ЧЕРНІВЕЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ЮРІЯ ФЕДЬКОВИЧА
ІНСТИТУТ ФІЗИКО-ТЕХНІЧНИХ ТА КОМП“ЮТЕРНИХ НАУК
КАФЕДРА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ КОМП“ЮТЕРНИХ СИСТЕМ

Остапов С.Е., Добровольський Ю.Г.

КВАНТОВА ІНФОРМАТИКА ТА КВАНТОВІ ОБЧИСЛЕННЯ

НАВЧАЛЬНИЙ ПОСІБНИК

ЧЕРНІВЦІ — 2021

УДК 004.056(075.8)
ББК 32.973-0.18.10я73
О-76
Друкується за ухвалою Вченої ради Чернівецького національного університету імені Юрія Федьковича
(протокол №10 від 27 вересня 2021 року)

Рецензенти:
Доктор технічних наук, старший науковий співробітник Інституту метрології Купко О.Д.
Кандидат фізико-математичних наук, доцент Чернівецького торговельно-економічного інституту Київського торговельно-економічного університету Дрінь І.І.

Остапов С.Е., Добровольський Ю.Г.
Квантова інформатика та квантові обчислення / С.Е.Остапов. Ю.Г. Добровольський - Чернівці: ЧНУ, 2021. - 99 с.

У пропонованому виданні викладено навчальні матеріали до курсу «Основи квантової інформатики», який читається на першому році магістратури за освітньою програмою «Інженерія програмного забезпечення». Друга частина посібника призначена для поглибленого вивчення квантового комп’ютингу аспірантами тієї ж спеціальності. Запропоновано навчальну програму курсу та конспект лекцій.

Для студентів спеціальностей: 121 - «Інженерія програмного забезпечення», 122 - «Комп“ютерні науки» та «Інформатика» усіх форм навчання, інших спеціальностей, де вивчаються дисципліни захисту інформації, а також для самостійного опанування його основами.

ББК 32.973-0.18.10я73

Зміст

ПЕРЕДМОВА....4
ПОЯСНЮВАЛЬНА ЗАПИСКА....5
НАЗВА ТА ЗМІСТ ТЕМ ДИСЦИПЛІНИ....6
Зміст лекційного курсу....6
Вступ....6
Предмет та мета курсу. Місце квантових обчислень та перспективи розвитку. Переваги та недоліки квантових обчислень....6
Фізичні основи квантових обчислень....6
Рекомендована література:....8
Розділ I. Фізичні основи квантових обчислень....9
Вступ....9
Фізичні основи квантових обчислень....11
Трохи історії квантових обчислень....12
Дослід з “кулеметом”....16
Дослід з хвилями....20
Дослід з електронами....22
Квантові біти....27
Розділ II. Квантові операції....31
Прості операції над кубітами....31
Багатокубітні операції....33
Часткові вимірювання....34
Переплутані стани....35
Квантовий паралелізм....38
Парадокс Ейнштейна-Подольські-Розена....40
Квантова телепортація....45
Протокол квантового щільного кодування....48
Алгоритм Дойча....50
Розділ III. Квантова криптографія....54
Алгоритм факторизації цілих чисел (алгоритм Шора)....54
Алгоритм пошуку у невпорядкованому масиві (алгоритм Гровера)....58
Квантові протоколи узгодження ключів....61
Атаки на протоколи квантового узгодження ключа....66
Квантові гроші Стівена Візнера....69
Розділ IV. Архітектура та основні вимоги до квантових комп’ютерів....72
Основні фізичні технології....73
Розділ V. Огляд фізичних реалізацій квантових комп’ютерів....74
Гармонічний осцилятор як модель квантового комп’ютера....76
Квантовий комп’ютер на фотонах....78
Квантовий комп’ютер на оптичних резонаторах....79
Йони у пастках....80
Ядерний магнітний резонанс....83
Лабораторний практикум....88
I. Загальний опис лабораторного практикуму....88
II. Опис інструментарію....89
III. Методичні вказівки до лабораторних робіт....90

ПЕРЕДМОВА

Захист інформації перетворюється сьогодні на одну з найактуальніших задач унаслідок надзвичайно широкого розповсюдження як власне різноманітних систем обробки інформації, так і розширення локальних та глобальних комп’ютерних мереж, якими передається величезний обсяг інформації державного, військового, комерційного, приватного характеру, власники якої часто були б категорично проти ознайомлення з нею сторонніх осіб. Проблема набула особливої гостроти після прийняття урядом України закону про захист персональних даних, який зобов’язує зберігати та передавати персональні дані працівників лише в захищеному вигляді.

Не менш важливим завданням вважається широке впровадження інформаційних технологій у різні сфери людської діяльності в Україні: стрімке зростання обігу пластикових карток, майбутнє введення електронних паспортів та медичних карт, студентських квитків та залікових книжок. Зрештою, дедалі більше державних установ і приватних підприємств переходять на електронний документообіг, який до того ж вимагає юридичної чинності підписів фізичних або юридичних осіб. Розповсюдження таких технологій також, безперечно, вимагає добре поставленого захисту інформації.

Основним засобом сучасного захисту інформації є криптографічні перетворення. На сучасному етапі використовують давно відомі та добре відлагоджені блокові, потокові шифри, а також асиметричну криптографію, яка виявилася дуже перспективною для розробки протоколів електронного цифрового підпису, яким ми його сьогодні знаємо.

Успіхи квантових технологій та сучасної математики, тим не менше, призвели до появи абсолютно нових алгоритмів і методів, які з успіхом можна використати для повної або часткової компрометації класичних криптографічних алгоритмів. На зміну їм приходить новий розділ науки, квантова інформатика, частиною якої є квантова криптографія.

Навчальний курс “Основи квантової інформатики призначений надати студентам базові знання з надзвичайно перспективної галузі сучасної науки — квантової інформатики та, в продовження циклу дисциплін захисту інформації, детальніше знайомить з квантовою криптографією.

Курс читається на першому році магістратури за освітньою програмою “Інженерія програмного забезпечення” і є логічним продовженням циклу дисциплін інформаційної безпеки бакалаврату: “Основи криптографії” та “Безпека програм та даних”.

Доповненням до викладеного теоретичного матеріалу служить лабораторний практикум, який, за задумом, виконується у середовищі

Друга частина посібника призначена для аспірантів, які навчаються за докторською програмою зі спеціальності “121 — Інженерія програмного забезпечення” і вивчають дисципліну “Квантовий комп’ютинг”, а також для тих, хто бажає самостійно вдосконалювати свої знання у галузі квантової інформатики та квантового комп’ютингу.

ПОЯСНЮВАЛЬНА ЗАПИСКА

Мета курсу: вивчення студентами основних положень та відомостей про роль і місце квантової криптографії у розвитку перспективних методів захисту інформації, про закономірності розвитку квантових алгоритмів, про організацію і розробку архітектурних рішень та електронних елементів квантової комп‘ютерної техніки.

Завдання курсу:

Методичні: забезпечити молодих спеціалістів методичною базою для проведення науково-технічних та дослідницьких робіт з найсучасніших методів захисту інформації, що дозволить їм орієнтуватися у перспективних напрямках розвитку сучасної обчислювальної техніки.

Пізнавальні: сформувати базові знання з фізичних основ, сучасних принципів та алгоритмів, принципів функціонування і технічних характеристик прототипів квантових комп‘ютерів.

Практичні: сформувати уміння та навички практичного використання набутих знань, уміння ставити перед собою завдання, для вирішення яких потрібні знання найсучасніших технологій обчислювальної техніки.

НАЗВА ТА ЗМІСТ ТЕМ ДИСЦИПЛІНИ

Зміст лекційного курсу

Розділ 1. Основні поняття квантових обчислень

Вступ

Предмет та мета курсу. Місце квантових обчислень та перспективи розвитку. Переваги та недоліки квантових обчислень.

Фізичні основи квантових обчислень

Класичні та квантові системи та різниця між ними. Поняття стану квантової системи. Приклади квантових систем. Квантова суперпозиція. Приклади суперпозиції станів. Вплив вимірів на стан квантової системи. Простір станів, переплутані стани та їх властивості.

Перетворення інформації у квантових системах.

Поняття про кубіти, перетворення кубітів. Прості однокубітні логічні операції. Дво- та багатокубітні операції. Поняття про переплутування. Логічні елементи (гейти) CNOT, Тоффолі. Парадокс Ейнштейна-Подольскі-Розена. Нерівність Белла.

Розділ 2. Квантові алгоритми

Класичні та квантові алгоритми. Поняття про квантове прискорення обчислень. Квантові паралельні обчислення. Алгоритм Дойча. Квантова телепортація. Клонування квантового стану. Квантове перетворення Фур’є та його використання.

Розділ 3. Квантові криптографічні алгоритми

Алгоритм факторизації Шора та його застосування. Переваги квантової факторизації. Класичні та квантові алгоритми пошуку. Алгоритм Гровера пошуку у невпорядкованому масиві. Причини квантового прискорення алгоритму Гровера.

Квантові протоколи узгодження криптографічних ключів. Протокол BB84. Протокол B92. Протокол E91. Інші квантові протоколи узгодження ключа. Основні атаки на квантові протоколи узгодження ключа. Квантові гроші С.Віснера.

Розділ 4. Архітектура та основні вимоги до квантових комп’ютерів

Основні вимоги до квантових комп’ютерів. Квантові комп’ютери на іонах у пастках. Рідинні та твердотільні комп’ютери на ядерному магнітному резонансі. Квантові комп’ютери на квантових точках. Квантові комп’ютери з надпровідниковими елементами. Прототипи сучасних квантових комп’ютерів.

Розділ 5. Огляд фізичних реалізацій квантових комп’ютерів

Гармонічний осцилятор як модель квантового комп’ютера. Квантовий комп’ютер на

фотонах. Квантовий комп’ютер на оптичних резонаторах. Йони у пастках. Ядерний магнітний резонанс.

Зміст лабораторного практикуму

Знайомство з інструментами квантових розрахунків. Вибір та встановлення обраного інструментарію. Реалізація простих однокубітних обчислень. Реалізація багатокубітних обчислень. Реалізація алгоритму квантової телепортації. Реалізація алгоритму Дойча-Джози. Реалізація алгоритму Гровера. Реалізація алгоритму Шора. Квантове перетворення Фур’є.

Рекомендована література:

1. Крохмальський Т. Вступ до квантових обчислень. Навчальний посібник. - Львів: ЛНУ, 2018. - 204 с.
2. Химено-Сеговиа М., Хэрриган Н., Джонстон Э. Программирование квантовых компьютеров. - СПб: Питер, 2021. - 336 с.
3. Баумейстер Д., Экерт А., Цайлингер А. Физика квантовой информации. – М.:Постмаркет, 2002. – 376 с.
4. Фейнман Р., Лейтон Р., Сэндс М. Фейнмановские лекции по физике (в 9 томах), т.3,9. – М.:Мир, 1978.
5. Валиев К.А., Кокин А.А. Квантовые компьютеры: надежды и реальность. – Ижевск:РХД, 2001. – 352 с.
6. Ожигов Ю.И. Квантове вычисления. Учебно-методическое пособие. – М.:МГУ, 2003. – 104 с.
7. Китаев А., Шень А., Вялый М. Классические и квантове вычисления. – М.:МЦНМО, 1999. – 193 с.
8. Ожигов Ю.И. Алгоритмический поход к квантовой физике. – М.: МГУФТИ, 2004. – 48 с.
9. Рейффел Е., Полак У. Основы квантових вичислений. – М.:Мир, 2001. – 54 с.
10. Стин Р. Квантове вычисления. – Ижевск: НИЦ «Регулярная и хаотическая динамика», 2000. – 100 с.
11. Нильсен М., Чанг И. Квантовые вычисления и квантовая информация. - М.:Мир, 2006. - 824 с.

Розділ І. Фізичні основи квантових обчислень

Вступ

В електроніці відомий *закон Мура* [1], згідно якого кількість транзисторів на кристалі інтегральних схем подвоюється кожні 24 місяці (див. рис.1). Відповідно, зменшуються розміри цих транзисторів, вдосконалюється технологічний процес. Сьогодні налагоджене масове виробництво мікропроцесорів на основі 20-22-нанометрових технологічних процесів, будуються заводи (наприклад, Fab42, штат Аризона) для 14-нанометрових виробництв, розробляються основи 10-нанометрового процесу. Чи значить це, що обчислювальні потужності, які доступні людству, будуть зростати необмежено? На жаль, відповідь на це питання негативна. Справа в тому, що сучасна технологія вже дуже близько підібралася до розміру атомів речовини. Дійсно, зараз йдеться про 10-нанометровий технологічний процес, розмір елемента в якому (10 нм) усього в 100 разів більший за розмір атома (0.1 нм). Це означає, що кожен елемент транзистора, наприклад, затвор, буде складатися з ~100 атомів. А що далі? Відомо, що побудувати транзистор (та й будь-який інший елемент мікросхем) з одного атома неможливо.

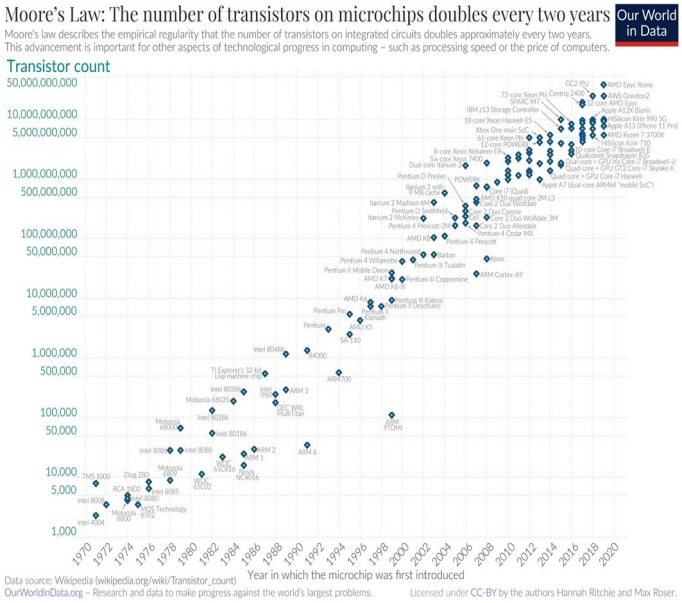


Рисунок 1: Закон Мура, який демонструє подвоєння кількості транзисторів у процесорах кожні 24 місяці

Однак, це ще не все. Сучасні комп’ютери використовують класичні алгоритми та способи збереження інформації. А ці методи для ряду дуже важливих задач вимагають астрономічних розмірів пам’яті і таких самих запасів часу. Наприклад, якщо ми хочемо з максимальною точністю змоделювати еволюцію молекули ДНК, що складається з кількох сотень мільярдів елементарних частинок, то ми повинні будемо керувати одночасно такою кількістю елементів пам’яті, що перевищує кількість елементарних частинок у Всесвіті. Так що навіть якщо би ми навчилися створювати транзистори з одного атома, ряд принципових задач однаково будуть недоступними для наших комп’ютерів. Ще один приклад. Вже зараз сучасні суперкомп’ютери, які моделюють ядерні вибухи, урагани та інші погодні явища, використовують 1,5-2 тисячі процесорів та терабайти оперативної пам’яті, споживаючи енергію, якою могли би користуватися жителі невеликого міста. Отже, необхідно змінювати принципи виконання обчислень.

Які тут можливі варіанти? Перший, який зараз досить успішно працює, це розпаралелювання обчислень. Сьогодні ми використовуємо багатоядерні процесори,

розподілені обчислювальні системи тощо. Однак, й тут існують принципові обмеження. Наприклад, відомий *закон Амдала* [2] стверджує, що час виконання обчислень паралельною системою не може бути меншим за час виконання найдовшого фрагменту коду.

Більше того, якщо подивитися на рисунок 2, який ілюструє закон Амдала, то можна побачити, що навіть якби ми розпаралелили 95% усього коду, ми не досягнемо більше як 20-разового прискорення обчислень.

Ще одним, правда тимчасовим фактором, який сповільнює прогрес швидкості обчислень, є те, що розробники сучасного програмного забезпечення не зовсім дбають про готовність своїх програм до паралельних обчислень. Свідченням цього можуть служити синтетичні тести процесорів, які час від часу виконують комп'ютерні журнали на кшталт iXBT. На рисунку 3 показано результати тестування процесорів 8-ядерного Core i7-5960X та 12-ядерного Xeon E5-4650 v3. З рисунку видно, що процесор з меншою кількістю ядер, але на вищій тактовій частоті виграє у багатоядерного Xeon.

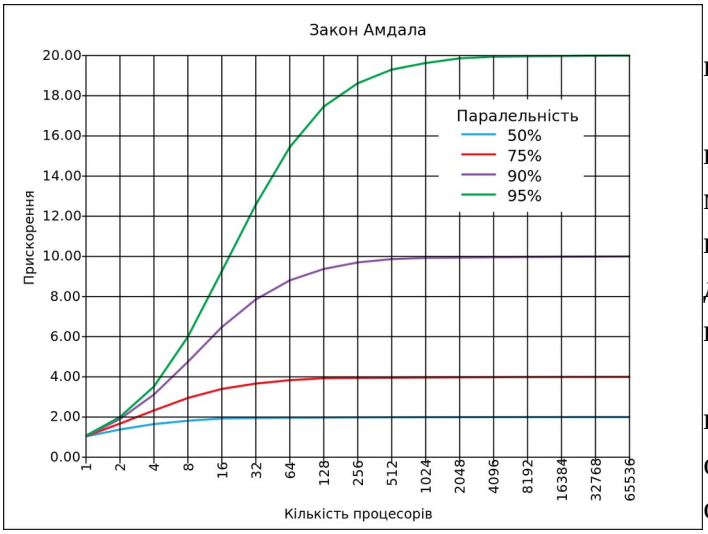


Рисунок 2: Ілюстрація закона Амдала

І знов ми повертаємось до часу виконання послідовних команд.

Іншим, досить перспективним, варіантом виходу з такого становища могло би бути використання принципів квантових обчислень, які, як ми побачимо далі, мають дивовижні властивості квантового прискорення.

Однак, не все так просто. По-перше, поки квантова система виконує обчислення, доступ до результатів обмежено. Ми не можемо зупинити систему, подивитись проміжні результати і продовжити обчислення. Таке принципово неможливо. По-друге, надзвичайні проблеми виникають сьогодні при практичній реалізації квантових комп'ютерів. І хоча тут досягнуто деяких важливих результатів, говорити про повний успіх в побудові квантових комп'ютерів зарано. Сьогодні існують лише окремі зразки частково-квантових обчислювальних систем *Orion*, які випускає канадська фірма D-Wave, але вони призначені лише для виконання окремих чітко визначених задач. Тим не менше, пригадаємо, що перші комп'ютери, ENIAC, EDVAC та інші також використовувалися лише для однієї задачі.

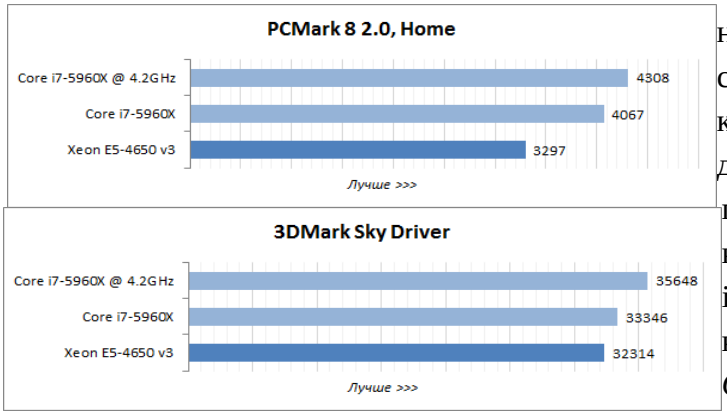


Рисунок 3: Результати тестування швидкодії процесорів Core i7 порівняно з Xeon E5

І усе ж таки, значні переваги квантових комп'ютерів та обчислювальних алгоритмів на основі квантової парадигми, змушують дослідників серйозно займатися цими новітніми

технологіями, які можуть спричинити чергову революцію в галузі інформаційних технологій.

Фізичні основи квантових обчислень

В 1890-х роках німецький фізик-теоретик Макс Планк вивчав випромінювання абсолютно чорного тіла. Його теоретичні розрахунки свідчили, що процес випромінювання відбувається не неперервно, а деякими порціями, енергію яких можна описати простою формулою: $E=h\nu$. Тут ν — частота хвилі, що випромінюється, а h — деяка постійна, $h=6{,}62\times10^{-34}$ Дж·с. Цю постійну пізніше назвали постійною Планка, а величину енергії, яку описує запропонована формула — квантом електромагнітної хвилі. Результати досліджень було опубліковано у статті, яка вийшла в друці 1900 року [3]. Таким чином, було доведено, що класичної фізики зовсім недостатньо для того, щоби описати явища мікросвіту. Більше того, мікросвіт, тобто світ елементарних частинок та окремих атомів не підкоряється законам класичної фізики. Це було першими кроками становлення нової фізичної теорії, яка отримала назву квантової механіки.

Таким чином, виходить, що світло поглинається та випромінюється порціями, квантами, які називаються фотонами, а одночасно поводить себе як хвиля, тобто виявляє властивості інтерференції та дифракції.

У 20-х роках XX сторіччя французький фізик-теоретик Луї де Бройль довів, що корпускулярно-хвильовий дуалізм (тобто явище, коли частинка, корпускула, поводить себе як хвиля) властивий усім іншим елементарним частинкам. Луї де Бройль увів поняття *хвилі де Бройля*, яка характеризує певну частинку: $\lambda = h/mv$, де λ — довжина хвилі; h — постійна Планка; m, v — маса та швидкість частинки [4]. Сьогодні, правда, поняття корпускулярно-хвильового дуалізму має лише історичне значення, оскільки в 1948 році воно було замінено Річардом Фейнманом описанням елементарних об’єктів за допомогою інтегралів по траєкторіях, що розв’язало проблему корпускулярно-хвильового дуалізму [5]. Тим не менше, для наших цілей це поняття досить корисне, тому ми будемо його використовувати.

Перелічені поняття є одними з основних у квантовій механіці, яка описує поведінку мікрооб’єктів. Ця поведінка настільки не схожа на таку класичних об’єктів, що до неї дуже важко звикнути. Більше того, коли стараннями Нільса Бора, Вернера Гейзенберга, Ервіна Шредінгера та багатьох інших фізиків було створено основи нової теорії, про яку Лев Ландау пізніше сказав, що “*... людина здатна зрозуміти ті речі, які вона вже не в змозі уявити*”, більшість фізиків не змогли її сприйняти. Серед них був і один з найвизначніших фізиків за всю історію науки, Альберт Ейнштейн, який якось відзначив, обговорюючи поняття квантової суперпозиції: “*...Бог не буде грати в кості...*”, вирішуючи яке значення надати змінній. Альберт Ейнштейн висунув уявний експеримент, який отримав назву парадоксу Ейнштейна-Подольскі-Розена, та досі не отримав однозначного пояснення. Цей парадокс ми розглянемо пізніше.

Рисунок 4: Чарлз Беннетт

Рисунок 5: Жіль Брассар

Трохи історії квантових обчислень

У 1970 році аспірант Колумбійського університету Стівен Візнер подав до журналу IEEE Information Theory статтю, але вона не була прийнята до публікації оскільки редакція вважала ідеї, висунуті автором, антинауковими. Крім того, технологічний рівень тих років не дозволяв навіть мріяти про такий рівень захисту. І тільки 1983 року робота Візнера “Conjugate coding” була опублікована в журналі SIGACT News та отримала високу оцінку в наукових колах [6].

Рисунок 6: Ескіз банкноти за С.Візнером

Суть ідеї С.Візнера полягає в тому, що кожна грошова банкнота повинна мати 20 “світлових пасток”, в кожній з яких розміщено по однму фотону з строго визначеним станом поляризації, як це показано на рис. 4. Така банкнота маркувалася би спеціальним серійним номером, який би містив деяку інформацію про напрями поляризації кожного фотона. Оскільки фальшивомонетник не знає, яку комбінацію фільтрів було застосовано для запису в пастки, він не зможе правильно зчитати інформацію в пастках, і тим більше, повторити таку комбінацію на фальшивій банкноті. Банк навпаки, зберігає цю послідовність у сховищі, і в будь-який час може перевірити коректність квантового запису на банкноті. Концепція С. Візнера довгий час була (та й зараз лишається) чисто теоретичною, оскільки створити пастки для тривалого зберігання квантового стану не вдається. Сьогодні можуть зберігати квантові частинки у стані суперпозиції на протязі секунд, що надзвичайно мало для такої задачі.

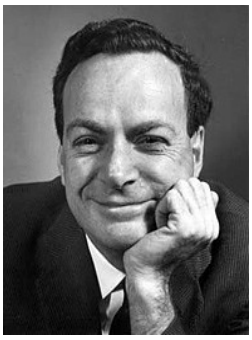


Рисунок 7: Річард Фейнман

Тим не менше, робота С.Візнера була однією з перших, яка мала відношення до захисту інформації з використанням квантових уявлень.

У 1981 році лауреат Нобелівської премії 1965 року, визначний фізик-теоретик Річард Фейнман на Першому конгресі по обчисленнях, який проходив у Масачусетському технологічному інституті, вперше запропонував використовувати способи обчислень на основі уявлень квантової механіки для моделювання квантових систем [7].

