

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

Факультет прикладної математики

Кафедра системного програмування і спеціалізованих комп'ютерних систем

«На правах рукопису»
УДК 519.6

До захисту допущено:

Завідувач кафедри

_____ Віталій РОМАНКЕВИЧ

« ____ » _____ 2021 р.

Магістерська дисертація

на здобуття ступеня магістра

за освітньо-професійною програмою

«Системне програмування і спеціалізовані комп'ютерні системи»

зі спеціальності 123 «Комп'ютерна інженерія»

**на тему: «Методи обробки інформації надпровідних гравіметрів на
основі квантових обчислень»**

Виконав:

студент II курсу, групи КВ-02мп

Без'язичний Максим Володимирович _____

Науковий керівник:

Професор кафедри СПСКС

Яценко Віталій Олексійович _____

Рецензент:

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.

Студент _____

Київ – 2021 року

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

Факультет прикладної математики

Кафедра системного програмування і спеціалізованих комп'ютерних систем

Рівень вищої освіти – другий (магістерський)

Спеціальність – 123 «Комп'ютерна інженерія»

Освітньо-професійна програма «Системне програмування і спеціалізовані комп'ютерні системи»

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____ Віталій РОМАНКЕВИЧ

«__» _____ 2020 р.

ЗАВДАННЯ

на магістерську дисертацію студенту

Без'язичний Максим Володимирович

1. Тема дисертації «Методи обробки інформації надпровідних гравіметрів на основі квантових обчислень», науковий керівник дисертації **Яценко Віталій Олексійович**, Професор кафедри СПСКС, затверджені наказом по університету від «5» 11. 2021 р. №3682-С
2. Термін подання студентом дисертації 7.12.2021
3. Об'єкт дослідження: Методи обробки інформації для надпровідних гравіметрів на основі квантових обчислень

4. Вихідні дані: існуючі квантові алгоритми, методи обробки даних у квантових системах, будови різних типів гравіметрів та принципи обробки інформації для них.

5. Перелік завдань, які потрібно розробити: дослідити літературу пов'язану з теорією про принципи роботи квантової системи та розглянути методи керуваності КС. Оптимізувати існуючий алгоритм гравіметра за допомогою квантових обчислень

6. Орієнтовний перелік графічного (ілюстративного) матеріалу - презентація

7. Орієнтовний перелік публікацій - 2 статті

9. Дата видачі завдання 7.10.2020

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Термін виконання етапів магістерської дисертації	Примітка
1	Дослідження літератури за тематикою роботи	15.09.2021	
2	Написання першого розділу	10.10.2021	
3	Написання другого розділу	26.10.2021	
4	Написання та публікація статей щодо результатів роботи	17.11.2021	
5	Написання заключного розділу та висновків	29.11.2021	
6	Розгляд матеріалів магістерської роботи на кафедрі	30.11.2021	

Студент

Максим БЕЗ'ЯЗИЧНИЙ

Науковий керівник

Віталій ЯЦЕНКО

РЕФЕРАТ

Актуальність теми. Квантова фізика принесла в наше звичайне життя багато винаходів і технологій, без яких зараз важко уявити навколишній світ. Наприклад, лазер, який зараз використовується скрізь, від побутової техніки (лазерні нівеліри та інше) до високотехнологічних систем. Логічно було б припустити, що рано чи пізно хтось висуне ідею про те, що чому б не використовувати квантові системи для обчислень. І ось 1980 року це сталося.

Про ідею квантових обчислень заговорив вперше відомий Р. Фейнман у доповіді на першій конференції з фізики обчислень, зазначивши, що неможливо моделювати еволюцію квантової системи на класичному комп'ютері ефективним способом. Він запропонував елементарну модель квантового комп'ютера, який зможе провести таке моделювання.

Минуло приблизно 17 років з моменту ідеї до її першої реалізації в комп'ютері з двома кубітами – (1998 рік), і 21 рік до моменту, коли кількість кубітів збільшилася до 53-х (2019 рік). Також лише відносно нещодавно ми підійшли до того, щоб реалізувати те, про що говорив Фейнман, та навчитися моделювати найпростіші фізичні системи.

Розвиток квантових обчислень йде повільно. Перед вченими та інженерами стоять дуже складні завдання, квантові стани дуже недовговічні і крихкі і, щоб зберегти їх досить довгий час для виконання обчислень, доводиться будувати саркофаги за десятки мільйонів доларів, в яких підтримується температура трохи вища за абсолютний нуль, і які максимально захищені від зовнішніх впливів. Далі ми проаналізуємо завдання та проблеми які ставить квантові обчислення перед людством, а також дослідимо можливі шляхи розвитку методів квантових обчислень на прикладі обчислення у гравіметрах.

Об’єктом дослідження є квантові алгоритми та методи обчислення інформації у надпровідних гравіметрах, можливість побудови групових дискретних автоматів на керуючих переходах квантової системи.

Предметом дослідження є побудова квантових алгоритмів і можливість їх застосування для обчислення інформації у надпровідних гравіметрах.

Мета роботи: проаналізувати проблематику процесів обчислення інформації у надпровідних гравіметрах, описати процес та побудову гравіметру. Дослідити існуючі квантові алгоритми, побудувати реалізацію квантового алгоритму, який зможе потенційно оптимізувати методи обчислення в гравіметрії. Змодельовати роботу алгоритму.

Наукова новизна: Побудовано схему квантового алгоритму та змодельована його робота. Розглянута практична користь квантових алгоритмів у порівнянні з класичними. Запропоновано використання реалізованого алгоритма у сфері обчислення інформації для гравіметрії.

Апробація роботи. Основні положення роботи були представлені та обговорювались на XIV науковій конференції магістрантів та аспірантів «Прикладна математика та комп’ютинг» ПМК-2021 (Київ, 17-19 листопада 2021 р.) та міжнародна науково-практична конференція “Topical issues of modern science, society and education” (Харків, 26 грудня 2021 р.).

Структура та обсяг роботи. Магістерська дисертація складається з вступу, трьох розділів та висновків.

У вступі подано загальну характеристику роботи, зроблено оцінку сучасного стану проблеми, обґрунтовано актуальність напрямку досліджень, сформульовано мету і задачі досліджень.

У першому розділі розглянуто складові квантової системи. Дослідження принципів побудови дискретних автоматів на управляючих переходах квантової системи.

У другому розділі міститься аналіз квантових алгоритмів та потенціальна користь в сфері розв'язку задач комбінаторики. Побудована блок схема квантового алгоритму та наведена по-крокова реалізація алгоритму на квантовій машині. Проаналізовано отриманий результат.

У третьому розділі описано принципи роботи гравіметра та методи обробки інформації для гравіметрів. Запропоновано використання реалізованого алгоритма у сфері обчислення інформації для гравіметрії.

У висновках представлені результати проведеної роботи.

Робота представлена на 86 аркушах, містить посилання на список використаних літературних джерел.

Ключові слова: квантова система, групові дискретні автомати, квантові алгоритми, гравіметр.

ABSTRACT

Actuality of theme. Quantum physics has brought many inventions and technologies into our ordinary lives, without which it is now difficult to imagine the world around us. For example, the laser, which is now used everywhere, from home appliances (laser levels, etc.) to high-tech systems. It would be logical to assume that sooner or later someone will come up with the idea of why not use quantum systems for calculations. And in 1980 it happened.

The idea of quantum computing was first discussed by the well-known R. Feynman in a report at the first conference on computational physics, noting that it is impossible to model the evolution of a quantum system on a classical computer in an efficient way. He proposed an elementary model of a quantum computer that could perform such modeling.

It took about 17 years from the idea to its first implementation in a computer with two qubits - (1998), and 21 years until the number of qubits increased to 53 (2019). Also, only relatively recently have we come to realize what Feynman was talking about and learn to model the simplest physical systems.

The development of quantum computing is slow. Scientists and engineers face very difficult tasks, quantum states are very short-lived and fragile, and to keep them long enough to perform calculations, they have to build sarcophagi for tens of millions of dollars, which maintain temperatures slightly above absolute zero, and which are protected from external influences. In this work, we will analyze the challenges and problems posed by quantum computing to humanity, as well as explore possible ways to develop methods of quantum computing on the example of computation in gravimeters.

The object of research is quantum algorithms and methods of calculating information in superconducting gravimeters, the possibility of constructing group discrete automata on the controlled transitions of a quantum system.

The subject of research is the construction of quantum algorithms and the possibility of their application to calculate information in superconducting gravimeters.

Purpose: to analyze the problems of information calculation processes in superconducting gravimeters, to describe the process and construction of the gravimeter. Investigate existing quantum algorithms, build an implementation of a quantum algorithm that can potentially optimize calculation methods in gravimetry. Simulate the algorithm on a working machine.

Scientific novelty: The scheme of quantum algorithm is constructed and its work is modeled. The practical usefulness of quantum algorithms in comparison with classical ones is considered. The use of the implemented algorithm in the field of information calculation for gravimetry is proposed.

Approbation of work. The main provisions of the work were presented and discussed at the XIV scientific conference of undergraduates and graduate students "Applied Mathematics and Computing" PMK-2021 (Kyiv, November 17-19, 2021) and the international scientific-practical conference "Topical issues of modern science, society and education "(Kharkiv, December 26, 2021).

Structure and scope of work. The master's dissertation consists of an introduction, three chapters and conclusions.

In the introduction the general characteristic of work is given, the estimation of a modern condition of a problem is made, the urgency of a direction of researches is proved, the purpose and tasks of researches are formulated.

The first section considers the components of the quantum system. Research of principles of construction of discrete automata on control transitions of quantum system.

The second section provides an analysis of quantum algorithms and the potential benefits of combinatorics. A block diagram of a quantum algorithm is

constructed and a step-by-step implementation of the algorithm on a quantum machine is given. The obtained result is analyzed.

The third section describes the principles of gravimeter operation and information processing methods for gravimeters. The use of the implemented algorithm in the field of information calculation for gravimetry is proposed.

The conclusions present the results of the work.

The work is presented on 86 sheets, contains references to the list of used literature sources.

Keywords: quantum system, group discrete automata, quantum algorithms, gravimeter.

Оглавление

ВСТУП.....	11
РОЗДІЛ 1. ОГЛЯД СКЛАДОВИХ КВАНТОВОЇ СИСТЕМИ.....	17
Базові поняття та терміни квантової системи	17
Квантова корекція помилок.....	28
Принцип побудови дискретних автоматів на управляючих переходах квантової системи	33
РОЗДІЛ 2. АНАЛІЗ КВАНТОВИХ АЛГОРИТМІВ ТА ПОТЕНЦІАЛЬНА КОРИСТЬ В СФЕРІ РОЗВ’ЯЗКУ ЗАДАЧ КОМБІНАТОРИКИ.	42
Загальний вступ до квантових алгоритмів	42
Квантові алгоритми на основі перетворення Фур'є	43
Алгоритми квантового пошуку	45
Квантова симуляція	46
Алгоритм Дойча та алгоритм Дойча – Йожі.....	48
Алгоритм Шора.....	52
Алгоритм Гровера	54
Складність задач комбінаторної оптимізації та перспективи квантових комп'ютерів для їх вирішення	56
Проблема домінуючого набору (ПДН)	58
Реалізація алгоритму для рішення ПДН	61
Аналіз складових алгоритму	66
РОЗДІЛ 3. ПРИНЦИПИ РОБОТИ ГРАВІМЕТРІВ.	69
Види гравіметрів та дослідження будови гравіметра.	69
Методи обробки інформації в гравіметрії і проблеми які вони вирішують.....	79
ВИСНОВКИ	84
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	86

ВСТУП

У сучасному світі з'являється все більше і більше інформації так, що звичайні комп'ютери вже не поспішають у методах обробки таких об'ємів. Більше того, перед людством ще існує ряд математичних завдань, які здаються не вирішеними при спробах знайти відповідь, використовуючи поточні потужності обчислення, навіть настільки великі як потужності суперкомп'ютерів. Завдяки можливості виконувати дуже складні обчислення значно швидше ніж звичайні, квантові комп'ютери можуть надати таке необхідне зростання продуктивності та швидкості. Більшість фахівців погоджуються з тим, що квантові комп'ютери – це наш шанс впоратися з викликами 21 століття.

Перша квантова революція відбулася у XX столітті, більш конкретно у другій половині, і призвела до появи лазерів, транзисторів, ядерної зброї, а згодом – мобільного телефонного зв'язку та інтернету. Технології першої квантової революції застосовують у комп'ютерах, мобільних телефонах, планшетах, цифрових камерах, системах зв'язку, світлодіодних лампах, МРТ-сканерах, скануючих тунельних мікроскопах тощо. Обсяг ринку відповідної продукції у світі становить \$3 трлн на рік. При цьому «закон Мура», згідно з одним із визначень якого, що продуктивність процесорів має подвоюватися кожні 18 місяців, більше не працює.

Зараз людство і світ знаходиться на порозі II квантової революції. У I квантовій революції технологи та прилади будувалися на управлінні колективними квантовими явищами. У другій квантової революції технології будуватимуться на здатності керування складними квантовими системами на рівні окремих частинок, наприклад, атомів та фотонів. Технології, засновані саме на такому високому рівні контролю над індивідуальними квантовими об'єктами прийнято об'єднувати терміном квантові технології.

Наразі існує дуже багато проблем при спробах створити квантового комп'ютера. Насамперед необхідно навчитися переводити кубіти у певні вихідні стани, об'єднувати кубіти у заплутані керовані системи, ізолювати ці системи, оскільки ще існує вплив зовнішніх перешкод, якій потрібно мінімізувати, зчитувати результати квантового розрахунку.

Також розробники квантового комп'ютера повинні обрати оптимальну елементну базу виготовлення кубітів. Є кілька конкуруючих підходів, і один із них — надпровідні кубіти з джозефсонівськими переходами, схожі на перші носії цифрової інформації — феритові кільця. Щоправда, кубіти приблизно в тисячу разів менше магнітних бітів в ті часи, що передували появі інтегральних мікросхем. Розробками в цій галузі зайнято безліч іноземних інститутів та лабораторій великих компаній. Володіння робочими прототипами квантового комп'ютера відкриває величезні можливості у розробці нових матеріалів, розшифровці найскладніших кодів, моделюванні складних систем, створенні універсального штучного інтелекту та багатьох інших галузей.

За своєю суттю, квантові обчислювальні системи є вершиною розвитку у паралельних обчисленнях. Обчислювальні завдання, вирішення яких недоступно традиційним комп'ютерам, дуже легко можуть бути вирішити такими квантовими системами. Наприклад, квантові комп'ютери можуть проводити моделювання природних процесів на у таких галузях як хімія, молекулярної фізики, матеріалознавства та інше. З такими потужностями в обчисленнях квантового комп'ютера, вчені зможуть створити ліки від невиліковних на цей час хвороб, каталізатори для вбирання вуглекислого газу з повітря, надпровідники, здатні працювати за кімнатних температур та багато інших винаходів. Це буде справжній технічний прорив.

Однак, незважаючи на прогрес у дослідженнях квантових систем та активні дискусії про поточні успіхи та відкриття, залишається актуальною проблема вирішення фізичних перешкод при створенні валідних масштабованих квантових систем, здатних до необхідної точності в обчисленнях. Однією з таких проблем є проблема виробництва одноманітних і стабільних кубітів (це базові елементи квантової обчислювальної системи, детальніше дивіться далі).

Кубіти вимагають ніжного поводження до себе. Випадковий шум і навіть випадкове спостереження за кубітом можуть призвести до втрати даних. Для того щоб кубіт стабільно працював необхідна надзвичайно низька температура середовища у якій він знаходиться – близько до абсолютного нуля по Кельвіну, що є подібним до температури відкритого космосу. Такий температурний режим пред'являє жорсткі вимоги до конструкції корпусів квантових систем, до складу яких і входять безпосередньо кубіти.

Ідеї квантового комп'ютингу та квантової зв'язку виникли через сто років після народження початкових ідей квантової фізики. Можливість побудови квантових комп'ютерів і систем зв'язку показана виконаними до теперішнього часу теоретичними та експериментальними дослідженнями. Квантова фізика "достатня" для проектування квантових комп'ютерів на різній "елементній базі". Квантові комп'ютери, якщо їх вдасться побудувати, будуть технікою XXI століття. Для їх виготовлення потрібно створення і розвиток нових технологій на нанометровому і атомному рівні розмірів. Ця робота може тривати, очевидно, кілька десятиліть. Побудова квантових комп'ютерів було б ще одним підтвердженням принципу невичерпності природи: природа має кошти для здійснення будь-якої коректно сформульованої людиною завдання.

У звичайному комп'ютері інформація кодується послідовністю бітів, і ці біти послідовно обробляються Булевського логічними елементами, щоб отримати потрібний результат. Аналогічно квантовий комп'ютер обробляє кубіти, виконуючи послідовність операцій квантовими логічними елементами, кожний з яких представляє собою унітарне перетворення, що діє на одиничний кубіт або пару кубітів. Послідовно виконуючи ці перетворення, квантовий комп'ютер може виконати складне унітарна перетворення над усім набором кубітів приготованих у деякому початковому стані. Після цього можна зробити вимір над кубітами, яке і дасть кінцевий результат обчислень. Ця схожість обчислень між квантовим і класичним комп'ютером дозволяє вважати, що, принаймні, в теорії, класичний комп'ютер може в точності відтворювати роботу квантового комп'ютера. Іншими словами, класичний комп'ютер може робити все те ж саме, що і квантовий комп'ютер. Тоді навіщо вся ця метушня з квантовим комп'ютером? Справа в тому, що, хоча теоретично класичний комп'ютер може симулювати квантовий комп'ютер, це дуже неефективно, настільки неефективно, що практично класичний комп'ютер не в змозі вирішувати багато завдань, які під силу квантовому комп'ютера. Симуляція квантового комп'ютера на класичному комп'ютері обчислювально складна проблема, тому що кореляції між квантовими бітами якісно відрізняється від кореляцій між класичними бітами, як було вперше показано Джоном Беллом. Для прикладу можна взяти систему тільки з декількох сотень кубітів. Вона існує в просторі Гільберта розмірністю $\sim 10^{90}$, що зажадає, при моделюванні класичним комп'ютером, використання експоненціально великих матриць (щоб виконати розрахунки для кожного окремого стану, який також описується матрицею). Це означає, що класичного комп'ютера

знадобиться експоненціально більше часу, аніж навіть з примітивним квантовим комп'ютером.

