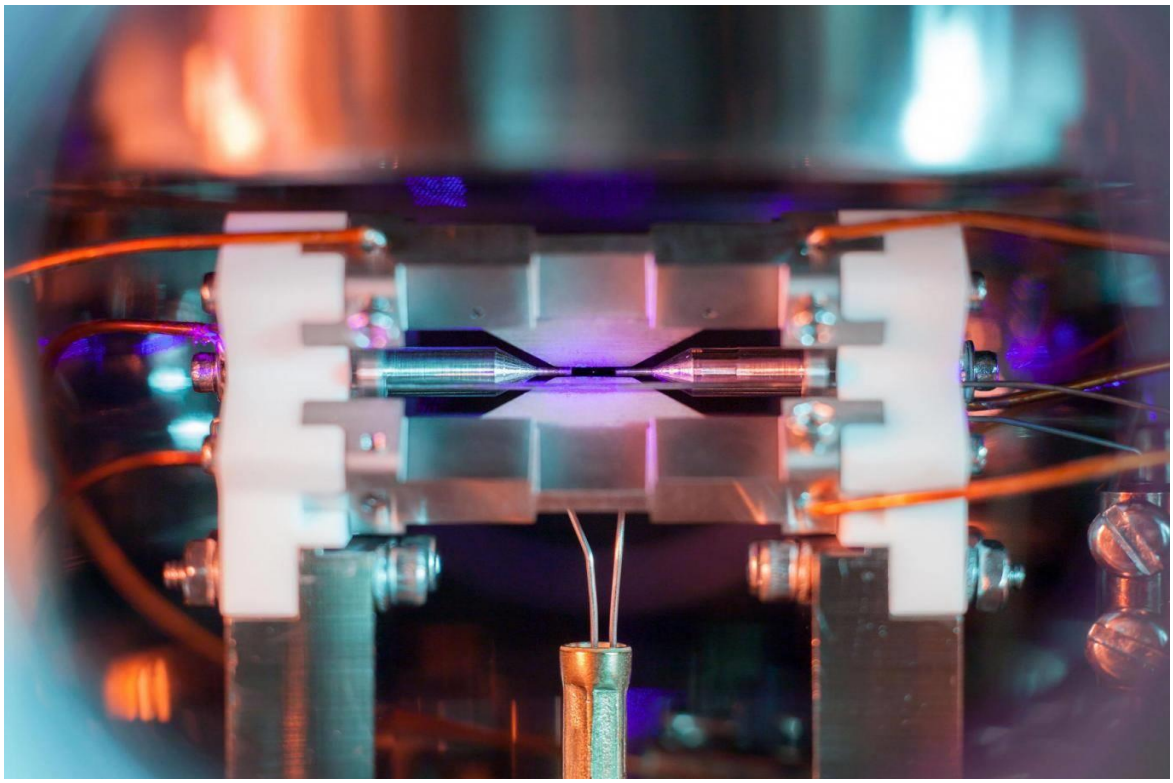


Рисунок № 3.2 – Зображення іонної пастки [1]

2. Схема з двох надпровідників та нанопровідника [21], в якій нанопровідник використовується для заміщення ізоляційного бар'єру, який використовується у звичайних кубітах для утворення Джозефсонівського з'єднання між двома надпровідниками.

Така структура також може поєднувати можливості управління надпровідковими кубітами з тривалим часом когерентності твердотільних спінових або майбутніх топологічних кубітів.

Ці гібридні напівпровідниково-надпровідникові схеми можуть допомогти дослідникам розробляти гнучкі архітектури квантового обчислення, які поєднують в собі різні компоненти та можливості.