У тому ж році професор Массачусетського технологічного інституту Томмазо Тоффолі запропонував квантовий вентиль Тоффолі, який використовується й сьогодні для побудови квантової логіки [8]. У 1982 році В.Вуттерсом, В.Зуреком та Д.Діксом було висунуто так звану “теорему про заборону клонування” у квантових обчисленнях, яка доводить, що невідомий квантовий стан частинки неможливо скопіювати, не зруйнувавши самий стан [9].

Приблизно в ті ж роки дослідники почали розробляти принципи квантового зв’язку та квантові протоколи передавання даних. Звичайно, до їхньої практичної реалізації було ще далеко, але основи закладалися саме тоді. Наприклад, у 1984 році було запропоновано перший квантовий протокол узгодження криптографічного ключа, який отримав назву BB84 за першими літерами розробників, Чарлза Беннетта з дослідницької лабораторії IBM та Жіля

Брассара з університету Монреаля [10]. Сьогодні цей та інші квантові протоколи узгодження криптографічного ключа разом з потоковими шифрами складають основу квантової криптографії. Ч.Беннетт та С.Візнер у 1992 році запропонували також принципи квантового надщільного кодування, - один з перших квантових протоколів, який надає можливість вибору однієї з чотирьох альтернатив за допомогою передавання одного кубіта [11]. У цьому ж році Чарлз Беннетт розробив модифікований протокол квантового узгодження ключа BB84, який отримав назву B92 [12]. Цей рік був дуже плодотворним для квантової інформатики: Девід Дойч також запропонував алгоритм, який вперше продемонстрував квантове прискорення обчислень [13].

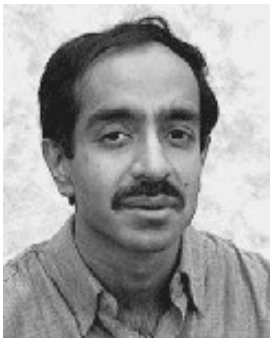


Рисунок 8: Лов Гровер

Оскільки існує квантова теорема про заборону клонування, дослідникам необхідно було розробити альтернативний метод перенесення невідомого квантового стану, оскільки без таких операцій створення обчислювальної техніки неможливе. У 1993 році Ч.Беннетт та Ж.Брассар запропонували зовсім нову концепцію, яка отримала назву квантової телепортації [14]. Розроблений протокол дозволяє перенести невідомий квантовий стан на новий квантовий об’єкт, тоді як квантовий стан оригіналу, тобто об’єкта, стан якого переносився, повністю руйнувався. Цей процес не має нічого спільного з телепортацією реальних об’єктів у творах фантастів, оскільки йдеться не про фізичний об’єкт, а про його квантовий стан. Квантову телепортацію сьогодні успішно реалізовано на відміну від “фантастичної” телепортації.

Рисунок 9: Пітер Шор

Настала черга складніших алгоритмів, які безпосередньо впливають на стан сучасної криптографічної науки. Зокрема, алгоритм, розроблений американським математиком Пітером Шором у 1994 році, дозволяє факторизувати великі цілі числа майже за той самий час, який потрібен для їх множення [15]. Зрозуміло, що після розробки цього алгоритму усі існуючі асиметричні криптоалгоритми незалежно від того, на якій математичній проблемі ґрунтується їх криптостійкість, можна вважати скомпрометованими. Це знайшло своє відображення у документах, випущених Національним інститутом стандартів і технологій США у квітні 2016 року (NISTIR 8105 Draft Report), де вважається, що асиметрична криптографія в тому вигляді, як вона застосовується зараз, не повинна більше використовуватися [16].

Через рік, у 1996 році, американський математик індійського походження, Лов Гровер, запропонував алгоритм швидкого пошуку у невпорядкованому масиві, який легко можна застосувати для пошуку криптографічного ключа будь-якого симетричного криптоалгоритму [17]. Тут важливий саме невпорядкований масив, оскільки у впорядкованому ефективний пошук організувати легше класичними алгоритмами, наприклад, методом дихотомії. За оцінками фахівців, існування цього алгоритму змушує збільшити довжину ключа симетричних алгоритмів у 2-3 рази.

Коротко подамо досягнення у технічній реалізації квантових алгоритмів та протоколів:

- у 1997 році групами фізиків під керівництвом Антона Цайлінгера (Інсбрук, Австрія) та Франческо де Мартіні (Рим, Італія) було реалізовано протокол квантової

телепортації стану одного квантового біту на відстань 1 метра. У 2012 році відстань, на яку телепортували квантовий стан, досягла вже 143 км;

- у 2001 році спеціалістами IBM реалізовано алгоритм П.Шора на прототипі квантового комп’ютера. Було розкладено число 15 на прості множники, 3 та 5.
- 2005 рік – в Японії продемонстровано програмований квантовий комп’ютер на основі квантового оперативного запам’ятовуючого пристрою з двох квантових бітів.
- 2009 рік – такий же за параметрами квантовий комп’ютер продемонструвало Агентство національної безпеки США.
- 2012 рік – спільнота з чотирьох американських університетів, Південно-Каліфорнійського, Каліфорнійського в Санта-Барбарі, технологічного університету Дельфта та університету штату Айова, реалізувала квантовий комп’ютер з двобітовим оперативним запам’ятовуючим пристроєм, який працює при кімнатних температурах. Пристрій складався з квантових комірок пам’яті – кристалів алмазу з домішками азоту. Повідомляють, що було реалізовано на такому комп’ютері алгоритм Гровера.

Рисунок 10: Квантовий комп'ютер D-Wave One

Окремим рядком в історії квантових обчислень стоїть канадська компанія D-Wave. У лютому 2007 року керівництвом цієї компанії було оголошено про реалізацію квантового комп’ютера з шістнадцятибітовим процесором (назва комп’ютера — *Orion*). В листопаді 2007 році, буквально через півроку після *Orion*’у було продемонстровано роботу прототипу 28-бітового квантового комп’ютера *Leda* на конференції, присвяченій суперкомп’ютерам, а вже у грудні 2009 року науковий співробітник Google Хартмут Невен продемонстрував на комп’ютері D-Wave роботу програми розпізнавання образів. У травні 2011 року компанія випустила квантовий комп’ютер *D-Wave One* с 128-кубітовим процесором. Планується створення комп’ютера з 1024-кубітовим процесором.

Зараз компанія D-Wave успішно випускає квантові комп’ютери “під замовлення”. Сьогодні це обчислювальні системи, орієнтовані під конкретну задачу, які працюють під глибоким охолодженням (див. рис.10). Вартість таких систем становить приблизно $10 млн. долларів США, отже дозволити собі такий комп’ютер можуть лише окремі транснаціональні корпорації. Серед них — Google, який експериментує з розпізнаванням образів за допомогою квантового комп’ютера; Martin-Lockheed, яка використовує квантовий комп’ютер для аналізу критичного програмного забезпечення свого винищувача-бомбардувальника F-35.

Квантові комп’ютери можуть застосовуватись для моделювання ураганів та інших кліматичних явищ, аналізу ДНК та складних ліків, аналізу складних криптоалгоритмів та інших задач, які не під силу класичним комп’ютерним системам, навіть розподіленим.

Тим не менше, компанія дуже довго знаходилася під вогнем критики з боку експертів у галузі квантових обчислень. Справа в тому, що інженери D-Wave ніколи не демонстрували свої комп’ютери світовій спільноті. Компанія продавала лише машинний час, відповідаючи

відмовою на вимоги науковців дозволити дослідити роботу цих комп’ютерів. Відповідно, у науковців виникли підозри про те, чи насправді компанія D-Wave розробила комп’ютер, що задовольняє усі вимоги до квантових обчислювальних систем. Основною вимогою є те, що під час обчислень основні вузли комп’ютера повинні знаходитися у стані квантової суперпозиції.

І лише в травні 2013 року компанія запросила канадського професора Кетрін МакГ’ю для порівняльних тестів швидкодії квантового комп’ютера *D-Wave One* на процесорі *Vesuvius* з тодішнім флагманом фірми Intel, *Core i*7. Оскільки *D-Wave One* був спеціально спроектований для розв’язку задач дискретної оптимізації, тести проводили саме на них. В цих задачах *D-Wave One* виконав тести у 3600 разів швидше за свого конкурента. Прискорення обчислень на інших задачах було незначним. І нарешті, в січні 2014 року інженери D-Wave експериментально довели існування квантової суперпозиції в процесорі під час обчислень, для чого використали кубітову тунельну спектроскопію, що було підтверджено інженерами Google, які виявили, що у 1000-кубітовому комп’ютері D-Wave, який вони використовували, кубіти дійсно організовані у кластери по вісім кубітів. Це дозволило досягти зростання швидкодії до 100 млн разів в одному з алгоритмів порівняно зі звичайним комп’ютером.

У вересні 2016 року на конференції у Сан-Франциско компанія показала свій новий комп’ютер *D-Wave 2X*, який містить 2000 кубітів. Як і раніше, він оптимізований для виконання задач дискретної оптимізації [18].

Таким чином, можна стверджувати, що наприкінці XX сторіччя на основі розвитку квантової механіки, теорії алгоритмів та теорії інформації було створено **новий розділ науки: квантову інформатику**, яка вивчає загальні принципи та закони, що керують динамікою складних квантових систем. Моделлю таких систем є **квантовий комп’ютер**. Сьогодні концептуальна математична та алгоритмічна бази квантової інформатики створена й успішно розвивається. Що стосується повноцінного універсального квантового комп’ютера, то вважається, що його ще не створено. Існують лише квантові комп’ютери, розроблені та оптимізовані для окремих задач. Таку ситуацію людство вже проходило зі звичайними класичними комп’ютерами у 40-х-50-х роках XX сторіччя, коли вони виконували лише одну задачу, для якої їх було розроблено.

Можна очікувати створення універсального квантового програмованого комп’ютера найближчим часом.

Дослід з “кулеметом”

Згадані алгоритми та протоколи квантових обчислень ми розглянемо пізніше. Зараз же опишемо кілька простих прикладів, що дозволять нам частково зрозуміти дивну поведінку квантових об’єктів, яку абсолютно неможливо пояснити класичним чином. Явище квантової суперпозиції, яке нам дуже потрібне надалі, містить саму суть квантової механіки. Однак, ми досі не можемо його однозначно пояснити, тобто не можемо відповісти на питання: “Чому це так?”. Просто розповімо про те, як воно працює [19].

Спочатку розглянемо пристрій, схожий на кулемет. Це поганий кулемет. “Кулі”, що він випускає, дуже сильно розсіюються.

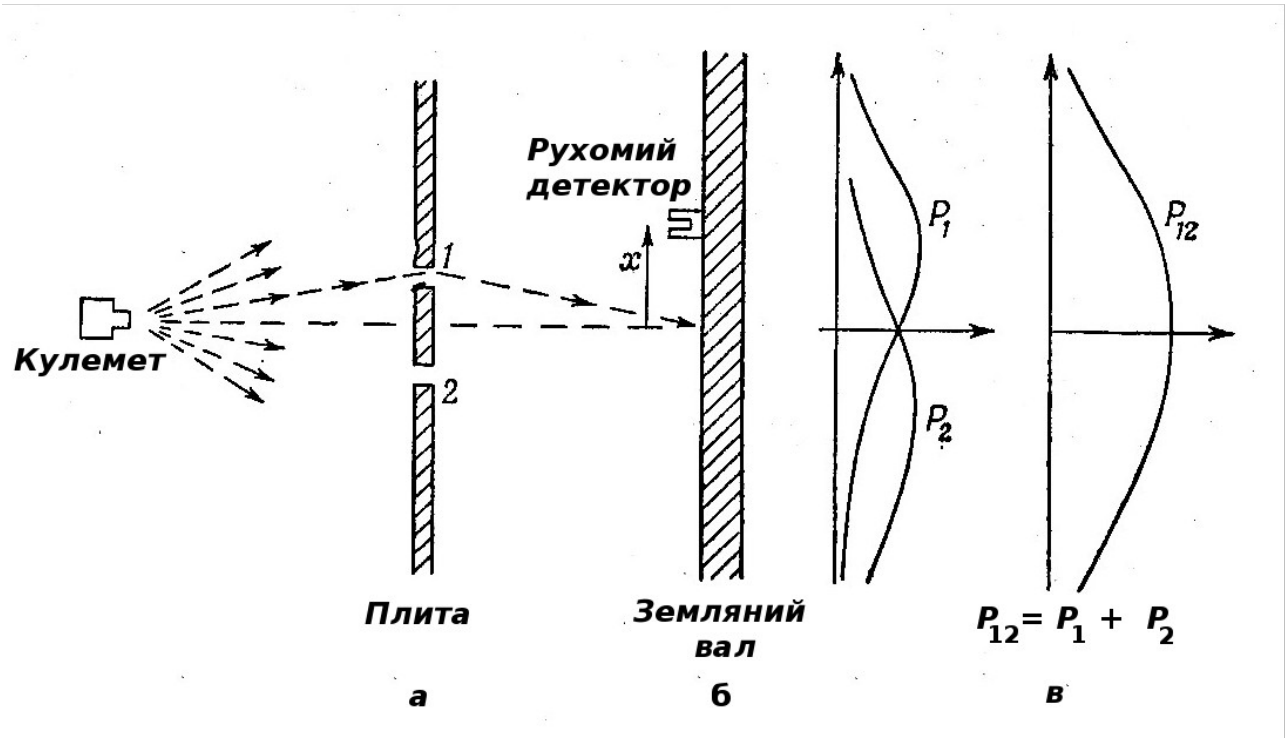


Рисунок 11: Ілюстрація до досліду з "кулеметом": а — схема “установки”; б — ймовірність “влучання” від кожної щілини; в — ймовірність “влучання від обох щілин

Перед кулеметом розташована броньова плита, а в ній є два отвори, 1 і 2, крізь які кулі проходять вільно. За плитою знаходиться земляний вал, куди влучають кулі, що пройшли крізь отвори. Перед земляним валом рухається “детектор”, наприклад, скриня з піском. Будь-яка куля, що влучає в “детектор”, лишається в ньому. Коли дослід закінчено, скриню відкривають та рахують кулі, що влучили у нього. “Детектор” рухається в обох напрямках вісі x і дозволяє відповісти на питання: “Яка ймовірність того, що куля, що пройшла крізь плиту, влучить у земляний вал на відстані x від центру?” Відзначу, що ми говоримо лише про ймовірність, тому що неможливо знати наперед, куди влучить куля. Цю ймовірність можна обчислити, підрахувавши, скільки куль влучило в “детектор” за певний проміжок часу, а потім розділити це число на загальну кількість куль, що влучали у земляний вал за цей же проміжок часу. Якщо швидкість стрільби на протязі експерименту не змінювалася, можна вважати ймовірність пропорційною кількості куль, що влучили у “детектор” за певний час.

Ми будемо вважати, що кулі влучають лише цілими. Не буває половинок куль або четвертих частинок. Це означає, що кулі “приходять” лиш дискретними однаковими порціями, по одній штуці. Навіть якщо швидкість стрільби стає дуже малою, в детекторі завжди знаходиться ціла кількість куль. Розмір порції не залежить від швидкості стрільби.

Результати такого уявного експерименту подані на рисунку 11в. Ми позначили ймовірність влучання кулі у детектор через P_{12}, щоби підкреслити, що вони можуть проходити і крізь перший отвір, і крізь другий. Очевидно, що ймовірність у центрі графіку буде більшою, а по його краях — меншою. Тим не менше, не так очевидно, що максимум ймовірності повинен бути при x=0, тобто у самому центрі графіку.

Це можна легко зрозуміти, якщо повторити дослід, закривши отвори 1 або 2. У першому випадку ми отримаємо криву P_2, а в другому - P_1 (рис.11б). Максимуми цих кривих, як і слід було чекати, розташовані просто навпроти відкритого отвору. Якщо порівняти рисунки 11б та 11в, то стає зрозумілим, що у випадку двох відкритих отворів, ймовірності P_1 та P_2 просто додаються, утворюючи максимум рівно в початку координат x=0, тобто: $P_{12}=P_1+P_2$. Такий результат ми назвем “відсутністю інтерференції” з причин, про які ви дізнаєтеся пізніше. На цьому ми закінчимо експеримент з “кулеметом”, сформулювавши такі висновки:

- Кулі прибувають лише цілими, «квантуються»; не буває 1,5 або 0,25 кулі.
- Закриваючи отвори, ми отримали відповідні ймовірності P_1 або P_2.
- Якщо обидва отвори відкрито, то загальна ймовірність $P_{12} = P_1 + P_2$.
- Інтерференція відсутня.

Такі висновки абсолютно традиційні для макроскопічних об’єктів, що й не дивно, оскільки кулі і є макроскопічними об’єктами.

Дослід з хвилями

Розглянемо аналогічний дослід з хвилями на воді, схема якого подана на рисунку 12.

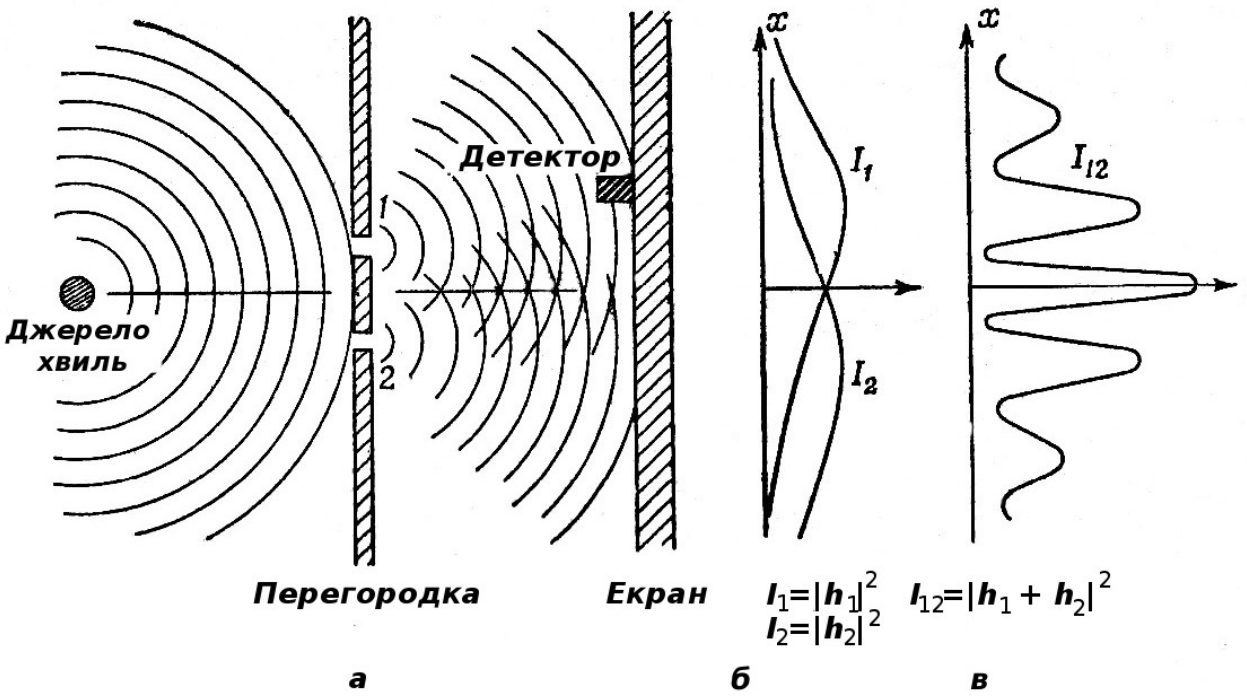


Рисунок 12: Ілюстрація досліду з хвилями на воді: а - схема установки; б - інтенсивність від кожної щілини; в - інтерференція хвиль від двох щілин

Устаткування являє собою мілку посудину, заповнену водою. Предмет, позначений як “Джерело хвиль”, коливаючись за допомогою маленького моторчика вгору-вниз, викликає кругові хвилі. Перегородка затримує хвилі, однак має два отвори, які, згідно з принципом Френеля, є джерелами вторинних хвиль, які досягають екрану та взаємодіють там, викликаючи картину, зображену на рисунку 12*б* та 12*в*. Перед екраном, як і в першому досліді, розміщено рухомий детектор. Якщо його “шкалу” відкалібрувати пропорційно квадрату висоти хвилі *h*, то відлік буде показувати інтенсивність хвилі. Таким чином, детектор буде вимірювати енергію, що її переносить хвиля, або, що точніше, ту частину енергії, яку передано саме детектору.

Перше, що можна стверджувати за допомогою такого хвилевого апарата, це те, що інтенсивність хвиль може бути довільною. Коли джерело рухається поволі, і детектор демонструє ледве помітний рух. Якщо інтенсивність руху джерела зростає, детектор показує більшу інтенсивність. Оскільки інтенсивність може бути будь-якою, ми вже не можемо стверджувати, що вона має хоча б якусь “порціонність”, квантується.

Давайте тепер змусимо джерело хвиль працювати стабільно та будемо вимірювати інтенсивність хвиль для різних значень координати *x*. Ми отримаємо таку криву, яку подано на рисунку 12*в*.

Як бачимо, хвилі взаємодіють між собою і, як це відомо зі шкільного курсу фізики, утворюють так звану інтерференційну картину. Саме таку картину у вигляді райдужних

кілець ми бачимо на поверхні калюж, куди розлито трохи бензину або олії. Зрозуміло, що первинна хвиля від джерела дифрагує на отворах 1 та 2, в результаті чого ми маємо дві когерентні вторинні хвилі, які й утворюють інтерференційну картину. Це типовий результат для хвильових процесів, чи то електромагнітних, чи механічних хвиль.

Тепер, якщо ми будемо закривати отвори по черзі, то отримаємо криві інтенсивності I_1 та I_2, зображені на рисунку 12*б*. Очевидно, що сумарна інтенсивність, I_{12} не дорівнює сумі інтенсивностей від кожної щілини, I_1+I_2. В цьому й полягає суть явища інтерференції. На деяких ділянках (де спостерігаються максимуми графіка I_{12}) хвиля від одного отвору підсилює хвилю від другого. Утворюється так звана конструктивна інтерференція, забезпечуючи більшу інтенсивність. Це буває тоді, коли окремі хвилі приходять до деякої точки “у фазі”, тобто відстань від цієї точки до однієї з щілин більше (або менше) відстані до другої на ціле число довжин хвилі. Якщо ж різниця відстаней певної точки екрану до кожної зі щілин кратна не цілому числу довжин хвилі, виникає “деструктивна інтерференція”, тобто загальна інтенсивність зменшується. У цих точках можна побачити мінімуми кривої I_{12}.

Якщо згадати шкільну фізику, ми зможемо записати, що наш хвильовий процес можна описати такою формулою:

$$H_1=h_1 e^{i\omega t};H_2=h_2 e^{i\omega t},$$

де $H_{1,2}$ — миттєва висота хвилі, t — час, ω — частота коливань.

Якщо відкриті обидві щілини, тоді будемо мати:

$$H_{12}=(h_1+h_2)e^{i\omega t},$$

що символізує той факт, що загальна висота хвилі є сумою висот хвиль від окремих щілин.

Відомо, що інтенсивність пропорційна квадрату висоти хвилі, тобто:

$$I_1=|h_1|^2;I_2=|h_2|^2;I_{12}=|h_1+h_2|^2.$$

Як бачимо, нічого спільного з тим, що було з кулями, не відбувається. Якщо ми розкриємо модуль $|h_1+h_2|^2$, отримаємо:

$$I_{12}=|h_1|^2+|h_2|^2+2|h_1||h_2|\cos(\delta),$$

де δ — різниця фаз між h_1 та h_2. Уводячи інтенсивності, можемо отримати:

$$I_{12}=I_1+I_2+2\sqrt{I_1 I_2}\cos(\delta).$$

Як бачимо, останній вираз суттєво відрізняється від випадку кулемета. Останній доданок цієї формули — так званий “інтерференційний доданок”, якого немає у випадку класичних об’єктів.

На цьому ми закінчимо приклад з хвилями, зробивши такі висновки:

- інтенсивність хвиль може бути довільною — “квантування” у цьому випадку не існує;

- закриваючи отвори почергово, ми отримали інтенсивності хвиль I_1 та I_2;
- якщо обидва отвори відкрито, маємо загальну інтенсивність $I_{12} \neq I_1 + I_2$;
- спостерігається явище інтерференції хвиль.

Такі висновки характерні для хвильових процесів.

Дослід з електронами

І, нарешті, розглянемо ще один дослід, схему якого подано на рисунку 13.