Річард Фейнман був серед перших, хто усвідомив потенціал, закладений в явищі квантової суперпозиції для вирішення таких завдань значно швидше. Наприклад, система з 500 кубітів, яку практично неможливо змодельовати класично, являє собою квантову суперпозицію з 2500 станів. Кожне значення такої суперпозиції класично еквівалентно списку з 500 одиниць і нулів. Будь-яка квантова операція над такою системою, наприклад, налаштований певним чином імпульс радіохвиль, який може виконати операцію кероване НЕ над, скажімо, 100-м і 101-м кубітом, одночасно впливати на 2 500 станів. Таким чином, за один тик комп'ютерних годин квантова операція обчислює не одне машинне стан, як звичайні комп'ютери, а 2 500 станів відразу! Однак, врешті-решт, над системою кубітів проводиться вимірювання, і система колапсує в єдине квантовий стан, відповідне єдиного вирішення завдання, єдиному набору з 500 одиниць і нулів, як це диктується вимірювальної аксіомою квантової механіки. Це воістину хвилюючий результат, оскільки це рішення, знайдене колективним процесом квантових паралельних обчислень, що беруть свої витoki в суперпозиції, еквівалентно виконання тієї ж самої операції на класичному суперкомп'ютері з ~ 10 150 окремих процесорів. Перші дослідники в цій області були, звичайно, натхненні такими гігантськими можливостями, і тому незабаром почалося справжнє полювання за відповідними завданнями для такої обчислювальної потужності. Пітер Шор, дослідник і комп'ютерний вчений з компанії AT & T's Bell Laboratories в Нью Джерсі, запропонував таку задачу, яку можна було б вирішити саме на квантовому комп'ютері і за допомогою квантового алгоритму. Алгоритм Шора використовує міць квантової суперпозиції, щоб розкласти великі числа (порядку ~

10 200 двійкових розрядів і більше) на множники за кілька секунд. Ця задача має важливе практичне застосування для шифрування, де загальноприйнятий (і найкращий) алгоритм шифрування, відомий як RSA, заснований саме на складності розкладання великих складених чисел на прості множники. Комп'ютер, який з легкістю вирішує таке завдання, звичайно, представляє великий інтерес для безлічі урядових організацій, що використовують RSA, який до цих пір вважався "незламуваним", і для будь-якого хто зацікавлений в безпеці своїх даних.

Шифрування, однак, тільки одне можливе застосування квантового комп'ютера. Шор розробив цілий набір математичних операцій, які можуть бути виконані виключно на квантовому комп'ютері. Деякі з цих операцій використовуються в його алгоритмі факторизації. Далі, Фейнман стверджував, що квантовий комп'ютер може діяти як моделює пристрій для квантової фізики, потенційно відкриваючи двері до багатьох відкриттів у цій області. В даний час потужність і можливості квантового комп'ютера, в основному, предмет теоретичних міркувань: появи першого посправжньому функціонального квантового комп'ютера, безсумнівно, принесе багато нових і хвилюючих практичних застосувань.

РОЗДІЛ 1. ОГЛЯД СКЛАДОВИХ КВАНТОВОЇ СИСТЕМИ

Базові поняття та терміни квантової системи

Зрозумілим законам класичної фізики підпорядковується сучасний комп'ютер, а квантовий комп'ютер це пристрій, який використовує квантово-механічні явища (особливо квантову інтерференцію), щоб здійснювати новий спосіб обробки інформації. У квантовому комп'ютері фундаментальна одиниця інформації кубіт. Ця властивість кубіта відбувається як прямий наслідок його підпорядкованості законам квантової механіки, які радикально відрізняються від законів класичної фізики. Кубіт може існувати не тільки в стані, що відповідає логічним 0 або 1, як класичний біт, але також у станах, відповідних суміші або суперпозиції цих класичних станів. Тобто кубіт може існувати як нуль, як одиниця, і як одночасно 0 і 1. При цьому можна вказати деякий чисельний коефіцієнт, що представляє ймовірність опинитися в кожному стані. Кубітом може виступати будь-який об'єкт, який має квантову поведінку, наприклад фотон.

Суперпозиція станів

Кубіт, що знаходиться в суперпозиції, при вимірюванні колапсує в одне з двох детермінованих станів (0 або 1). Ймовірність стану 1 або 0 визначається суперпозицією кубіта. Якщо кубіт знаходиться в рівній суперпозиції, то він знаходиться наполовину в стані 0, наполовину в стані 1. Отже, при вимірюванні кубіт з 50% ймовірністю перейде в стан 0 і з такою ж вірогідністю - в стан 1. Якщо кубіт, скажімо, в 75 % переходить в стан 0 і в 25% в стан 1, при 100 вимірах кубіт перейде в стан 0 приблизно 75 раз і в стан 1 приблизно 25 раз.

Суперпозицію станів кубіта зображують графічно у вигляді

координатної сітки на сфері, де кожний вузол відповідає певному стану (рис. 1.1).

Якщо кожний стан кубіта позначити як $\alpha|0\rangle$ (функція, яка описує стан, коли спин квантової частинки направлений проти зовнішнього поля) та $\beta|1\rangle$ (спин квантової частинки направлений по напрямленню зовнішнього поля), тоді будь-який стан із множини можливих буде визначатись наступним співвідношенням (суперпозицією):

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

де α , β – комплексні функції, які задовольняють відношення $|\alpha|^2 + |\beta|^2 = 1$ ($|\alpha|^2$ та $|\beta|^2$ являються амплітудами ймовірності переходів у стани $\alpha|0\rangle$ та $\beta|1\rangle$).

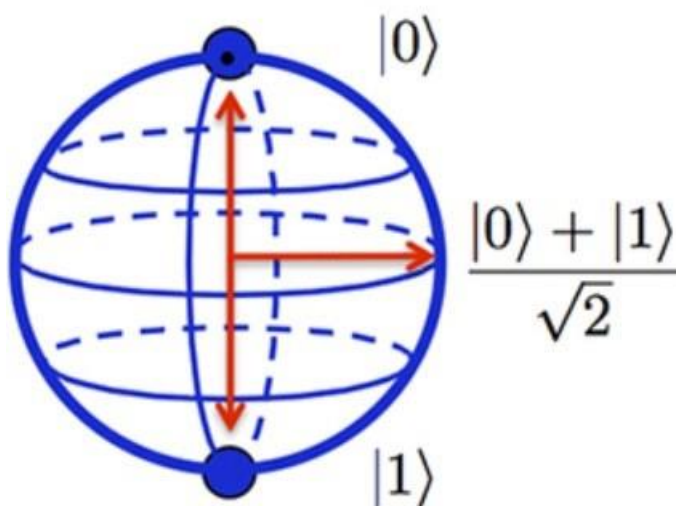


Рисунок 1.1 - Представлення кубіта

Стани $|0\rangle$ та $|1\rangle$ називають спеціальними станами обчислювального базису, які утворюють ортонормований базис цього векторного простору. Можна виміряти біт, щоб визначити стан, в якому

він знаходиться. Наприклад, комп'ютери роблять це кожного разу, зчитуючи вміст своєї пам'яті. Проте ми не можемо виміряти кубіт, щоб визначити його квантовий стан. Квантовий біт може приймати нескінченно багато значень, проте як результат вимірювань ми можемо отримати або стан $|0\rangle$ з імовірністю $|\alpha|^2$, або стан $|1\rangle$ з імовірністю $|\beta|^2$. Цей розрив між спостережуваним станом кубіта та доступними нам спостереженнями лежить в основі квантових обчислень та квантової інформації.

Кубіти можуть бути зв'язані (або заплутані) між собою. Що означає накладений зв'язок на них, внаслідок чого зміна стану одного із кубітів впливає наузгоджену зміну станів інших. Сукупність заплутаних між собою кубітів визначається як заповнений квантовий регістр бітів. Він спроможний знаходитись не тільки в усіх можливих комбінаціях складових його бітів, а і реалізовувати залежності між ними, що суттєво збільшує обчислювальні можливості систем, оснований на кубітах.

Отже, кубіти можуть містити значно більше інформації, ніж біти. Один біт містить таку ж кількість інформації, що і кубіт - обидва вони можуть містити однезначення. Однак чотири біти використовуються для зберігання того ж обсягу інформації, що два кубіта. Двох-кубітна система в рівній суперпозиції містить значення для чотирьох станів, що в класичному обчисленні вимагає чотирьох бітів. Вісім біт зберігають інформацію, яку можна зберегти в трьох кубітах, так як трьох-кубітна система може зберігати вісім станів - 000, 001, 010, 011, 100, 101, 110 і 111. І так далі.

Кубіт «живе» одночасно в абстрактному двовимірному гільбертовому просторі та у звичайному тривимірному евклідовому. Операції обчислення над кубітом задають через унітарні (оборотні) обертання вектора стану на сфері Блоха. Параметри обертання (напрямок

осі та величину кута) задаються фізичною дією на квантовий об'єкт: напруженість електричного поля, частота електромагнітного імпульсу, поляризація фотона тощо.

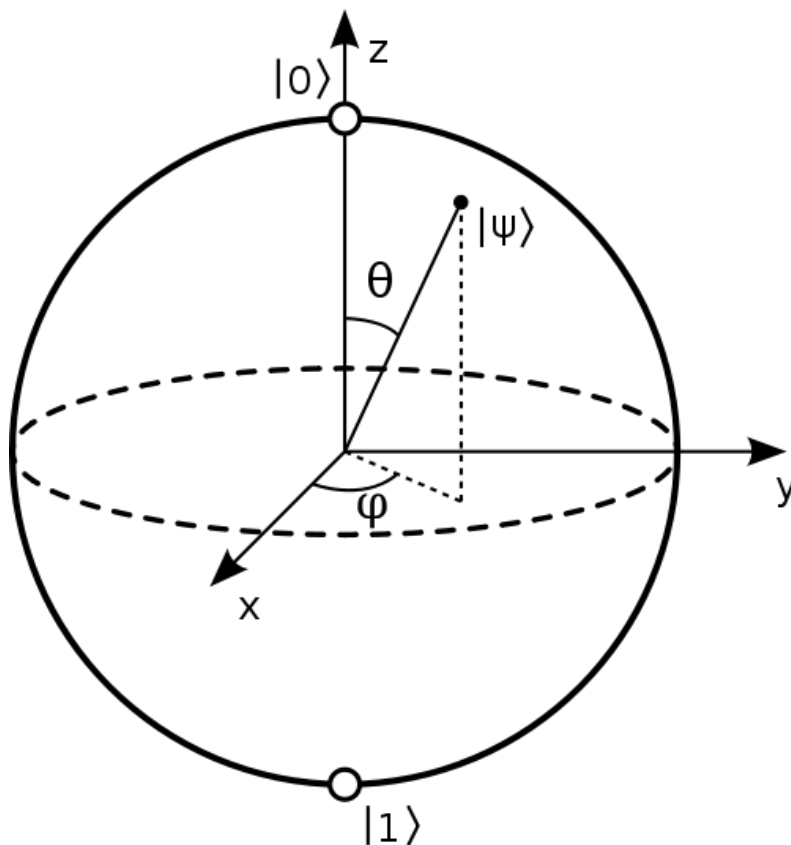


Рисунок 1.2 - Представлення стану кубіта на сфері Блоха

Ще пару прикладів візуалізації станів кубітів за допомогою сфери Блоха зображено на рис. 1.3.

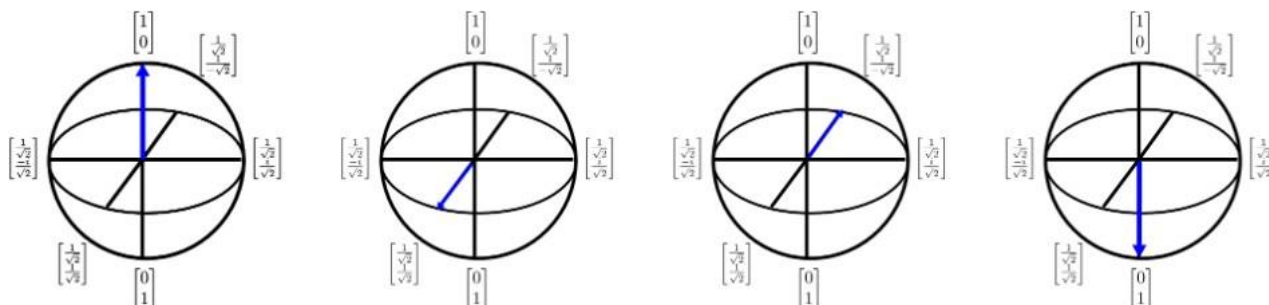


Рисунок 1.3 - Приклади візуалізації сфери Блоха

Стрілки на цій діаграмі показують напрямок, в який спрямований вектор квантового стану, і кожне перетворення стрілки можна розглядати як обертання навколо однієї з основних осей. Хоча думка про квантові обчислення як про послідовність обертань є потужною інтуїцією, використовувати цю інтуїцію для розробки та опису алгоритмів складно.

За допомогою нескінченної кількості вимірювань на однакових кубітах можливо визначити стан кубіта. У випадку не проведення вимірів, на сфері Блоха буде приховано всю еволюцію стану кубіта, так звана прихована квантова інформація. Об'єм цієї додаткової інформації зростає експоненційно зі збільшенням кількості кубітів. Розуміння прихованої інформації є визначальним упитанням про те, що саме робить квантову механіку таким ефективним інструментом обробки інформації.

Різні фізичні сутності можуть бути використані як кубіти, включаючи іони, надпровідні заряди, спіни атомного ядра тощо. Однак кожен із них має той чи інший недолік, який впливає при реалізації повно масштабного квантового комп'ютера з використанням цієї сутності. У цій гонці квантових комп'ютерів фотони також забезпечують кілька переваг порівняно з іншими сутностями, які використовують в якості кубітів.

Найбільша перевага використання фотонів в якості кубітів полягає в тому, що оптичний квантовий комп'ютер може запропонувати в порівнянні з іншими обчислювальними системами те, що вони забезпечують безперервну інтеграцію квантового зв'язку, це відбувається саме завдяки допомозі фотонів та квантових обчислень. Окрім того, використовуючи фотони не легко отримати декогерентність в порівнянні з багатьма іншими системами. Крім того, на відміну від інших претендентів на роль кубіта, фотони не потребують експлуатування при

екстремально низьких температурах для того, щоб забезпечити мінімальний тепловий шум.

Фотони мають деякі властивості, які роблять їх надзвичайно привабливими для використання в квантових комп'ютерах: фотони мають відносно слабку взаємодію з навколишнього середовища та між собою. Це причина, по якій фотони можуть розповсюджуватись досить далеко у багатьох матеріалах, не розсіюючись і не поглинаючись, надаючи фотонним кубітам хороші властивості когерентності та роблячи їх корисними для передачі квантової інформації на великі відстані. Таким чином, дослідження та розробки в цій галузі важливі для створення міжміських квантових каналів зв'язку, навіть якщо інші технології обертаються переважно для широкомасштабних обчислювальних програм. Розвиток можливостей фотонного квантового маніпулювання може мати трансформативні програми для квантового зондування та квантового зв'язку.

Експерименти, що доводять квантову заплутаність фотонів, тривалі історії, що сягає найдавніших експериментів з пошуку порушень Теорема Белла в 1970-х. За останні кілька десятиліть методи були розроблені, що подолали багато перешкод для створення, маніпулювання та вимірювання багатофотонних переплутаних станів.

Багато в чому фотони - чудові кубіти; однокубітові ворота можуть бути виконуються із використанням стандартних оптичних пристроїв, таких як фазообмінники та роздільники променів, і, як уже згадувалося раніше, вони слабо взаємодіють з речовиною та один з одним, надаючи їм хорошої злагодженості. Але їх сила – слабка взаємодія - також створює велику перешкоду для розвитку фотонній квантові комп'ютери, оскільки двокубітні ворота стає важко створити. У лінійному оптичних квантових обчислень, ефективна сильна взаємодія створюється а поєднання

однофотонних операцій та вимірювань, які можуть бути використаним для реалізації двокубітного затвора. Другий підхід, який використовує оптично активні дефекти та квантові точки, які сильно взаємодіють фотони для індукції сильної ефективної взаємодії між фотонами, щодо оптично керованих напівпровідникових кубітів.

У фотонних квантових обчисленнях, як правило, кубіти індивідуальні фотони, з двома різними поляризаціями фотонів (вгору-вниз і ліворуч), що виконують роль двох кубітових станів. Однокубітні ворота можуть бути реалізовані зі стандартними пасивними оптичними компонентами, що використовуються для обертання поляризації, але двокубітні ворота вимагають нелінійності з низькими втратами, що є важко досягти. Як описано в розділі "захоплені іони", створюються випадкові вимірювання на двох вихідних портах роздільника променя сильна ефективна нелінійність і реалізація двокубітових воріт, але ворота імовірнісні. На щастя, ворота сигналізують про успіх (фотони виявляються на обох детекторах), що означає, що алгоритми можуть бути реалізовані, але вимоги до часу є складними, і а необхідне постійне джерело відповідних ініціалізованих фотонів. Останнім часом, квантові обчислювальні схеми на основі вимірювань, в яких дуже переплутаний "стан кластера" будується перед початком обчислень а саме обчислення здійснюється шляхом проведення вимірювань, викликали значний інтерес.

Багато технічних розробок, необхідних для реалізації фотонного квантові обчислення були досягнуті за останні кілька років. Фотонні чіпи продовжують вдосконалюватися, і рівень втрати фотонів як усередині фотонні елементи та інтерфейси наближаються до необхідних значень мати можливість реалізувати квантову корекцію помилок. Дуже висока ефективність були розроблені фотонні детектори, які є ключовими для

здійснення корекції помилок. Ці детектори на основі нанопроволок працюють на температури гелію (близько 4 K), тому охолодження до цієї температури буде потрібно, але, як було описано раніше, таке охолодження, як очікується, буде цілком можливо. Припускаючи постійний прогрес у зменшенні рівня втрат фотонів, Основна перешкода на шляху виготовлення пристроїв помірних розмірів - розробити джерело, яке з високою швидкістю генерує триплети заплутаних фотонів. Джерела триплетів переплутаних фотонів існують, але швидкість становить які генеруються сплутані фотонні триплети, потрібно збільшити по суті для цієї стратегії, щоб забезпечити широкомасштабні обчислення. Щодо 2018 рік був найбільшою заплутаною і повністю пов'язаною системою кубітів продемонстровано з використанням трьох ступенів свободи на кожному з шести фотонів, хоча цей метод стикається зі своїми проблемами і навряд чи буде масштабним.