На рис. 3.3 зображена схема кубітів на основі нанопровідників[21]:

[1] URL: https://www.ox.ac.uk/news/science-blog/image-strontium-atom-wins-national-science-photography-prize (дата звернення: 19.05.2023)

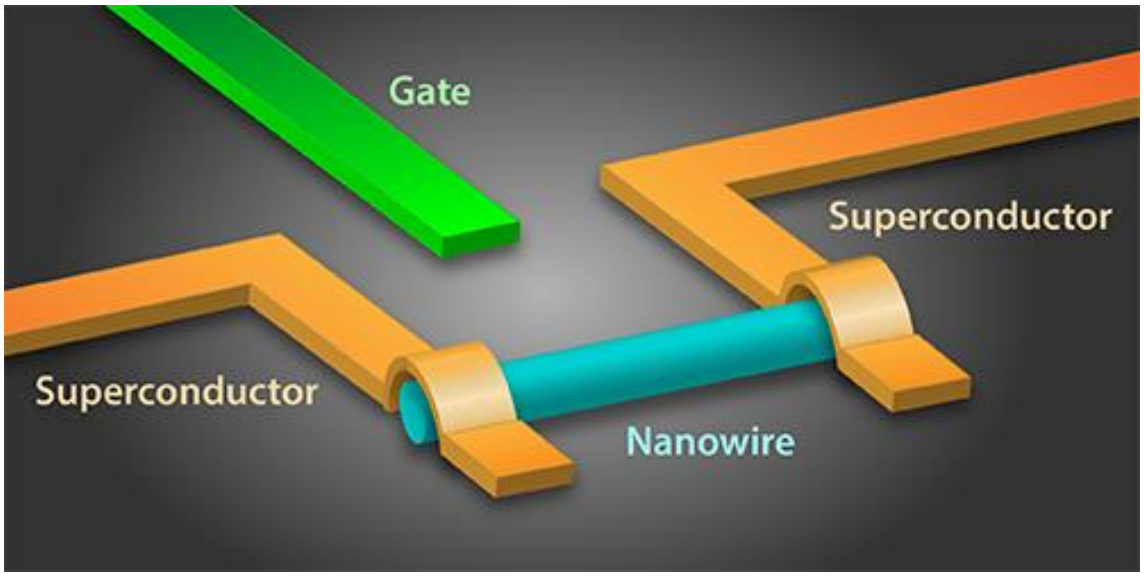


Рисунок №3.3 – система кубітів на основі двох надпровідників та нанопроводу[21].

3. Ядерний магнітний резонанс (ЯМР) – це технологія, яка широко використовується на практиці для вивчення структури молекул. Квантовий процесор у цьому випадку складається з окремої молекули речовини, в якій спінами деяких атомів (зазвичай водню) можна точно управляти. Система переміщується в поєднання сильного постійного та резонансного змінного магнітних полів. Квантові біти представлені станами ядерних спінів, а унітарні оператори реалізуються за допомогою імпульсів змінних магнітних полів. Розщеплення рівнів через спін-спінову взаємодію надає можливість реалізувати двобітові операції. Вимірювання стану досягається звичайним методом ЯМР – виявленням індукованого радіоізотопного випромінювання. Звичайно в ЯМР-спектрометрі спостерігається не окрема молекула, а велика кількість речовини в цілому. Таким чином, насправді використовується "властивість" не чистого стану, а матриці щільності, але цього виявляється достатньо. Однак для більшої кількості квантових бітів ця техніка стає менш ефективною, оскільки сигнал, який ми вимірюємо для n біт, зменшується як 2^{-n}. На рис.3.4 наведено зображення лабораторії спектроскопії.

Рисунок № 3.4 – Лабораторія спектроскопії ЯМР[2]

4. Фотони як основа квантового комп'ютера, виявляються дуже привабливою платформою для реалізації квантових обчислень. Вони майже повністю унеможливлюють вплив шуму і декогеренції, що є серйозними проблемами для інших систем. Фотони можуть бути легко контрольовані та маніпульовані для реалізації квантових вентилів та операцій над кубітами. Крім того, фотони дозволяють кодування інформації в різних ступенях свободи, таких як поляризація, часовий інтервал або шлях, що відкриває широкі можливості для квантової обробки інформації.

Одним із ключових переваг фотонів як кубітів є їхня висока швидкість передачі інформації. Фотони можуть легко рухатися по оптичним шляхам та волокнам, що дозволяє ефективно зв'язувати різні компоненти квантового комп'ютера. Крім того, фотони добре сумісні зі звичайною оптикою і мають добру збереженість квантового стану при передачі по волокну[22].