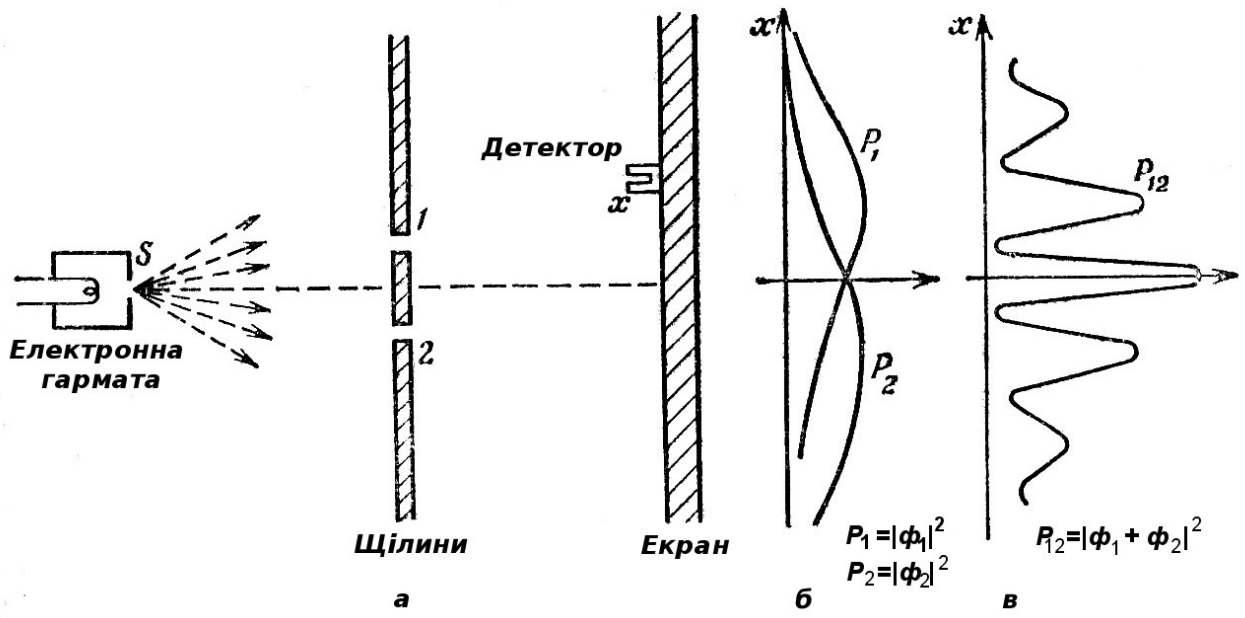


Рисунок 13: Ілюстрація досліду з електронами: а - схема "установки"; б - інтенсивність від кожної щілини; в - інтенсивність від обох щілин

Цей уявний експеримент виконується з електронами, які генерує електронна гармата. Найпростіша за конструкцією електронна гармата складається з вольфрамового дроту, розміщеного у металічній коробочці з отвором. Дріт нагрівається електричним струмом. Якщо на нього подати негативний потенціал, а на коробочку — додатній, то електрони, що їх випромінює дріт, будуть розганятися різницею потенціалів, і деякі з них вискочать назовні крізь отвір. Такі електрони будуть мати приблизно однакову енергію. Перед гарматою розміщено металічний екран з двома щілинами, а за ним — ще один екран, який поглинає електрони. Перед поглинаючим екраном розташовано рухомий детектор електронів, скажімо лічильник Гейгера.

Увімкнувши наше обладнання, ми почуємо клацання детектора. Усі сигнали однакові за інтенсивністю. Не буває слабших або сильніших сигналів. Сигнали можуть бути частішими або рідшими, але завжди однаковими за інтенсивністю (гучністю). Коли процес генерування електронів стабілізується, ми зможемо побачити, що кількість зареєстрованих лічильником Гейгера електронів за однакові проміжки часу буд майже однаковою. Тому можна говорити про середню частоту клацань детектора, тобто певну кількість клацань, скажімо, на хвилину в середньому.

Якщо ми пересуваємо детектор по вісі *x*, частота клацань змінюється, але величина (гучність) кожного клацання лишається постійною. Якщо би ми розмістили перед поглинаючим екраном другий детектор (в іншому місці, звичайно), ми би почули, що клацає то один детектор, то другий, і ніколи обидва разом (хіба що іноді наше вухо не в змозі розрізнити два клацання підряд). Тому ми можемо зробити висновок про те, що електрони, як кулі в першому досліді, приходять “порціями”. Усі “порції” однакові за величиною, в детектор або в поглинаючий екран влучає лише одна “порція”. Тоді ми говоримо: “Електрони завжди приходять однаковими порціями”.

Як і в досліді з кулеметом, спробуємо знайти відповідь на питання: “Яка відносна ймовірність того, що електрон влучить у поглинаючий екран на різних віддалях від середини?”. Ми можемо отримати відповідь на це питання, підрахувавши частоту клацань лічильника під час стабільної роботи електронної гармати.

В результаті нашого уявного експерименту отримана дуже цікава крива, яка подана на рисунку 13*в*. Слід відзначити, що саме так і поводять себе електрони в умовах реального експерименту.

Спробуємо пояснити таку дивну поведінку електронів. Оскільки ці електрони, як ми бачили, приходять “порціями”, тобто квантуються, то кожен з них проходить або крізь отвір 1, або крізь отвір 2. Тоді усі електрони, які влучили у поглинаючий екран, можна розділити на два класи: ті, що пройшли крізь перший отвір, і ті, що пройшли через другий. Це значить, що крива 13*в* — це сума ефектів від електронів, які пройшли крізь різні отвори. Тепер закриємо отвір 2 і будемо вивчати тільки електрони, що пройшли крізь отвір 1. Результат таких вимірів подано на рисунку 13*б*, крива P_1. Там же подано результати для отвору 2, - крива P_2. Вони виглядають звичним чином.

Крива P_{12}, яку отримано, коли обидва отвори відкрито, зовсім не узгоджується з сумою P_1+P_2. Очевидно, що вона аналогічна до такої в досліді з хвилями. Отже, ми чомусь бачимо інтерференційну картину. Звідки вона взялася? Що з чим тут взаємодіє, щоби дати таку картину? Може, взаємодіють електрони, що пройшли крізь різні отвори? Але як це можливо, якщо вони “прибувають” до екрану дискретно і у різний час? Може вони рухаються складніше, проходячи спочатку через один отвір, а потім — через другий? Але тоді, закривши один отвір, ми маємо зменшити кількість електронів, що досягли екрану. Тим не менше, ми бачимо на кривій 13*б* точки, де кількість електронів більша за таку, коли відкрито обидва отвори. Виходить, що закриття одного отвору збільшує кількість електронів, що проходить крізь другий. І навпаки, середній пік кривої P_{12} більш, ніж удвічі вища за суму значень кривих P_1 та P_2. Очевидно, що цих два факти протирічать один одному! Пояснити обидва факти з точки зору складних траєкторій рух електронів неможливо. В усякому разі досі нікому це не вдалося зробити.

При всьому цьому, як не дивно, математика, що описує зв’язок P_{12}, P_1 та P_2 зовсім проста. Вона дуже схожа на ту, яка описувала дослід з хвилями. Такий результат не вдається отримати, якщо вважати, що електрони рухаються по складних траєкторіях.

Отже, у нас немає іншого виходу, як визнати: електрони прибувають “порціями”, тобто виявляють при цьому властивості частинок (корпускул), а ймовірність їх влучання в екран розподіляється так само, як інтенсивність хвиль. Саме в такому розумінні електрон поводить себе частково як частинка, частково як хвиля.

А як тепер бути з твердженням, що крива P_{12}, є сумарний ефект від електронів, які пройшли крізь отвір 1 і крізь отвір 2? Ми бачимо, що $P_{12} \neq P_1+P_2$. Очевидно, твердження про те, що електрони проходять або крізь отвір 1, або крізь отвір 2, неправильне.

Так як же вони проходять?

Спробуємо модифікувати наш уявний експеримент. Відомо, що електрони добре взаємодіють зі світлом. Схема такого експерименту подана на рисунку 14. Якщо ми візьмемо деяке джерело світла і розмістимо його на шляху електронів, то за спалахами світла, наприклад, біля отвору 1 (чи 2) ми будемо знати,через який з них пройшов черговий електрон. А якщо ми побачимо спалах світла біля обох отворів, це буде свідчити, що ми невірно уявляємо собі реальність мікросвіту.

Запустивши устаткування, прослідкуємо, що відбувається з електронами. Щоразу, коли ми чуємо клацання детектора, ми бачимо спалах або біля першого, або біля другого отвору, але ніколи біля обох одразу. Так відбувається при будь-якому положенні детектора. Звідси можна зробити висновок про те, що коли ми спостерігаємо за електроном, він з необхідністю проходить лише через один отвір: або через перший, або через другий. Продовживши спостереження, побачимо, що цього разу ми отримаємо ймовірність від двох щілин точно таку ж, як і в досліді з “кулеметом”, тобто $P'_{12}=P'_1+P'_2$. Чому ж тоді в попередньому експерименті ми отримали $P_{12} \neq P_1+P_2$? В чому різниця між експериментами? Єдина різниця полягає в тому, що в модифікованому експерименті ми спостерігали за електронами. Ну, що ж, цей результат можна зрозуміти: електрони настільки тендітна річ, що ми своїм джерелом світла збурюємо електрони, змінюючи їхню поведінку.

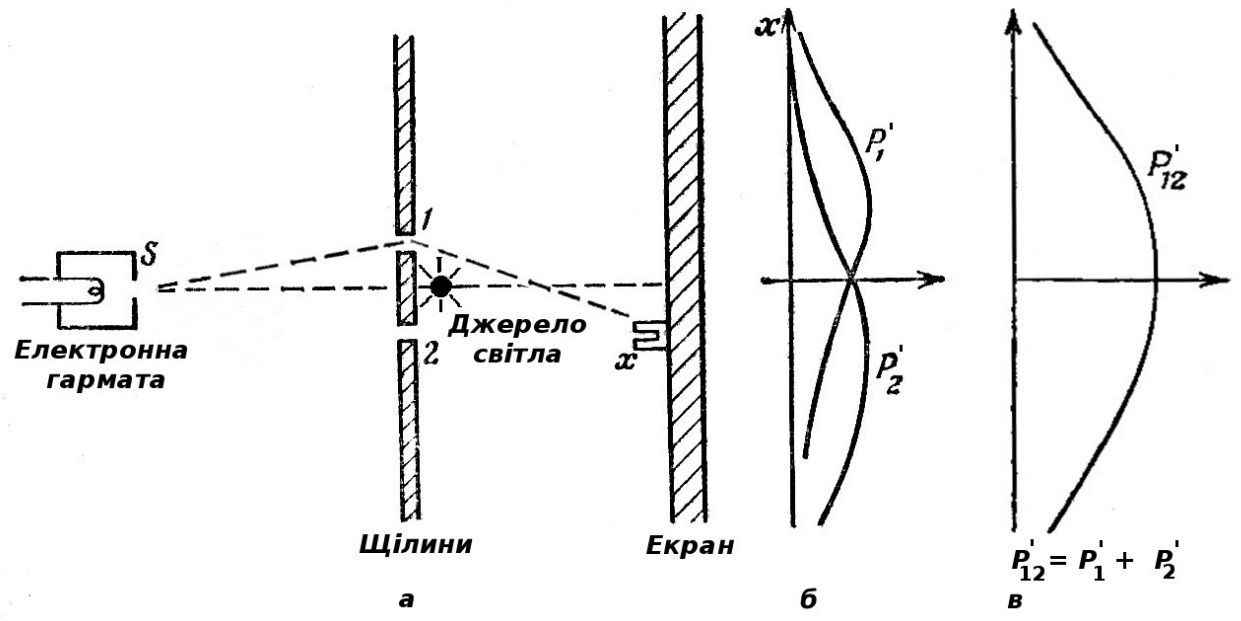


Рисунок 14: Ілюстрація модифікованого досліду з електронами

Перевіримо це. Будемо зменшувати яскравість джерела світла, і ми не будемо надавати електронам такого збурення, щоби впливати на їхню поведінку. Перше, що ми відзначимо, це те, що яскравість спалаху при взаємодії світла з електроном не зменшується. Це й зрозуміло, оскільки світло — це потік фотонів. При зменшенні яскравості світла параметри самих фотонів не змінюється, а лише зменшується їх кількість у потоці. Зменшуючи яскравість, ми, нарешті, прийдемо до такої ситуації, що фотонів для взаємодії з електронами не буде ставати, і ми будемо пропускати електрони, тобто, лічильник клацнув, зафіксувавши електрон, але ми не побачили спалаху, бо на тому місці, де перебував електрон, в той час не було фотона. Таким чином, у нас буде вже три типи електронів: ті, що пройшли крізь перший отвір, ті, що крізь другий, і ті, яких ми не побачили. І саме тоді явище інтерференції знову з'являється!

Ну, що ж, це вже можна пояснити. Коли ми не побачили електрон, фотон не збурив його; а якщо ми його помітили, — то фотон провзаємодіяв з електроном, змінивши його енергію якимось чином. Оскільки фотони усі однакові, значить ступінь збурення електрона завжди одна й та ж, достатня для того, щоби зруйнувати явище інтерференції.

Якщо ми міркуємо правильно, то існує ще один можливий спосіб "неруйнуючого" спостереження за електронами. Якщо взаємодія фотона з електроном, як це описується у фізиці, супроводжується передаванням електрону імпульсу фотона ($p=h/\lambda$), очевидно, що чим більша довжина хвилі, тим менший імпульс ми йому передамо. Для цього треба подіяти світлом червоного (може, навіть, інфрачервоного) діапазону.

Якщо ми будемо модифікувати дослід у такий спосіб, побачимо наступну картину. При збільшенні довжини хвилі спочатку нічого не зміниться. Однак, потім трапиться дуже неприємна річ: як тільки довжина світла стане порядку віддалі між щілинами, спалахи стануть такими розмитими, що ми не зможемо визначити, біля якої з них він відбувся. Бачимо, що електрон проскочив, а крізь яку щілину — не зрозуміло. І знову, саме в цей момент, коли почнуть з'являтися "невраховані" електрони, крива P_{12} продемонструє появу інтерференції! При подальшому збільшенні довжини хвилі інтерференція стане все помітнішою, і нарешті, коли довжина хвилі буде набагато більшою за відстань між щілинами, і вже зовсім незрозуміло де відбувся спалах, картина інтерференції стане подібною на таку, подану на рисунку 13*в*.

Як з'ясувалося в роки становлення квантово механіки, така поведінка мікрооб'єктів була помічена в багатьох експериментах. Вернер Гейзенберг припустив, що закони мікросвіту та макросвіту можна було би узгодити, якщо вважати, що існують деякі фундаментальні обмеження наших експериментальних можливостей, яких раніше не помічали. Він запропонував як загальний принцип так званий принцип невизначеності Гейзенберга. Цей принцип звучить так: "*Принципово неможливо одночасно виміряти з довільною точністю координати й імпульси квантового об'єкта*". У термінах нашого експерименту він звучить трохи інакше: "*Неможливо створити устаткування для визначення того, через яку щілину пройшов електрон, не збурюючи його настільки, що інтерференційна картина зникає*". Якщо устаткування здатне визначити, крізь яку щілину пройшов електрон, воно не здатне бути настільки делікатним, щоби не спотворити картину інтерференції. Жодній людині ніколи не вдавалося винайти устаткування, чи просто вказати спосіб, як обійти принцип невизначеності. Тому ми зобов'язані припустити, що він відображає одну з фундаментальних властивостей природи.

Принцип невизначеності Гейзенберга надає нам єдиний спосіб, за допомогою якого ми повинні розмірковувати, щоби не зробити помилкових передбачень. Цей спосіб полягає в тому, що якщо у нас є прилад, здатний визначити, крізь яку щілину пройшов електрон, ми можемо говорити про те, пройшов він крізь першу (або другу). Але якщо ви не намагалися дізнатися де пройшов електрон, то ви не можете навіть думати про те, чи електрон пройшов крізь першу, чи крізь другу щілину. Якщо ж почати розмірковувати на цю тему, а потім робити з цього якісь припущення, можна прийти до протиріч та помилкових фізичних висновків. Отже ми повинні балансувати на цьому логічному лезі, щоби успішно описувати явища мікросвіту.

Якщо рух усієї речовини подібний до руху електронів в нашому уявному експерименті, і його можна описувати за допомогою хвилевих понять, то як бути з кулями в нашому першому експерименті? Чому там ми не побачили інтерференційної картини? Спробуємо це пояснити.

Хвиля де Бройля визначається з виразу: $\lambda = h/mv = 6.62 \times 10^{-34}/mv$. Припустимо, що швидкість кулі та електрона однакова — 1000 м/с. Тоді отримаємо довжину хвилі де Бройля:

- Для електрона: $\lambda = 6.62 \times 10^{-34}/9.1 \times 10^{-31} \times 10^{3} \approx 0.7$ м;
- Для «кулі»: $\lambda = 6.62 \times 10^{-34}/10^{-2} * 10^{3} \approx 7 \times 10^{-35}$ м.

Чи існує такий прилад, який може виміряти сигнал з довжиною хвилі 10^{-34} м? З такою довжиною хвилі інтерференційні піки будуть настільки тонкими, що жоден детектор їх просто не зможе розрізнити, а буде просто показувати середнє значення або огинаючу такого коливного руху.

Які ж висновки можна зробити з наших уявних експериментів?

1. Електрони, як й інші квантові об’єкти, поводять себе частково як частинки (вони прибувають до екрану дискретними порціями), частково — як хвилі (дають на екрані інтерференційну картину).

2. Надзвичайно важливим є висновок про те, що вимірювання в мікросвіті впливають на стан квантової системи. Цей висновок накладає просто екстремальні обмеження на усю квантову інформатику, адже читання чи запис даних еквівалентні процесу вимірювання. Отже необхідно буде розробляти алгоритми, які працюють без проміжного читання/запису.

3. Цей висновок, до деякої міри, випливає з попереднього. Якщо неможливо чітко визначити траєкторію руху електрона без впливу на результат, то ми повинні говорити лише про ймовірність тієї чи іншої траєкторії. Це справедливо не тільки для руху електронів, але й для усіх квантових систем: ми можемо лише говорити про ймовірність того чи іншого значення в квантовій системі. Якщо ми захочемо дізнатися точно, яке значення міститься у квантовому ОЗП, ми повинні провести вимірювання, а значить, вплинемо на саме це значення. Чи отримаємо ми в результаті таких дій істинне значення змінної — велике питання. Воно буде виникати перед нами усюди в квантовій інформатиці.

Незвичність подій, які виникають при виконанні квантових обчислень, і не мають аналогів у класичних обчисленнях, ставить перед математиками досить незвичні завдання, які необхідно вирішити в процесі розробки квантових алгоритмів. Тим не менше, ці завдання успішно вирішуються, що говорить про те, що основні засади квантової інформатики розроблено, а на часі — технічна реалізація універсальних квантових комп’ютерів.

Квантові біти

Опис простої квантової системи

Як же ми можемо математично описати таку систему, про яку ми говорили вище? Для коректного описання придумано спеціальний формалізм.

Позначимо стан квантової системи, коли частинка пройшла крізь верхній отвір як $|0\rangle=\begin{pmatrix}1\\0\end{pmatrix}$. Кутові дужки вказують на те, що це не просто “0”, а стан квантової системи. Як бачимо, тут існує деякий зв’язок з реальністю, оскільки одиниця стоїть там, де пройшла частинка, а нуль — там, де її не було. Аналогічно можна записати для випадку, коли частинка пройшла крізь нижній отвір: $|1\rangle=\begin{pmatrix}0\\1\end{pmatrix}$. Для цього випадку міркування абсолютно аналогічні. Описані стани називаються базисними, оскільки вони описують ситуацію, коли частинка точно пройшла крізь один отвір, і не проходила крізь другий. Однак, ми з’ясували, що існують такі ситуації, коли ми не можемо напевне сказати, крізь який отвір пройшла частинка. Ми знаємо лише, що з деякою ймовірністю вона може проскочити крізь отвір 1, і з деякою — крізь отвір 2.

Такий стан квантової системи ми можемо описати суперпозицією станів $|0\rangle$ та $|1\rangle$:

$$|Q\rangle=a|0\rangle+b|1\rangle. \qquad (1)$$

Коефіцієнти *a* та *b* описують ймовірності проходження частинки крізь відповідні отвори. Ці коефіцієнти повинні задовольняти деякі умови нормування. Вони описують той факт, що частинка точно пройшла або крізь перший, або крізь другий отвір, тобто сума ймовірностей проходження крізь кожен отвір повинна дорівнювати одиниці: $|a|^2+|b|^2=1$.

Формула (1) є відображенням так званого *принципу суперпозиції*, одного з основних і найважливіших принципів квантової механіки. Цей принцип формулюється так:

> *якщо квантова система може перебувати в станах* $|0\rangle$ *та* $|1\rangle$, *то вона може перебувати й у будь-якій суперпозиції цих станів.*

Розглянемо простий приклад опису квантової системи. Нехай система перебуває в стані, що описується виразом:

$$|Q\rangle=\frac{4}{5}|0\rangle+\frac{3}{5}|1\rangle.$$

Якою буде ймовірність того, що при вимірюванні ми отримаємо нуль?

$$P(0)=\left|\frac{4}{5}\right|^2=\frac{16}{25}=0.64.$$

Ймовірність отримати при вимірюванні одиницю:

$$P(1)=\left|\frac{3}{5}\right|^2=\frac{9}{25}=0.36.$$

Це означає, що в 64% випадків вимірювань ми отримаємо “0”, а в 36% - “1”.

Які ж реальні фізичні системи, крім проходження частинки крізь щілини, можуть бути такою квантовою системою?

Однією з найпростіших та найбільш популярних вважається спін мікрочастинки, наприклад, електрона.

Коротко та дуже умовно спін частинки можна описати таким чином. Якщо уявити собі заряджену частинку як маленьку кульку, то її обертання, як обертання будь-якого зарядженого тіла, створює магнітний момент, як це показано на рисунку 1. Цей магнітний момент і називається спіном (від англ. *to spin* - обертатись).

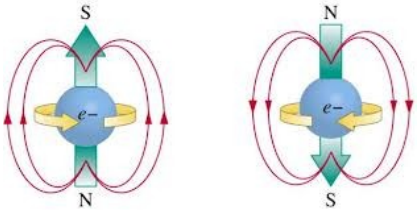


Рисунок 15: Ілюстрація до поясненні спіну електрона

І хоча насправді це зовсім не так, але така аналогія прижилася, і ми будемо нею користуватися.

В залежності від напрямку обертання частинки напрям магнітного моменту може бути різним. Якщо спін частинки напрямлений вгору (як це показано на рис. 15 ліворуч), будемо позначати такий стан як $|0\rangle$, а стан, коли спін напрямлено вниз, — через $|1\rangle$. Тоді знову стан, коли ми не знаємо куди напрямлений спін частинки, тобто стан суперпозиції, можна записати як

$$|Q\rangle = a|0\rangle + b|1\rangle.$$

І знов коефіцієнти при базисних станах вказують на ймовірність отримати при вимірюваннях нуль або одиницю. Звичайно, вони повинні задовольняти ту саму умову нормування: $|a|^2 + |b|^2 = 1$.

Як буде реагувати така система на вимірювання? Припустимо, що ми при першому вимірюванні отримали нуль. В якому стані тоді перебуватиме система?

$$|Q\rangle = 1 \cdot |0\rangle + 0 \cdot |0\rangle = |0\rangle.$$

Як бачимо, система перейшла в стан $|0\rangle$ і при наступних вимірюваннях із 100% ймовірністю ми її знайдемо в такому стані. Що це означає? Ми бачимо, що до вимірювання система знаходилася в стані суперпозиції, а після вимірювання перейшла у строго визначений стан $|0\rangle$. Таким чином, ми можемо припустити (і це підтверджується численними експериментами), що ***вимірювання впливають на стан квантової системи***. Більше того, скільки разів ми би не повторювали вимірювання, квантова система більше не змінить свій стан, і ми отримуємо ***звичайну класичну систему з чітко визначеним станом***.

Квантові біти

Оперативний запам'ятовувальний пристрій сучасного комп’ютера складається з комірок, двом станам яких (більший рівень напруги - менший рівень напруги, є електричний заряд - немає заряду, є електричний струм — немає струму тощо) привласнюються значення “1” та “0”. У наборі комірок (регістрі) записується та обробляється інформація у вигляді двійкових чисел. Один біт має два стани: “1” та “0”; регістр з N бітів має 2^N станів, тобто в такому регістрі можна закодувати двійкове число з N знаків.

Розглянемо систему з трьох бітів. В такому класичному регістрі ми можемо зберігати одне з чисел: 000; 001; 010; 011; 100; 101; 110; 111. Якщо ми хочемо зберігати усі ці числа *одночасно*, то для цього буде потрібно вісім трибітових регістрів, тобто 24 біти.

У квантовому комп’ютері елементарними комірками для запису та обробки інформації є *квантові біти* або ***кубіти***. Кубіт — це квантова система, яка має два базисних стани, $|0\rangle$ та $|1\rangle$. Однак, на відміну від класичного біта, кубіт може знаходитися не тільки в одному визначеному стані, а й в суперпозиційному стані: $|Q\rangle = a|0\rangle + b|1\rangle$. Тут, з логічної точки зору, класична булева логіка, “1/0” - *True/False* не має місця. Суперпозиційний стан кубіта — частково “*true*” (з ймовірністю $|b|^2$), частково “*false*” $|a|^2$. Найважливішою відмінністю кубіта від класичного біта полягає в тому, що в системі кубітів можливий так званий “переплутаний” стан або стан суперпозиції. В такому стані кожен кубіт одночасно містить і “0” і “1”, а отже, квантова система з N кубітів одночасно містить усі можливі двійкові числа від 0 до N, тобто 2^N бітів.

Дійсно, якщо один кубіт у стані суперпозиції містить одночасно і “1”, і “0”, тобто $2^1 = 2$ значення; два кубіти будуть містити суперпозицію $(a|0\rangle + b|1\rangle)(c|0\rangle + d|1\rangle) = (ac|00\rangle + ad|01\rangle + bc|10\rangle + bd|11\rangle)$, тобто $2^2 = 4$. Відповідно, N кубітів у суперпозиційному стані будуть містити 2^N бітів.

Очевидно, що це приводить до значної економії використаної пам’яті комп’ютера. Більше того, деякі математичні операції над таким регістром можна виконувати усього один раз, оскільки вони виконуються над усіма значеннями одночасно. Такий спосіб обробки даних називають “*квантовим прискоренням обчислень*”. Його та алгоритми, які використовують таке прискорення ми розглянемо пізніше.