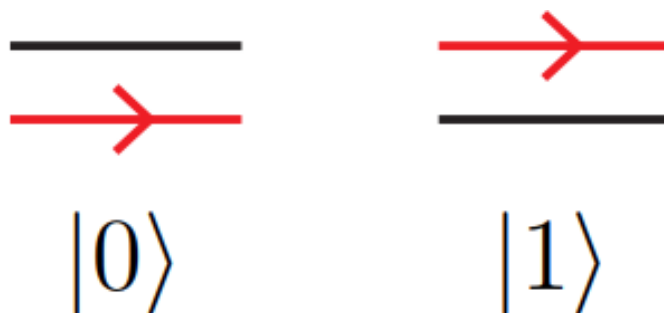
Максимальна масштабованість: оскільки фотони використовуються у фотонному кванті обчислювальні машини зазвичай мають довжини хвиль, які становлять близько мікрона, і оскільки фотони рухаються зі швидкістю світла і, як правило, направляються вздовж одного виміру оптичного чіпа, кількість фотонів і отже, кількість кубітів у фотонному пристрої не може бути такою великою як у системах з кубітами, які можна локалізувати у просторі. Однак масиви з багатотисячними кубітами, як очікується, буде можливим. Крім того, технологія буде вирішальною для розвитку комутаційних мереж що дозволить квантовий зв'язок у великих масштабах.

Існують різні властивості фотонів, які дозволяють їм бути використовуватись як кубіти. Серед основних - рух по прямій, вони рухаються з постійною швидкістю в даному середовищі та їх поляризацією, тобто полем вібрації електричного поля. Використовуючи

ці властивості ми можемо побудувати два основних типи фотонних кубітів:

1) Двоканальні кубіти. (dual-rail qubits)

Фотони рухаються по прямій. Отже, якщо обрано два шляхи руху і покладено фотон на будь-який з них, залежно від того, на якому шляху



виявлений фотон, ми можемо сказати стосовно квантового стану фотону $|0\rangle$ або $|1\rangle$ відповідно. На рис. 3 зображено двоканальний кубіт.

Рисунок 1.4 - Двоканальний фотонний кубіт. В залежності від того в якому каналі знаходиться фотон, стан кубіту є $|0\rangle$ або $|1\rangle$

2) Поляризаційний кубіт.

Виходить, що площина вібрації електричного поля може бути під будь-яким кутом, незалежним від напрямку поширення світла (якщо воно перпендикулярне напрямку розповсюдження у 3 вимірах). Отже, електричне поле може приймати будь-який напрямок у двовимірному просторі. Цей двовимірний простір може бути представлений основою, що складається з горизонтальної поляризації, $|H\rangle$ та вертикальної поляризації, $|V\rangle$. Тоді будь-який інший напрямок можна записати як суперпозицію цих двох.

Квантова декогерентність

Здається, що квантові обчислення з кожним днем стають дедалі

прогресивнішими. Кубіти стають чистішими, ворота покращуються, а алгоритми ускладнюються. Очевидно, лише питання часу, коли квантові обчислення стануть основною технологією. Однак залишається велика перешкода, яка потребуватиме величезних зусиль для подолання: декогерентність.

Квантові комп'ютери обіцяють експоненціальне прискорення у вирішенні певних типів задач за допомогою квантових принципів, таких як суперпозиція та переплутування, але використання квантових станів також робить квантовий комп'ютер набагато вразливішим до помилок, ніж класичний комп'ютер. Ці помилки виникають внаслідок декогеренції - процесу, в якому середовище взаємодіє з кубітами, неконтрольовано змінюючи їх квантові стани і спричиняючи втрату інформації, що зберігається квантовим комп'ютером.

Декогерентність може виникати в багатьох аспектах навколишнього середовища: зміна магнітного та електричного полів, випромінювання теплих предметів поблизу або перехресні взаємодії між кубітами. Квантові вчені вирішили для них роботу з боротьби з усіма цими потенційними джерелами декогеренції.

Ще одне застосування квантової механіки таке, що експлуатує, а не нарікає на надзвичайну чутливість квантового стану до навколишнього середовища. Це поле квантових вимірювань.

Метою квантових вимірювань є використання накладених та заплутаних станів, які набагато чутливіші до навколишнього середовища, ніж звичайні класичні стани. Вища чутливість цих станів дозволяє нам виміряти довкілля точніше, ніж ми могли б.

Ось як це працює. Принцип невизначеності Гейзенберга говорить, що якщо ми дуже точно вимірюємо один аспект системи, наприклад, позицію об'єкта, то мивтрачаємо інформацію про інший аспект системи,

наприклад, як швидко об'єкт рухається. У регулярному класичному стані, який не поводить квантово механічно, невизначеність положення та імпульсу є фіксованими значеннями. Але якщо ми маємо квантовий контроль над станом, ми можемо зігнути правила на свою користь.

Квантовий процес зменшення невизначеності в одному напрямку також влучно називають стисканням.

Квантова корекція помилок

Протоколи квантової корекції помилок відіграють центральну роль у реалізації квантових обчислень; вибір коду виправлення помилок вплине на весь стек квантових обчислень, починаючи з макета кубітів на фізичному рівні для створення стратегій компіляції на програмному рівні. Як такий, знайомство з квантовим кодуванням є важливою передумовою розуміння поточної та майбутньої архітектур квантових обчислень.

Замість бітів у традиційних комп'ютерах квантові комп'ютери працюють, керуючи та маніпулюючи квантовими бітами (кубітами). Через точний контроль квантових явищ, таких як переплутування, в принципі можливо, щоб такі пристрої на основі кубітів перевершили свої класичні аналоги. З цією метою були розроблені ефективні алгоритми квантових обчислень додатки, такі як цілочисельна факторизація, пошук, оптимізація та квантова хімія.

В даний час не існує кращої технології кубіта; досліджуються різноманітні фізичні системи для використання в якості кубітів, включаючи фотони, захоплені іони, надпровідні ланцюги та спіни в напівпровідниках. Недоліком усіх цих підходів є те, що він є важко достатньо ізолювати кубіти від впливу зовнішніх шумів, що означає помилки під час квантового обчислення неминучі. На відміну від цього, біти в класичному комп'ютері зазвичай реалізуються як надійні стани ввімкнення / вимкнення транзисторних перемикачів, які диференціюються на мільярди електронів. Це забезпечує класичні біти з великими межами помилок, які майже викорінюють фізичні помилки рівень. Для квантових комп'ютерів, де кубіти реалізуються як крихкі квантові системи, цього немає такий захист від помилок. Як такий, будь-яка квантова модель комп'ютерної моделі на основі струму і майбутні

кубітові технології вимагатимуть певного виду активної корекції помилок.

Керуючись вимогами високопродуктивних мереж зв'язку та Інтернету, єдобре розроблена теорія класичного виправлення помилок. Однак адаптація існуючої класичної Методи квантової корекції помилок не є простими. Кубіти підлягають забороні клонування теорема, що означає квантову інформацію, не можна дублювати так само, як класичну інформацію. Крім того, неможливо проводити довільні вимірювання на кубітному регістрі через проблему колапсу хвильової функції. Спочатку побоювалися, що ці обмеження будуть створюють непереборний виклик життєздатності квантових обчислень. Однак прориву було досягнуто в 1995 році Пітером Шором, в якому пропонується перша квантова корекція помилок схеми. Метод Шора продемонстрував, як квантову інформацію можна надмірно кодувати заплутавши його через розширену систему кубітів. Подальші результати тоді це продемонстрували розширення цієї методики в принципі можуть бути використані для довільного придушення квантової помилки норми, за умови дотримання певних фізичних умов на самих кубітах. Це було с ці розробки в квантовій корекції помилок, з яких перейшло поле квантових обчислень теоретична цікавість до практичної можливості.

Від класичної до квантової корекції помилок

Основним принципом виправлення помилок в класичних обчисленнях, в яких дані представлені у вигляді послідовностей бітів є те, що збільшується кількість бітів, що використовуються для кодування заданого обсягу інформації. Точний спосіб це надлишкове кодування досягається, визначається набором інструкцій, відомим як виправлення помилок код.

Наприклад, припустимо, ми хочемо передати біт з одного місця в інше через шумний класичний канал зв'язку. Ефект шуму в каналі полягає в перевертанні біт, що передається з імовірністю $p > 0$, тоді як з імовірністю $1 - p$ біт передається безпомилко. Такий канал відомий як двійковий симетричний канал, і показаний на рис. 1.5. Простий засіб захисту від впливу шуму у двійковому симетричному каналі має замінити біт, який ми хочемо захистити, трьома копіями себе.

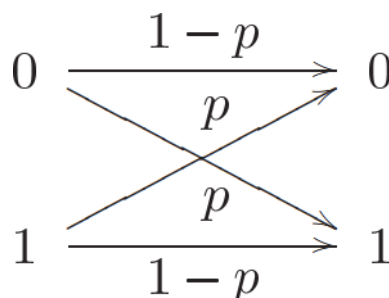


Рисунок 1.5 - Бінарний симетричний канал

Такий спосіб виправлення помилок є трибітний код повторення, шифратор що дублює кожне бітове значення $0 \rightarrow 000$ та $1 \rightarrow 111$. Більш формально ми можемо визначити три біти шифратор як відображення від «необробленого» двійкового алфавіту β до кодового алфавіту C_3 :

$$\beta = \{0, 1\} \rightarrow C_3 = \{000, 111\}$$

де закодовані бітові рядки «000» та «111» називаються логічними кодовими словами коду C_3 . Як приклад, розглянемо простий випадок, коли ми хочемо передати однібітове повідомлення «0» одержувачу в іншому місці. Використовуючи трибітове кодування, повідомлення, яке ми хотіли б відправити буде кодовим словом «000».

А тепер уявимо, що повідомлення під час передачі спричиняє одну помилку відхилення біта бітовий рядок, який отримує одержувач, -

«010». У цьому випадку одержувач зможе зробити висновок про це передбачене кодове слово - «000» за допомогою більшості голосів. Те саме буде справедливим для всіх випадків, коли кодове слово зазнає лише однієї помилки. Однак, якщо кодове слово зазнає двох помилок фліп-фліпу, більшість голосів призведе до неправильного кодового слова. Остаточний сценарій, який слід врахувати, - це коли всі три біти перевертаються так, що кодове слово «000» стає «111». У цьому випадку повідомлення пошкоджене також є кодовим словом: одержувач, таким чином, не зможе дізнатися, що сталася помилка. Відстань коду визначається як мінімальна кількість помилок, які змінять одне кодове слово на інший таким чином. Ми можемо пов'язати відстань d коду з кількістю помилок, які він може виправити наступним чином:

$$d = 2t + 1,$$

де t - кількість помилок, які може виправити код. Зрозуміло, що наведене вище рівняння виконується для трибітового коду, де $t = 1$ і $d = 3$.

Загалом коди виправлення помилок описуються в термінах позначення $[n, k, d]$, де n – це загальна кількість бітів на кодове слово, k - кількість закодованих бітів (довжина оригіналу біт-рядок), а d - відстань коду. Під цим позначенням трибітний код повторення позначений $[3, 1, 3]$.

Таким чином, для захисту квантових станів від впливу шуму ми хотіли б розробити квантові коди для виправлення помилок, засновані на подібних принципах. Існують деякі важливі відмінності між класичною інформацією та квантовою інформацією, що вимагає нових ідей бути введеними, щоб зробити можливими такі квантові коди, що виправляють помилки. Зокрема, на перший погляд, у нас є три досить суттєві труднощі:

- Немає клонування: можна спробувати реалізувати код повторення

квантово механічно шляхом дублювання квантового стану три або більше разів. Це заборонено Теорема про відсутність клонування. Навіть якщо клонування була можливо, неможливо було б виміряти і порівняти три квантові стани вихід з каналу.

- Помилки постійні: на одному кубіті може виникати континуум різних помилок. Визначення помилки, яка сталася для того, щоб її виправити, здається, вимагає нескінченна точність, а отже і нескінченні ресурси.
- Вимірювання руйнує квантову інформацію: при класичній корекції помилок ми спостерігаємо за виходом з каналу та вирішити, яку процедуру декодування прийняти. Спостереження в квантовій механіці зазвичай руйнує квантовий стан при спостереження, і робить процес відтворення неможливим.

На щастя, жодна з цих проблем не є фатальною, як ми продемонструємо. Припустимо, ми відправляємо кубіти через канал, який залишає кубіти недоторканими з імовірністю $1 - p$, і перевертає кубіти з ймовірністю p . Тобто, з імовірністю p приймається стан $|\psi\rangle$ стан $X|\psi\rangle$, де X - звичайний оператор сигма x Паулі або оператор фліп-біту. Це Канал називається бітовим фліп-каналом, і тепер ми пояснимо код фліп-біту, який може використовувати для захисту кубітів від впливу шуму від цього каналу.

Припустимо, ми кодуємо єдиний кубітовий стан $\alpha|0\rangle + \beta|1\rangle$ в три кубіти наступним чином $\alpha|000\rangle + \beta|111\rangle$. Зручний шлях запису цього шифрування є наступним:

$$|0\rangle \rightarrow |0_L\rangle \equiv |000\rangle$$

$$|1\rangle \rightarrow |1_L\rangle \equiv |111\rangle$$

де розуміється, що суперпозиції базових станів беруться за відповідні суперпозиції закодованих станів. Позначення $|0_L\rangle$ та $|1_L\rangle$ вказують на те, що це логічний $|0\rangle$ та логічний $|1\rangle$ стани, а не фізичний нуль та один стан. Схема виконання цього кодування показано на рис. 1.6.

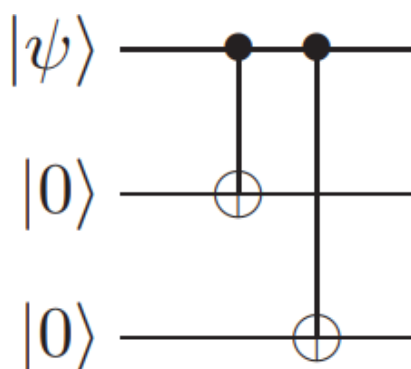


Рисунок 1.6. - Схема кодування для трикубітного бітового фліп-коду. Дані, що кодуються, надходять у схему на верхню лінію

Принцип побудови дискретних автоматів на управляючих переходах квантової системи

Як відомо, розвиток обчислювальної техніки в деяких перспективних напрямках передбачає використання керованих колективних процесів квантової природи. Вимога подальшого підвищення швидкодії, надійності та ступеня інтеграції кібернетичних пристроїв призводить до необхідності синтезу автоматів на основі квантових процесів.

Розглянемо можливість побудови групових автоматів на квантових переходах. Функціонування квантових дискретних автоматів (КДА) $H = (A, S, B, \alpha, \beta)$ засноване на використанні керованих автоморфних перетвореннях дискретних множин станів квантових систем. Для цього простір станів квантової динамічної системи з керованими переходами

поділяється на комірки, що попарно перетинаються та містять у собі вектори базисних станів $|\psi\rangle \in S$, відповідні вершинам заданого автоматного графа Γ . Множина управляючих впливів на систему викликає квантові переходи між базисними станами, утворюючи вхідний алфавіт A , а множина макроскопічних станів підсистеми виведення інформації - вихідний алфавіт B . Функціонування КДА визначають дві основні операції: операція переходу між станами $\alpha: S \times A \rightarrow S$; та операція виведення інформації $\beta: S \times A \rightarrow B$. Операції введення інформації, виведення інформації та управління станами повинні розглядатися як взаємодія квантових та макроскопічних процесів. У складних КДА окремі підсистеми можуть взаємодіяти безпосередньо на квантовому рівні.

При такому підході, оскільки йдеться про елементарні квантомеханічні процеси, істотну роль відіграють не тільки випадкові явища, характерні для ймовірнісних автоматів взагалі, а й специфічні для квантової механіки ефекти суперпозиції когерентних хвильових функцій. Необхідно мати на увазі фазові співвідношення між комплексними амплітудами ймовірностей станів і принцип невизначеності Гейзенберга. Тому доцільно обговорити питання про фізичну здійсненність дискретного автомата на квантових переходах і принципову можливість реалізації на його основі детермінованих або майже детермінованих операцій. Конкретна фізична природа робочої речовини, що використовується для побудови КДА, та його просторова конфігурація не суттєві для виявлення принципової сторони питання. У той же час, операторна структура моделей, що описують еволюцію станів, має вирішальне значення в сенсі керованості та спостережуваності КДА.

Мета управління квантовими процесами в КДА зводиться до здійснення заданого автоморфізму α дискретного підмножини S простору квантових станів, а також реалізації необхідної функції β виведення

інформації з мікрорівня на макрорівень. Управління здійснюється з допомогою макроскопічного впливу на гамільтоніан мікросистеми.

Вказаним вимогам відповідає наступний гамільтоніан мікросистеми:

$$H = H_0 + \sum_{\mu=1} u_{\mu}^a(t) H_{\mu} + V(t, q^f),$$

Де H_0 - гамільтоніан, u_{μ}^a - вхідні керуючі впливу макрополя, H_{μ} - оператори мікросистеми,

$V(t, q^f)$ - потенціал збурень, що діє на мікросистему з боку макросистеми з координатами $q^f(t)$ на етапі виведення інформації.

Функції $u_{\mu}^a(t)$ та $q^f(t)$ повинні розглядатись як літери алфавітів А і В відповідно. Потенціал взаємодії на етапі перетворення внутрішнього стану КДА рахується «вимкнутим»: $V(t, q^f) = 0$ ($t_0 < t < t_1$). Тоді визначене на вказаному інтервалі часу перетворення одного стану $|\psi_{S_0} >$ в інший $|\psi_{S_1} >$ ($S_0, S_1 \in S$) можливо представити в вигляді:

$$|\psi_{S_1} = U_a(t_1, t_0) |\psi_{S_0} >,$$

Де $U_a(t_1, t_0)$ - оператор еволюції квантової системи, задовольняючий рівнянню Шредингера

$$i\hbar U_a = [H_0 + \sum_{\mu=1}^m u_{\mu}^a(t) H_{\mu}] U_a,$$

І початковій умові $U(t_0, t_0) = I$, (I – одиничний оператор).

Якщо квантова система з кінцевим дискретним спектром керована в цілому, функції $u_{\mu}^a(t)$ можна вибрати такими, щоб перетворити в себе деяку кінцеву множину S , і тоді дана система стає дискретним автоматом.

Питання повноти системи таких різноманітних перетворень тісно пов'язані з проблемою керованості динамічних систем на групах Лі. За наявності керованості, використовуючи структурні властивості автоматів, визначених групах, можна побудувати заданий граф переходів Γ і здійснити абстрактний синтез КДА по заданій функції перетворення α . Граф групового автомата є групою, що зображує деякі підгрупи симетричної групи S_n , тобто групи всіх перестановок та символів.

У разі нескінченного спектру керованість в цілому має місце не завжди, однак і в цьому випадку може існувати дискретна підгрупа керованості кінцевої розмірності, що достатньо умовою для реалізації довільного кінцевого графа Γ . Кодуючи керуючі впливи літерами вхідного алфавіту $a \in A$ і встановлюючи відповідність між станом мікросистеми та станом $b \in B$ підсистеми виведення, отримуємо реалізацію перехідної та вихідної функцій α та β .