Хоча реалізація квантових операцій з використанням фотонів потребує складних систем оптичних компонентів та вимагає високої якості джерел одиночних фотонів та детекторів, недавні досягнення в цій галузі показують

[2] URL: https://www.istockphoto.com/photo/3d-nmr-nuclear-magnetic-resonance-spectroscopy-machine-laboratory-2-gm1346961860-424583732 (дата звернення: 20.05.2023)

великий потенціал фотонів для створення масштабованих квантових комп'ютерів.

На рис. 3.5. наведено зображення двох поляризованих станів фотона, які можуть застосовуватися для реалізації квантового комп’ютера[22].

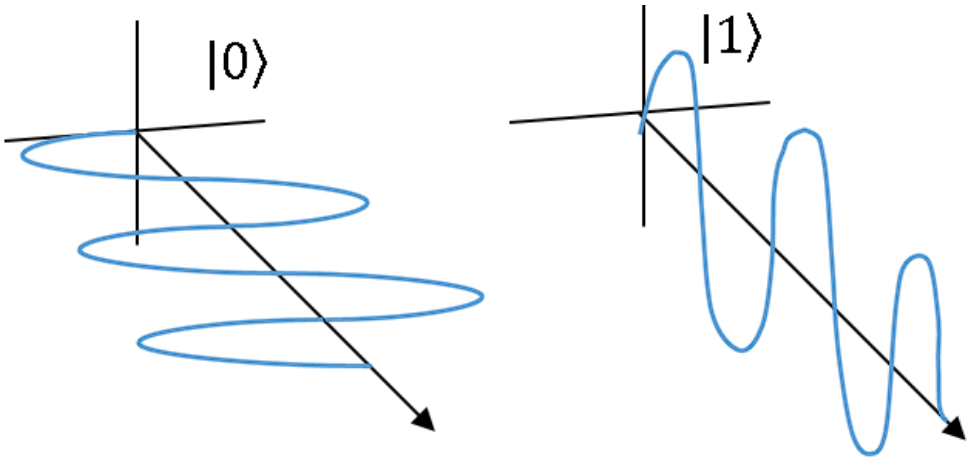


Рисунок № 3.5. Поляризовані стани фотона[22]

Приведені методи є до певної міри традиційними. Надамо короткий опис більш продвинутих можливостей:

1. Системи сверхпровідних гранул. При низьких температурах мікроскопічні сверхпровідні гранули можуть нести заряд у вигляді кількох пар електронів (електрони в сверхпровіднику зв'язані в пари). Гранули взаємодіють між собою за допомогою двохфазних контактів, і ця взаємодія може бути керована. Однак точність управління кожною гранулою повинна бути дуже високою.

2. Аніони – це особливі збудження в двовимірних квантових системах, наприклад, у двовимірній електронній рухомості в магнітному полі. При руху одного такого збудження навколо іншого стану системи змінюється строго визначеним способом. При наявності у рухомості кількох неабелевих аніонів стан рухомості стає виродженим, причому кратність виродження експоненціально залежить від кількості аніонів. Усі ці вироджені стани можуть утворювати квантові суперпозиції. На таку суперпозицію неможливо впливати, не зміщуючи аніони, тому вона ідеально захищена від втручань. Якщо об'єднати один аніон навколо іншого, суперпозиція піддасться визначеному унітарному перетворенню. Це перетворення є абсолютно точним. Таким чином, ми маємо

систему, захищену від помилок на фізичному рівні. Це може бути основою для інших топологічних квантових обчислень.