А зараз з’ясуємо, які найпростіші операції ми можемо виконувати над кубітами.

Розділ II. Квантові операції

Прості операції над кубітами

Операції над кубітами часто називають *ґейтами* або *вентилями*. Для визначеності будемо вважати, що ми маємо справу зі спіном електрона, хоча яка саме фізична система розглядається неважливо. Важливим є те, що вона виявляє квантові властивості.

Отже, нехай ми маємо систему, базисні стани якої складаються з $|0\rangle=\begin{pmatrix}1\\0\end{pmatrix}$ та $|1\rangle=\begin{pmatrix}0\\1\end{pmatrix}$. Найпростішими ґейтами, які працюють з одним кубітом будемо вважати: *тотожну операцію* (*I*), *заперечення* (*NOT*), *ґейт Адамара* (*H*).

Тотожна операція (I)

За своїм змістом дія тотожної операції не змінює операнд. Це означає, що $I|0\rangle=|0\rangle$ та $I|1\rangle=|1\rangle$. Визначимо тотожну операцію так: $I=\begin{pmatrix}1&0\\0&1\end{pmatrix}$. Перевіримо її дію:

$$I|0\rangle=\begin{pmatrix}1&0\\0&1\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}=\begin{pmatrix}1\cdot1+0\cdot1\\0\cdot1+0\cdot0\end{pmatrix}=\begin{pmatrix}1\\0\end{pmatrix}=|0\rangle;$$

$$I|1\rangle=\begin{pmatrix}1&0\\0&1\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix}=\begin{pmatrix}1\cdot0+0\cdot1\\0\cdot0+1\cdot1\end{pmatrix}=\begin{pmatrix}0\\1\end{pmatrix}=|1\rangle.$$

Як бачимо, дія такої матриці на стани $|0\rangle$ та $|1\rangle$ дійсно не призводить до зміни операндів. Це значить, що тотожна операція визначена нами вірно.

Заперечення (NOT)

Стандартна унарна операція заперечення (*NOT*) повинна перетворювати стани $|0\rangle$ в $|1\rangle$ та навпаки.

Визначимо операцію заперечення таким чином: $NOT=\begin{pmatrix}0&1\\1&0\end{pmatrix}$. Перевірка дасть такі результати:

$$NOT|0\rangle=\begin{pmatrix}0&1\\1&0\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}=\begin{pmatrix}0\cdot1+1\cdot0\\1\cdot1+0\cdot0\end{pmatrix}=\begin{pmatrix}0\\1\end{pmatrix}=|1\rangle;$$

$$NOT|1\rangle=\begin{pmatrix}0&1\\1&0\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix}=\begin{pmatrix}0\cdot0+1\cdot1\\1\cdot0+0\cdot1\end{pmatrix}=\begin{pmatrix}1\\0\end{pmatrix}=|0\rangle.$$

Бачимо, що уведений оператор діє саме так, як нам потрібно.

Ґейт Адамара (Hadamard, H)

Перетворення Адамара є одним з найважливіших ґейтів квантових обчислень. Чому це так, зараз ми зрозуміємо.

Уведемо це перетворення наступним чином: $H=\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$. Застосуємо його до нашої квантової системи. Будемо мати:

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

Що ж ми отримали в результаті? Як бачимо, ґейт Адамара, діючи на строго визначений стан переводить його у стан суперпозиції. Ця дія надзвичайно важлива і використовується практично в усіх квантових алгоритмах, наприклад, для ініціалізації квантових регістрів, де вимагається переплутаний стан.

Зрозуміло також, що подвійне застосування ґейта Адамара є тотожною операцією. Доведемо це:

$$H|0\rangle=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle);$$
$$H[\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)]=\frac{1}{2}[|0\rangle+|1\rangle+|0\rangle-|1\rangle]=|0\rangle.$$

Аналогічне доведення і для стану $|1\rangle$.

Ґейт Адамара має просту фізичну інтерпретацію. Це може бути простий оптичний дільник, який ділить падаючий промінь у співвідношенні 50:50, тобто напівпрозорий фільтр.

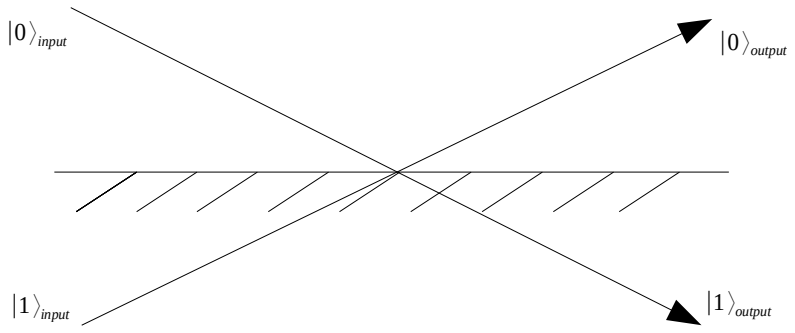
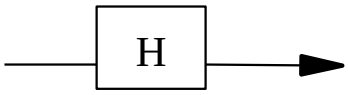


Рисунок 16. Фізична інтерпретація ґейта Адамара

Той факт, що промінь світла знаходиться над пластинкою, позначимо як стан системи $|0\rangle$ незалежно від того, чи він тільки падає на пластинку, чи вже відбивається від неї. Аналогічно, якщо промінь знаходиться під пластинкою, позначимо через $|1\rangle$. Оскільки пластинка напівпрозора, то ймовірність відбиття падаючого променя та ймовірність того, що

він пройде крізь пластинку, рівні. Отже, направляючи промінь на пластинку, ми не знаємо точно де знайдемо оброблений промінь: вище, чи нижче пластинки. Якщо вважати промінь квантовою системою, то вхідний стан системи буде чітко визначеним, а вихідний — переплутаним. Так само себе поводить ґейт Адамара.

На квантових схемах ґейт Адамара, як би він не був реалізований, позначається так:



Багатокубітні операції

Розглянуті ґейти працюють з одним кубітом. Існує багато ґейтів, які працюють з кількома кубітами. Ми розглянемо лиш два з них: контрольоване заперечення та ґейт Тоффолі.

Контрольоване заперечення (Controlled NOT, CNOT)

Ґейт CNOT використовує два кубіти, один з яких контрольний, а другий — контрольований. Логіка роботи цього ґейта така: якщо контрольний кубіт дорівнює одиниці, то контрольований кубіт інвертується:

$$|00\rangle \rightarrow |00\rangle$$
$$|01\rangle \rightarrow |01\rangle$$
$$|10\rangle \rightarrow |11\rangle$$
$$|11\rangle \rightarrow |10\rangle.$$

Тут контрольним вважається перший кубіт, а контрольованим — другий. Дуже схоже на таблиці істинності логічних операцій. Цим ми пізніше скористаємося.

Ґейт Тоффолі (T)

Ґейт Тоффолі або подвійний *CNOT (CCNOT)*, використовує три кубіта: два контрольних та один контрольований. Працює він так: якщо обидва контрольних кубіти дорівнюють одиниці, контрольований кубіт інвертується. Дію ґейта Тоффолі можна зобразити таким чином:

$$|000\rangle \rightarrow |000\rangle$$
$$|001\rangle \rightarrow |001\rangle$$
$$|010\rangle \rightarrow |010\rangle$$
$$|011\rangle \rightarrow |011\rangle$$
$$|100\rangle \rightarrow |100\rangle$$
$$|101\rangle \rightarrow |101\rangle$$
$$|110\rangle \rightarrow |111\rangle$$
$$|111\rangle \rightarrow |110\rangle.$$

Тут перші два біти вважаються контрольними, а останній — контрольованим.

В принципі, маючи такий набір ґейтів, можна спроектувати довільний пристрій для

обробки інформації. Розглянемо, наприклад, суматор за модулем два на основі контрольованого заперечення.

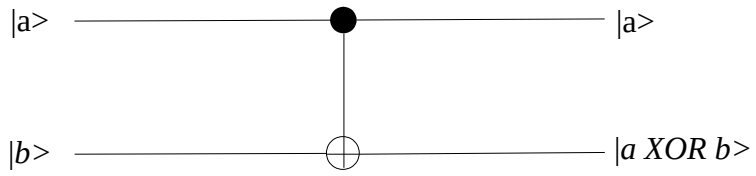


Рисунок 17. Приклад логічного елемента XOR

Елемент складається з двох кубітів: верхній — контролюючий, нижній — контрольований. Якщо верхній кубіт несе одиницю, то нижній кубіт інвертується. Розглянемо відповідність такого елемента додаванню за модулем два.

Значення *a*	**Значення *b***	**Результат *CNOT***	**Результат *XOR***
0	0	0	0
0	1	1	1
1	0	1	1
1	1	0	0

Як видно з таблиці, результат дії CNOT повністю відповідає додаванню за модулем два. Це яскравий приклад того, як за допомогою квантових ґейтів можна побудувати оператори булевої алгебри, а відповідно, й інші пристрої обчислювальної техніки.

Часткові вимірювання

Раніше ми обговорювали той факт, що вимірювання впливають на стан кубітів, перетворюючи його з суперпозиційного у класичний, цілком визначений стан. При подальших вимірах цей стан вже не змінюється, залишаючись весь час однаковим.

Тим не менше, ми можемо виконувати так звані *часткові вимірювання*, вимірюючи окремі біти квантової системи.

Розібратися в тому, як це відбувається і до чого приводить, можна на простому прикладі.

Розглянемо систему з двох квантових бітів у стані:

$$|Q\rangle = \frac{3}{5}|00\rangle + \frac{2}{5}|01\rangle + \frac{2}{5}|10\rangle + \frac{2\sqrt{2}}{5}|11\rangle.$$

Спробуємо виміряти другий кубіт. З якою ймовірністю ми отримаємо одиницю?

Другий кубіт не дорівнює нулю у другому та четвертому доданках. Тоді ймовірність того, що ми при вимірюванні отримаємо одиницю можна записати так:

$$P(1)=\left(\frac{2}{5}\right)^2+\left(\frac{2\sqrt{2}}{5}\right)^2=\frac{4}{25}+\frac{8}{25}=\frac{12}{25}.$$

В якому стані опиниться система, якщо ми отримаємо одиницю в другому біті? Зрозуміло, що після вимірювань другий біт буде завжди дорівнювати одиниці, отже перший та третій доданки зникнуть, оскільки там другий біт дорівнює нулю. Але просто так забрати ці доданки не можна, оскільки необхідно задовольнити умову нормування. Отже треба обчислити нові коефіцієнти біля доданків з таких умов:

$$|a|^2+|b|^2=1;\frac{a}{b}=\frac{2/5}{2\sqrt{2}/5}=\frac{\sqrt{2}}{2}.$$

Отже для обчислення нових коефіцієнтів необхідно розв’язати систему:

$$\begin{cases}\frac{a}{b}=\frac{\sqrt{2}}{2};\\ |a|^2+|b|^2=1.\end{cases}$$

Обчисливши коефіцієнти, отримуємо такий стан системи:

$$|Q\rangle=\frac{1}{\sqrt{3}}|01\rangle+\sqrt{\frac{2}{3}}|11\rangle.$$

Як бачимо, часткові вимірювання хоч і не руйнують систему, однак також змінюють її квантовий стан.

Переплутані стани

Розглянемо систему з двох кубітів. Простір станів такої системи буде описуватися виразом:

$$\{|0\rangle\otimes|0\rangle,|0\rangle\otimes|1\rangle,|1\rangle\otimes|0\rangle,|1\rangle\otimes|1\rangle\};\quad \text{або}$$

$$\{|00\rangle,|01\rangle,|10\rangle,|11\rangle\}$$

де $\otimes$ - тензорний добуток, який визначається наступним чином:

$$\begin{pmatrix}a\\b\end{pmatrix}\otimes\begin{pmatrix}c\\d\end{pmatrix}=\begin{pmatrix}a\cdot c & a\cdot d\\ b\cdot c & b\cdot d\end{pmatrix}.$$

Як бачимо, тензорний добуток збільшує розмірність вектора до матриці. Тензорний добуток підкоряється стандартним для математики властивостям лінійності, асоціативності та комутативності, що дозволяє в деяких випадках працювати з ним аналогічно до

звичайного добутку.

У загальному випадку, як це було показано раніше, система з n кубітів має 2^n базисних станів, тобто станів, тензорний добуток яких дає повний простір квантових станів системи.

Однак, не завжди усі стани квантової системи можна зобразити станами окремих кубітів.

Наприклад, стан $\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)$ не можна зобразити через стани окремих кубітів. Це означає, що не існує таких коефіцієнтів a_1, a_2, b_1, b_2, щоби:

$$(a_1|0\rangle+b_1|1\rangle)(a_2|0\rangle+b_2|1\rangle)=\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle). \qquad (2)$$

Дійсно:

$$(a_1|0\rangle+b_1|1\rangle)(a_2|0\rangle+b_2|1\rangle)=a_1a_2|00\rangle+a_1b_2|01\rangle+b_1a_2|10\rangle+b_1b_2|11\rangle.$$

Для того, щоби виконувалася рівність (2), необхідно, щоби $a_1b_2=0$ та $b_1a_2=0$. Це означає, що $a_1a_2=0$ та $b_1b_2=0$. Отже стан $\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)$ не може бути суперпозицією станів $(a_1|0\rangle+b_1|1\rangle)$ та $(a_2|0\rangle+b_2|1\rangle)$.

Таким чином, стан $\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)$ є так званим *переплутаним* станом по відношенню до базису $(a_1|0\rangle+b_1|1\rangle)$ та $(a_2|0\rangle+b_2|1\rangle)$.

Іншим способом визначення *переплутаного* стану є таке. Ми знаємо, що тензорний добуток має властивості асоціативності та комутативності. Отже, ми можемо виносити за знак тензорного добутку спільні множники. Наприклад, стан

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

можна зобразити як

$$|\psi\rangle=\frac{1}{\sqrt{2}}|0\rangle\otimes(|0\rangle+|1\rangle)$$

або $|\psi\rangle=\frac{1}{\sqrt{2}}(|01\rangle+|11\rangle)$ - у вигляді $|\psi\rangle=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\otimes|1\rangle$. Такі стани будемо вважати не переплутаними. А от квантовий стан $|Q\rangle=\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)$ не можна подати у вигляді тензорного добутку двох однокубітових станів. Отже “винести спільний множник” з такої конструкції не можна. Такий стан будемо вважати переплутаним. З такої точки зору квантовий стан $|\phi\rangle=\frac{1}{\sqrt{2}}(|01\rangle+|10\rangle)$ також вважається переплутаним.

Можна подивитися на переплутані стани ще з іншого боку, з точки зору вимірювань. Частинки не будуть переплутаними, якщо вимірювання однієї з них не вплинуть на стан

іншої. Наприклад, стан $|\psi\rangle=\frac{1}{\sqrt{2}}(|00\rangle+|01\rangle)=\frac{1}{\sqrt{2}}|0\rangle\otimes(|0\rangle+|1\rangle)$ не вважається переплутаним, оскільки при будь-якому вимірюванні першого біта ми отримаємо нуль незалежно від того, вимірювався другий біт, чи ні. Аналогічно й вимірювання другого біта може дати нуль або одиницю з такою ж ймовірністю незалежно від того, чи вимірювався перший біт.

Цього не можна сказати про стан $|Q\rangle=\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)$. В цьому випадку отримані значення будь-яких кубітів істотно залежать від того, чи проводилося вимірювання іншого біта. Наприклад, якщо при вимірюваннях першого біта ми отримали нуль, то значення другого біта може бути тільки нуль, і ніяк не одиниця. Якщо ж при вимірюванні першого біта отримано одиницю, то другий автоматично також дорівнює одиниці. Аналогічні міркування справедливі й для другого біта. Таким чином, цей стан буде переплутаним. Переплутаними будуть також стани $|\phi\rangle=\frac{1}{\sqrt{2}}(|01\rangle+|10\rangle)$ або $|\theta\rangle=\frac{1}{\sqrt{2}}(|10\rangle+|01\rangle)$, який, по суті, є тим самим станом $|\phi\rangle$.

Підсумуємо викладену інформацію. Квантовий стан, наприклад, двокубітний, будемо вважати переплутаним, якщо:

- його не можна зобразити у вигляді суперпозиції двох однокубітних станів;
- з виразу, який характеризує стан квантової системи, не можна винести “спільний множник”;
- значення, отримані при вимірюванні одного з кубітів істотно залежать від результатів вимірювання іншого.

Переплутані стани грають визначальну роль у квантових алгоритмах, безпосередньо відповідаючи за квантове прискорення обчислень.

Квантовий паралелізм

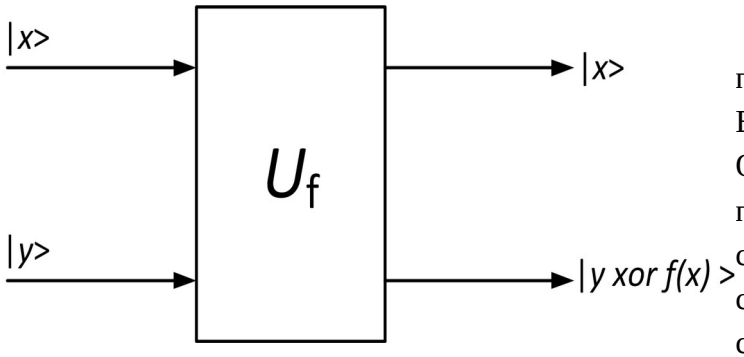
Для початку уведемо поняття квантового оракула. Припустимо, що ми маємо деяку квантову схему (гейт), яка реалізує на практиці обчислення якоїсь функції *f*(*x*). Нехай це буде унарна операція такого типу:

$$U_f : |x, y\rangle \rightarrow |x, y \oplus f(x)\rangle.$$

Ми не знаємо ані структури цієї схеми, ні як вона реалізує обчислення функції *f*(*x*). Для нас головне, що вона це робить. У цьому випадку така схема виступає як “чорна скринька”. На вхід цієї “скриньки” подається значення аргументів, на виході ми маємо результат обчислення функції. Ми будемо називати таку “чорну скриньку” *квантовим оракулом* або просто *оракулом*.

Для того, щоби обчислити *f*(*x*), нам треба подати на вхід оракула стан $|x,0\rangle$, тоді на виході отримаємо:

$$U_f : |x,0\rangle \rightarrow |x,0 \oplus f(x)\rangle \rightarrow |x, f(x)\rangle.$$



Що відбудеться, якщо ми подамо на оракул переплутаний стан? Відповідь проста, але досить дивна. Оскільки U_f - лінійне унарне перетворення, то застосування його до суперпозиційного стану приводить до суперпозиції результатів. Отже таким способом можна обчислити *f*(*x*) для усіх значень аргументу одразу, при одноразовому застосуванні оракула. Такий ефект називають *квантовим паралелізмом*.

На практиці це реалізується в такий спосіб. Регістр з *n*-кубітів заповнюють нулями. Далі до цього регістра застосовують гейт Адамара для отримання суперпозиційного стану:

$$|Q\rangle = \frac{1}{\sqrt{2^n}}(|000...0\rangle + |000...1\rangle + ... + |111...1\rangle) = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle.$$

До цього стану додається регістр нулів і все подається на вхід квантового оракула. Тоді на виході отримаємо:

$$U_f : \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x,0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} U_f |x,0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x, f(x)\rangle.$$

Необхідно відзначити, що оскільки *n*-кубітів дозволяють одночасно працювати з 2^n станами, то квантовий паралелізм може надати користувачеві експоненційне зростання

обчислювального простору при лінійному зростанні об’єму фізичного простору.

В якості прикладу розглянемо дію оператора Тоффолі для обчислення кон’юнкції двох величин.

На вхід системи подамо суперпозицію усіх можливих значень *x* та *y* крім *x*=1, *y*=1.

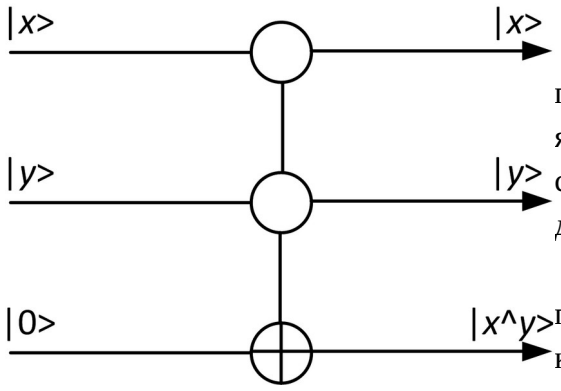
$$H|0\rangle\otimes H|0\rangle\otimes|0\rangle=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\otimes\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\otimes|0\rangle=\frac{1}{2}(|000\rangle+|010\rangle+|100\rangle+|110\rangle).$$

На результат подіємо гейтом Тоффолі:

$$T:\{\frac{1}{2}(|000\rangle+|010\rangle+|100\rangle+|110\rangle)\}=\frac{1}{2}(|000\rangle+|011\rangle+|101\rangle+|111\rangle).$$

Цю результуючу суперпозицію можна розглядати як таблицю істинності деякої логічної функції. Тут перші два біти розглядаються як вхідні значення, а третій — як значення функції. Видно, що ці результати повністю відповідають таблиці істинності кон’юнкції двох змінних: *x* та *y*.

Схематично це можна зобразити таким чином, як подано на рисунку.



На перший погляд тут немає жодної переваги над класичними обчисленнями, адже якщо ми проведемо вимірювання такої суперпозиції, ми отримаємо лише один результат, до того ж невідомо який.

Насправді ж важливість квантового паралелізму важко переоцінити. Існує цілий клас квантових перетворень, які дають змогу значно збільшити ймовірність отримання потрібного результату. Керування квантовим паралелізмом такого роду зовсім не має класичних аналогів і часто є основою тих чи інших квантових обчислень. Однак, розв’язання таких задач вимагає від дослідника використання спеціальних математичних методів та нестандартних засобів програмування.

Парадокс Ейнштейна-Подольські-Розена

Використовуючи поняття переплутаного стану, Альберт Ейнштейн, Борис Подольські та Натан Розен, запропонували уявний експеримент, який, здається порушує основні принципи теорії відносності. Цей експеримент було описано у їх статті “Чи можна вважати квантово-механічне описання фізичної реальності повним?”, яка вийшла у друці 1935 року [20]. Цей експеримент пізніше було названо парадоксом Ейнштейна-Подольські-Розена (ЕПР-парадоксом).

Суть цього парадоксу полягає в наступному.

Припустимо, у нас є джерело, яке генерує максимально переплутані частинки, наприклад, в стані $|Q\rangle=\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)$. Ці частинки називаються ЕПР-парою. Припустимо, що учасники експерименту отримали по одній частинці з цієї пари і роз'їхалися на максимально можливу відстань.

Нехай власник першої частинки виконав її вимірювання і з'ясовується, що його частинка знаходиться в стані $|0\rangle$. Це означає, що загальний стан системи повинен бути $|00\rangle$. Отже, коли власник другої частинки виконає вимірювання, він також отримає $|0\rangle$. Аналогічно, якщо перша частинка при вимірюваннях продемонструє стан $|1\rangle$, то друга неодмінно буде в такому ж стані $|1\rangle$. Зміна стану відбувається миттєво, не дивлячись на те, що частинки знаходяться на довільній відстані. Виходить, що учасники експерименту можуть миттєво обмінюватися інформацією. Однак, це протирічить спеціальній теорії відносності, яка доводить, що найбільша швидкість передавання інформації дорівнює швидкості світла у вакуумі.

Насправді суть парадоксу значно глибше. В загальному вона полягає в тому, чи може квантова механіка адекватно описувати фізичну реальність, тобто чи це повна наука, і вона не протирічить іншим, відомим та доведеним теоріям, чи квантова механіка є наукою, яка вимагає значного вдосконалення й узгодження з цими теоріями.

Сьогодні існує кілька інтерпретацій цього парадоксу.

1. Теорія прихованих параметрів Девіда Бома.
2. Теорема Белла та її експериментальні перевірки.
3. Багатосвітова інтерпретація.
4. Квантовомеханічна інтерпретація (інтерпретація Н.Бора).

Розглянемо ці тлумачення детальніше.

Теорія прихованих параметрів Девіда Бома

У 1952 році Девід Бом у своїй книзі “Квантова теорія” запропонував реальний фізичний експеримент, який на той час здійснити було нереально, однак, він дозволяв безпосередньо перевірити правильність різних тлумачень ЕПР-парадоксу [21]. Суть експерименту полягає в тому, що деяке джерело випромінює два фотони у переплутаному стані в різні боки. Кожен фотон має якісь свої конкретні значення компонентів спіну в напрямках *x*, *y*, *z*. Ми можемо вимірювати ці значення, але тільки один компонент за раз. Нехай ми виміряли *x*-компонент спіну першого фотона і отримали якусь величину x_0.

Оскільки фотони знаходяться у переплутаному стані, то яке б не було значення *y*-компоненти першого фотона, *y*-компонента спіну другого фотона обов'язково повинна бути протилежною за напрямом. Таким чином, вимірюючи *y*-компоненту першого фотона, ми неявним чином вимірюємо таку саму компоненту другого, як це й було описано в ЕПР-парадоксі. Якщо би така картина була справедливою для усіх вимірів та усіх напрямів випромінювання фотонів, то це протирічило би твердженням нерівності Гейзенберга, яка стверджує, що не можна достовірно виміряти дві величини однієї частинки.