Для опису еволюції координат $q^f(t)$ підсистеми виводу слід використовувати класичні рівняння

$$p^f = -\frac{\partial H^f}{\partial q^f}, \quad q^f = -\frac{\partial H^f}{\partial p^f}$$

З гамільтоніаном

$$H^f(p^f, q^f) = H_0^f(p^f, q^f) + \langle \psi_a | V(t, q^f) | \psi_a \rangle$$

в якому потенціал взаємодії усереднений за допомогою хвильової функції $|\psi_a\rangle$ стану мікросистеми. Підсистеми мікрорівнів і макрорівнів КДА виявляються взаємопов'язаними, якщо $V(t, q^f) \neq 0$. Для того, що би макросистема була чутлива до стану мікросистеми, вона повинна

перебувати в метастабільному стані, що визначається видом незбудженого гамільтоніана H_0^f .

Зменшення небажаного впливу теплових флуктуацій досягається охолодженням КДА до температур, близьких до абсолютного нуля. Релаксаційні процеси видаються корисними як відновлення початкового стану автомата, так і для стабілізації базисних станів за умов параметричного збудження.

Цикл роботи автомата складається з наступних етапів:

- 1) релаксація до вихідного (основного) стану КДА при вимкненій підсистемі виведення та відсутності управління;
- 2) послідовне керування з метою перевodu автомата в заданий початковий стан (введення початкових даних);
- 3) перетворення станів автомата відповідно до заданого графа переходів шляхом послідовності входніх управляючих впливів;
- 4) включення підсистеми введення та зчитування кінцевого стану (переведення інформації з мікрорівень на макрорівень).

На останньому етапі принциповим є питання про вплив макросистеми на мікростан в процесі вимірювання результату обчислень. Детально цей процес описується у наведеній вище моделі і може бути оптимізований згідно з критеріями мінімуму вирогідності помилки.

Відповідно до принципу Гейзенберга, мінімальний час зчитування Δt і різниця енергетичних рівнів вихідного пристрою ΔE пов'язані співвідношенням невизначеності.

Вводячи дискретні відліки часу $t_m = m\Delta t$ враховуючи групові властивості оператора еволюції $U(t, t_1)$, при багатоетапному перетворенні $a_n, \dots, a_1$ отримуємо

$$U_{a_n, \dots, a_1}(t_n, t_1) = U_{a_n(t_n, t_{n-1})}, \dots, U_{a_m(t_m, t_{m-1})}, \dots, U_{a_1(t_1, t_0)}$$

Завдяки унітарності U_{am} , управління відбувається на сфері, що має силу ймовірнісного нормування $\langle \psi | \psi \rangle = 1$ одиничний радіус. Це дозволяє застосувати відомі методи дослідження керованості на групових різноманіттях і, зокрема, на сфері, засновані на теорії груп і алгебр Лі. Процеси управління квантової системою з цієї точки зору можуть розглядатися на групі Лі.

Істотно відзначити, що при реалізації заданого графа переходів недостатньо здійснити переклад лише одного стану в інше. Необхідно одним і тим же керуючим впливом перевести цілу сукупність станів в іншу наперед задану сукупність.

Використання тут чистих станів $|\psi\rangle$ не є єдиною можливістю для опису функціонування КДА. Управління змішаними станами, заданими оператором щільності ρ , також можна описати за допомогою керованого оператора еволюції U . При цьому стає можливим оцінювати надійність роботи КДА.

Проблема ідентифікації кінцевих станів у КДА пов'язана з впливом макросистеми на мікростан у процесі вимірювання. Для того, щоб мінімізувати помилку вимірювання, в залежності від цілей управління можна ставити завдання про знаходження станів квантової системи, що забезпечують мінімум невизначеності (мінімальну дисперсію) або максимум ймовірності певного результату вимірювання. У першому випадку можуть бути використані когерентні стани, які реалізують знак рівності у співвідношенні невизначеності, у другому – отримані стани, з максимальною ймовірністю дії в Гейзенбергівському осередку. Переважність кожного із них залежить від способу оцінювання помилки у вимірюваннях. Разом тим, як у першому, так і в другому випадку процес

вимірювання повинен бути поставлений так, щоб взаємодія мікрооб'єкта з вимірювальним приладом була належним чином підготовлена.

Розглянемо квантову систему, наприклад, в (p, q) просторі з l ступенями свободи, що знаходиться в деякому стані $|\psi\rangle$, що описується хвильовою функцією, фінітною в імпульсному уявленні. Припустимо, що координати $\{q_n\}$ утворюють повний набір комутуючих спостерігачів та мають суцільний спектр власних значень.

Відомо, що математичне очікування результату вимірювання дорівнює ймовірності знаходження величини a належній до A в інтервалі Δ . Для визначення процесу вимірювання достатньо A представити через проекційний оператор $\Pi(\Delta) = \int_{\Delta} |a\rangle\langle a| da$, де Δ - набір власних значень a оператора A . Проекційний оператор має лише два власні значення 1 і 0. В результаті вимірювання ми отримаємо 1 або 0 в залежності від того, чи лежить значення a в інтервалі A чи ні. Завдання полягає у максимізації функціоналу

$$\langle \psi | \Pi(R) | \psi \rangle = \int_R \prod_{j=1}^l dq_j |\{q_n\} \psi|^2,$$

При додатковій умові

$$\langle \psi | \Pi(D) | \psi \rangle = \int_D \prod_{j=1}^l dp_j |\{p_n\} \psi|^2 = 1,$$

де $\langle \{q_n\} \psi \rangle$, - функція імпульсного уявлення вектора стану $|\psi\rangle$, системи. Область інтегрування (R, D) виберемо таким чином, щоб обсяг фазового осередку дорівнював $(h/2)^{2l}$, при цьому

$$R = \left\{ q : (2n_i - 1)\varepsilon \frac{a}{2} \leq q_i \leq (2n_i + 1)\varepsilon \frac{a}{2} \right\},$$

$$D = \left\{ p : (2m_i - 1) \frac{\hbar}{4a} \leq p_i \leq (2m_i + 1) \frac{\hbar}{4a} \right\}.$$

Для багатовимірного випадку необхідно використовувати гіперсфероїдальні функції. У будь-якому осередку фазового простору отримуємо хвильову функцію, що відрізняється від хвильової функції центрального осередку фазовим множником. Утворена таким чином система функцій вибирається за базис. Коефіцієнти розкладання довільної функції в цьому базисі дають амплітуди ймовірності знаходження системи в тому чи іншому осередку.

Отже, якщо припустити, що система квантова керована, то в результаті процесу управління простір початкових станів перетворюється на простір кінцевих станів. Якщо врахувати, що при «вимірюванні» використовувалися проекційні оператори, то можна говорити про майже детермінований вимір результату обчислення автомату.

Висновки до I розділу

В першому розділі ми розглянули та описали базові поняття квантової системи, якими будемо надалі оперувати для пояснення алгоритмів у другому розділі. Переконалися що квантова декогерентність є однією з головних перешкод перед сучасними квантовими обчисленнями. Розглянули побудову кубіта та частинки що можуть виступати в ролі кубітів, а також позначили основні складнощі у роботі з кубітами такі як: відсутність клонування, постійність помилок постійні, руйнування інформації при вимірюванні.

У другій частині першого розділу було доведено, що на управляючих переходах квантової системи можна побудувати детермінований автомат. Розглянуто принципи побудови та цикл роботи такого автомата.

РОЗДІЛ 2. АНАЛІЗ КВАНТОВИХ АЛГОРИТМІВ ТА ПОТЕНЦІАЛЬНА КОРИСТЬ В СФЕРІ РОЗВ'ЯЗКУ ЗАДАЧ КОМБІНАТОРИКИ.

Загальний вступ до квантових алгоритмів

Алгоритм Дойча–Йожі припускає, що квантові комп'ютери будуть здатні вирішувати деякі обчислювальні задачі набагато ефективніше, ніж класичні комп'ютери. На жаль, проблема, яку він вирішує, не представляє практичного інтересу. Чи є цікавіші задачі, вирішення яких можна отримати більш ефективно за допомогою квантових алгоритмів? Які принципи лежать в основі таких алгоритмів? Які кінцеві межі в потужності обчислення у квантових комп'ютерів?

Загалом, існує три класи квантових алгоритмів, які забезпечують перевагу перед відомими класичними алгоритмами. По-перше, це клас алгоритмів на основі на квантових версіях перетворення Фур'є, інструмент, який також широко використовується в класичних алгоритмах. Прикладом цього типу алгоритму є алгоритм Дойча–Йожі, як і алгоритм Шора для розкладання на множники та дискретного логарифма. Другий клас алгоритмів – це алгоритми квантового пошуку. Третій клас алгоритмів – квантова симуляція, при якому квантовий комп'ютер використовується для моделювання квантової системи. Зараз я хочу навести короткий опис кожного із цих класів алгоритмів, а потім узагальнити те, що наразі відомо про обчислювальну потужність квантових комп'ютерів.

Квантові алгоритми на основі перетворення Фур'є

Дискретне перетворення Фур'є зазвичай описується як перетворення множини $x_0, \dots, x_{N-1}$ N комплексних чисел у множину комплексних чисел $y_0, \dots, y_{N-1}$, визначених як

$$y_k \equiv \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{2\pi i j k / N} x_j .$$

Звичайно, це перетворення має величезну кількість застосувань у багатьох галузях науки. Загальна теорія перетворення Фур'є включає деякі технічні ідеї з теорії характерів кінцевих груп, але ми не будемо зупинятися на ній більш детально і описувати це тут. Важливо те, що перетворення Адамара, що використовується в алгоритмі Дойча–Йожі, є прикладом цього узагальненого класу перетворень Фур'є. Крім того, багато інших важливих квантових алгоритмів також включають певний тип перетворення Фур'є.

Найважливіші відомі квантові алгоритми — швидкі алгоритми Шора для розкладання на множники та дискретний логарифм — це два приклади алгоритмів, заснованих на перетворенні Фур'є. Попереднє рівняння не виглядає дуже квантово-механічним у тому вигляді, який я навів. Проте уявіть собі, що ми визначаємо лінійне перетворення U на n кубітів шляхом його дії на обчислювальні базисні стани $|j\rangle$, де $0 \leq j \leq 2^n - 1$

$$|j\rangle \longrightarrow \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi i j k / 2^n} |k\rangle .$$

Можемо перевірити, що це перетворення є унітарним, що і насправді його можна реалізувати як квантовий контур. Більше того, якщо записати його дію на суперпозицію,

$$\sum_{j=0}^{2^n-1} x_j |j\rangle \longrightarrow \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} \left[\sum_{j=0}^{2^n-1} e^{2\pi i j k / 2^n} x_j \right] |k\rangle = \sum_{k=0}^{2^n-1} y_k |k\rangle ,$$

ми побачимо, що він відповідає векторному позначенню для перетворення Фур'є для випадку $N = 2^n$. Як швидко ми можемо виконати перетворення Фур'є? Класичне швидке перетворення Фур'є займає приблизно $N \log(N) = n2^n$ кроків для того щоб перетворити $N = 2^n$ чисел. На квантовому комп'ютері перетворення Фур'є можна виконати використовуючи $\log^2(N) = 2^n$ кроків, тобто це експоненціальна економія!

Цей результат, здається, свідчить про те, що квантові комп'ютери можна використовувати дуже швидко для обчислень перетворення Фур'є для векторів з 2^n комплексних чисел, і це було б фантастично корисно у широкому діапазоні застосувань. Однак це не зовсім так, оскільки перетворення Фур'є виконується над інформацією, «прихованою» в амплітудах квантового стану. Ця інформація не доступна безпосередньо для вимірювання. Проблема, звичайно, полягає в тому, що якщо виміряти вихідний стан, кожен кубіт буде згорнуто до стану $|0\rangle$ або $|1\rangle$, що заважає нам безпосередньо дізнатися результат перетворення у. Цей приклад говорить про суть загадки розробки квантового алгоритму. З одного боку, ми можемо виконати певні обчислення для 2^n амплітуд, пов'язаних з n кубітами набагато ефективніше, ніж це було б можливо на класичному комп'ютері. Але з іншого боку, результати такого розрахунку нам недоступні, якщо ми будемо дивитися на це прямолінійно, як на класичні алгоритми. Потрібна більша кмітливість, щоб бути в змозі використовувати силу квантових обчислень.

На щастя, виявляється можливим використати квантове перетворення Фур'є для того щоб ефективно розв'язати кілька проблем, які, як вважають, не мають ефективного рішення на класичному комп'ютері. Ці проблеми

включають задачу Дойча та алгоритми Шора для дискретних логарифмів і розкладання чисел на множники. Цей напрямок думок увінчався відкриттям Китаєва методу вирішення «Проблеми Абелевого стабілізатора» та узагальненням до проблеми прихованої підгрупи:

Нехай f — функція від скінченно породженої групи G до скінченної множини X така, що f є постійною на східних класах підгрупи K і унікальною на кожному класі. Маємо квантовий чорний ящик для виконання унітарного перетворення $U|g|h = |g|h \oplus f(g)$, для $g \in G$, $h \in X$ і $\oplus$ належним чином вибрана бінарна операції над X . Потрібно знайти генераторний клас для K .

Алгоритм Дойча–Йожі, алгоритми Шора та пов’язані з ними «експоненціально швидкі» квантові алгоритми можна розглядати як окремі випадки цього алгоритму.

Алгоритми квантового пошуку

Зовсім інший клас алгоритмів представлений алгоритмом квантового пошуку, чийі основні принципи були відкриті Гровером. Алгоритм квантового пошуку вирішує наступну проблему: заданий простір пошуку розміром N і відсутність попередніх знань про структурі інформації в ньому, тобто наприклад невпорядкований вектор елементів, ми хочемо знайти елемент цього простору пошуку, що задовольняє деякій відомій нам властивості. Скільки часу потрібно, щоб знайти елемент, що задовольняє цій властивості? У класичному варіанті ця задача вимагає приблизно N операцій, але для квантового пошуку алгоритм дозволяє вирішити проблему за допомогою приблизно $\sqrt{N}$ операцій.

Алгоритм квантового пошуку пропонує лише квадратичне прискорення, на відміну від більш вражаючого експоненціального прискорення, яке пропонують алгоритми, засновані на квантовому

перетворенні Фур'є. Однак алгоритм квантового пошуку все ще представляє великий інтерес, оскільки пошукова евристика має ширший діапазон застосування, ніж задачі, що вирішуються за допомогою квантового перетворення Фур'є, і адаптації алгоритму квантового пошуку можуть мати корисне рішення для дуже широкого кола практичних проблем.

Квантова симуляція

Моделювання природних квантово-механічних систем є очевидним кандидатом для завдань, в якому квантові комп'ютери можуть досягти успіху, але яке вважається непомірно складним на класичному комп'ютері. Класичні комп'ютери мають труднощі з моделюванням загальної квантової системи майже з тих самих причин, з яких їм важко моделювати квантові комп'ютери – кількість комплексних чисел, необхідних для опису квантової системи, як правило, зростає експоненціально з розміром системи, а не лінійно, як це відбувається в класичних системах. Загалом, зберігання квантового стану системи з n різних компонентів займає щось на кшталт c^n бітів пам'яті на класичному комп'ютері, де c є константою, що залежить від деталей системи, що моделюється, і бажаної точності моделювання.

І навпаки, квантовий комп'ютер може виконувати моделювання з використанням kn кубітів, де k знову є константою, яка залежить від кількості деталей системи, що моделюється. Це дозволяє квантовим комп'ютерам ефективно виконувати моделювання квантової механіки системи, які, як вважають, не можна ефективно моделювати на класичному комп'ютері. Важливим застереженням є те, що навіть попри те, що квантовий комп'ютер може моделювати набагато більше квантові системи набагато ефективніше класичного комп'ютера, це не означає, що швидке моделювання дозволить отримати потрібну інформацію про квантову систему.

Під час вимірювання симуляція кубіта kn згорнеться у певний стан, даючи лише kn фрагментів інформації; c^n бітів «прихованої інформації» у хвильовій функції буде не зовсім доступно. Таким чином, вирішальним кроком у тому, щоб зробити квантове моделювання корисним, є розробка систематичних засобів, за допомогою яких можна ефективно отримувати бажані відповіді; але як це зробити, наразі зрозуміло лише частково.

Незважаючи на ці застереження, квантове моделювання, ймовірно, буде важливим додатком до квантових комп'ютерів. Моделювання квантових систем є важливою проблемою в багатьох областях, зокрема квантової хімії, де накладаються обчислювальні обмеження на класичні комп'ютери, оскільки процес ускладнює необхідність точного моделювання поведінки навіть помірних молекул, а тим паче дуже великих молекул, які зустрічаються в багатьох важливих біологічних системах. Отримання швидшого та точнішого моделювання таких систем може мати бажаний ефект, що дозволить досягти прогресу в інших областях, в яких квантові явища також важливі.

Все ж таки у майбутньому ми можемо виявити в природі фізичні явища, які не зможуть бути ефективно змодельовані на квантовому комп'ютері. Але це було б далеко не поганою новиною. Принаймні, це буде стимулювати людство до розширення існуючих моделей обчислень для того, щоб охопити нове явище та збільшити потужність наших обчислювальних моделей за межі існуючої моделі квантових обчислень.

Іншим застосуванням квантового моделювання є загальний метод отримання уявлень про інші квантові алгоритми. Наприклад, як квантовий алгоритм пошуку можна розглядати як рішення задачі квантової симуляції. Підходячи до проблеми таким чином, стає набагато легше зрозуміти походження алгоритмів квантового пошуку.

Нарешті, квантова симуляція також породжує цікавий і оптимістичний «квантовий наслідок» із закону Мура. Нагадаємо, що закон Мура стверджує, що сила обчислювальна класичних комп'ютерів подвоюватимуться раз на два роки або близько того, за постійну вартість. Однак припустимо, що ми моделюємо квантову систему на класичному комп'ютері і хочемо додати єдиний кубіт (або більшу систему) до системи, що моделюється. Це подвоює або, навіть, потроює вимоги до пам'яті, необхідні класичному комп'ютеру для зберігання описів стану квантової системи з аналогічною або більшою вартістю по часу, необхідного для динамічної симуляції такої системи. З цього спостереження випливає квантовий наслідок із закону Мура - що квантові комп'ютери йдуть в ногу з класичними комп'ютерами з різницею тільки в те, що один кубіт додається до квантового комп'ютера кожні два роки. Такий висновок не повинно сприймати занадто серйозно, оскільки хід квантових обчислень ще не досі до кінця зрозумілий. Тим не менш, це евристичне твердження допомагає повідомити людству, чому нам слід цікавитися квантовими комп'ютерами і сподіватися, що колись вони зможуть перевершити найпотужніші класичні комп'ютери, принаймні для деяких розрахунків.

Алгоритм Дойча та алгоритм Дойча – Йожі.