На рис.3.6 наведено зображення квантових комп’ютерів IBM а, на рис.3.7 Google:

Рисунок № 3.6 – Квантовий комп’ютер IBM[3]

[3]URL:https://newsroom.ibm.com/media-quantum-innovation?keywords=quantum&l=100#gallery_gallery_0:21596/ (дата звернення: 02.06.2023)

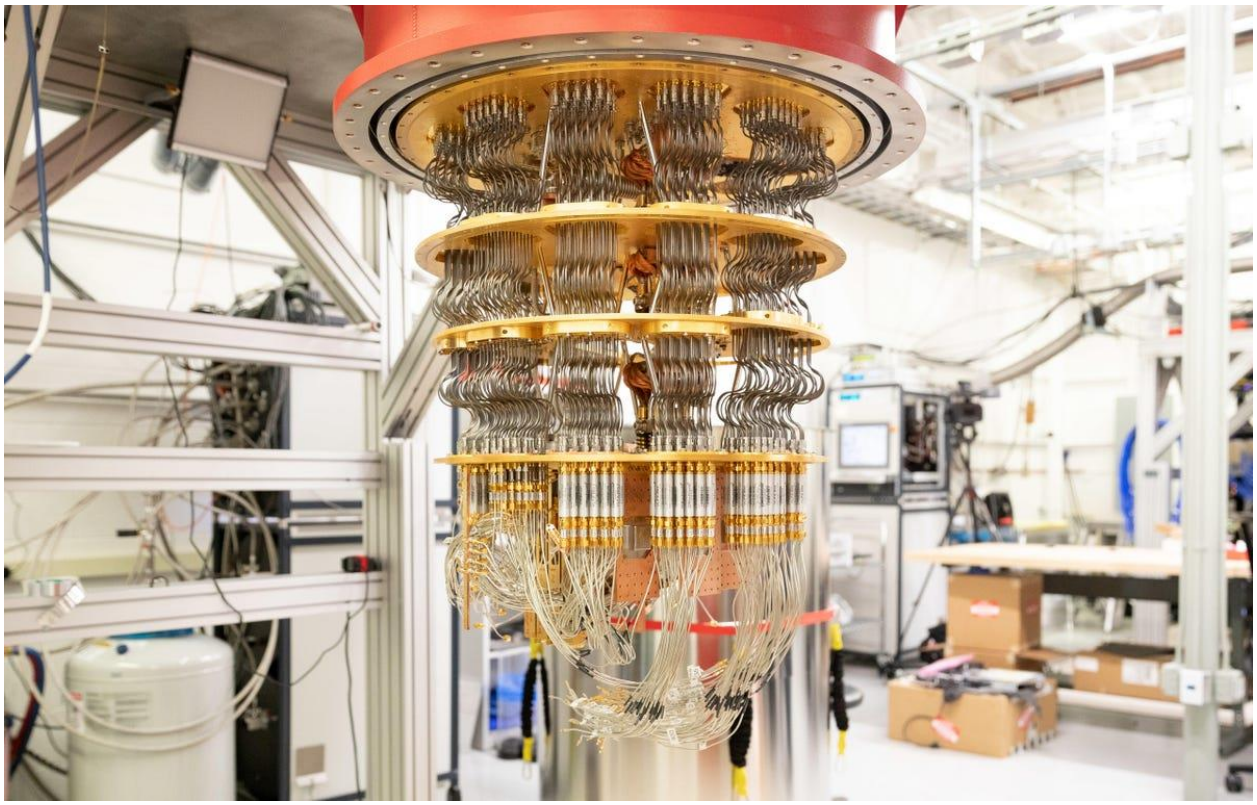


Рисунок № 3.7 – Квантовий комп’ютер Google[4]

[4] URL: https://www.cnet.com/pictures/take-a-look-at-googles-quantum-computing-technology/null/ (дата звернення: 02.06.2023)

ОСНОВНІ РЕЗУЛЬТАТИ ТА ВИСНОВКИ

Квантова теорія інформації досі знаходиться на ранніх етапах свого розвитку, і її потенціал і межі розвитку поки що не повністю відомі. Експериментальні дослідження та практичне застосування деяких її результатів вже можливі (наприклад, квантова криптографія), але реалізація практичних квантових обчислювальних методів наразі ще є складною задачею. Перспективи теоретичного розвитку є дуже значущими. Можливо вдасться пройти глибше в основні принципи вимірювання у квантовій механіці, побудувати щось подібне до інформаційної динаміки, виявити загальні принципи виникнення, поширення та передачі інформації, виділити класичні обчислювальні процеси як стійке підмножини квантових, знайти причини втрати когерентності на макрорівні та виявити причини виникнення принципу зростання ентропії. У великій мірі квантова теорія інформації може мати величезний вплив на науку та суспільство в цілому.