На основі таких міркувань, Д. Бом робить висновок про те, що квантова механіка як наука неповна, таким чином припускаючи існування прихованих параметрів, що можуть розв’язати цю проблему:

“*... сучасна форма квантової теорії вказує на те, що Всесвіт не можна однозначно відобразити ніякою сукупністю строго визначених математичних величин, і що повна теорія завжди вимагатиме більш загальних понять, ніж розкладання на точно визначені компоненти ...*”

Що означає поняття “прихованих параметрів”? Розглянемо два таких висловлювання:

1) В момент часу t=1 с частинка буде знаходитися в точці з координатою x=1 м. Це — приклад класичного, детерміністичного твердження.

2) В момент часу t=1 с частинка буде знаходитися між координатами x=1 м та x=1,1 м з ймовірністю P=0,8. Це — приклад того, що можуть дати квантовомеханічні обчислення.

Як бачимо, квантовомеханічні обчислення передбачають наявність деякого елемента випадковості у фізичних процесах. У зв’язку з цим, фізики й розділилися на два (як мінімум!) табори. Одні вважали, що випадковість притаманна самій фізичній природі. Інші були впевнені, що ніякої випадковості в природі не існує, а ймовірності, які виникають у квантовомеханічних розрахунках насправді є наслідком недосконалості самої теорії та нашого неповного знання про природу речей. Загалом ці два підходи можна охарактеризувати так:

Класичний підхід: поточний стан фізичної системи повністю та однозначно визначає її майбутній стан. Наприклад, якщо зараз система знаходиться в стані “А”, то через секунду вона буде знаходитися в стані “В”. І якщо квантова механіка стверджує, що через секунду квантова система буде знаходитися або в стані “В”, або в стані “С”, то це лиш значить, що вона при розрахунках не враховує якісь невідомі (приховані) параметри системи, врахування яких може однозначно визначати її майбутній стан.

Квантовий підхід: поточний стан системи несе в собі кілька (загалом — безмежну кількість) можливих варіантів її майбутнього стану. Який саме з цих можливих варіантів буде реалізовано — принципово неможливо передбачити, оскільки вибір тут відбувається абсолютно випадково, причому немає ніяких прихованих параметрів, які б могли вплинути на цей вибір. Можна говорити лише про ймовірність того чи іншого вибору.

Прибічники класичного та квантового підходу сперечаються вже багато років але жодна сторона не може надати вирішальних доказів на користь тієї чи іншої моделі. Тим не менше, часто результати експериментів, наприклад, таких, як запропонував Д.Бом, можна пояснити за допомогою понять квантової механіки досить просто, не залучаючи до розгляду теорії прихованих параметрів.

Дійсно, нехай у нас є поляризатор, який випромінює фотони. Поляризатор має два канали “+” та “-”, напрямлені в різні боки. Ймовірність виявити фотон в будь-якому каналі — випадкова величина, причому рівноймовірна. Отже, $P_+(a)=P_-(a) = 0{,}5$. Аналогічно й для іншого фотона: $P_+(b)=P_-(b) = 0{,}5$. Саме цей результат говорить про те, що ми не можемо сказати точно яка поляризація у кожного фотона переплутаної пари, оскільки це процес ймовірнісний, і кожне вимірювання її дасть випадковий результат з ймовірністю 0,5. Тоді можна підрахувати ймовірності того, що фотони будуть однакової або різної поляризації :

$$P_{++}(a,b) = P_{--}(a,b) = 1/2 \cos^2(a,b);$$
$$P_{+-}(a,b) = P_{-+}(a,b) = 1/2 \sin^2(a,b).$$

Якщо фотони летять строго в різні боки (кут між a та b дорівнює 180^o), то

$$P_{++}(a,b) = P_{--}(a,b) = 1/2;$$
$$P_{+-}(a,b) = P_{-+}(a,b) = 0.$$

Звідси слідує, що якщо ми виявляємо один фотон в каналі “+”, то інший не може бути в каналі “-” і навпаки. Отже тут спостерігається кореляція між двома випадковими подіями. Якщо ввести коефіцієнт кореляції, то у розглянутому випадку вона буде повною.

Теорема Белла та її експериментальні перевірки

У 1964 році з’явилася теорема, яка може примирити прибічників класичного та квантового підходів. Запропонував її Джон Стюарт Белл [22]. Вона стверджує, що незалежно від того, містить квантова теорія деякі приховані параметри чи ні, можна провести серійний експеримент, статистичні результати якого підтвердять або спростують наявність таких параметрів. Коротше кажучи, Дж. Белл запропонував спосіб, яким можна було перевести перевірку існування прихованих параметрів з філософської площини в експериментальну. Белл вивів деяку формулу (нерівність) для математичної обробки запропонованого їм експерименту та довів таке:

- якщо нерівність виконується, то праві прибічники класичного підходу, тобто квантова механіка не враховує деякі приховані параметри;
- якщо нерівність не виконується, то квантова механіка — повна наука, не треба шукати прихованих параметрів, ймовірнісність притаманна фізичній реальності і є її властивістю.

Суть експерименту Белла полягає в такому.

Нехай у нас є джерело переплутаних частинок, які випромінюються ним у протилежні боки. Частинки проходять через поляризатори (якщо це фотони) або через прилади з магнітним полем (прилади Штерна-Герлаха, якщо це частинки з напівцілим спіном). Проходячи через поляризатори (прилади Штерна-Герлаха), частинки набувають певної поляризації (напряму спіну), а потім реєструються детекторами поляризації (спіну). Якщо вектор поляризації (спіну) частинки напрямлений вгору, таку частинку будемо позначати “+”; якщо вниз - “-”. Таким чином, позначивши частинки, що випромінюються в протилежні боки, як “a” та “b”, можна записати таке: $N_{++}(a,b)$ — кількість частинок, які мали поляризацію

(спін) вгору в обох детекторах, тобто кількість частинок, поляризація (спін) яких були: тип *a* — вгору; тип *b* — вгору. Аналогічно можна позначити $N_{--}(a,b)$ — кількість частинок з поляризацією “-” “-” в обох напрямках; $N_{+-}(a,b)$, $N_{-+}(a,b)$ — аналогічно.

Тоді коефіцієнт кореляції можна записати таким чином:

$$E(a,b) = 1/N\,[N_{++}(a,b) + N_{--}(a,b) — N_{+-}(a,b) — N_{-+}(a,b)\,],$$

де N — повна кількість частинок, що їх випромінило джерело. Виконавши такі вимірювання з різною орієнтацією (a,b); (a,b'); (a',b) та (a',b'), можна обчислити величину:

$$S(a,a',b,b') = E(a,b) + E(a',b') + E(a',b) — E(a,b')$$

та скласти нерівність Белла:

$$-2 \le S(a,a',b,b') \le 2.$$

З 1972 року нерівність Белла перевірялася неодноразово. Результати подано в таблиці.

Автори експериментів	**Отримані значення S**
Фрідман і Клаузер (1972 рік)	2.28 ± 0.04
А.Аспе зі співр. (1982 рік)	2.23 ± 0.05
Дж. Вайс зі співр. (1998 рік)	2.23 ± 0.09
Шайдл зі співр. (2010 рік)	2.37 ± 0.02

Як бачимо з таблиці, результати усіх експериментів доводять, що нерівність Белла не виконується. Це означає, що правильною виявляється квантова механіка, отже класичний підхід до парадоксу ЕПР застосовувати не можна. Тим не менше, прибічники теорій прихованих параметрів весь час знаходять в експериментах слабкі місця, що дає їм право сумніватися в наведених результатах. На сьогодні питання все ще не закрито, повної ясності немає.

Багатосвітова інтерпретація

Іншим способом пояснення парадоксу ЕПР була й залишається багатосвітова інтерпретація. Суть її полягає в наступному.

Стан частинок переплутаної пари являє собою квантову суперпозицію усіх можливих станів. Згідно з цими теоріями це можна інтерпретувати як суперпозицію станів однакових паралельних всесвітів, що не взаємодіють між собою. Кожен всесвіт містить альтернативну історію частинок пари і характеризується окремими значеннями фізичних величин, тобто містить один визначений стан. Поки не проведено вимірювань, неможливо встановити в якому саме всесвіті відбувається експеримент. В момент вимірювання обирається один з паралельних всесвітів, відбувається незворотне їх “розщеплення” й історія частинок стає визначеною. Ось чому подальші вимірювання не впливають на частинки і протиріччя з принципом причинності відсутнє.

Квантовомеханічна інтерпретація

Цю інтерпретацію було сформульовано засновниками квантової механіки Нільсом Бором та Вернером Гейзенбергом приблизно у 1927 році під час спільної роботи у Копенгагені. Тому часто її називають копенгагенською інтерпретацією. Вона стверджує, що ймовірнісного характеру передбачень квантової механіки принципово не можна позбавитися, причому він зовсім не свідчить про те, що наші знання обмежені, квантова наука не повна, що вона містить якісь приховані параметри. Це означає, що в квантовій механіці результат вимірювань принципово недетермінований.

Н.Бор та В.Гейзенберг відзначають, що фізика взагалі та квантова механіка зокрема, є наукою вимірювальних процесів. Тому питання типу "*... де була частинка до того, як я зареєстрував її положення ...*" або "*... якими були параметри частинки до вимірювання ...*" беззмістовні. Процес вимірювання приводить до випадкового вибору в точності одного з можливих варіантів значень параметрів, що вимірюються, які "містилися" у переплутаному стані.

Автори цієї інтерпретації відзначають також, що тут немає ніякого протиріччя з теорією відносності, оскільки переплутаний стан квантової системи з кількох частинок описується однією математичною функцією, яка називається хвильовою, причому її не можна розділити на окремі функції, які б описували стан кожної частинки системи окремо. Оскільки це так, то говорити про передавання якоїсь інформації між частинами хвильової функції всередині її також беззмістовно.

Звичайно, така інтерпретація також не позбавлена недоліків. Наприклад, процесу вимірювання тут надається якійсь дуже особливий статус, але пояснення, що ж він таке, які його визначальні риси, як його відділити від інших, невимірювальних процесів, немає.

Довгі роки копенгагенська інтерпретація була найпопулярнішою серед спеціалістів з квантової механіки. Зараз картина змінюється.

У 1997 році на симпозіумі в Мерилендському університеті було проведено опитування про підтримку тієї чи іншої інтерпретації квантової механіки. Результати подано в таблиці.

Інтерпретація	**Віддано голосів**
Копенгагенська	13
Багатосвітова	8
Теорія прихованих параметрів	4
Критерій непротирічивості	4
Модифікована динаміка	1
Жодна з наведених	18

Як бачимо, популярність копенгагенської інтерпретації, яка раніше була домінуючою, поступово спадає.

Сьогодні багато фізиків схиляються до так званої "ніякої" інтерпретації квантової механіки, а значить, і ЕПР-парадоксу, яку вдало висловив Девід Мермін: "*Shut up and calculate!*", що в м'якому перекладі з англійської можна подати як: "*Мовчи і працюй!*"

Підсумовуючи, можна сказати, що парадокс Ейнштейна-Подольські-Розена належить до такого класу задач, точного вирішення якого сьогодні не існує. Можливо колись, з розвитком квантовомеханічної науки, це питання буде вирішено, однак відбудеться це, по всьому видно, дуже не скоро.

Квантова телепортація

Однією з найчастіше використовуваних в комп'ютерній техніці операцій є копіювання інформації. У класичних комп'ютерах все відбувається звичним для нас чином: зчитуються дані з однієї комірки пам'яті та записуються в іншу. У квантовому випадку читання інформації з кубіта може прирівнюватися до вимірювання його стану. Таким чином, існує певна підозра, що операцію копіювання стану кубіта в цьому випадку взагалі виконати неможливо.

Дійсно, припустимо, що нам треба скопіювати невідомий квантовий однокубітний стан. Припустимо, що ми маємо деякий унарний оператор, який виконує цю операцію. Тоді ми зможемо записати:

$$U:|a0\rangle=|aa\rangle. \tag{3}$$

Формула (1) справедлива для усіх станів $|a\rangle$. Нехай $|a\rangle$ та $|b\rangle$ - деякі ортогональні стани. Тоді справедливо: $U:|a0\rangle=|aa\rangle$ та $U:|b0\rangle=|bb\rangle$. Припустимо також, що ми маємо квантовий стан $|c\rangle=\frac{1}{\sqrt{2}}(|a\rangle+|b\rangle)$. Тоді можна записати:

$$U:|c0\rangle=\frac{1}{\sqrt{2}}(U|a0\rangle+U|b0\rangle)=\frac{1}{\sqrt{2}}(|aa\rangle+|bb\rangle). \tag{4}$$

З другого боку:

$$U:|c0\rangle=|cc\rangle, \tag{5}$$

оскільки U — клонуюче перетворення. Підставляючи в (3) значення $|c\rangle$, отримаємо:

$$|cc\rangle=\frac{1}{\sqrt{2}}(|a\rangle+|b\rangle)\otimes\frac{1}{\sqrt{2}}(|a\rangle+|b\rangle)=\frac{1}{2}(|aa\rangle+|ab\rangle+|ba\rangle+|bb\rangle)\neq\frac{1}{\sqrt{2}}(|aa\rangle+|bb\rangle). \tag{6}$$

Звідси явно видно, що унарної операції, яка може копіювати (клонувати) невідомий стан, не існує. Цей факт отримав назву *теореми про заборону клонування*. Очевидно, що клонувати стан за допомогою вимірювання також неможливо, оскільки виміри руйнують квантовий стан. Відзначимо, що відомий квантовий стан легко копіюється або клонується. Проблема стосується лише невідомого стану.

Як же можна передати квантовий стан системи? Без вирішення цієї проблеми будь-які обчислення неможливі.

Для розв’язання цієї задачі розроблено схему *квантової телепортації*. Цей термін з’явився після публікації в 1993 році статті Чарлза Беннетта та Жіля Брассара [14]. Там пояснюється протокол квантової телепортації та її відмінності від того, який зміст вкладається у це поняття звичайними людьми. Квантова телепортація не передає ні енергії, ні речовини на відстані. Це гарантує, що під час квантової телепортації не порушуються закони фізики. Більше того, квантовий стан кубіта, який телепортується, після закінчення операції руйнується.

Припустимо, що сторона *A* хоче передати стороні *B* невідомий квантовий стан $|Q\rangle = a|0\rangle + b|1\rangle$. Сторони вже мають по квантовому біту з переплутаної пари $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Ідея полягає в тому, що сторона А підмішує невідомий кубіт до свого “переплутаного” біта, проводить вимірювання і відправляє результати стороні В. Та, у свою чергу, виконує допоміжні перетворення і отримує $|Q\rangle$.

Розглянемо протокол квантової телепортації детальніше.

Стартовий стан. Сторона *A* має один кубіт з “переплутаної” пари і кубіт з невідомим станом $|Q\rangle$. Сторона *B* має лише один “переплутаний” кубіт.

Сторона А підмішує невідомий кубіт до пари, ставлячи його ліворуч:

$$|\psi\rangle = \frac{a}{\sqrt{2}}|000\rangle + \frac{a}{\sqrt{2}}|011\rangle + \frac{b}{\sqrt{2}}|100\rangle + \frac{b}{\sqrt{2}}|111\rangle. \qquad (7)$$

Сторона *A* застосовує *CNOT* до перших двох кубітів стану (5):

$$|\psi\rangle = \frac{a}{\sqrt{2}}|000\rangle + \frac{a}{\sqrt{2}}|011\rangle + \frac{b}{\sqrt{2}}|110\rangle + \frac{b}{\sqrt{2}}|101\rangle. \qquad (8)$$

Якщо тепер сторона *A* виміряє середній кубіт, то вона отримає стан системи або $\frac{1}{\sqrt{2}}(a|00\rangle + b|11\rangle)$, або $\frac{1}{\sqrt{2}}(a|01\rangle + b|10\rangle)$.

Результати вимірювань відправляються стороні *B*. В разі, якщо цей результат дорівнює $|1\rangle$, сторона *B* інвертує свій кубіт. Таким чином, стан системи завжди буде однаковим і дорівнюватиме $|\psi\rangle = \frac{1}{\sqrt{2}}(a|00\rangle + b|11\rangle)$.

Тепер сторона А застосовує гейт Адамара до першого кубіта (це той самий невідомий біт, стан якого треба передати). В результаті отримаємо:

$$|\Psi\rangle = \frac{a}{2}|00\rangle + \frac{a}{2}|10\rangle - \frac{b}{2}|11\rangle + \frac{b}{2}|01\rangle. \qquad (9)$$

Тепер сторона А вимірює перший кубіт. Якщо результат дорівнює $|0\rangle$, то стан системи буде $|\Psi\rangle = \frac{1}{2}(a|0\rangle + b|1\rangle)$. Якщо ж він дорівнює $|1\rangle$, тоді маємо

$|\Psi\rangle=\frac{1}{2}(a|0\rangle-b|1\rangle)$. В останньому випадку сторона *B* змінює знак біля свого кубіта, і тоді ми завжди отримуємо стан системи $|\Psi\rangle=\frac{1}{2}(a|0\rangle+b|1\rangle)$. Таким чином, ми телепортували стан квантового біта від сторони *A* до сторони *B*. Однак для того, щоби здійснити таку телепортацію, необхідно передати два класичних біти, - результати вимірів сторони *A*. Підсумовуючи, складемо табличку, яка продемонструє вищенаведене.

Результати вимірювань сторони A	**Стан кубіта сторони B**	**Операції сторони B над кубітом**	**Результуючий стан**
0, 0	$(a\|0\rangle+b\|1\rangle)$	Тотожна операція, Тотожна операція	$(a\|0\rangle+b\|1\rangle)$
0, 1	$(a\|0\rangle-b\|1\rangle)$	Тотожна операція, Інверсія знаку кубіта	$(a\|0\rangle+b\|1\rangle)$
1, 0	$(a\|1\rangle+b\|0\rangle)$	Інверсія кубіта, Тотожна операція	$(a\|0\rangle+b\|1\rangle)$
1, 1	$(a\|1\rangle-b\|0\rangle)$	Інверсія кубіта, Інверсія знаку кубіта	$(a\|0\rangle+b\|1\rangle)$

Слід відзначити, що описаний протокол не порушує жодних принципів сучасної фізики, як це може здаватися, зокрема, принципів спеціальної теорії відносності. Дійсно, стан кубіта сторони B не несе ніякої інформації про стан кубіта сторони A, тому не можна стверджувати, що під час квантової телепортації інформація передається зі швидкістю, що перевищує швидкість світла. Більше того, для перенесення стану необхідно передати два класичних біти про результати вимірювань. Це здійснюється стандартними класичними каналами зв’язку, які також не порушують жодних фізичних законів.

Протокол квантової телепортації не порушує також теорему про заборону клонування, оскільки результуючий кубіт знаходиться в стані $|Q\rangle=a|0\rangle+b|1\rangle$, а вихідний кубіт — в одному з базисних станів: $|0\rangle$ або $|1\rangle$.

У практичному розумінні телепортація свідчить, що EPR-пара спільно з двома класичними бітами інформації утворюють ресурс для передавання одного кубіта інформації.

Експериментальну реалізацію квантової телепортації поляризаційного стану фотона було здійснено у 1997 році майже одночасно групами фізиків під керівництвом А. Цайлінгера з університету Інсбрука [23] та Ф. Де Мартіні (університет Риму) [24]. У 2004 році було оголошено про успішну телепортацію квантового стану атомів кальцію (група М. Рібе) та атома берилію (група М. Барретта). У 2006 році науковою групою з Інституту Нільса Бора (Копенгаген) вперше було здійснено телепортацію між об’єктами різної природи: квантами лазерного випромінювання та атомами цезію [25].

У січні 2009 року вченим вперше вдалося телепортувати квантовий стан іона на один метр, а у травні 2010 року дослідниками з університету Сіньхуа виконано передавання квантового стану на 16 кілометрів [26]. На сьогодні, однак, рекорд телепортації належить

вченим Китайського університету науки і технологій, які у 2017 році здійснили передавання квантового стану на відстані 1200 кілометрів [27].

Протокол квантового щільного кодування

Протокол квантового щільного кодування використовує один кубіт разом з EPR-парою для кодування та передавання такої кількості інформації, яку можна передати лише двома класичними бітами [11]. Оскільки бітами EPR-пари можна обмінятися завчасно, виходить, що у випадку маніпулювання квантовими бітами треба фізично передати лише один біт там, де в класичному випадку були б потрібні два. Цей результат до деякої міри дивний, оскільки ми звикли до того, що один біт містить лише одну одиницю інформації.

Щоб зрозуміти в чому тут суть, розглянемо протокол квантового щільного кодування детальніше [11].

Припустимо, що сторони інформаційного обміну *A* та *B* мають по одному кубіту з переплутаної пари:

$$|Q\rangle=\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle). \tag{10}$$

У такому разі вони можуть виконувати операції лише над своїми кубітами.

Припустимо, що сторона *A* хоче передати стороні *B* якусь інформацію, наприклад, здійснити вибір одного з чотирьох можливих варіантів або закодованих повідомлень. Для цього сторона А виконує деякі операції над своїм кубітом і відправляє його стороні *B*. Отримавши кубіт, сторона *B* виконує деякі перетворення над парою і дізнається, яку операцію виконала сторона *A*.

Отже, первісний стан описується співвідношенням (1).

Що може зробити сторона *A* зі своїм кубітом?

1. Може нічого не робити. Тоді стан системи не зміниться: $|Q_1\rangle=\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)$.

2. Може змінити знак біля $|1\rangle$. Отже, будемо мати: $|Q_2\rangle=\frac{1}{\sqrt{2}}(|00\rangle-|11\rangle)$.

3. Може переставити місцями $|0\rangle$ та $|1\rangle$. Тоді (1) матиме вигляд:

$$|Q_3\rangle=\frac{1}{\sqrt{2}}(|10\rangle+|01\rangle).$$

4. Може переставити місцями $|0\rangle$ та $|1\rangle$ та змінити знак біля $|1\rangle$. В цьому випадку (1) перетвориться у: $|Q_4\rangle=\frac{1}{\sqrt{2}}(|10\rangle-|01\rangle)$.

Оскільки пара кубітів переплутана, то відповідних змін зазнає й кубіт, який знаходиться у сторони *B*.

Після виконання однієї з чотирьох дій сторона *A* відправляє свій кубіт стороні *B*, яка тепер матиме обидва кубіти переплутаної пари. Виконавши відповідні операції над нею та провівши вимірювання, сторона *B* може сказати, яку операцію було виконано над кубітом сторони *A*.

Які ж це операції?

1. Сторона *B* застосовує до пари кубітів *CNOT*:

а) Для випадку першої операції (коли сторона *A* нічого не зробила зі своїм кубітом):

$$CNOT:|Q_1\rangle=CNOT:\{\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)\}=\frac{1}{\sqrt{2}}(|00\rangle+|10\rangle)=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)|0\rangle=|\psi_1\rangle.$$

Як бачимо, перший кубіт пари має переплутаний стан, а другий — дорівнює $|0\rangle$.

б) Для випадку другої операції будемо мати:

$$CNOT:|Q_2\rangle=CNOT:\{\frac{1}{\sqrt{2}}(|00\rangle-|11\rangle)\}=\frac{1}{\sqrt{2}}(|00\rangle-|10\rangle)=\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)|0\rangle=|\psi_2\rangle.$$

Як бачимо, другий кубіт знову дорівнює $|0\rangle$.

в) У випадку, коли сторона *A* застосувала третю функцію, отримаємо:

$$CNOT:|Q_3\rangle=CNOT:\{\frac{1}{\sqrt{2}}(|10\rangle+|01\rangle)\}=\frac{1}{\sqrt{2}}(|11\rangle+|01\rangle)=\frac{1}{\sqrt{2}}(|1\rangle+|0\rangle)|1\rangle=|\psi_3\rangle.$$

В цьому випадку вже другий кубіт дорівнює $|1\rangle$.

г) Для четвертої функції:

$$CNOT:|Q_4\rangle=CNOT:\{\frac{1}{\sqrt{2}}(|10\rangle-|01\rangle)\}=\frac{1}{\sqrt{2}}(|11\rangle-|01\rangle)=\frac{1}{\sqrt{2}}(|1\rangle-|0\rangle)|1\rangle=|\psi_4\rangle.$$

І в цьому випадку другий кубіт дорівнює $|1\rangle$.

2. Сторона *B* вимірює значення другого кубіта. Якщо воно дорівнює нулю, то сторона *A* застосувала або першу, або другу функції, якщо ж отримано одиницю — третю або четверту. Далі необхідно з’ясувати, яку саме функцію було застосовано.