Алгоритм Дойча — це простий випадок більш загального квантового алгоритму, який ми і розглянемо і який має назву Дойча-Йожі. У додатку до цього розглянемо проблему Дойча, яку можна описати як наступну гру. Аліса, яка живе в місті А, вибирає деяке число x в межах від 0 до $2n - 1$, і надсилає його поштою в листі Білу, який живе в місті В. Білл обчислює деяку функцію $f(x)$ і відповідає з результатом, який дорівнює 0 або 1. Тепер Білл пообіцяв використати і надалі цю функцію f , яка є одного з двох видів: або $f(x)$ є постійним для всіх значень x , або $f(x)$ є збалансованим, тобто

дорівнює 1 рівно для половини всіх можливих x , і 0 для другої половини. Мета Аліси — з упевненістю визначити, чи використовує Білл постійну або збалансовану функція, при цьому надсилати листи Біллу Аліса повинна якомога менше. Як швидко вона зможе досягти успіху?

У класичному випадку (тобто при розв'язанні задачі за класичними алгоритмами) Аліса може надіслати Бобу лише одне значення x у кожній літері. У гіршому, Алісі потрібно буде запитати Боба принаймні $2^{n/2} + 1$ раз, оскільки вона може отримати $2^{n/2}$ нулів перед отриманням одиниці, що буду свідчити про те, що функція Білла збалансована. Найкращий детермінований (класичний) алгоритм, яка вона може використовувати, вимагає $2^{n/2} + 1$ запитів. Зверніть увагу, що в кожному листі Аліса надсилає Біллу n бітів інформації. Крім того, у цьому прикладі фізична відстань використовується для штучного підвищення вартості обчислення $f(x)$, але це не так в загальній задачі, на практиці, де $f(x)$ може бути просто функцією яку важко обчислити.

Якби Білл Аліса змогли обмінятися кубітами, а не просто класичними бітами, і якби Білл погодився обчислити $f(x)$ за допомогою унітарного перетворення U_f , тоді Аліса зможе досягти своєї мети лише за один лист до Білла, використовуючи наступний квантовий алгоритм.

Аналогічно алгоритму Дойча, Аліса має n регістр кубітів для зберігання її запиту, і єдиний кубітний регістр, який вона передасть Біллу для зберігання її відповіді. Аліса почине алгоритм з підготовки регістрів запитів і відповідей у стані суперпозиції. Після цього Білл оцінить $f(x)$ за допомогою квантового паралелізму і залишить результат у регістрі відповідей.

Потім Аліса зробить зміни в стани в суперпозиції за допомогою перетворення Адамара в реєстрі запита та заверше операцію виконанням контрольного вимірювання, яке визначає, чи функція $f(x)$ постійна або збалансована.

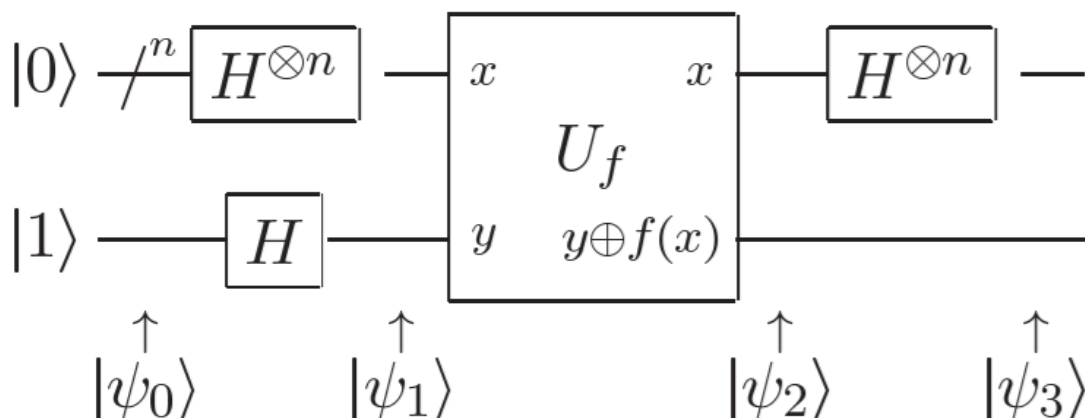


Рисунок 2.1 - Квантова схема алгоритму Дойча-Йожі

Конкретна діаграма алгоритму зображена на рисунку 2.1. Давайте відслідкуємо по крокам цей алгоритм. Вхідний стан:

$$|\psi_0\rangle = |0\rangle^{\otimes n} |1\rangle$$

Тут регістр запиту описує стан n кубітів які підготовлені в стані $|0\rangle$. Після перетворення Адамара над регістром запитів і застосування гейту Адамара над регістром відповідей, ми маємо:

$$|\psi_1\rangle = \sum_{x \in \{0,1\}^n} \frac{|x\rangle}{\sqrt{2^n}} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right].$$

Регістр запиту тепер є суперпозицією всіх значень, а регістр відповідей знаходиться в рівномірно зваженій суперпозиції 0 і 1. Далі, розраховуємо функцію $f(x)$ використовуючи $U_f : |x, y\rangle \rightarrow |x, y \oplus f(x)\rangle$

$$|\psi_2\rangle = \sum_x \frac{(-1)^{f(x)} |x\rangle}{\sqrt{2^n}} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right].$$

Тепер Аліса має набір кубітів, в яких зберігається результат оцінки функції Білла в амплітуді стану суперпозиції кубіта. Вона знов вносить

зміни до суперпозиції за допомогою перетворення Адамара в регістрі запитів. Для визначення результату перетворення Адамара спочатку потрібно обчислити ефект перетворення Адамара на стані $|x\rangle$. Перевіривши випадки $x = 0$ і $x = 1$ окремо, ми бачимо, що для кожного кубіту $H|x\rangle = \sum (-1)^{xz} |z\rangle / \sqrt{2}$. Таким чином

$$H^{\otimes n} |x_1, \dots, x_n\rangle = \frac{\sum_{z_1, \dots, z_n} (-1)^{x_1 z_1 + \dots + x_n z_n} |z_1, \dots, z_n\rangle}{\sqrt{2^n}}.$$

Це можна узагальнити більш коротко у наступному рівнянні

$$H^{\otimes n} |x\rangle = \frac{\sum_z (-1)^{x \cdot z} |z\rangle}{\sqrt{2^n}},$$

де $x \cdot z$ — порозрядний внутрішній добуток x і z за модулем 2. Використовуючи це рівняння

і рівняння $|\psi_2\rangle$ тепер ми можемо розрахувати $|\psi_3\rangle$:

$$|\psi_3\rangle = \sum_z \sum_x \frac{(-1)^{x \cdot z + f(x)} |z\rangle}{2^n} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right]$$

Тепер Аліса спостерігає за реєстром запитів. Зауважимо, що амплітуда для стану $|0^{\otimes n}\rangle$ дорівнює $H|x\rangle = \sum (-1)^{f(x)} |z\rangle / 2^n$. Давай розглянемо два можливі випадки — коли $f(x)$ постійна і $f(x)$ збалансована. У випадку, коли функція постійна, амплітуда для $|0^{\otimes n}\rangle$ дорівнює $+1$ або -1 , залежно від постійного значення функції. Оскільки $|\psi_3\rangle$ має одиничну довжину з цього випливає, що всі інші амплітуди повинні бути нульовими, і спостереження дасть 0 для всіх кубітів в реєстрі запитів. Якщо ж функція збалансована, то всі позитивні і негативні внески амплітуди для $|0^{\otimes n}\rangle$ будуть скасовані, залишивши амплітуду нульовою, і вимірювання має давати результат, відмінний від 0, принаймні в одному кубіті в регістрі запиту. Підводячи

підсумок, якщо Аліса вимірює всі 0, тоді функція постійна, інакше - функція збалансована.

Алгоритм Шора

Алгоритм Шора - це насправді деяка надбудова над іншим базовим алгоритмом - алгоритм пошуку періоду. Він використовується для вирішення задачі про чорну скриньку, що реалізує деяку функцію, що веде себе періодичним чином. Ми знаємо функцію, її період слід знайти. І виявляється, що при класичному розв'язку, якщо період досить великий, то все, що ми можемо, — це перебирати варіанти доти, доки не знайдемо два аргументи, які дають одне й те саме значення. У квантовому випадку алгоритм будується інакше. Нам потрібен квантовий оракул, що реалізує цю функцію, а також квантове перетворення Фур'є — аналог дискретного (швидкого) перетворення Фур'є (FFT).

На вхід квантового оракула подаються два реєстри кубітів: перший відповідає вхідним значенням функції, другий вихідним. У першому реєстрі готується суперпозиція всіх можливих вхідних значень, другий реєстр ініціалізується фіксованим станом, після чого на виході отримуємо квантову суперпозицію всіх можливих входів і відповідних їм виходів. Потім робимо вимір вихідного реєстру, у результаті отримуємо деяке випадкове значення функції, а іншому реєстрі — суперпозицію всіх аргументів функції, відповідних отриманому значенню. Далі застосовуємо квантове перетворення Фур'є над першим реєстром і в вимірюванні, що зчитує, отримуємо величину, пропорційну зворотному періоду функції. Повторюючи цю операцію кілька разів і використовуючи класичний алгоритм Евкліда для пошуку найбільшого спільного дільника (НДД), ми отримуємо період.

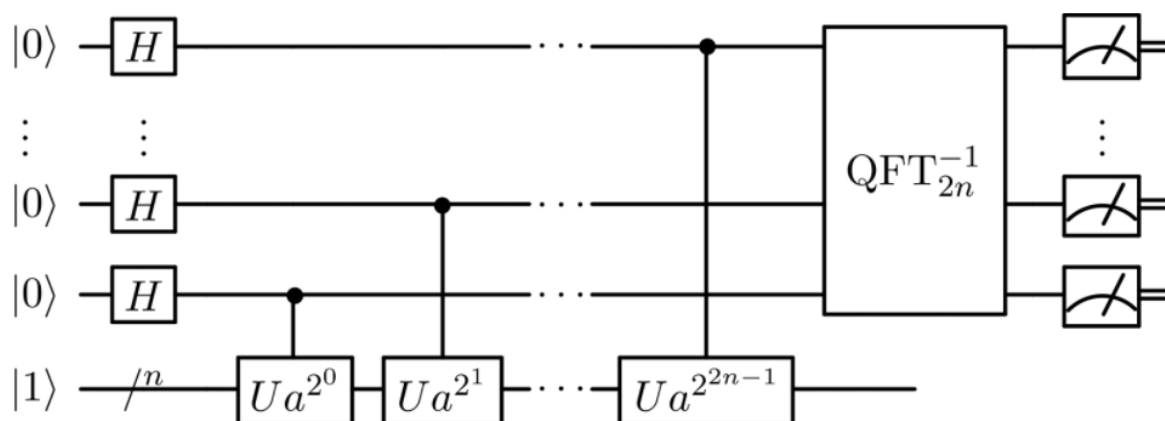


Рисунок 2.2 - Квантова схема алгоритму Шора.

Виявляється, що завдання факторизації - розкладання чисел на прості множники - і завдання дискретного логарифмування можна звести до пошуку періоду. Важливим практичним наслідком цього є те що, що з реалізації алгоритму Шора можна розкласти числа на прості множники і розв'язувати завдання дискретного логарифмування значно швидше, ніж з допомогою будь-яких відомих нині класичних алгоритмів. Тому це серйозна загроза криптографії з відкритим ключем, побудованої на цих принципах. Все це зародило колосальний інтерес до технології квантових обчислень як потенційного інструменту для вирішення завдань, недоступних для класичних комп'ютерів.

Швидкий квантовий алгоритм факторизації (розкладу на множники цілого числа) важливий з трьох причин. По-перше, наявність такого алгоритму є відображенням того факту, що квантові комп'ютери по суті своїй є більш ефективними, ніж класичні. По-друге, задача факторизації є цікавою сама по собі, так що будь-який новий алгоритм для її вирішення, чи то класичний, чи квантовий, представляє інтерес. По-третє, ефективний алгоритм факторизації може бути використано для зламу криптосистеми RSA з відкритим ключем, яка широко використовується в сучасних

інформаційних системах, зокрема, для кодування інформації у всесвітній мережі.

Алгоритм Шора вирішує проблему факторизації числа N шляхом розв'язку еквівалентної проблеми: маючи довільне число a , взаємно просте з N , знайти порядок r елемента $a \bmod N$ (залишок від ділення числа N на a). (Порядком елемента $a \bmod N$ називається найменше ціле r таке, що $ar \equiv 1 \bmod N$). Для цього a обирають рівноімовірно. Використовуючи алгоритм Евкліда, можна ефективно визначити, чи є a взаємно простим з N . Якщо це так, тоді порядок r елемента $a \bmod N$ буде дільником числа N .

Алгоритм Гровера

Як обговорювалося раніше, алгоритм Гровера виконує пошук за невпорядкованим набором $N = 2^n$ елементів, щоб знайти унікальний елемент, який задовольняє деякій умові. Хоча найкращий класичний алгоритм пошуку за невпорядкованими даними вимагає $O(N)$ часу, алгоритм Гровера виконує пошук на квантовому комп'ютері лише за $O(\sqrt{N})$ операції, що є квадратичним прискоренням. Як зазначає сам Гровер, якби алгоритм працював у кінцевій степені $O(\lg N)$ кроків, то це би забезпечило алгоритм у BQP для проблем у NPC. Однак, Алгоритм Гровера не забезпечує такого часу виконання і є асимптотично оптимальним рішенням, тому наразі не можна зробити остаточне твердження щодо зв'язку між класами складності BQP і NP на основі продуктивності алгоритму Гровера.

Алгоритм пошуку Гровера є хорошим вступом до квантових алгоритмів, оскільки він демонструє, як якості квантових систем можна використовувати для покращення нижньої межі часу виконання класичних алгоритмів. Щоб досягти такого прискорення, Гровер спирається на квантову суперпозицію станів. Як і багато квантових алгоритмів, алгоритм

Гровера починається з встановлення машини в рівній суперпозиції всіх можливих кубітів. Це означає, що існує рівна амплітуда $1/\sqrt{2^n}$

пов'язана з будь-якою можливою конфігурацією кубітів у системі та рівною ймовірністю $1/2^n$, що система буде в будь-якому з 2^n станів. Усі ці можливі стани відповідають всім можливим записам у базі даних Гровера, починаючи з однакових амплітуд призначених відповідно кожному елементу в просторі пошуку, кожен елемент якого можна розглядати відразу в квантовій суперпозиції, і звідти можна маніпулювати амплітудами для отримання правильного результату з бази даних з ймовірністю «не менше» $1/2$.

Поряд із суперпозицією станів, алгоритм Гровера і в цілому сімейство квантових алгоритмів, які використовують так зване амплітудне посилення, використовують переваги квантових амплітуд так щоби відрізняють ці амплітуди від простих ймовірностей. Ключем до цих алгоритмів є вибіркове зміщення фази одного стану квантової системи, такої, що задовольняє деякій умові, на кожній ітерації. Виконання фазового зсуву на π еквівалентно множенню амплітуди цього стану на -1 : амплітуда для цього стану змінюється, але ймовірність перебування в цьому стані залишається рівною (оскільки ймовірність не враховує знак амплітуди). Однак наступні перетворення, що виконуються в системі, використовують цю різницю в амплітуді щоб виділити цей стан різної фази і в кінцевому підсумку збільшити ймовірність того, що система знаходиться в такому стані. Такі послідовності операцій були б неможливими, якби амплітуди не містили додаткової інформації щодо фази стану на додаток до ймовірності. Ці алгоритми амплітудного посилення є унікальними квантовими обчисленнями завдяки якості амплітуд, якої не має аналогів у класичній ймовірності.

Якщо розглянути реалізацію загальної версії алгоритму то можна вважати, що у нас є чорна скринька з якоюсь фіксованою кількістю входів, що дорівнює N , серед яких є лише один, на який чорна скринька верне 1, тоді як на решту поверне 0. Завдання - найбільш оптимальним чином знайти цей елемент у класичному та квантовому випадку. Виявляється, що квантовий алгоритм вирішення такого завдання дає перевагу — оскільки в даному випадку замість порядку N запитів, які нам потрібні в класичному випадку, знадобиться лише корінь із N запитів. Якщо в класиці ми вирішували б це завдання, пробуючи один варіант за іншим, то в квантовому випадку алгоритм будується так, що ми створюємо деякий квантовий стан, що містить відразу всі можливі варіанти входів. Потім подаємо його на квантовий оракул, а з виходом робимо деякі перетворення. Потім знову подаємо результуючий стан в оракул і робимо деякі перетворення. Після порядку кореня з N ітерацій фінальний вимір майже точно покаже на потрібний вхід.

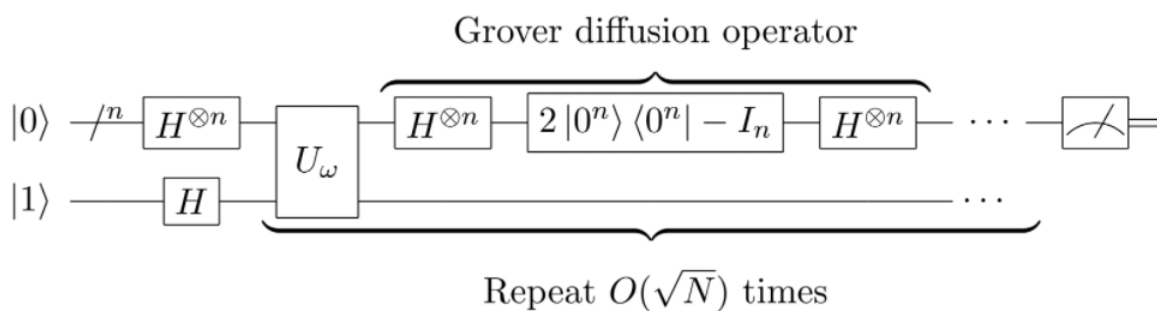


Рисунок 2.3 - Квантова схема алгоритму Гровера.