СПИСОК ВИКОРИСТАНИХ ЛІТЕРАТУРНИХ ДЖЕРЕЛ

1. E. Rieffel Quantum Computing: A Gentle Introduction / E. Rieffel, W. Polak // Cambridge[et al.]. – 2011 – P. 1 - 7.

2. N. D. Mermin Quantum computer science: an introduction // Cambridge. – 2007 – P. 12 - 20.

3. R. P. Feynman Quantum mechanical computers // Foundations of Physics, 1986 – Vol. 16 – P. 507–531.

4. P. Benioff The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines // Journal of Statistical Physics. – 1080. – Vol. 22. – №5.

5. D. P. DiVincenzo Quantum Computation // *Science*. – 1995. – Vol. 270. – P. 255-260.

6. P.W. Shor Fault-tolerant quantum computation // Proceedings of 37th Conference on Foundations of Computer Science. IEEE Press. – 1996. – P. 1-10.

7. R. P. Feynman Quantum mechanical computers // Foundations of Physics, 1986. – Vol. 16. – P. 507–520.

8. M.A. Nielsen Quantum Computation and Quantum Information: 10th Anniversary Edition / M.A. Nielsen., I. L. Chang // Cambridge. – 2010. – P. 425– 430.

9. D. Deutsch Universality in quantum computation / , A. Barenco, A. Ekert // Proc. r. soc. Lond. – 1995. – Vol. 449. – P. 1 - 9.

10. Wooters W.K. A single quantum cannot be cloned / Wooters W.K., Zurek W.H // Nature. – 1982. – Vol. 299. – P.802-803.

11. A.Einstein Can Quantium-Mechanical Description of Physical Reality Be Considered Complete? / A.Einstein, B.Podolsky, N.Rosen // Physical Review. – 1935. – Vol. 47. – P. 777-780.

12. J.S. Bell On the Einstein-Podolsky-Rosen paradox // Physics. – 1964. – Vol.1. – P.195-200.

13. C.H. BennettTeleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. Physical Review Letters, 1993; vol.70. № 13.

14. D. Bouwmeester, J.-W. Pan, K. Mattle[et al.] Experimental Quantum Teleportation / C.H. Bennett, G. Brassard, C. Crepeau [et al.].// Nature. – 1997. – Vol.390. – P. 575-579.

15. A. Aspect Testing Bell's inequalities // Europhysics News. – 1991. – Vol. 22. – P. 73–75.

16. P.G. Kwiat New high-intensity source of polarization-entangled photon pairs / P.G. Kwiat, K. Mattle, H. Weinfurter [et al.] // Physics. – 1995. – Vol.75. – P. 4337-4339.

17. A.Yu. Kitaev. Fault-tolerant quantum computations by anyons // Annals of Physics. – 2008. – Vol. 303. – P. 1-13.

18. L.K. Grover Quantum mechanics helps in searching for a needle in a haystack // Physical Review. – 1997. – Vol. 79. – P. 1-4.

19. L.K. Grover A fast quantum mechanical algorithm for database search. In Proceedings of the twenty-eighth annual ACM Symposium on Theory of computing/ / International Journal of Intelligence Science. – 1996. – Vol.9. – №.1.

20. K. Wright Benchmarking an 11-qubit quantum computer /, K.M. Beck, S. Debnath [et al.] // Nature communications. – 2019. – Vol. 1. – P. 1-2.

21. M. J. Nichol Wiring Up Superconducting Qubits // Physical Review. – 2015. – Vol. 8. – P. 1-3.

22. J. L. O'Brien, et al., Optical Quantum Computing // Science. – 2007. – Vol.318. – P. 1567-1568.