3. Застосуємо гейт Адамара до першого кубіта:

$$H:|\psi_1\rangle=\frac{1}{\sqrt{2}}(H|0\rangle+H|1\rangle)|0\rangle=\frac{1}{\sqrt{2}}[\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)+\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)]=\frac{1}{2}2|0\rangle=|0\rangle. \quad (11)$$

Аналогічно отримаємо вирази для другої, третьої та четвертої функцій:

$$H:|\psi_2\rangle=\frac{1}{\sqrt{2}}(H|0\rangle-H|1\rangle)|0\rangle=\frac{1}{\sqrt{2}}[\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)-\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)]=\frac{1}{2}2|1\rangle=|1\rangle. \quad (12)$$

$$H:|\psi_3\rangle=\frac{1}{\sqrt{2}}(H|0\rangle+H|1\rangle)|1\rangle=\frac{1}{\sqrt{2}}[\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)+\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)]=\frac{1}{2}2|0\rangle=|0\rangle. \quad (13)$$

$$H:|\psi_4\rangle=\frac{1}{\sqrt{2}}(H|0\rangle-H|1\rangle)|1\rangle=\frac{1}{\sqrt{2}}[\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)-\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)]=\frac{1}{2}2|1\rangle=|1\rangle. \quad (14)$$

З формул (2) — (5) видно, що дія гейтом Адамара на перший кубіт дозволяє остаточно визначити, яку ж саме функцію було застосовано:

Значення другого кубіта	**Значення першого кубіта**	**Використана функція**
$\|0\rangle$	$\|0\rangle$	$\|Q_1\rangle=\frac{1}{\sqrt{2}}(\|00\rangle+\|11\rangle)$ - перша функція
	$\|1\rangle$	$\|Q_2\rangle=\frac{1}{\sqrt{2}}(\|00\rangle-\|11\rangle)$ - друга функція
$\|1\rangle$	$\|0\rangle$	$\|Q_3\rangle=\frac{1}{\sqrt{2}}(\|10\rangle+\|01\rangle)$ - третя функція
	$\|1\rangle$	$\|Q_4\rangle=\frac{1}{\sqrt{2}}(\|10\rangle-\|01\rangle)$ - четверта функція

Таким чином, використовуючи квантову переплутану пару, ми можемо вибрати одну з чотирьох можливих альтернатив за допомогою передавання каналами зв’язку лише одного біту інформації. Такий факт називається *квантовим надщільним кодуванням*.

Очевидно, що для вирішення такої задачі класичними методами необхідно було би передати по каналах зв’язку два класичних біти:

Значення бітів	**Використана функція**
00	Перша функція
01	Друга функція
10	Третя функція
11	Четверта функція

Описаний протокол був запропонований Чарлзом Беннеттом та Стівеном Візнером у 1992 році. Це один з перших прикладів квантового прискорення обчислень та ущільнення передавання інформації.

Алгоритм Дойча

Алгоритм Дойча (часто відомий як алгоритм Дойча-Джоза) був запропонований Девідом Дойчем та Річардом Джозом у 1992 році і став одним з перших алгоритмів, призначених для квантових комп'ютерів [13]. Ці алгоритми використовують суто квантові явища, такі як квантова суперпозиція та квантова заплутаність, та демонструють значний приріст швидкості виконання порівняно з аналогічними класичними алгоритмами.

Суть задачі Дойча-Джоза полягає у визначенні, чи є вибрана функція двійкової змінної постійною (тобто такою, що дорівнює 0 або 1 незалежно від значення аргументу) або збалансованою (тобто дорівнює 0 для половини області визначення, а для іншої половини — 1). При цьому апріорі відомо, що функція може бути або константою, або збалансованою.

Для розв'язку цієї задачі класичному алгоритму необхідно виконати $2^{n+1}+1$ обчислень функції $f(n)$. Квантовий алгоритм Дойча-Джоза здатний дати правильну відповідь, один раз виконавши фазовий запит, що відповідає функції $f(n)$. Алгоритм Дойча-Джоза ґрунтується на алгоритмі, розробленому Девідом Дойчем у 1985 році. Він є частковим випадком першого, і розглядає функцію однієї змінної. Ми розглянемо цей алгоритм якраз у варіанті функції однієї змінної [13].

Нехай у нас є деякий квантовий оракул, який реалізує деяку функцію $f(x)$.

$$U_f=(|x\rangle|0\rangle)\rightarrow|x\rangle|y\rangle\oplus f(x) \tag{15}$$

Ця функція отримує на вході один кубіт та повертає також один кубіт. Які тут можуть бути варіанти? Наведена нижче таблиця дає відповідь на це запитання.

	x=0	x=1	$f(x)$	Тип
f_0	0	0	I_O	Постійна
f_1	0	1	$CNOT_{iO}$	Збалансована
f_2	1	0	$NOT_O CNOT_{iO}$	Збалансована
f_3	1	1	NOT_O	Постійна

Як видно з таблиці, функції f_0 та f_3 не змінюють своїх значень для усього вхідного діапазону, тобто вони є постійними, а f_1 та f_2 — збалансовані. Функцію f_0 можна вважати як тотожну операцію за виходом I_O, f_1 — $CNOT$ за входом та виходом (iO); f_2 — можна зобразити як $NOT_O CNOT_{iO}$, а f_3 — як заперечення за виходом.

Суть алгоритму Дойча зводиться до наступного.

Нехай ми маємо два кубіти в нульовому стані: $|0\rangle|0\rangle$. Подіємо на них гейтом NOT, щоби перевести у стан $|1\rangle|1\rangle$. Можна було би, звичайно, приготувати кубіти в одиничному стані, але простіше зробити це для нульового, а потім отримати одиничний за допомогою заперечення.

Подіємо гейтом Адамара на кожен кубіт пари:

$$(H\otimes H)|1\rangle|1\rangle=\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)=\frac{1}{2}(|00\rangle-|10\rangle-|01\rangle+|11\rangle)=|Q\rangle. \tag{16}$$

Ми сформували вихідний стан і можемо діяти на нього квантовим оракулом.

$$U_f:|Q\rangle=\frac{1}{2}\{U_f|00\rangle-U_f|10\rangle-U_f|01\rangle+U_f|11\rangle\}=$$
$$=\frac{1}{2}\{|0\rangle|f(0)\rangle-|1\rangle|f(1)\rangle-|0\rangle|1\oplus f(0)\rangle+|1\rangle|1\oplus f(1)\rangle\}.$$

Згрупуємо доданки біля однакових кубітів. Будемо мати:

$$|Q\rangle=\frac{1}{2}\{|0\rangle(|f(0)\rangle-|1\oplus f(0)\rangle)-|1\rangle(|f(1)\rangle-|1\oplus f(1)\rangle)\}. \quad (17)$$

Формула (3) буде робочою для наступного матеріалу.

Розглянемо випадок постійної функції. В такому разі можна записати: $f(0)=f(1)$. Тоді формула (3) буде мати вигляд:

$$|Q\rangle=\frac{1}{2}\{|0\rangle(|f(0)\rangle-|1\oplus f(0)\rangle)-|1\rangle(|f(0)\rangle-|1\oplus f(0)\rangle)\}=$$
$$=\frac{1}{2}\{(|0\rangle-|1\rangle)(|f(0)\rangle-|1\oplus f(0)\rangle)\}. \quad (18)$$

У випадку збалансованої функції ми можемо записати такі співвідношення:

а) якщо $f(0)=0$:

$$1\oplus f(0)=1\oplus 0=1=\overline{f(0)}=f(1);$$

б) якщо $f(0)=1$:

$$1\oplus f(0)=1\oplus 1=0=\overline{f(0)}=f(1);$$

в) якщо $f(1)=0$:

$$1\oplus f(1)=1\oplus 0=1=\overline{f(1)}=f(0);$$

г) якщо $f(1)=1$:

$$1\oplus f(1)=1\oplus 1=0=\overline{f(1)}=f(0).$$

З урахуванням цього формула (3) для збалансованої функції буде мати вигляд:

$$|Q\rangle=\frac{1}{2}\{|0\rangle(|f(0)\rangle-|1\oplus f(0)\rangle)-|1\rangle(|f(1)\rangle-|1\oplus f(1)\rangle)\}=$$
$$=\frac{1}{2}\{|0\rangle(|f(0)\rangle-|f(1)\rangle)+|1\rangle(|f(0)\rangle-|f(1)\rangle)\}.$$

Винесемо спільний множник:

$$|Q\rangle=\frac{1}{2}\{(|0\rangle+|1\rangle)(|f(0)\rangle-|f(1)\rangle)\}. \quad (19)$$

Тепер подіємо на отримані результати гейтом Адамара.

Для постійної функції будемо мати:

$$H|Q\rangle=\frac{1}{2}H(|0\rangle-|1\rangle)(|f(0)\rangle-|1\oplus f(0)\rangle)=\frac{1}{2}\frac{1}{\sqrt{2}}\{(|0\rangle+|1\rangle)-(|0\rangle-|1\rangle)\}\{|f(0)\rangle-|1\oplus f(0)\rangle\}=$$
$$=\frac{1}{2}\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle-|0\rangle+|1\rangle)\{|f(0)\rangle-|1\oplus f(0)\rangle\}=\frac{1}{\sqrt{2}}|1\rangle\{|f(0)\rangle-|1\oplus f(0)\rangle\}.$$

Для збалансованої функції:

$$H|Q\rangle=\frac{1}{2}H(|0\rangle+|1\rangle)(|f(0)\rangle-|f(1)\rangle)=\frac{1}{\sqrt{2}}|0\rangle\{|f(0)\rangle-|f(1)\rangle\}.$$

Відзначимо, що ми застосували квантовий оракул лише один раз.

Тепер нам потрібно виміряти перший кубіт. Якщо ми отримаємо в результаті вимірювання одиницю, то використовували постійну функцію, якщо ж нуль, - збалансовану.

Якщо би ми використовували класичні обчислення, то нам необхідно було б використати оракул двічі: для x=0 та x=1. Однак, ми тоді могли би не тільки сказати яку функцію використали, а й обчислити значення цієї функції. У квантовому випадку ми не можемо обчислити значення функції, однак можемо сказати тип використаної функції лише за одне її застосування. В цьому і є суть квантового прискорення обчислень.

Розділ III. Квантова криптографія

Алгоритм факторизації цілих чисел (алгоритм Шора)

Алгоритм П. Шора — це квантовий алгоритм, призначений для швидкого розкладання цілих чисел на прості множники. Він дозволяє розкласти число N за час $O(\lg^3 N)$, використовуючи $O(\lg N)$ кубітів. Алгоритм було розроблено Пітером Шором 1994 року [15]. Лише через сім років, 2001 року, змогли продемонструвати його працездатність: група спеціалістів з компанії IBM розклали число 15 на множники 3 та 5, використавши лабораторний зразок квантового комп'ютера з сімома кубітами.

Як бачимо, алгоритм Шора не тільки здатен розкласти числа на множники, але може це зробити, як довів сам Пітер Шор, за поліноміальний час. Вважається, що швидкодія алгоритму дозволить розкладати числа майже так само швидко, як і виконувати їх множення.

Що це означає?

В курсі криптографії вивчають, що стійкість асиметричних криптоалгоритмів ґрунтується на так званих односторонніх задачах, тобто на таких математичних задачах, коли пряма функція знаходиться значно швидше за обернену. Найвідомішим прикладом такої задачі є факторизація великих цілих чисел, тобто розкладання їх на прості множники. З математичної практики відомо, що задача розкладання великих цілих чисел на прості множники є проблемою надзвичайної обчислювальної складності. На цій задачі побудований криптоалгоритм RSA. Модуль криптоалгоритму утворюється множенням двох великих простих чисел. Цю операцію виконати не складно. А от обчислити приватний ключ, знаючи публічний, можна лише розклавши модуль на множники. При спробі виконати такі обчислення ми наштовхуємося на задачу надзвичайної обчислювальної складності.

Якщо квантовий алгоритм дозволить значно прискорити ці обчислення, асиметрична криптографія може припинити своє існування. Більше того, йдеться не тільки про RSA, а й про інші асиметричні алгоритми, які квантовий комп'ютер здатен зламати аналогічним чином.

Відмінністю алгоритму Шора порівняно з класичними алгоритмами факторизації є його ймовірнісний характер, оскільки задача факторизації зводиться до задачі знаходження періоду функції. Необхідно також спостерігати за квантовою пам'яттю, що теж призводить до випадкових результатів.

Припустимо, що нам треба розкласти ціле число N на прості множники. Це означає, що необхідно знайти таке просте число $a=(1 \div N-1)$, на яке N ділиться без залишку.

Для цього виберемо якесь ціле число a та за допомогою алгоритму Евкліда обчислимо найбільший спільний дільник двох чисел НСД (a, N). Якщо він більший за одиницю, то задачу розв'язано, число N розкладено на множники. Якщо ж числа a та N взаємно прості, то за теоремою Ейлера відомо, що існує такий степінь a, який ділиться на N із залишком 1.

Нехай r — найменший такий степінь. Тоді

$$a^r \equiv 1 \, mod \, N. \qquad (20)$$

Нагадаємо, що *r* називають порядком *a* за mod *N*. Покажемо, що інформація про *N* може нам надати інформацію про дільник *N*.

Розглянемо послідовність степенів двійки за модулем 15 тобто $2^x \bmod 15$. Послідовність буде така:

2, 4, 8, 1, 2, 4, 8, 1, ...

Як бачимо, степені двійки за модулем 15 являють собою періодичну послідовність з періодом 4.

Інший приклад: $2^x \bmod 21$:

2, 4, 8, 16, 11, 1, 2, 4, 8, 16, 11, 1, 2, 4, ...

Бачимо, що ми також маємо періодичну послідовність з періодом 6.

Згідно теореми Ейлера, якщо число *N* є добутком двох простих чисел *p* та *q*, тоді якщо *a* в послідовності (1) не ділиться націло ні на *p*, ні на *q*, то послідовність буде мати період, який є дільником числа (*p*-1)(*q*-1).

Наприклад, якщо *N*=15, то числа *p*=3, *q*=5, (*p*-1)(*q*-1)=2x4=8. І дійсно, період такої послідовності дорівнює 4, що є дільником 8.

Аналогічно, якщо *N*=21, *p*=3, *q*=7, (*p*-1)(*q*-1) = 2x6 = 12. В цьому випадку період послідовності дорівнює 6, що також є дільником 12.

Отже, ми бачимо, що знання періоду дійсно надасть нам корисні відомості про (*p*-1)(*q*-1).

Тепер з'ясуємо, як ми можемо використати отриману інформацію.

Припустимо, що ми знайшли період *r*. Нехай він виявився парним. Тоді (1) можна записати таким чином:

$$a^r - 1 \equiv 0 \bmod N. \qquad (21)$$

Якщо період парний, то ліву частину (2) можна розкласти на множники як різницю квадратів:

$$\left(a^{(r/2)} - 1\right)\left(a^{(r/2)} + 1\right) \equiv 0 \bmod N. \qquad (22)$$

Нехай $A = \left(a^{(r/2)} - 1\right); B = \left(a^{(r/2)} + 1\right)$ Тоді добуток *AB* ділиться на *N*. Якщо ні *A*, ні *B* окремо не діляться на *N*, тоді кожен з них обов'язково має з ним спільний множник. В такому разі знайшовши НСД(*A*, *N*) та НСД(*B*,*N*), за допомогою того ж алгоритму Евкліда, ми знайдемо нетривіальний дільник числа *N*.

Продемонструємо це на простому прикладі. Розглянемо *N*=15. Оберемо взаємно просте з *N* число *a*=7.

Обчислимо:

$$7^1 \bmod 15 \equiv 7;$$
$$7^2 \bmod 15 \equiv 14;$$
$$7^3 \bmod 15 \equiv 343 \bmod 15 \equiv 13;$$
$$7^4 \bmod 15 \equiv 2401 \bmod 15 \equiv 1.$$

Отже, ми маємо порядок 7 за *mod* 15 = 4. Ми знайшли *r*. Воно парне. Використаємо формулу (22):

$$(7^2-1)(7^2+1)=48\times 50=2400.$$

Це число має ділитися на 15 без залишку: 2400 : 15 = 160. Оскільки ж ні 48, ні 50 окремо не діляться без залишку на 15, то вони повинні мати з ним спільні множники. Очевидно, що НСД(15, 48) = 3, а НСД (15, 50) = 5.

Таким чином, ми розклали число *N* на прості множники.

Що трапиться, якщо знайдене *r* буде непарним або взаємно простим з *N*? Тоді вибирається інше число *a* й алгоритм повторюється спочатку.

Тепер нам залишилося з'ясувати, як можна обчислити період послідовності *a*. Для цього використовують квантове перетворення Фур'є [28].

Перетворення Фур'є у загальному випадку переносить дані з часової області аргументів у частотну. Наприклад, якщо подіяти перетворенням Фур'є на функцію з періодом *r*, то її буде перетворено у функцію з ненульовими коефіцієнтами там, де значення частоти кратні 2π/*r*.

Наприклад, нехай ми маємо періодичний процес типу exp(2*iπωx*). Припустимо, що частота цього процесу невідома. Як її визначити?

Уведемо перетворення Фур'є як:

$$F\to\Phi(\lambda)=\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\infty}e^{(-i\lambda x)}f(x)dx.$$

Обернене перетворення Фур'є:

$$F^{-1}\to f(x)=\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\infty}e^{(i\lambda x)}\Phi(\lambda)d\lambda.$$

Подамо на вхід цього перетворення наш коливний процес:

$$FT:e^{(2i\pi\omega x)}\to\Phi(\lambda)=\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\infty}e^{(i(2\pi\omega-\lambda)x)}dx.$$

Якщо аргумент λ близький до 2π*ω*, то значення інтегралу будуть ненульовими. І навпаки, якщо 2π*ω* і *λ* далекі, то інтеграл прямує до нуля. Таким чином, після перетворень Фур'є ми чітко можемо побачити, з яких періодичних процесів складається наш коливний процес, які частоти цих коливань та іншу інформацію про нього. Цей факт робить перетворення Фур'є незамінним інструментом для дослідження коливних процесів. Варто сказати, що на основі Фур'є- аналізу працює уся радіотехніка та системи розпізнавання.

Дискретне перетворення Фур'є діє на *N* рівновіддалених вибірок у напівінтервалі (0, 2π] для деякого *N*, і видає на виході функцію, чия область визначення — цілі числа від 0 до *N*-1. Дискретне перетворення Фур'є функції з періодом *r* — це функція, зосереджена біля значень *N*/*r*. Отже, якщо період *r* ділить *N* без залишку, то результатом перетворення буде функція, ненульові значення якої будуть лише в точках, кратних *N*/*r*. В іншому разі результат буде наближеним, і відмінні від нуля числа з'являться в точках, близьких до кратних *N*/*r*.

Швидке перетворення Фур'є — різновид дискретного перетворення Фур'є, де *N* — степінь двійки, тобто $N=2^m$.

Квантове перетворення Фур'є є варіантом дискретного перетворення Фур'є, де також використовуються степені двійки.

Квантове перетворення Фур'є діє не на функцію, а на квантові стани так, що

$$\sum_x g(x)|x\rangle \rightarrow \sum_c G(c)|c\rangle,$$

де $G(c)$ — перетворення функції $g(x)$, x, c — цілі числа від 0 до N-1 у двійковому представленні. Якби ми виміряли значення квантового регістра, то ймовірність того, що ми б отримали в результаті c буде $|G(c)|^2$.

Застосовуючи квантове перетворення Фур'є до періодичної функції $g(x)$ з періодом r, ми отримаємо $\sum_c G(c)|c\rangle$ з відмінним від нуля G(c) лише там, де значення c кратні N/r. Отже, коли стан виміряно, то результатом будуть лише значення jN/r. Квантове перетворення Фур'є дає лише наближений результат для періодів, які не є степенями двійки, однак чим більший степінь двійки використаний як база, тим точнішим буде результат.

Квантове перетворення Фур'є можна увести в такий спосіб:

$$QFT:|a\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{b=0}^{N-1} e^{(\frac{-2i\pi ab}{N})}|b\rangle;$$

$$QFT^{-1}:|b\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{a=0}^{N-1} e^{(\frac{2i\pi ab}{N})}|a\rangle.$$

Отже, якщо в квантовому регістрі буде двійкове представлення якоїсь функції з періодом, кратним N, то після перетворення в ньому будуть відмінні від нуля значення лише в точках, кратних N.

Квантове перетворення Фур'є з базою $N=2^m$ визначимо так:

$$QFT:|x\rangle \rightarrow \frac{1}{\sqrt{2^m}} \sum_{c=0}^{2^m-1} e^{(\frac{2i\pi cx}{2^m})}|c\rangle.$$

Тепер розглянемо як використовується квантовий алгоритм Фур'є для знаходження періоду функції $a^x \bmod N$ в алгоритмі Шора.

Для його реалізації потрібно мати два квантових регістри, X та Y в нульовому стані.

<u>*Крок 1*</u>. На першому кроці за допомогою оператора Адамара регістр X переводиться до стану суперпозиції. Квантова система тоді буде знаходитися в стані:

$$|Q\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x,0\rangle.$$

<u>*Крок 2*</u>. Нехай ми маємо квантовий оракул, який діє звичним нам чином:

$$U_f:|x,0\rangle \rightarrow |x, a^x mod\, N\rangle.$$

Подіявши на стан $|Q\rangle$, будемо мати:

$$U_f:|Q\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x, a^x mod\, N\rangle.$$

Це значить, що в другому регістрі ми отримали значення функції, розраховані для усіх x одночасно. Оскільки функція в другому регістрі періодична, нам треба залучити квантове перетворення Фур'є для знаходження періоду.

<u>*Крок 3*</u>. Для цього подіємо на результуючий стан системи оракулом, який реалізує квантове перетворення Фур'є:

$$QFT:|Q\rangle \rightarrow \frac{1}{N}\sum_{x=0}^{N-1}\sum_{k=0}^{N-1} e^{(-2i\pi\frac{kx}{N})}|k, a^x \bmod N\rangle.$$

Крок 4. Зі стандартного Фур'є-аналізу ми знаємо, що експонента буде відмінною від нуля лише там, де *k* кратне *N*, тобто в точках *jN/k*. Вимірювання першого регістру нам дає стан $|k, a^k \bmod N\rangle$ з ймовірністю

$$\left(\left|\frac{1}{N}\sum_{x:a^x \bmod N = a^k \bmod N} e^{(-2i\pi\frac{kx}{N})}\right|\right)^2.$$

Отже, ми знайшли значення *k*. Решту часу працює класичний комп'ютер.

Крок 5. Нехай при цьому вимірюванні ми отримали в другому регістрі значення *v*. Якщо період дорівнює $r=2^k$, то ми можемо записати:

$$v = j\frac{2^m}{r}$$

для деякого *j*. Тоді $\frac{v}{2^m} = \frac{j}{r}$, звідки знаходиться *r*.

Якщо період не дорівнює степені двійки або він непарний, або алгоритм видає саме число *N* як його дільник, чи період r та множник j мають спільний множник, то операція знаходження періоду повторюється $O(\lg \lg N)$ разів з тим же самим *a*. Якщо й цього разу період не знайдений, змінюють *a* і алгоритм повторюється спочатку.

Пітер Шор довів, що невелика кількість повторень алгоритму знаходить множник числа *N* з великою ймовірністю.

Значення алгоритму Шора полягає в тому, що з його допомогою, використовуючи квантовий комп'ютер з кількома сотнями логічних кубітів, стає можливим злам криптосистем з публічним ключем. Однією з найпопулярніших двоключових криптосистем є RSA. Відомо (теорема Рабіна [29]), що криптостійкість такої системи дорівнює складності розкладання великого цілого числа (модуль криптосистеми) на прості множники. За допомогою такої факторизації можна, знаючи публічний ключ криптосистеми, обчислити приватний. Найкращий з класичних алгоритмів факторизації потребує часу порядку $N^{1/3}$. Алгоритм Шора, використовуючи можливості квантових комп'ютерів, здатен виконати факторизацію числа не просто за поліноміальний час, а й ненабагато повільніше за множення цілих чисел. Таким чином, реалізація масштабованого квантового комп'ютера зробила би абсолютно безперспективною усю асиметричну криптографію, оскільки він здатен зламати аналогічним чином й інші схожі схеми.

Алгоритм пошуку у невпорядкованому масиві (алгоритм Гровера)

Алгоритм був розроблений американським математиком Ловом Гровером у 1996 році [17].

Припустимо, що ми маємо базу даних з *N* невпорядкованих записів, один з яких задовольняє певну умову. Ми хочемо знайти цей особливий запис. Будь-якому класичному алгоритму для знаходження такого запису потрібно не менше за $O(N)$ кроків. З елементарних міркувань зрозуміло, що якщо ми перевіримо *k* записів, то знайдемо потрібний з ймовірністю

k/N. Ця ймовірність прямує до нуля зі зростанням *N*, якщо *k* не того ж порядку, що й *N*.

Квантовий алгоритм Гровера розв'язує цю задачу з прискоренням у $\sqrt{N}$ разів, тобто за $O(\sqrt{N})$ кроків.

Неструктурованість даних дуже важлива, оскільки на сортованому масиві класичний алгоритм дихотомії гарантує швидкість $O(\lg N)$ кроків [17].

Переформулюємо задачу таким чином. Нам дано "чорну скриньку", яка обчислює потрібну нам функцію від *N* вхідних даних зі значеннями на виході, що дорівнюють нулю або одиниці. Крім того, відомо, що $f(x)=1$ лише в одному випадку, для деякого вхідного значення x_0. Наша задача полягає в тому, щоби знайти x_0.

Нехай *N* таке, що $2^n \geq N$, U_P — квантовий оракул, який обчислює класичну функцію $P(x)$, що перевіряє істинність твердження (істині відповідає одиниця):

$$U_P:|x\rangle \rightarrow |x, P(x)\rangle.$$

Для того, щоби реалізувати в таких умовах алгоритм Гровера, необхідно виконати такі кроки.

Перший крок — стандартний для квантових обчислень. Необхідно заповнити регістр нулями, тобто отримати стан $|0\rangle$. Після цього ми діємо на цей квантовий регістр гейтом Адамара:

$$H:|0\rangle \rightarrow \frac{1}{\sqrt{2^n}} \sum_{x=0}^{n-1} |x\rangle.$$

Таким чином ми отримаємо суперпозицію усіх можливих станів *x* в нашому регістрі.