Складність задач комбінаторної оптимізації та перспективи квантових комп'ютерів для їх вирішення

Переглянемо типові приклади задач комбінаторної оптимізації:

- Проблема комівояжера (TSP). Вам надається список міст і відстані між ними, і ви повинні надати найкоротший маршрут, щоб відвідати їх усі.
- Проблема ранця. Вам надано ваги та значення вагів предметів, знайти якомога повну множину предметів, яку можна взяти з собою, враховуючи певні межі загальної ваги.
- Сортування. Дано N чисел, поверніть їх у порядку зростання.
- Проблема розкладання цілих чисел. Вам дано велике число M , і ви повинні вказати два цілі множники, p і q , таких, що $M = pq$.
- Проблема задовільності (SAT). Вам надано логічний вираз багатьох змінних $x_i \in \{0, 1\}$, наприклад, $P(x_1, x_2, x_3, x_4) = x_1 \vee x_2^{-} \wedge (x_3 \vee x_4^{-})$. Знайти вираження змінних які зроблять вираз істинним. Наприклад, у наведеному випадку $X_i = 1$ є вірним рішенням

Не всі проблеми оптимізації однаково важкі. Зупинимось на мінімально можливому часі, необхідному для вирішення алгоритму, тобто до якого класу складності по часу вони належать. Усі проблеми в списку вище є NP: якщо є рішення проблеми, його валідність завжди можна перевірити за поліноміальний час. Але відомо, що тільки одна з них знаходиться в P: проблема сортування, тому що його завжди можна вирішити за час $O(N \log(N))$, який менше, ніж $O(N^2)$. Щодо задачі факторізації ми не знаємо до якого класу її віднести, в P чи NP. Інші три належать до особливої підмножини: вони NP-повні. Це означає, що вони належать до особливої групи з такою властивістю: якщо поліноміальний алгоритм знайде розв'язок одного з них, то у нас буде поліноміальний алгоритм для розв'язання всіх NP задач. Яким чином вирішення однієї NP-повної задачі буде корисною для вирішення всіх NP задач? За допомогою стратегії, яка називається скорочення. Наприклад, задачу сортування можна звести до задачі SAT за поліноміальний час. Таким чином, стратегія вирішення будь-якої NP-задачі

буде: (1) перевести нашу задачу у задачу SAT, (2) вирішити нову задачу SAT, і (3) перевести назад отримане рішення. Для фізиків дуже важливо знати, які задачі комбінаторної оптимізації є NP-повними а які ні. Це важливо для того щоб уникнути втрати дорогоцінного часу наївною спробою розв'язати їх за поліноміальний час. Насправді, ми також не очікуємо, що квантові комп'ютери ефективно розв'яжуть задачі, які є NP-повними. Це означало б, що NP міститься в BQP, і ми не віримо, що це так. Проте ми очікуємо, що деякі проблеми, які є в NP і не є в P можуть бути ефективно розв'язані за допомогою квантового комп'ютера, тобто вони належать до BQP. Для вирішення цих проблем квантові алгоритми можуть забезпечити експоненційну перевагу. Крім того можливо ми зможемо вирішити деякі NP-повні задачі на квантовому комп'ютері з квадратичною перевагою порівняно з класичним рішенням.

Проблема домінуючого набору (ПДН)

Уявіть собі набір цілей, які потребують спостереження. Між певними цілями розташовані «лінії переходу», які дозволяють апарату спостереження одночасно переглядати більше однієї цілі. Наприклад, ми можемо використовувати дрони, щоб спостерігати за гірським регіоном, змінюючи точку зору за такою лінією вгору по долині. Тоді цілі спостереження можна розглядати як вузли графа, а лінії переміщення уявити як ребра графа, що з'єднує вузли. Тут можна поставити оптимізаційне питання – яке найменше число дронів необхідно для огляду всієї мережі.

Проблема може бути розв'язана використовуючи наступні пункти для мережі з n вузлів. Для вхідного $z = z_0 z_1 \dots z_{n-1}$, перше положення вимірює кількість цілей спостереження:

$$T_k(z) = \begin{cases} 1, & \text{якщо } k\text{-тий вузол з'єднаний з} \\ & \text{деяким } i\text{-тим вузлом, де } z_i = 1; \\ 0, & \text{в іншому випадку;} \end{cases}$$

Для пояснення цього визначення можна сказати, що кожен вузол пов'язаний сам із собою. Функція вартості (C) більша, чим більше вузлів в мережі для спостереження. Друге положення вимірює кількість дронів, що потрібні для використання:

$$D_k(z) = \begin{cases} 1, & \text{якщо } z_k = 0 \\ 0, & \text{якщо } z_k = 1 \end{cases}$$

Розглянемо наступний граф з чотирьох вузлів:

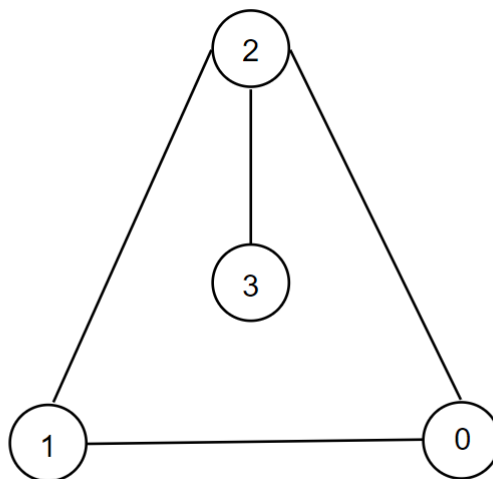


Рисунок 2.4 – Граф з чотирьох вузлів.

Вершини були позначені від 0 до 3 відповідно до загально прийнятої нумерації програмування. Складемо таблицю з усіх можливих поєднань вершин z :

z	$z_0z_1z_2z_3$	T_0	T_1	T_2	T_3	D_0	D_1	D_2	D_3	$C(z)$
0	0000	0	0	0	0	1	1	1	1	4
1	0001	0	0	1	1	1	1	1	0	5
2	0010	1	1	1	1	1	1	0	1	7
3	0011	1	1	1	1	1	1	0	0	6
4	0100	1	1	1	0	1	0	1	1	6
5	0101	1	1	1	1	1	0	1	0	6
6	0110	1	1	1	1	1	0	0	1	6
7	0111	1	1	1	1	1	0	0	0	5
8	1000	1	1	1	0	0	1	1	1	6
9	1001	1	1	1	1	0	1	1	0	6
10	1010	1	1	1	1	0	1	0	1	6
11	1011	1	1	1	1	0	1	1	0	5
12	1100	1	1	1	0	0	0	1	1	5
13	1101	1	1	1	1	0	0	1	0	5
14	1110	1	1	1	1	0	0	0	1	5
15	1111	1	1	1	1	0	0	0	0	4

Таблиця 2.1. Повна таблиця пунктів для наведеного в прикладі графа

У таблиці 2.1 перераховано всі можливі $D_k(z)$, $T_k(z)$ і $C(z)$ для $z \in \{0, 1, \dots, 2^4 - 1\}$. З чотирма вузлами таблиця відображає 16 станів. Однак зі збільшенням кількості вузлів кількість можливих станів збільшується в геометричній прогресії, отже запис повної таблиці має сенс тільки для невеликих графіків. З таблиці видно, що $z = 2$ (або $z = 0010$ у двійковій формі), що відповідає дрону на вузлі 2 і є нашим розв'язком. Звичайно, це було зрозуміло з першого погляду на рисунок графа, де вузол 2 з'єднаний з усіма іншими вузлами, але дуже важливо описати алгоритм для тих графів, що ми не зможемо(дуже складно) представити за їх великого розміру.

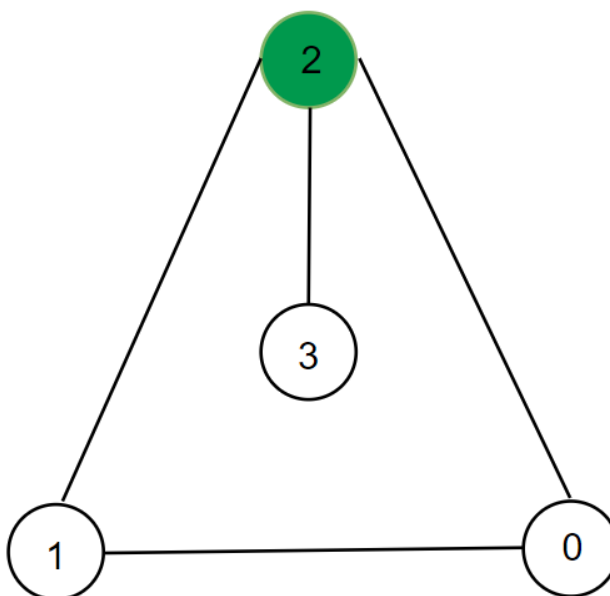


Рисунок 2.5 – Розв'язок задачі, друга вершина є домінуючою

Реалізація алгоритму для рішення ПДН

Крок 1: Реалізація алгоритму для розв'язання ПДН вимагає додаткового допоміжного кубіта понад кількістю кубітів що представляють вершини графа.

Тобто якщо граф має N вершин, нам потрібно ініціювати $N+1$ кубітів. Назвемо всі основні кубіти z -кубітами, для того щоб не плутатись у майбутньому.

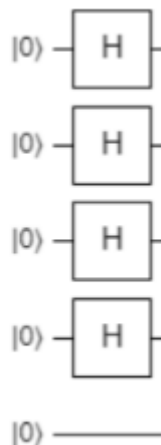


Рисунок 2.6 - Перший крок реалізації алгоритму.

Першим кроком для фактичної реалізації є додавання до схеми вентиля Адамара для кожного z -кубіту. Додатковий кубіт (наразі порожній) буде використаний пізніше для проведення $-\gamma$ обертань. Перший кубіт зверху знаходиться в 0, другий під ним кубіт в 1 і так далі для всіх кубітів нижче.

Така схема є еквівалентна виразу

$$|\psi_1\rangle = H^{\otimes 4} \otimes I |\psi_0\rangle = \frac{1}{4} (|0000\rangle + |0001\rangle + |0010\rangle + \dots + |1110\rangle + |1111\rangle) \otimes |0_4\rangle$$

Крок 2: Наступним кроком у реалізації алгоритму є імплементація положень D_k . Ці положення визначаються як

$$D_k(z) = \begin{cases} 1, & \text{якщо } z_k = 0 \\ 0, & \text{якщо } z_k = 1 \end{cases}$$

Таким чином схема буде виглядати як зображено на рисунку 2.7.

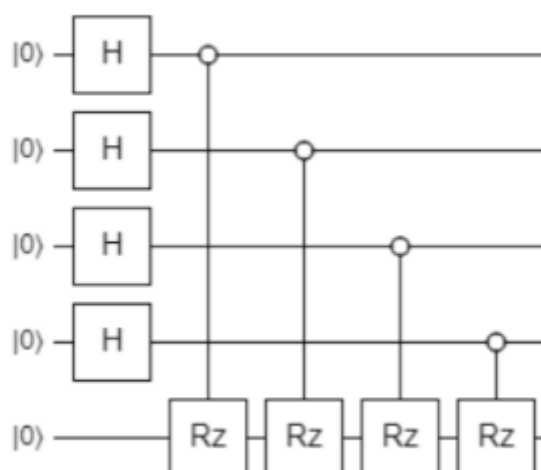


Рисунок 2.7 - Другий крок. Реалізація положень D_k . Які є звичайним квантовим вентилям $U1(\gamma)$.

Крок 3: Третій крок це імплементація положень T_k . Ці положення визначаються як

$$T_k(z) = \begin{cases} 1, & \text{якщо } k\text{-тий вузол з'єднаний з} \\ & \text{деяким } i\text{-тим вузлом, де } z_i = 1; \\ 0, & \text{в іншому випадку;} \end{cases}$$

Хоча ці положення дуже складно визначити, насправді виявилось що їх досить легко реалізувати. Для деякого вузла k , нехай T буде множиною вузлів таких, що $i \in T$ буде означати, що вузол i покриває вузол k . Зауважимо, що $k \in T$ також. Тепер додамо вентиль АБО подавши на входи кубітах з T і на виходах видаймо зміну фази на $-\gamma$.

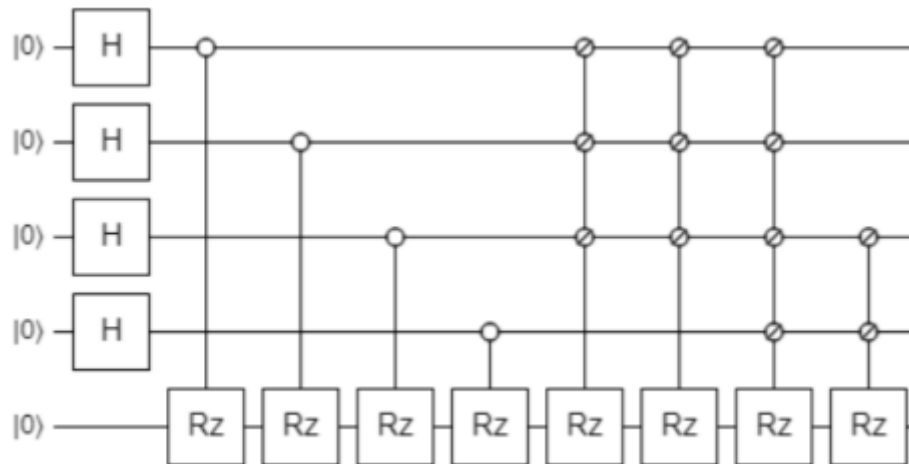


Рисунок 2.8 – Третій крок. Додавання вентилів АБО, що роблять зсув(обертання) стану кубіта на кут $-\gamma$.

Наприклад, у стандартному прикладі алгоритму, Кроки 2 і 3 будуть мати ефект обертання на $-\gamma$ для кожного з $2n$ положень. Для нашого прикладу це

$$|\psi_3\rangle = \frac{1}{4} (e^{-4i\gamma}|0000\rangle + e^{-5i\gamma}|0001\rangle + e^{-7i\gamma}|0010\rangle + \dots + e^{-4i\gamma}|1111\rangle)$$

Крок 4: Четвертий крок це реалізувати обертання на $-\beta$ градусів в алгоритмі майже так само, як ми це зробили в попередньому кроці. Нам потрібно реалізувати наступний квантовий вентиль для всіх z-кубітів:

$$U_B(\beta) = U_3 \left(2\beta, \frac{3\pi}{2}, \frac{\pi}{2} \right) = \begin{pmatrix} \cos(\beta) & -i \sin(\beta) \\ -i \sin(\beta) & \cos(\beta) \end{pmatrix}$$

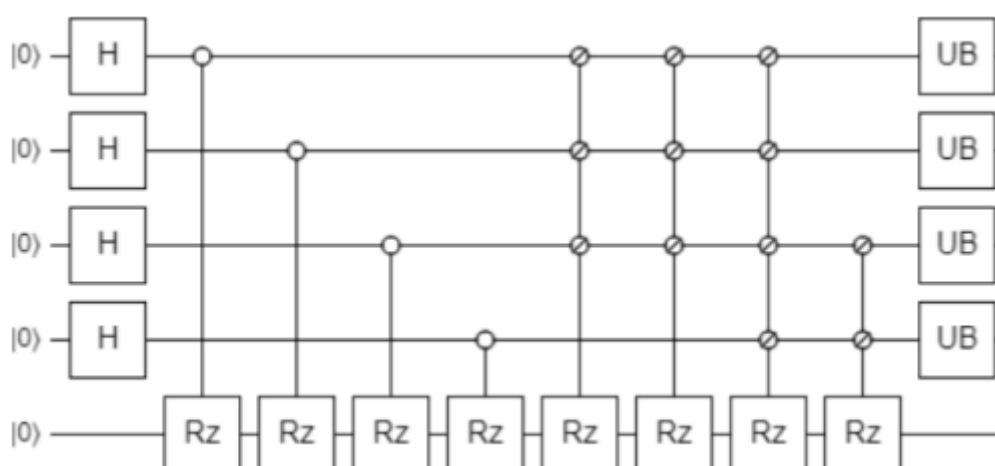


Рисунок 2.9 – Четвертий крок. Обертання кожного z-кубіта на кут $-\beta$ навколо осі z.

Крок 5: Останнім кроком в реалізації алгоритму є вимірювання z-кубітів. Це дає остаточну схему роботи алгоритму (рис. ЧЧЧ)

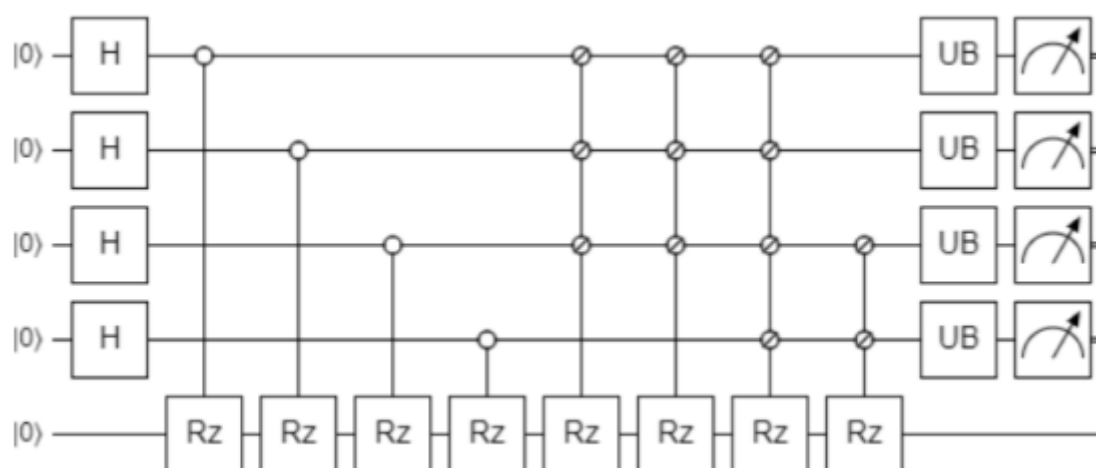


Рисунок 2.10 - Повна Схема реалізації алгоритму для розв'язання часткового прикладу ПДН.

Запуск та симуляція роботи алгоритму для $\gamma = \beta = \frac{\pi}{5}$ надає наступну гістограму:

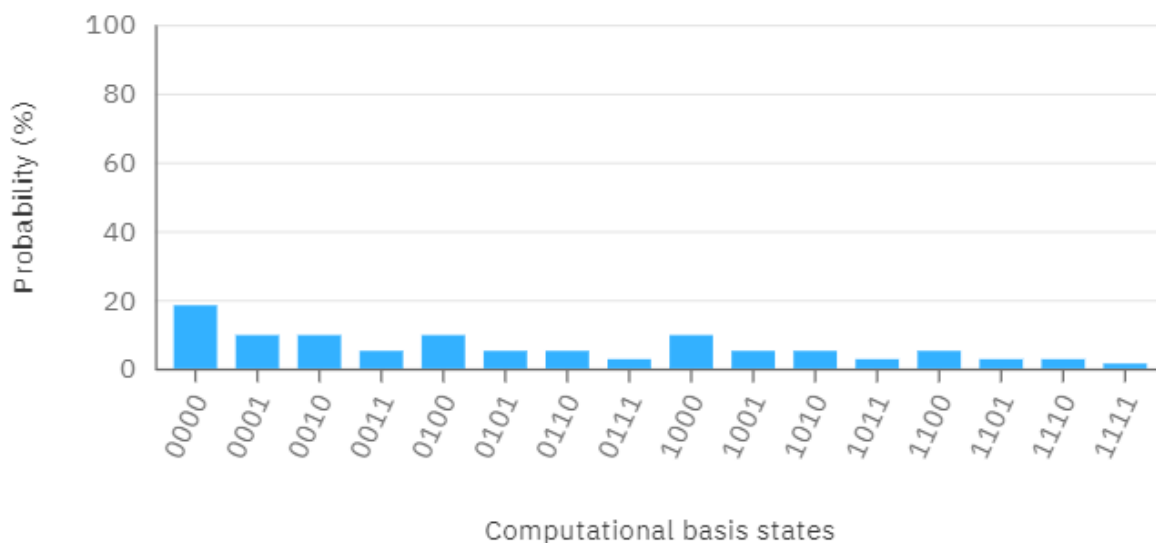


Рисунок 2.11 – Гістограма результатів симуляції алгоритму

Аналіз складових алгоритму

Наразі можна обмежити кількість вентилів, що використовуються для реалізації ПДН на довільному графі. Розглянемо граф з n вершинами, та перерахуємо ворота, які використовувались на кожному кроці:

- Алгоритм починається з n воріт Адамара
- Положення D_k є керованими квантовими фазовими вентилями. Для їх реалізації використовуються $2n$ SWAP вентилів і n керованих фазових вентилів. Кожен з них реалізується з 4 однокубітних вентилів і 2 вентилів CX. Отже загалом знадобиться всього $6n$ однокубітних вентилів і $2n$ вентилів CX.
- Положення T_k важче аналізувати, оскільки воно відрізняється від графа до графа. Однак очевидно, що вузол, підключений до i -вузлів, потребує більше гейтів для реалізації, ніж вузол, підключений до $i-1$ вузлів. Це означає, що щонайбільше кожне положення буде n керованим елементом АБО. Це спрощує до підрахунки до максимум $16n^2 - 14n$ CX гейтів і $18n^2 - 14n$ однокубітних гейтів.
- Останнім кроком є реалізація вентилів обертання на кут β . Це однокубітні вентилялі, отже можемо додати n вентилів до загальної суми.

Додавши всі рахунки гейтів разом, ми знаходимо, що кількість гейтів може бути обмежена наступними цифрами:

- не більше $18n^2 - 6n$ однокубітних вентилів.
- не більше $16n^2 - 12n$ CX вентилів.
- не більше n допоміжних кубітів. Для z -кубітів це дорівнює сумі з $2n$ кубітів.

Висновки до II розділу

У другому розділі ми систематизували існуючі квантові алгоритми і виявили що за призначенням алгоритми поділяються на алгоритми пошуку, алгоритми симуляції та алгоритми на основі перетворення Фур'є. Навели стислий опис трьох основоположників квантових алгоритмів, а саме: алгоритм Дойча та Дойча-Йожі, алгоритм Шора, алгоритм Гровера. Також було проаналізована можлива користь та майбутній вклад квантових обчислень в рішення проблем комбінаторики. Було зроблено висновок, що квантові обчислення відкривають новий клас комбінаторних проблем BQP. Для вирішення цих проблем квантові алгоритми можуть забезпечити експоненційну перевагу. Крім того можливо ми зможемо вирішити деякі NP-повні задачі на квантовому комп'ютері з квадратичною перевагою порівняно з класичним рішенням.

В другій частині ми навели приклад задачі домінуючої множини у графі, і розв'язали його за допомогою класичного алгоритма. Потім покроково побудували квантовий алгоритм для рішення тієї самої задачі. Переконалися що реалізована схема алгоритма працює коректно шляхом емуляції алгоритма на квантовій машині. Проаналізували отримані результати і виявили що алгоритм є майже непосильний для реалізації практичного завдання на сучасній квантовій машині, оскільки потребує багато кубітів для імплементації. Сучасні квантові потужності розвинуті ще не так далеко, як людство потребує, саме тому наразі для вирішення реальних проблем класичні комп'ютери виграють «гонку».

РОЗДІЛ 3. ПРИНЦИПИ РОБОТИ ГРАВІМЕТРІВ.

Види гравіметрів та дослідження будови гравіметра.

Гравіметричні дані використовуються в багатьох сферах діяльності людини, як наукових, так і практичних. Так, наприклад, на зв'язку форми Землі з елементами гравітаційного поля заснований фізичний спосіб визначення постаті нашої планети. Усі явища, що відбуваються на Землі, пов'язані з переміщенням мас всередині неї. Ці явища можна фіксувати при постійному моніторингу гравітаційного поля в тектонічно активних областях і тим самим прогнозувати можливі землетруси або виверження вулканів. Гравіметрія – розділ геофізики – наука про вимірювання та вивчення розподілу сили тяжіння та її складових на земній поверхні. До предмета «Гравіметрія» входять питання використання результатів вимірювання сили тяжіння для визначення фігури Землі та її внутрішньої будови, а також вивчення геологічної будови її верхніх шарів: земної кори та мантиї. Завданням гравіметрії є визначення гравітаційного поля Землі та інших небесних тіл як функції розташування та часу за вимірами сили тяжіння та гравітаційних градієнтів на поверхні тіла або поблизу нього.

Гравіметр – прилад вимірювання сили тяжкості. Робота гравіметра заснована на статичному методі, в якому спостерігають положення рівноваги тіла, що під дією сили тяжкості та сили, прийнятої за еталонну. За еталонну силу приймають пружну силу деформації пружин та ниток. Пристрій, за допомогою якого компенсується дія сили тяжіння на тіло постійної маси та її зміна перетворюється на переміщення тіла, називається чутливим елементом. Більшість сучасних гравіметрів є механічними. Чутливий елемент такого гравіметра називається пружною системою, яка є головним вузлом будь-якого гравіметра. Гравіметр, по суті, є багатопрофільним приладом, застосування якого можливе в багатьох

областях. Його використовують археологи, палеонтологи, а також можливе застосування в гідрології, ґрунтознавстві, сільському господарстві, картуванні та багатьох інших областях. Гравіметри встановлюються на автомобілях, суднах, літаках, космічних супутниках та інше, але більш поширені переносні вручну конструкції. Також їх застосовують у навігації балістичних (у тому числі ядерних) ракет. В основі системи орієнтації ракети застосовується гравіметрія, тому що саме гравітаційне поле Землі є сильним і стабільним орієнтиром: на відміну від орієнтації магнітним полем, або наведення шляхом радіосигналу, гравітаційне поле неможливо спотворити або перехопити. З зрозумілих причин неможливо і «замаскувати» атаковану мету штучною гравітаційною аномалією, оскільки для її створення буде потрібно швидке і потайне переміщення мільярдів тонн породи з однієї точки планети в іншу. Точність та діапазон гравіметра залежать від його призначення. Як правило, його чутливість складає прибл. 10–4 діапазони в якому верхня межа вимірювань без перебудови діапазону становить не менше 500 мГал, називають широкодіапазонним, інакше – вузькодіапазонним. У гравітаційній розвідці вимірювання малих прирощень сили тяжіння здійснюється вузькодіапазонними приладами з високою чутливістю. При встановленні гравіметра на дні водойм застосовується дистанційне керування. Для вимірювання малих варіацій сили тяжіння (напр., що викликають припливи) застосовують стаціонарні гравіметри, чутливість яких становить десятки частки мікрогалу. Для спец. досліджень, передусім на вирішення завдань геодинаміки, застосовують особливо чутливі стаціонарні кріогенні гравіметри, у яких вага пробного тіла врівноважується магнітними силами, створюваними надпровідними елементами за умов низьких температур.

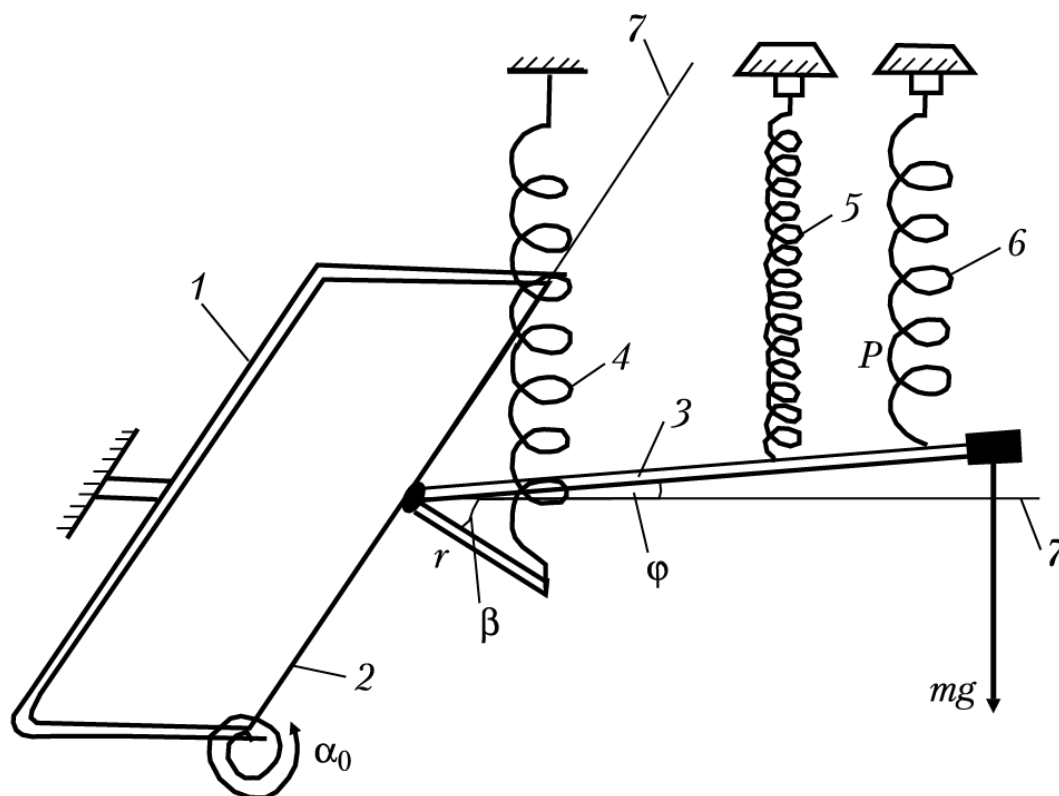


Рисунок 3.1 - Принципова схема чутливої системи перших гравіметрів.

1 - рамка; 2 - пружна нитка; 3 - важіль з грузиком; 4 - головна пружина; 5 - вимірювальна пружина; 6 - діапазонна пружина; 7 - лінія горизонту

Спочатку в гравірозвідці та гравіметрії для точних вимірювань поля сили тяжіння застосовувалися різні градієнтметри та варіометри. Дані прилади дозволяють виміряти повні значення других похідних потенціалу, що досить інформативно, але вони мають вкрай низьку продуктивність - один вимір сили тяжкості може йти до 40 хвилин і більше. Через це поширення набули більш прості, але в той же час більш продуктивні гравіметри різних конструкцій, які вимірюють лише вертикальну похідну потенціалу - Δg . У СРСР 1953 року було налагоджено випуск власних гравіметрів і виробництво вариометрической апаратури різко знизилося, а 1968 року припинилося. В даний час градієнтметри та варіометри використовуються лише для високоточних вимірювань поля сили тяжіння з їх допомогою можливі археологічні дослідження, пошук великих

підземних приміщень - галерей та бункерів, коли точності гравіметрів не вистачає. Гравіметр являє собою досить тонкий вимірювальний прилад, робота якого залежить від цілого ряду факторів, що заважають: температури, тиску, вібрацій всілякі мікросейсми або тряска. Тому вимірювання проводять виключно у спокої, встановлюючи гравіметр по черзі на кожному пікеті заздалегідь підготовленої мережі. Чутлива частина гравіметра поміщена у захисний корпус, у якому підтримуються постійні температура та тиск. Сучасні гравіметри вже досягли точності визначення g на рівні $\sim 10^{-7} - 10^{-9}$ при відносних вимірах, а точність при абсолютних вимірах може становити $0.03 - 0.07$ мГал. Існує багато різних конструкцій чутливої системи, робота якої обумовлена впливом сили тяжіння на якесь явище: вільне падіння тіл, коливання маятника струни, мембрани, прецесія важкого гіроскопа, викривлення поверхні обертової рідини або підйом рідини в капілярі, левітація провідника з током поле, а також рівновагу будь-якої системи з ваги з важелів або пружин. Виміряні показання може бути як абсолютними, і відносними у разі вимірюється різниця сили тяжкості у двох сусідніх пунктах. Також вимірювання можуть проводитися у русі на воді, а останнім часом "модною" стає авіагравірозвідка, але частіше гравіметри нерухомо встановлюють на пункті вимірювання, і лише після закінчення вимірювань переносять на новий пункт. Методи розв'язання прямої задачі гравіметрії:

- а) Фізико-геологічне моделювання;
- б) Апроксимаційні методи (вирішення обернених задач способами розв'язання прямих задач);
- в) Способи аналітичного продовження поля в нижній напівпростір.

Існує багато типів гравіметрів. Перший вітчизняний астазований кварцовий гравіметр ГАК-3М був створений в 1953 р. у ВНДІ геофізики

групою фахівців, очолюваної К.Є. Веселовим. Надалі на його основі були розроблені гравіметри ГАК-ПТ, ГАК-7Т, ГАК-7Ш та ін. Найбільш широке застосування практично знайшов гравіметр ГАК-7Т. Похибка вимірювання сили тяжіння цим гравіметром в залежності від методики спостереження, що застосовується, становить 0,03–0,06 мГал. Основні характеристики гравіметрів наведено у стандарті ГОСТ 13017-83 «Гравіметри наземні. Загальні технічні умови» та у стандарті РЕВ 5578–86 «Загальні технічні вимоги та методи випробувань». Усі типи гравіметрів відрізняються конструктивними особливостями пристрою пружних систем, що впливає їх точнісні характеристики. Механічна частина у всіх гравіметрів залишається практично незмінною, що спрощує процес виготовлення та налагодження чутливих систем. У практиці гравірознавства застосовуються переважно статичні гравіметри. Вони ґрунтуються на компенсації сили тяжіння силою пружності пружини або силою кручення нитки. Гравіметри служать лише відносних вимірювань прискорення сили тяжкості.

Робота гравіметра наземного вузькодіапазонного кварцового другого класу точності ГНУ-КВ. Цей гравіметр використовується для детальних розвідувальних робіт. Похибка виміру ним сили тяжіння в рейсах тривалістю не понад 4 години становить $\pm 0,03$ мГал, поріг чутливості $\pm 0,006$ мГал. Вага приладу 4,5 кг. На рис. 1 представлений гравіметр. На внутрішній поверхні, на дні та під кришкою футляра укріплені поролонові амортизатори, обшиті тканиною.(рис.1)



Рисунок 3.2 - Гравіметр: а) внутрішня частина приладу; б) загальний вигляд приладу; в) транспортувальний футляр циліндричної форми, виготовлений з жерсті

Середня частина гравіметра поміщена у зовнішній кожух 1, який являє собою порожнистий циліндр із листової нержавіючої сталі діаметром 132 мм із дзеркальною зовнішньою поверхнею. В середину кожуха поміщений циліндр з пінопласту 2, який вставляється Посудина/сосуд Дьюара 3, а в середину його щільно входить середня частина гравіметра 5. Ущільнення досягається за допомогою вовняного чохла 4, що одягається на середню частину. Вовняний чохол виконує також роль утеплювача та запобігає зіткненню металу середньої частини гравіметра зі скляними стінками судини Дьюара, оберігаючи тим самим його від розбиття. Нижній торець циліндра зовнішнього кожуха з'єднаний із масивною основою з текстоліту, на якій по колу, через 120° , укріплені три установчі гвинти. На нижній частині підйомних гвинтів укріплені шарнірні круглі під'ятники, які збільшують площу опори гравіметра на ґрунт. На верхній частині

гвинтів знаходяться головки з ебоніту за допомогою яких обертаються підйомні гвинти. База гравіметра d – відстань між лінією, що з'єднує центри двох підйомних гвинтів та лінією, що проходить через третій гвинт паралельно першій – 120 мм. Середня частина приладу складається з основи кварцової системи, теплозахисного стовпа та верхньої панелі.

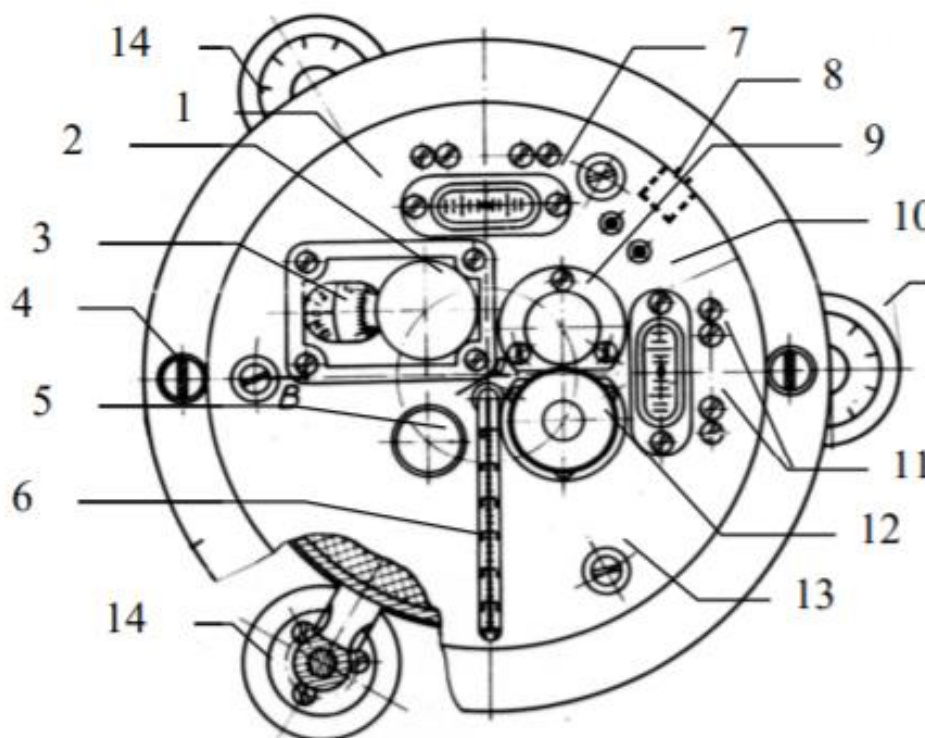


Рисунок 3.3 - Середня частина гравіметра, зріз.

Середня частина гравіметра показана на рисунку 3.3. Основа представлена як циліндр, на його нижньому краю розміщена конусоподібна стійка, на стійку кріпиться спеціальна кварцева втулка, до якої приварюється основна монтажна рамка кварцової системи. Кварцева система закріплюється захисним «стаканом», який притягується до основи спеціальною кільцевою гайкою.