Крок 2. Діємо квантовим оракулом на отриманий стан квантової системи:

$$U_P:|Q\rangle \rightarrow \frac{1}{\sqrt{2^n}} \sum_{x=0}^{n-1} |x, P(x)\rangle.$$

Тепер задача полягає в тому, щоби отримати з цієї суперпозиції корисний результат. Очевидно, що тут буде присутній й потрібний нам результат: $|x_0, 1\rangle$. Оскільки амплітуда такого стану буде $2^{-n/2}$, то ніякої користі поки що немає. Значить, нам треба буде змінити квантовий стан таким чином, щоби амплітуда при потрібному нам результаті була значно більшою. Якщо нам вдасться це зробити, тоді при вимірюванні з великою ймовірністю ми зможемо отримати $|x_0, 1\rangle$.

Крок 3. Для збільшення амплітуди біля одиничних членів алгоритм пропонує такий спосіб. Перше — це зміна знаку біля одиничних членів, друге — інверсія відносно середнього значення.

Розглянемо простий приклад того, як можна змінити знак лише біля одиничних значень функції.

Нехай у нас є квантовий оракул, який виконує перетворення:

$$U_P:|x, b\rangle \rightarrow |x, b \wedge P(x)\rangle.$$

Застосувавши такий оракул до суперпозиції $|\psi\rangle=\frac{1}{\sqrt{2^n}}\sum_{x=0}^{n-1}|x\rangle$ з $b=\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$ отримаємо стан, де знак усіх x, при яких $P(x) = 1$ буде змінено, а b залишиться незмінним.

Дійсно,

$$|\psi,b\rangle\rightarrow\frac{1}{\sqrt{2^n}}\sum_{x=0}^{n-1}|x,b\wedge P(x)\rangle=\frac{1}{\sqrt{2^n}}\Big(\sum_{x=X_0}|x,0\rangle+\sum_{x=X_1}|x,1\rangle\Big)\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)=\frac{1}{\sqrt{2^{(n+1)}}}$$

$$\Big(\sum_{x=X_0}|x,0\wedge 0\rangle+\sum_{x=X_1}|x,1\wedge 0\rangle-\sum_{x=X_0}|x,0\wedge 1\rangle-\sum_{x=X_1}|x,1\wedge 1\rangle\Big)=\frac{1}{\sqrt{2^{(n+1)}}}$$

$$\Big(\sum_{x=X_1}|x,0\rangle-\sum_{x=X_1}|x,1\rangle\Big).$$

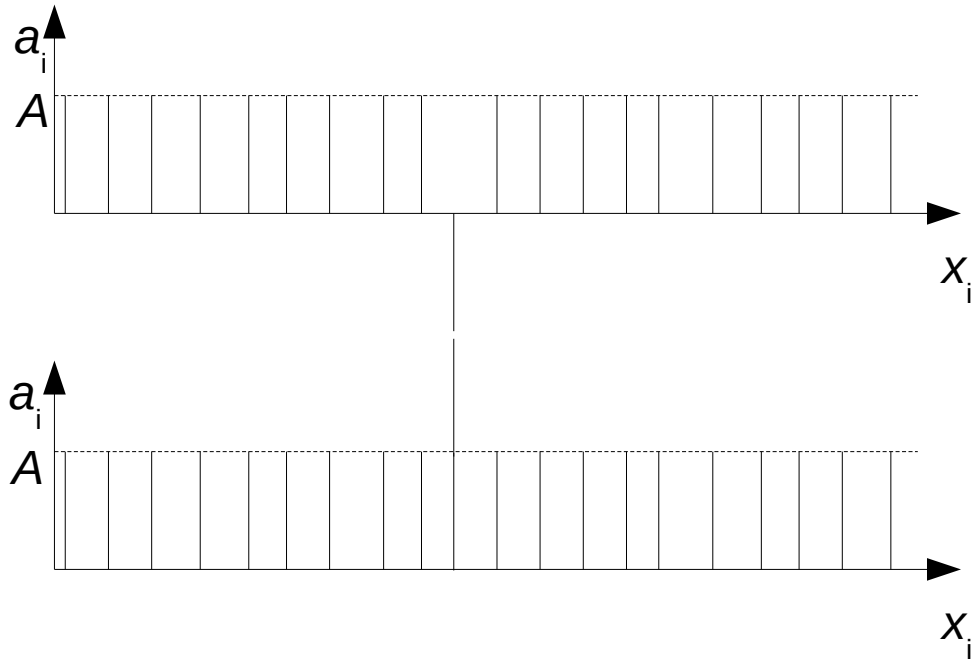
Тут X_0 — ті стани, де $P(x) = 0$, а X_1 — де $P(x)=1$. Ми бачимо, що знак біля одинички змінився.

Інверсія відносно середнього. Щоби виконати інверсію відносно середнього значення, необхідно побудувати таке перетворення:

$$\sum_{i=0}^{n-1}a_i|x_i\rangle\rightarrow\sum_{i=0}^{n-1}(2A-a_i)|x_i\rangle.$$

Тут A — середнє значення, a_i — коефіцієнти біля x_i, які визначають ймовірність того чи іншого стану системи.

Почергове застосування цих операцій приведе до того, що ймовірність біля одиничних станів зросте порівняно з нульовими, як це показано на рисунку.



Верхній рисунок демонструє зміну знаку у елементів, де значення функції дорівнює одиниці, а нижній — інверсію відносно середнього значення A.

Лов Гровер довів, що повторення цих кроків $\frac{\pi}{4}\sqrt{2^n}$ разів дозволяє максимізувати ймовірність отримання при вимірюванні одиничного значення.

Цікавим є той факт, що подальше застосування вказаних операцій не тільки не приводить до збільшення ймовірності, але й зменшує її. Цей факт стає зрозумілим, якщо взяти до уваги, що процедури, які виконуються над регістром, є обертанням комплексного простору на певний кут. Отже, спочатку застосування квантового перетворення повертає стан до бажаного, а потім, очевидно, подальші повороти будуть віддаляти вектор від потрібного кута. Таким чином, щоби отримати задовільні результати від застосування цього перетворення, необхідно чітко знати можливу кількість повторень. Для цього існують спеціальні алгоритми, які ми розглядати не будемо.

Квантові протоколи узгодження ключів

Якщо дослідникам та конструкторам вдасться реалізувати універсальний квантовий комп’ютер, який зможе ефективно реалізувати алгоритми Шора та Гровера, то цілі розділи класичної криптографії опиняться під загрозою зникнення. Дійсно, швидкий алгоритм факторизації зробить неефективною асиметричну криптографію, причому це стосується не лише RSA, оскільки з не меншою ефективністю, напевне, можна буде розв’язати й задачі дискретного логарифмування та знаходження точок кратності еліптичних кривих. В той же час, швидкий пошук у невпорядкованому масиві робить тривіальною атаку “грубою силою” на криптографічні ключі симетричних криптосистем.

Таким чином, необхідно шукати альтернативу класичним криптоалгоритмам. Сьогодні одним з новітніх підходів до рішення цієї проблеми є квантова криптографія.

Квантова криптографія — це розділ квантової інформатики, який вивчає методи захисту інформації з використанням квантових носіїв. Можливість такого захисту визначається, перш за все, теоремою про неможливість клонування невідомого квантового стану. Існування цієї теореми привело до розробки протоколу квантової телепортації, вона ж забезпечує захист інформації від прослуховування в квантових каналах зв’язку.

Здається, тоді достатньо встановити такий канал зв’язку між учасниками інформаційного обміну, й можна обмінюватися відкритими повідомленнями без використання криптографічного захисту. Однак, сьогодні це занадто дорого й повільно.

З другого боку, квантовий канал зв’язку можна використати для узгодження криптографічних ключів симетричних алгоритмів, оскільки популярні сьогодні протоколи узгодження ключа на основі асиметричних алгоритмів знаходяться під найбільшою загрозою з боку алгоритму Шора. Це також можливо, але існує алгоритм Гровера, який дозволить досить швидко підібрати ключ до перехопленого, зашифрованого симетричним алгоритмом, повідомлення. Отже симетричні алгоритми також використовувати небажано.

Єдиний варіант, який залишається нам — це потокові шифри, наприклад, шифр Вернама, ключ до якого узгоджується за допомогою квантових протоколів.

Саме так сьогодні й виглядає найпопулярніша схема квантової криптографії [30].

Квантовий протокол узгодження криптографічного ключа BB84

Цей протокол був розроблений Чарлзом Беннеттом та Жілем Брассаром у 1984 році, звідки й походить його назва. Потім він зазнав кількох модифікацій, однак ми розглянемо його першу інтерпретацію, - на чотирьох квантових станах [10].

Нехай ми маємо канал зв’язку, чистий настільки, що він може пропускати окремі фотони без значних втрат. Нехай у нас є також обладнання, яке вміє випромінювати фотони поодинці. Ці фотони мають довільну, але строго визначену поляризацію.

Назвемо поляризацією електромагнітних хвиль напрямлені коливання векторів електричного та магнітного полів. Будемо вважати, що такою ж поляризацією володіють й окремі фотони, хоча насправді це не зовсім так.

Припустимо, що фотони можуть мати або вертикально-горизонтальну поляризацію, яку будемо називати ортогональною, або діагональну, як це показано на рисунку. Як цього можна досягти, адже лазер випромінює фотони довільної поляризації? Справа в тому, що на виході нашого устаткування стоїть поляризаційний фільтр, який може пропускати фотони лише певної поляризації. Наприклад, якщо фільтр може пропускати лише фотони вертикальної поляризації і затримувати усі горизонтальної, то після нього всі фотони будуть мати тільки вертикальну поляризацію.

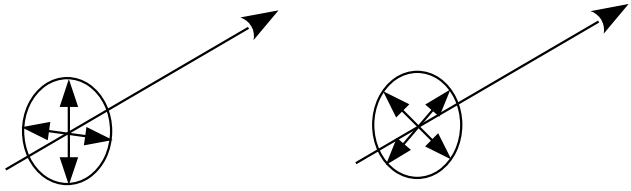


Рисунок 18: Типи поляризації фотонів: ліворуч — ортогональна поляризація; праворуч — діагональна.

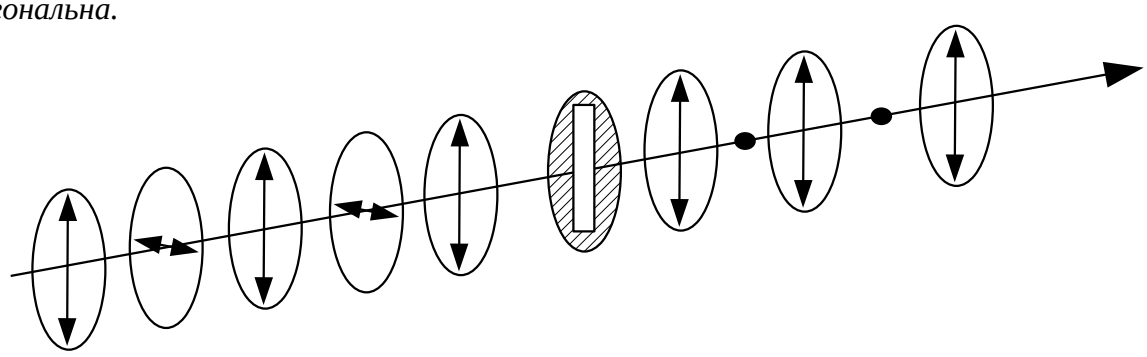


Рисунок 19: Схема фільтрування потоку фотонів поляризаційним фільтром.

Це приведе до зменшення кількості фотонів після фільтру, тобто до зменшення інтенсивності потоку. Так ми платимо за те, що потік фотонів буде чітко поляризований, наприклад, вертикально.

Якщо ж лазер випромінює фотони діагональної поляризації, частину їх також буде затримано, однак тут ми можемо лише говорити про те, з якою ймовірністю той чи інший фотон буде затриманий. Отже, у цьому випадку працює звична для нас квантова схема. Можливі, наприклад, такі варіанти, які показано на рис. 20.

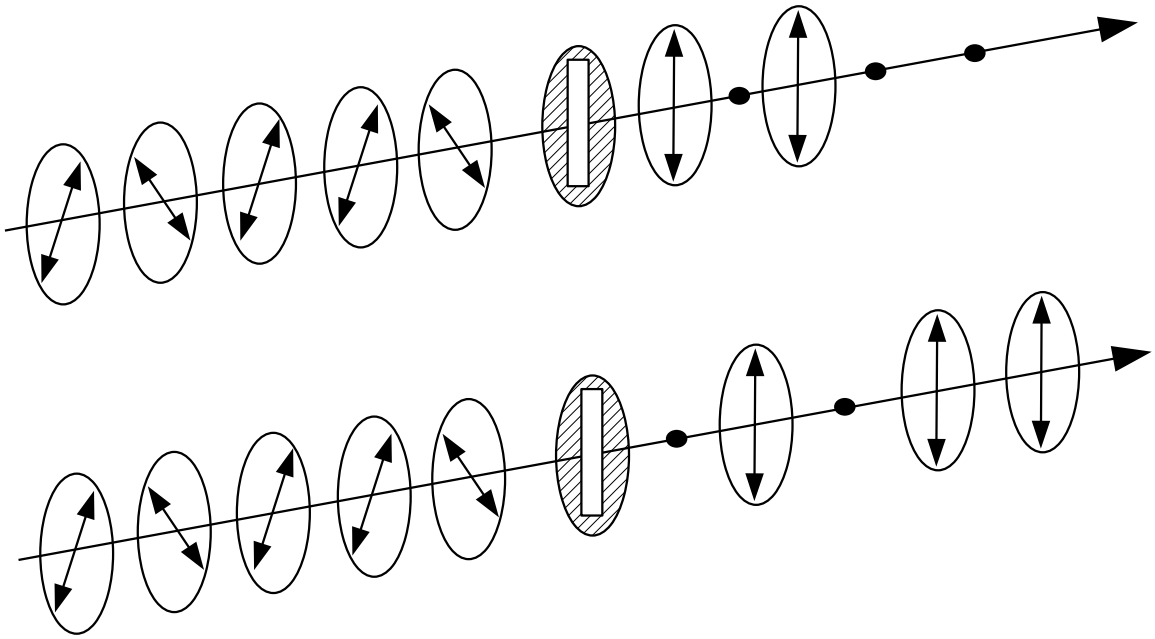


Рисунок 20: Різні варіанти пропускання фільтром фотонів діагональної поляризації.

Одним словом, ми не знаємо, яким чином піде процес, а лише можемо говорити про певну ймовірність того чи іншого стану системи.

Яким же чином цю ситуацію можна використати для узгодження криптографічних ключів?

Припустимо, що абонент А має таку систему, вдосконалену тим, що фільтр може довільним чином змінювати напрям поляризації, вибираючи з чотирьох позицій, які показано на рис. 21.

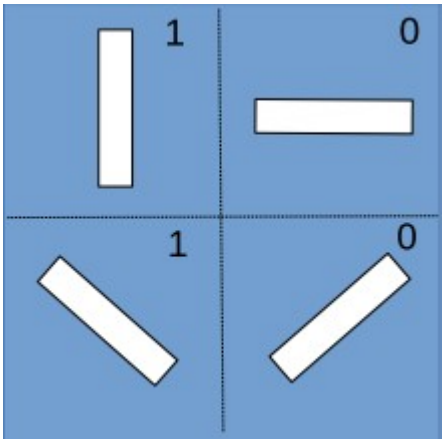


Рисунок 21: Схема поляризаційного фільтру, використаного у протоколі узгодження ключа.

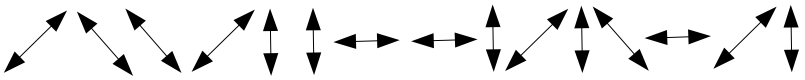
Вибір позиції щоразу випадковий. Будемо приймати за “1” вертикальну поляризацію фотона, а за “0” - горизонтальну. Одиниця та нуль діагональної поляризації показані на рисунку.

Нехай абонент А передає потік одиничних фотонів, весь час змінюючи положення поляризаційного фільтру випадковим чином. На виході ми отримаємо потік фотонів кожної з чотирьох поляризацій. На приймальному боці у абонента Б є приймальна апаратура, яка

використовує такий самий фільтр, також орієнтуючи його випадковим чином. Отже, якщо фільтр зорієнтовано горизонтально, а на нього потрапляє вертикально зорієнтований фотон, то його буде затримано, на виході приймальної апаратури не буде нічого. Якщо ж фільтр зорієнтовано діагонально, а фотон поляризований вертикально, то він з певною ймовірністю може бути пропущений. І ми не можемо стверджувати, що станеться напевне.

Розглянемо, як ми можемо узгодити криптографічний ключ за допомогою такої схеми.

Припустимо, що лазер абонента А згенерував послідовність фотонів з такою поляризацією:



Тоді ми отримали такий бітовий рядок: 0, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1.

Ці та подальші дії, а також отримані результати подано в таблиці.

1	0	1	1	0	1	1	0	0	1	0	1	1	0	0	1
2	X	+	X	+	+	+	+	+	X	X	+	X	X	X	+
3	0	-	1	-	1	1	0	0	-	0	1	1	-	0	1
4	+	X	X	+	+	X	X	+	X	+	X	X	X	X	+
5	1		1		1	0	0	0		1	1	1		0	1
6	+		X		+	X	X	+		+	X	X		X	+
7			√		√			√				√		√	√
8			1		1			0				1		0	1
9					1									0	
10					√									√	
11			1					0				1			1

Записані в таблиці дії слід читати в такий спосіб.

Перші п'ять дій виконуються квантовим каналом зв'язку.

1. В цьому рядочку поданий бітова послідовність, яку згенерував лазер абонента А.

2. Орієнтація (базиси) поляризаційного фільтра, які були обрані абонентом А: X — діагональний; + - ортогональний.

3. Фотони (бітовий рядок), відправлений абонентом А в канал зв'язку.

4. Випадкові базиси, обрані абонентом Б під час приймання сигналу.

5. Результуючий бітовий рядок, отриманий абонентом Б.

Решта дій виконуються відкритим каналом зв'язку.

6. Абонент Б повідомляє А обрані ним базиси.

7. А відзначає, які базиси узгоджуються.

8. Узгоджені біти ключа, які можна використовувати, якщо не було порушень під час узгодження ключа.

Якщо є підозра, що канал прослуховується, виконуються наступні операції:

9. Абонент Б вказує деякі, вибрані випадково, біти ключа.

10. Абонент А підтверджує ці біти.

Результат

11. Секретні біти, які можна використовувати як узгоджений криптографічний ключ.

Коли цей одноразовий ключ буде повністю використано, протокол узгодження нової порції ключа повторюється спочатку.

Цей протокол досить малоефективний, оскільки, як ми бачимо, з переданих 15 бітів в цьому прикладі узгодили лише 4.

Протокол узгодження ключа B92

Протокол BB84 використовує чотири напрями поляризації фотонів. У 1992 році Чарлз Беннетт показав, що аналогічний протокол можна побудувати за допомогою лише двох напрямів поляризації [12]. Протокол було названо B92 за аналогією з BB84.

Він використовує фотони, поляризовані у двох різних напрямках: за “1” приймається поляризація під кутом +45°, а за нуль — під кутом 0°.

Процедуру узгодження ключа за цим протоколом схематично подано на рисунку 22.

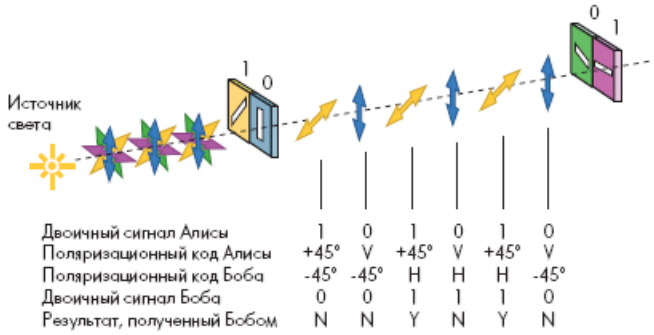
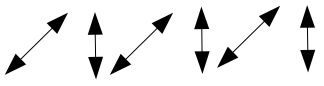


Рисунок 22: Схема узгодження ключа за протоколом B92.

Апаратура абонента А генерує фотони, поляризовані в напрямках 0 та +45 градусів. Відповідно, вони представляють нулі та одиниці, причому поляризація кожного фотона випадкова. Детектувальна апаратура на приймальному боці приймає фотони крізь фільтри, орієнтовані під кутами 90 та -45 градусів. При цьому, якщо фотон аналізується крізь фільтр, орієнтований під кутом 90° відносно його поляризації, то фотон буде затримано. Якщо ж цей кут становить 45°, то фільтр пропустить фотон з ймовірністю 50%.

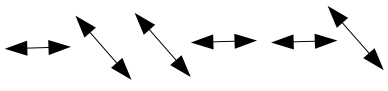
Розглянемо приклад узгодження бітів ключа за цим протоколом.

Припустимо, що абонент А згенерував таку послідовність фотонів:



Це означає бітовий рядок 1, 0, 1, 0, 1, 0.

На приймальному боці абонент Б застосував до цих фотонів такі фільтри:



Ми бачимо, що в такому разі тільки для 3-го та 4-го фотонів напрям приймальних фільтрів був перпендикулярний до напряму поляризації фотонів. Відповідно, ці фотони точно були затримані апаратурою. Отже, ми отримаємо таку послідовність з прийнятих та затриманих фотонів: +, +, -, -, +, +, де “+” - це прийнятий фотон, а “-” - затриманий. Однак, тут не враховано той факт, що в разі кута між поляризацією фільтра і фотона в 45 градусів, крізь фільтр проходять лише 50% фотонів. Нехай і в нашому випадку з чотирьох можливих система пропустила лише два. Тоді послідовність пропущених та затриманих фотонів буде виглядати приблизно так: -, +, -, -, +, -. Залишилося з’ясувати, які саме двійкові значення отримав абонент Б. Напрям поляризації 2-го фотона на вході був 0^o (це “0” за нашими домовленостями). Якщо він пройшов крізь приймальний фільтр, то його поляризація стала -45^o, що також відповідає нулю, як це показано на рисунку 5. Отже значення, яке “приніс” другий фотон — нуль. Аналогічно, передостанній фотон мав напрям поляризації $+45^o$, що відповідає одиниці. Якщо ж його пропустила приймальна апаратура, то напрям поляризації став 90^o, що відповідає одиниці. Таким чином, ми узгодили два біти ключа: 0, 1.

Для цього протоколу використовується така ж процедура просіювання ключа, як і для BB84.

Протокол B92 ще більш витратний, ніж BB84. Дійсно, ймовірність того, що абонент Б застосує для чергового фотона фільтр з поляризацією в 45^o в середньому буде дорівнювати 50%. В свою чергу, ймовірність того, що цей фільтр пропустить фотон також дорівнює 50%. Отже, на приймальному боці зможуть виявити лише 25% відправлених абонентом А фотонів. Тим не менше, в цьому є й позитивний момент: дії зловмисника, який буде прослуховувати канал, буде легше виявити, оскільки спотворення інформації будуть більшими.

Атаки на протоколи квантового узгодження ключа

Розглянемо, які дії повинен виконати зловмисник для того, щоби перехопити цей ключ, і чи зможе він це зробити.

Можливі варіанти такі:

1. Скопіювати ключ під час передавання неможливо, оскільки ми знаємо, що існує теорема про неможливість клонування невідомого квантового стану. Це саме такий випадок, оскільки зловмисник не знає, який стан того чи іншого фотона. Саме це він і прагне з'ясувати. Копіювання змінить стан фотонів, і перевірка абонентів А та Б це виявить. Отже, цей варіант не проходить.

2. Скористатися протоколом квантової телепортації зловмисник також не може, оскільки при цьому руйнується стан оригінального фотона.

Тим не менше, припустимо, що зловмисникові якимось невідомим для нас чином вдалося виміряти поляризацію кожного фотона, який мандрував каналом зв'язку. Хай навіть так! Однак, він не в змозі дізнатися, яка випадкова послідовність положень фільтра була на приймальному боці у абонента Б. Отже, зловмисник спробує вгадувати ці стани, тобто застосує свою послідовність. Звичайна теорія ймовірностей говорить про те, що в такому разі він може вгадати не більше 50% положень фільтра, що значно менше, ніж потрібно. Однак, це ще не всі його проблеми. Якщо він при цьому сформує свій фотон для того, щоби

відправити його абоненту Б, то його поляризація буде неправильною внаслідок редукції хвильової функції. Вимірюючи цей “неправильний” фотон в своєму базисі, абонент Б неодмінно помітить помилку і зрозуміє, що канал прослуховують. Значення похибки на приймальному боці можна оцінити з таких міркувань. Припустимо, зловмисник атакував не кожний фотон, а якусь їх частину з ймовірністю p. Тоді 1-p сигналів приходить абоненту Б без змін. Для сигналів, що були атаковані, існує два варіанти розвитку подій: 1) зловмисник правильно вгадав базис, а отже правильно передав сигнал абоненту Б, не вносячи ніяких спотворень; 2) базис був вгаданий неправильно, ймовірність чого дорівнює 0,5. Отже з цією ймовірністю результат вимірювань був неправильним, і абсолютно точно він передав “неправильний” фотон абоненту Б. Це призводить до помилки на його боці з такою самою ймовірністю 0,5.