Між основою і стаканом прокладається ущільнювальне гумове кільце 43, яке забезпечує герметизацію захисного стакана. З простору під стаканом відкачується повітря. Для цього на боковій поверхні основи є

отвір, в який вмонтований вакуумний кран, у вигляді запорного вентеля 31, з ущільнювачами і гайками. Для того, щоб відкачати повітря, застосовується два ключа. Відкачка повітря не потребує розбирання вимірювальної частини гравиметра. В торець основи вмонтовани три стойки 33 що оберігають систему від ушкодження під час зняття стакана. В основі є п'ять наскрізних, осьових отворів: два – для вимірювального та діапазонного пристрою, два- для оптичної системи та один – для термометра 10. Всередині цього циліндра розташовано 5 трубочок, в яких проходять стрижні вимірювального 11 та діапазонного 45 винтів, стрижень з оргскла 20, термометр та оптичний канал 44. Для захисту кварцевої системи від теплообміну через верхню панель, простір між трубками заповнений теплоізолюючими матеріалами.

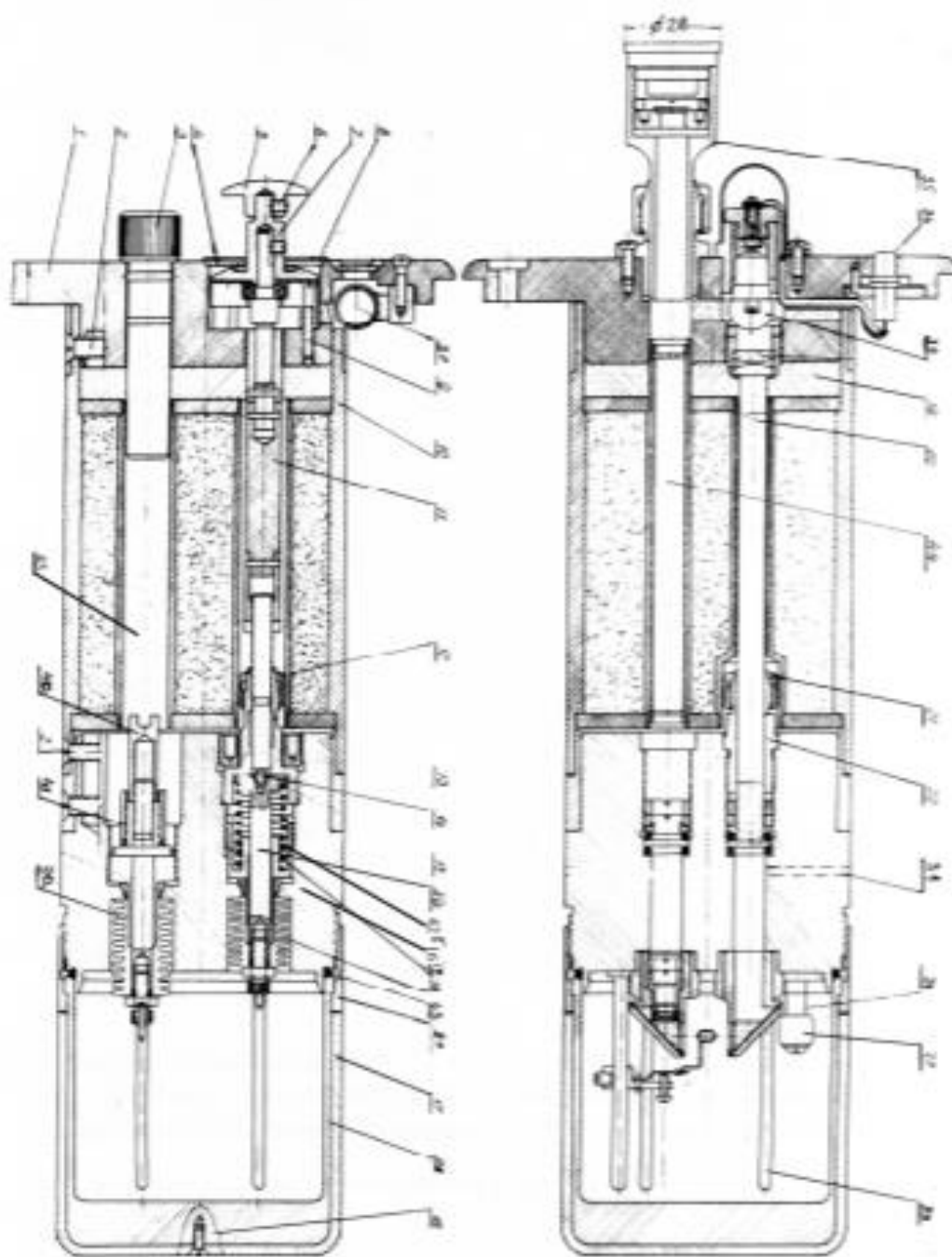


Рисунок 3.4 - Середня частина гравіметра, профіль.

Верхня панель (3) є товстим диском з текстоліту, що служить одночасно кришкою приладу та пробкою, яка закриває посуд Дьюара зверху. Панель кріпиться трьома гвинтами 13 до фігурного кільця зовнішнього корпусу. Під гвинти підкладені амортизуючі втулки (мал 3). На верхній панелі розміщені: мікрогвинт 2, відліковий пристрій 3, лампочка підсвічування з

конденсором 9, окуляр мікроскопа 12, гніздо для підведення електроживлення 8, два рівні 7 і 10 з юстирувальними гвинтами 11, а також ртутний термометр 6 з ціною поділу $0,5\text{ }^{\circ}\text{C}$ для вимірювання температури всередині приладу та отвір для діапазонного ключа 5. Гравіметр включає кілька систем: чутливу, або кварцову, нівелювання, електричну, оптичну, діапазонну, вакуумування та термостатування.

1. У гравіметрах 1-го роду мірою зміни прискорення сили тяжіння служить зміна довжини пружини, один кінець якої закріплений, а до іншого підвішено вантаж масою m . Тоді при обертанні сили тяжіння між цими точками можна розрахувати за формулою $\Delta g \approx \tau \Delta l / m$.

2. Схема чутливої системи гравіметра 2-го роду представлена рис.2. Тут важіль із грузиком кріпиться до горизонтальної пружної нитки і під впливом сили тяжіння нахиляється, закручуючи нитку. За допомогою вимірювальних пружин з мікрометричним гвинтом грузик виводиться в горизонтальне положення. Переходячи на іншу точку, під впливом збільшення сили тяжіння грузик відхиляється. Для виведення його в горизонтальне положення знову необхідно використовувати вимірювальну пружину, а на мікрометричному гвинті за спеціальною шкалою взяти відлік Δn .

На підвищення точності гравіметрів застосовується астазування, тобто. Штучне збільшення чутливості. Це досягається за рахунок того, що пружна система встановлюється в положення, близьке до нестійкого, завдяки чому невеликі зміни прискорення сили тяжкості викликають великі зміни відліку за шкалою приладу.

Насправді зазвичай використовуються гравіметри другого роду. Залежно від матеріалу, з якого виготовлено чутливу систему приладу, їх ділять на кварцові, металеві та кварцово-металеві. Найбільшого

поширення набули кварцові, оскільки властивості кварцу залежать від температури, чутливі системи поміщають у термостатовані судини. Однак гравіметри мають істотний недолік - сповзання нуля-пункту, яке необхідно враховувати.

Методи обробки інформації в гравіметрії і проблеми які вони вирішують

Однією з трудомістких процедур при обробці результатів польових гравіметричних вимірювань є запровадження поправок через вплив навколишнього рельєфу місцевості, облік якого, згідно з діючою «Інструкцією з гравірозвідки», повинен здійснюватися в радіусі 200 км (для масштабів 1:50 000 і дрібніше).

При традиційному підході до визначення результатів гравіметричної розвідки внаслідок необхідності підготовки та введення в ЕОМ масивів висотних позначок великої розмірності, особливо у центральній зоні радіусом 100–300 м, визнано недоцільним використання обчислювальних засобів. Обчислення поправки за вплив центральної зони здійснюється вручну з використанням великомасштабних карток рельєфу або матеріалів радіального нівелювання навколо пунктів (метод «зірочок»). Для визначення поправок у далеких зонах складаються матриці висот, знятих вручну з топографічних карток великого та середнього масштабів; як правило, після обчислення значень масивів поправок за вплив рельєфу навколишньої місцевості у вузлах квадратної мережі проводиться інтерполяція значень поправок до пунктів гравіметричних спостережень. Таким чином, вся процедура обліку впливу рельєфу місцевості дуже трудомістка і займає, згідно з нормами, не менше половини часу камеральних робіт. Крім того, при такому підході точність апроксимації рельєфу може бути достатньо низька.

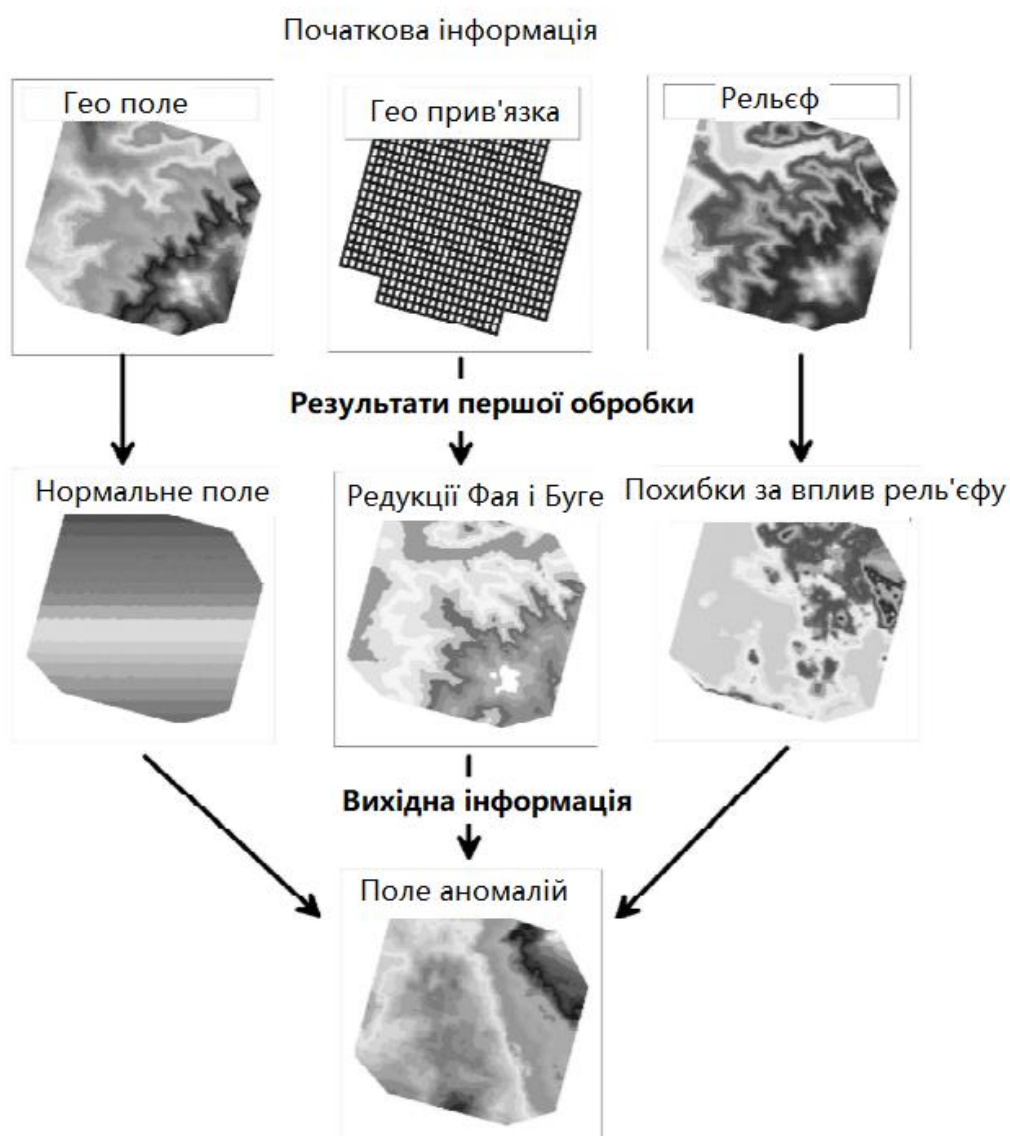


Рисунок 3.5 – Схема першої обробки гравіметричних даних

Розвиток обчислювальної та периферійної техніки, а також сучасного програмного забезпечення та ГІС-технології дозволяє здійснити принципово новий підхід до обліку впливу рельєфу поверхні Землі при обчисленні аномалій Буга з використанням нових джерел інформації.

Для визначення поправок за вплив рельєфу місцевості при гравіметричній зйомці потрібно вирішувати такі завдання:

- Побудова аналітичної моделі рельєфу (АМР) на основі вихідної цифрової моделі рельєфу (ЦМР) з використанням швидкого перетворення Фур'є (ШПФ);
- обчислення та підсумовування топографічних поправок;
- Виконання оцінки точності визначення топографічних поправок.

Для побудови АМР, а також для високоточного обчислення похибки необхідно використовувати високоточні цифрові моделі рельєфу великої розмірності. В даний час основними способами отримання даних про рельєф місцевості для вирішення поставлених завдань є:

- топографо-геодезичні роботи (топографічні висоти пунктів гравіметричних спостережень, метод «зірочок»);
- Використання великомасштабних топографічних карт (картографічні висоти точок цифрової моделі рельєфу);
- Застосування Internet-ресурсів.

Бурхливий розвиток супутникової геодезії та мережі Інтернет в останні роки забезпечило створення принципово нових систем аналізу гравіметричних даних, що відрізняються високою детальністю опису рельєфу місцевості.

Найбільшого практичного значення для розвідувальної геофізики отримав проект NASA з вимірювання висот земної поверхні за допомогою супутникового радіоінтерферометра SRTM (Shuttle Radar Topography Mission). Через Інтернет можна отримати доступ до архівів даних про висоти рельєфу поверхні Землі з кроком 3 кутові секунди майже на всю поверхню материків. Для прикладу, можлива цифрова модель рельєфу, побудована за даними радіоінтерферометра є матрицею розміром ~7000 рядків, ~5000 стовпців, з відстанями між вузлами мережі висотних

позначок ~ 50 м по широті, ~ 90 м - по довготі. Тобто це доволі великий обсяг даних.

Як ми переконались, гравіметрія використовує для обчислень алгоритми апроксимації даних, а отже теоретично є таке завдання де можна буде використати реалізований квантовий алгоритм, як альтернатива класичному. Також у попередньому розділі я навмисно привів такий приклад задачі (про покриття місцевості мережею дронів для спостереження), який може буди в нагоді гравіметрії. Оскільки в останні часи набуває розвитку якраз авіаційна гравіметрія, разом з тим технології дронів стають також більш розвиненими. Але якщо абстрагуватись від дронів, то на мою думку алгоритм може бути використаний і в інших задачах. Оскільки багато гравіметричних даних зберігаються у таблицях з багатьма критеріями, і побудувати граф з таблиці не нерозв'язною задачею перед людиною.

Технологія квантових обчислень хоч і не молода, але розвивається дуже повільними кроками. І для того щоб потягатися з потужністю класичних алгоритмів на великих об'ємах даних квантовим системам не вистачає багато кубітів. Насамперед це може стати основною проблемою в застосуванні даного алгоритма на практиці, так як більшість задач виконуються на великих вибірках даних.

Висновки до III розділу

В третьому розділі було розглянуто побудову гравіметрів та принципи їх роботи. Було описано основні проблеми з якими стикається гравіметрія як підчас геологічної розвідки так і підчас обробки отриманих даних. Як ми можемо переконатися гравіметрія використовує алгоритми апроксимації даних і алгоритми на основі перетворення Фур'є. Реалізований в другому розділі алгоритм містить у собі реалізацію квантового апроксимаційного алгоритму, а отже він може використовуватись для розв'язку тих самих задач, як альтернатива класичний обчисленням.

Але суттєва проблема полягає в тому, що наразі квантові комп'ютери та обчислення лише починають розвиватись і роблять це дуже повільними темпами. Як наслідок, квантові системи мають дуже низьку кількість кубітів, яка напряду впливає на обчислювальну здатність систем.

ВИСНОВКИ

В першому розділі роботи ми розглянули та описали базові поняття квантової системи та переконалися що квантова декогерентність є однією з головних перешкод перед сучасними квантовими обчисленнями. Розглянули побудову кубіта та частинки що можуть виступати в ролі кубітів, а також позначили основні складнощі у роботі з кубітами такі як: відсутність клонування, постійність помилок постійні, руйнування інформації при вимірюванні.

У другій частині першого розділу було доведено, що на управляючих переходах квантової системи можна побудувати детермінований автомат. Ми зробили систематизацію існуючих квантових алгоритмів і виявили що за призначенням алгоритми поділяються на алгоритми пошуку, алгоритми симуляції та алгоритми на основі перетворення Фур'є. Навели стислий опис трьох основоположників квантових алгоритмів, а саме: алгоритм Дойча та Дойча-Йожі, алгоритм Шора, алгоритм Гровера. Також було проаналізована можлива користь та майбутній вклад квантових обчислень в рішення проблем комбінаторики. Було зроблено висновок, що квантові обчислення відкривають новий клас комбінаторних проблем BQP. Для вирішення цих проблем квантові алгоритми можуть забезпечити експоненційну перевагу. Крім того можливо ми зможемо вирішити деякі NP-повні задачі на квантовому комп'ютері з квадратичною перевагою порівняно з класичним рішенням.

Під час роботи був по-кроково побудований квантовий алгоритм для рішення тієї самої задачі. Переконалися що реалізована схема алгоритма працює коректно шляхом емуляції алгоритма на квантовій машині. Проаналізували отримані результати і виявили що алгоритм є майже непосильний для реалізації практичного завдання на сучасній квантовій машині, оскільки потребує багато кубітів для імплементації реальної задачі. Сучасні квантові потужності розвинуті ще не так далеко, як

людство потребує, саме тому наразі для вирішення реальних проблем класичні комп'ютери виграють «гонку». Але я все одно вірю, що квантові комп'ютери це технологія майбутнього, через великі можливості які вона відкриває людству.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Pradosh K. Roy. Quantum Logic Gates. August 2020. [Електронний ресурс]. – Режим доступу: https://www.researchgate.net/publication/343833536_Quantum_Logic_Gates
2. Johnston E.R., Harrigan N., Gimeno-Segovia M. Programming Quantum Computers. Essential Algorithms and Code Samples. Sebastopol: O'Reilly, 2019
3. Emma Strubell. An Introduction to Quantum Algorithms. 2011
4. Холево А.С. Введение в квантовую теорию информации. 2002
5. A complexity theorist's (non)apology [Електронний ресурс]. – Режим доступу: <https://www.scottaaronson.com/blog/?p=206>
6. Д.Р. Дорошин. Методика обработки данных авиационной гравиметрии с учетом пространственной неоднородности гравитационной аномалии.