Ймовірність кожного сценарію дорівнює 0,5, а отже легко бачити, що на приймальному боці накопичується 25% неправильних результатів, що занадто багато для якісного каналу. Більше того, теоретичні оцінки для каналів зв'язку, згідно з критерієм Шеннона, зменшують цю ймовірність до 11%. Таким чином, прийнято вважати, що 11% помилок - це межа до якої можливе секретне узгодження ключа.

Отже, будь-які дії зловмисника призведуть до того, що абонент Б, проходячи по отриманій послідовності, обов'язково помітить, що у деяких ситуаціях він застосував правильну схему, а чомусь результату (ні “0”, ні “1”) не отримав. Це буде свідчити, що канал зв'язку знаходиться під контролем сторонньої особи. Цей факт буде сигналом для переходу на інший канал і повторення усієї процедури узгодження ключа з самого початку.

Сьогодні на ринку немає однофотонних випромінювачів, тому в апаратурі для квантового узгодження ключа використовують слабкі когерентні імпульси, які випромінюються високоякісними лазерними діодами. Це дає змогу реалізувати так звану атаку розділення фотонів. Якщо зловмисник помічає в імпульсі більше одного фотона, він відділяє один з них, дозволяючи решті безперешкодно відправитися до абонента Б. Далі зловмисник підмішує цей фотон до свого, утворюючи переплутану пару, і чекає оголошення базисів. Виконуючи потім часткові вимірювання свого фотона в парі, він може точно визначити стан підмішаного фотона, не вносячи жодних змін в ключ.

Якщо ж імпульс складається з одного фотона, то стратегія зловмисника може бути різною. Наприклад, він може просто пропускати одиничні фотони, не втручаючись в хід подій, або заставити їх провзаємодіяти з пробним фотоном і відправити абоненту Б. Проби так само зберігаються до оголошення результатів просіювання ключа.

Таким чином, ми бачимо, що існують деякі типи атак на протокол квантового узгодження ключів, які, скоріше, можна назвати теоретичними. Однак, сьогодні існують й атаки на реалізацію. Одну з таких атак продемонстрував Ларс Лідерсен зі співробітниками [31].

Атака виконується на особливості апаратної частини устаткування.

Оскільки імпульси, якими обмінюються сторони, дуже слабкі, на приймальному боці використовують фотоелектричні помножувачі — лавинні фотодіоди. Ці фотодіоди можуть працювати в двох режимах. Коли на вхід поступає слабкий сигнал, фотодіод підсилює його, відправляючи на вихід електричний сигнал. Коли ж інтенсивність падаючого світла зростає, прилад перестає реагувати на окремі фотони, і працює лише з потужними імпульсами.

Цю особливість помножувачів використала для зламу протоколу й група Л.Лідерсена. Вони повністю перехоплюють потік фотонів від абонента А і генерують потужні імпульси тієї самої поляризації, що й перехоплені фотони, які відправляють на попередньо “засліплений” фотодіод, який вже не здатен реагувати на окремі фотони.

Таку атаку було реалізовано на діючій системі квантового узгодження ключа в Сингапурському університеті, коли за 5 хвилин було перехоплено більше 8 млн. фотонів, залишившись повністю непомітними для учасників інформаційного обміну.

Тим не менше, від такої атаки існує дуже простий захист. Він полягає в тому, що перед приймачем розміщують додаткове джерело одиничних фотонів, яке відправляє їх у випадкові моменти часу. Якщо фотодіод на них не реагує, значить канал прослуховується.

Реалізації протоколу квантового узгодження ключа.

Практичні роботи у галузі квантової криптографії виконують такі компанії як IBM, Mitsubishi, Toshiba, лабораторія GAP-Optique, Національна лабораторія в Лос-Аламосі, Каліфорнійський технологічний інститут, MagiQ, холдинг QinetiQ.

Досягнуті успіхи:

- Ніколя Гісен (GAP-Optique) — реалізовано протокол BB84 на відстані 67 км;
- компанія Mitsubishi — 87 км зі швидкістю 7,2 біти за секунду;
- - Toshiba Research Europe — 100 км.

Створено також комерційну квантову криптосистему id 3000 Clavis Quantum Key Distribution System, яка підтримує:

- безпечне узгодження ключа на відстані до 100 км;
- підтримку протоколу BB84;
- вбудований протокол просіювання ключа;
- протокол шифрування та передавання файлів;
- бітрейт — 1500 біт за секунду.

Розглянуті протоколи квантового узгодження криптографічного ключа вважаються основними. Існують, тим не менше, багато різних модифікацій, які не принципово відрізняються від оригіналів.

Протокол E91

Тим не менше, існує ще один дуже цікавий протокол узгодження криптографічного ключа, який ґрунтується на зовсім іншій ідеї. Цей протокол був запропонований Артуром Екертом у 1991 році і називається E91 [32]. Інша назва цього протоколу — ЕПР-протокол, оскільки він використовує ЕПР-пари фотонів. Такі пари фотонів породжуються симетричним атомом. Поляризація фотонів невизначена, однак, оскільки вони переплутані, то їх напрями поляризації строго протилежні.

$$|S_0\rangle = 1/\sqrt{2}\ (|0\rangle|3\pi/6\rangle + |3\pi/6\rangle\ |0\rangle);$$

$$|S_1\rangle = 1/\sqrt{2}\ (|\pi/6\rangle|4\pi/6\rangle + |4\pi/6\rangle\ |\pi/6\rangle);$$

$$|S_2\rangle = 1/\sqrt{2}\ (|2\pi/6\rangle|5\pi/6\rangle + |5\pi/6\rangle\ |2\pi/6\rangle).$$

Якщо у абонента А є подібне обладнання, він зможе реалізувати такий протокол узгодження ключа.

Один фотон зі згенерованої пари абонент залишає у себе, а другий — відправляє на приймальний бік абоненту Б. Обидва абоненти не знають, яка поляризація їхніх фотонів. Більше того, вони зможуть це з’ясувати лише після вимірювання.

Отже, згенерувавши певну кількість переплутаних фотонів, учасники інформаційного обміну можуть починати вимірювання. Для отримання ідентичних послідовностей абонент А записує істинні значення, а абонент Б — їх доповнення до одиниці.

Така ідея цього протоколу. Звичайно, тут також існують процедури просіювання ключа.

Реалізація такого протоколу значно складніша за розглянуті раніше, оскільки сьогодні не існує джерел переплутаних пар фотонів з високим ступенем кореляції та великим часом життя.

Квантові гроші Стівена Візнера

У кінці 60-х рр. XX сторіччя аспірант Колумбійського університету Стівен Візнер (син директора MIT, радника багатьох президентів США з науки Джерома Візнера) запропонував своєму керівникові ідею квантового захисту грошей. Науковий керівник не звернув на цю ідею жодної уваги. С.Візнер відправив статтю в журнал.

Редакція відхилила статтю, визнавши її антинауковою.

Лише 1983 року стаття «Conjugate Coding» (журнал «ACM SIGACT News») вийшла в друці та була визнана однією з основних у галузі квантового захисту інформації [6].

Основна перевага ідеї полягає в тому, що захист побудовано не на складності підробки, а на принциповій неможливості цього.

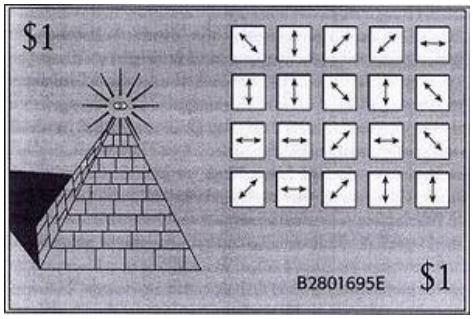
Ідея полягала в наступному. Припустимо, ми маємо такі квантові пастки, в яких можемо утримувати окремі фотони необмежений час.

Тоді ми можемо реалізувати такий захист грошей.

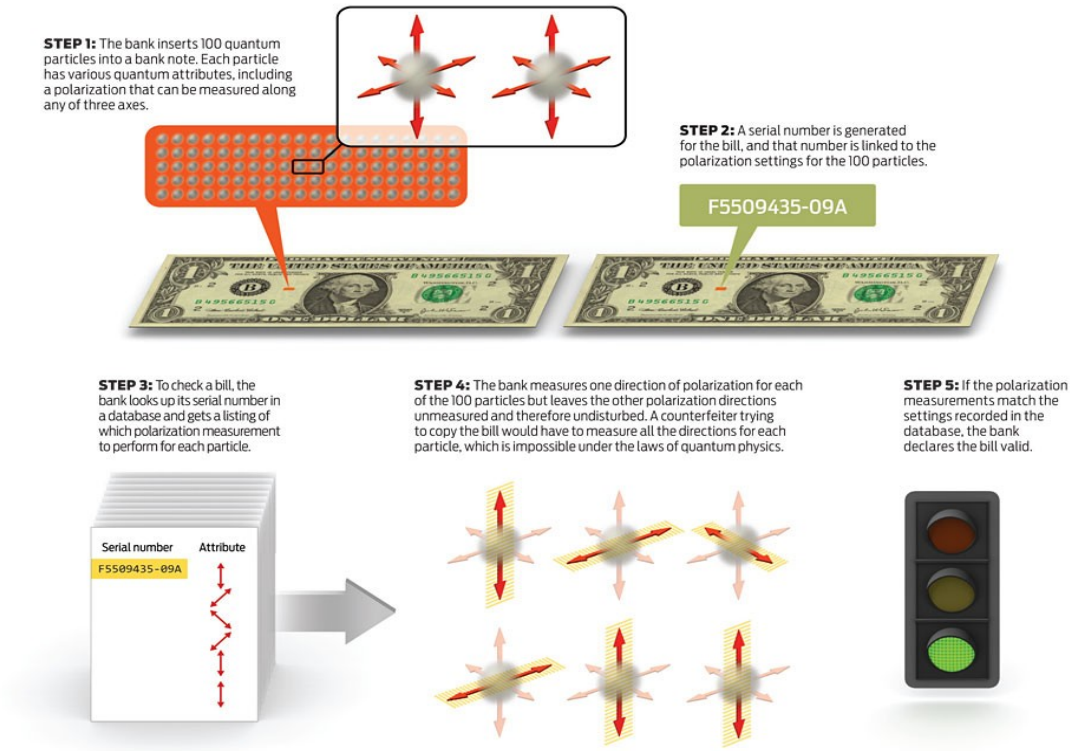
На кожній купюрі розміщено деяку кількість таких пасток, які заповнюються поляризованими фотонами під час випуску купюр.

Банк зберігає дані про поляризацію кожного фотона на кожній купюрі у своїй базі даних.

Схематично С.Віснер уявляв це собі таким чином:



Детальніше підхід, запропонований С.Віснером, пояснено на наступному малюнку.



Система захисту банкноти складається зі 100 пасток, де знаходяться квантові частинки, кожна з яких має багато квантових атрибутів, які можна вимірювати у трьох напрямах.

Серійний номер банкноти пов’язаний з квантовою конфігурацією цих частинок, і зберігається у базі даних емітента валюти. Для перевірки істинності банкноти банк шукає в базі даних номер банкноти і отримує квантову конфігурацію кожної зі ста частинок, що знаходяться у пастках цієї банкноти. Після цього банк випадковим чином вибирає один з напрямів, в якому виконує часткові вимірювання квантових характеристик кожної частинки, не зачіпаючи решти напрямів. Якщо результати вимірів збігаються з даними, записаними в базі даних банку, він вважає, що банкнота справжня. Зловмиснику для копіювання банкноти необхідно виконати вимірювання в усіх трьох напрямах, що заборонено принципами квантової механіки.

Звичайно, недоліком такої схеми є ніким не контрольовані права банку на необмежений випуск банкнот.

Співробітники Массачусетського технологічного інституту запропонували модифікацію ідеї С.Візнера: банк генерує кілька станів квантових частинок та змішує їх при заповненні пасток. У цьому випадку банк не знає, який отримується результат. При цьому банк публікує «публічний ключ» – алгоритм, за допомогою якого кожне відділення може перевірити справжність купюри, але не зможе відтворити цей стан квантових частинок.

Стверджується, що такий підхід позбавляє банк-емітент монополізму на випуск купюр.

Довгий час ідея С.Візнера була лише теоретичною іграшкою, оскільки не існувало квантових пасток, які могли би утримувати частинки хоча би макроскопічний час, не кажучи вже про необмежений.

Однак, у 2012 році Серж Арош (Франція) та Девід Вайнленд (США) отримали Нобелівську премію з фізики за розроблені методики маніпулювання квантовими частинками, які могли утримуватися в пастках протягом однієї секунди, а це вже макроскопічний час [33]. Проте, це відбувається за дуже низьких температур.

Інший варіант пасток пропонується науковцями Центру квантової фізики Гарвардського університету, які можуть утримати квантовий стан атому азоту при кімнатній температурі в матриці надчистих кристалів кремнію.

Таким чином, ідеї Стівена Візнера сформували фундамент нового напряму науки – **квантової інформаційної безпеки**.

Суть цього напряму– використання фундаментальних квантових властивостей мікросвіту для захисту інформації.

Основна перевага – теоретична стійкість квантових протоколів та способів захисту.

Основний недолік – складність практичної реалізації.

Розділ IV. Архітектура та основні вимоги до квантових комп’ютерів

Будь-який комп’ютер повинен мати як мінімум два стани: основний та неосновний. Для класичного ОЗП цими станами можуть бути:

- Відсутність/наявність струму (або малий його рівень);
- Відсутність/наявність напруги (або малий її рівень);
- Відсутність/наявність заряду тощо.

Для квантового комп’ютера основним станом є |0>, а неосновним - |1>. Окрім регістру пам’яті повинен бути пристрій обробки інформації, яка в ньому зберігається.

У випадку квантових комп’ютерів повинні бути:

- Гейти для виконання однокубітних операцій (I, NOT, гейт Адамара);
- Гейти для виконання багатокубітних операцій (CNOT, гейт Тоффолі тощо);
- Пристрої для виконання інших квантових операцій (квантові оракули).

Необхідно передбачити також систему вимірювання результатів обчислень. Також необхідні системи зв’язку та передавання даних (шини, канали тощо).

Виходячи з наведеного, можна зобразити архітектуру квантового комп’ютера таким чином:

Квантова система не може безмежно перебувати у неосновному стані. Під дією зовнішніх факторів:

- Температурного фону;
- Електромагнітних полів (у тому числі електромагнітного поля Землі);
- Взаємодії з іншими кубітами;
- Самовільно (спонтанно)

вони повертаються до основного стану. Стан суперпозиції зникає. Таке явище отримало назву *декогерентизації*. Отже, необхідно регулярно виконувати операцію регенерування інформації у квантовому регістрі пам’яті.

Сукупність усіх можливих операцій, що формують вихідний стан, виконують обчислення, усувають декогерентизацію, виправляють помилки, виконують у квантовому комп’ютері роль програмного забезпечення (*software*).

Обираючи ту чи іншу схему квантового комп’ютера, необхідно розв’язати інше завдання:

- Яку фізичну систему обрати для створення квантового регістру пам’яті;

- Який фізичний механізм буде відповідати взаємодію між кубітами, що необхідно для реалізації багатокубітних операцій;
- Визначити спосіб селективного керування кубітами та вимірювання їх стану на виході.

Усе це утворює аналог апаратного забезпечення квантового комп’ютера (*hardware*).

Сьогодні вважається, що для реалізації повноцінного квантового комп’ютера необхідно забезпечити виконання таких вимог:

- Фізична система квантового регістру повинна складатися з великої кількості кубітів (1024 та більше);
- Необхідно забезпечити умови для ініціалізації, тобто для організації основного стану $|0>$.
- Необхідно забезпечити максимально можливе усунення декогерентизації. Час декогерентизації повинно як мінімум у 10^4 разів перевищувати такт. Для цього система кубітів повинна бути ретельно ізольованою від оточуючого середовища.

Необхідно також забезпечити виконання за час такту необхідної сукупності унарних операцій, яка може складатися з багатьох одно- та багатокубітних операцій та забезпечити найвищу надійність вимірювань, оскільки «другої спроби» виконати їх вже не буде. Це є однією з головних проблем квантового комп’ютингу.

Отже, необхідно забезпечити ефективне керування квантовим обчислювачем з боку класичного керуючого комп’ютера.

Основні фізичні технології

Твердотільні квантові точки у напівпровідниках. У якості кубітів використовують або зарядові стани (наявність/відсутність електрона у квантовій ямі) або напрям його спіну. Керування здійснюється або зовнішнім потенціалом, або лазерним імпульсом.

Надпровідникові елементи (NEC Research Laboratories) – джозефсонівські переходи, сквіди тощо. Як кубіт використовують наявність/відсутність куперівської пари у певній точці простору. Керують зовнішнім потенціалом або магнітним полем.

Переваги цього способу: високий ступінь інтеграції; значно вищі температури (високотемпературні надпровідники); порівняно легке керування кубітами.

Недоліки - недостатня стабільність станів; високий ступінь декогерентизації.

Іони у вакуумних пастках Пауля або оптичних пастках (NIST, Los Alamos National Laboratories):

- Кубіти – основний та збурений стан зовнішнього електрона цього іона;
- Керування – лазерними імпульсами.

Переваги – просте керування кубітами; недоліки – наднизькі температури; жорсткі обмеження на кількість іонів у пастці.

Використання методів ядерного магнітного резонансу — ЯМР (MIT, LANL, Оксфорд).

Кубіти – атоми рідин з непарними ядерними спінами; взаємодія – скалярна взаємодія між атомами, керування – методами ЯМР.

Переваги цього способу - просте, добре відлагоджене керування методами ЯМР ,якими користуються вже багато років у магніто-резонансному устаткування, кімнатні температури та великий час декогерентизації (секунди та більше). Недоліки — складність ініціалізації, обмежена кількість кубітів, невелика швидкодія.

Атоми азоту у ґратці алмазу (Гарвардський університет). Тут як кубіти використовують магнітні моменти атомів азоту в ґратці суперчистого кремнію. Керування здійснюють електромагнітними імпульсами.

Переваги такого методу — високий ступінь інтеграції, оскільки кремнієві технології добре налагоджені, сьогодні досягнуто великого часу декогерентизації (секунди). Та основною перевагою є кімнатні температури. Ця технологія не позбавлена й недоліків. До них можна віднести невідпрацьовані технології та поки що невелика кількість кубітів у регістрі.

Розглянемо детальніше перелічені варіанти фізичної реалізації квантових комп’ютерів у наступних розділах.

Розділ V. Огляд фізичних реалізацій квантових комп’ютерів

Цей розділ присвячено деталізації тих ідей, про які було згадано у попередньому параграфі, з аналізом переваг та недоліків кожної технології. Матеріал викладається за книгами [34] та [35].

Раніше ми обговорювали вимоги до квантових комп’ютерів та фізичні принципи, якими повинні керуватися розробники для їх фізичної реалізації. Ми повинні не лише знайти вдалу фізичну реалізацію для кубітів, а й знайти керовану систему кубітів. Звісно, необхідно обрати метод організації первісного стану та вимірювальну підсистему.

Технічно задовольнити такі вимоги надзвичайно складно. Часто квантові стани в системі добре розрізняються але існують вони дуже короткий час внаслідок впливу зовнішнього середовища, і необхідно витрачати значні ресурси для їх підтримки. Іноді навпаки: квантовий стан може існувати макроскопічний час, але виміряти його дуже складно. Водночас кубіти мають бути легко доступними для того, щоби виконувати квантові обчислення та вимірювати результати. Такі, часто протилежні вимоги, спонукають змінити питання з “чи можна побудувати квантовий комп’ютер” на “наскільки якісним його можна побудувати”.

Для того, щоби оцінити перспективність тієї чи іншої фізичної “платформи” для побудови квантового комп’ютера, необхідно порівняти час декогерентизації системи (час існування когерентного стану, $\tau_д$) з часом, за який виконується унарна квантова операція $\tau_{оп}$ [34].

Система	$\tau_д$, **сек.**	$\tau_{оп}$, **сек.**	$n_{оп}=\tau_д/\tau_{оп}$
Спін ядра	10^{-2} - 10^{8}	10^{-3} - 10^{-6}	10^{5} — 10^{14}
Спін електрона	10^{-3}	10^{-7}	10^{4}
Йонна пастка	10^{-1}	10^{-14}	10^{13}
Електрон — Au	10^{-8}	10^{-14}	10^{6}
Електрон - GaAs	10^{-10}	10^{-13}	10^{3}
Квантові точки	10^{-6}	10^{-9}	10^{3}
Оптичний резонатор	10^{-5}	10^{-14}	10^{9}
НВЧ-резонатор	10^{0}	10^{-4}	10^{4}

З таблиці ми бачимо, що усі зазначені технології перспективні з точки зору організації квантових обчислень, оскільки час декогерентизації значно більший за час виконання квантової операції, а отже кількість операцій, $n_{оп}=\tau_д/\tau_{оп}$, що їх можна виконати за час існування когерентного стану, досить велика.

Значну проблему також являє можливість приготування первісного (вхідного) стану квантового регістра пам’яті. Навіть якщо система виконує обчислення абсолютно точно, це буде малоефективним в разі неможливості контролювати вхідний стан. Ми повинні надійно вміти приготувати хоча би один початковий стан, оскільки інші можна отримати з нього за допомогою унарних операцій.

Для більшості фізичних систем приготування початкового стану часто є складною проблемою. Наприклад, йони у пастці могли би приводитися у початковий стан охолодженням, але реалізувати це непросто.

Для фізичних систем, що реалізують ансамблі квантових комп’ютерів, виникають додаткові складнощі. Наприклад, у випадку ЯМР-реалізації кожна молекула повинна розглядатися як окремий квантовий комп’ютер. Щоби отримати сигнал, придатний для вимірювання, необхідно багато молекул, причому в одному й тому ж квантовому стані. Це непросто, оскільки енергія між |0> та |1> набагато менша за kT.

З другого боку, з початкового стану, у більшості випадків, необхідно отримати стан квантової суперпозиції, інакше зміст стартового стану втрачається, оскільки він є незмінним.

Іншою проблемою є вимірювання результатів квантових обчислень. Зручно розглядати вимірювання як взаємодію квантової системи з деякою класичною. Ця взаємодія відбувається протягом деякого часу, після чого стан класичної системи вказує нам на результати вимірювання. Наприклад, вимірювання стану кубіта $a|0>+b|1>$, який подано основним та збудженим станами дворівневої атомної системи, може бути подано спостереженням флуоресценції. Тоді ми будемо впевнені, що кубіт був у стані |1>. Якщо ж флуоресценції не спостерігалося, - в стані |0>. Однак, тут злий жарт з дослідниками можуть зіграти шуми вимірювань та недосконаліть апаратної частини, в результаті чого ми можемо неправильно оцінити стан кубіта. Вимірювання також не повинні виконуватися, коли їх не потрібно; це призведе до втрати когерентності системи.

Вимірювання можуть бути “сильними”, коли взаємодія з вимірювальною системою сильно впливає на квантову систему, і “слабкими”, коли як квантова система

використовуються ансамблі частинок. Тоді сигнал від такої системи є макроскопічною величиною і несе інформацію про її квантовий стан.

Якість вимірювання можна оцінити за відношенням сигналу до шуму. Воно дає інформацію про силу сигналу та взаємодію вимірювального пристрою із квантовою системою.

Гармонічний осцилятор як модель квантового комп’ютера

Спочатку давайте розглянемо дуже просту квантову систему: гармонічний осцилятор та з’ясуємо, чому вона не може бути вдалою моделлю квантового комп’ютера. Підходи цього прикладу будемо вважати основою для наступних фізичних систем.

Гамільтоніан системи

Прикладом простого гармонічного осцилятора є частинка у параболічній потенціальній ямі. У класичній механіці це може бути вантаж на пружині; в електриці — коливальний контур з ємністю та індуктивністю.

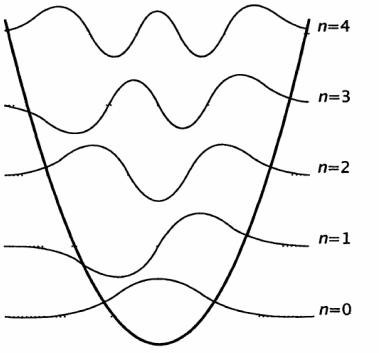
У квантовій механіці, яка починає працювати, коли зв’язок системи з оточуваним середовищем дуже малий, повна енергія системи може набувати дискретних значень, на відміну від класичних випадків.

Для простого осцилятора власні стани з певною енергією позначаються як $|n>$, де n=0,1,2, ... Час життя кубітів визначається фізичними параметрами системи. Для того, щоби застосувати унарний оператор, необхідно надати системі можливість еволюціонувати протягом певного часу при певних умовах. Така схема, однак, має цілий ряд недоліків, які ми обговоримо пізніше. Почнемо з опису гамільтоніана системи та перейдемо до простих квантових логічних операцій.

Гамільтоніан частинки у одновимірному параболічному потенціалі має вигляд:

$$H=\frac{p^2}{2m}+1/2\,m\,\omega^2\,x^2;$$

де p — імпульс частинки; m — маса; x — координата та ω — параметр потенціалу. Графічно це виглядатиме так:



Зображена функція описує амплітуду ймовірності того, що частинку буде виявлено у тій чи іншій точці в області дії потенціалу.

Стани системи еволюціонують з часом згідно рівняння Шредінгера. Ми також будемо вважати, що можемо точно приготувати довільний початковий стан осцилятора, виконувати проективні виміри, але взаємодія осцилятора з оточуваним середовищем відсутня.

Квантові обчислення

Спробуємо використати простий гармонічний осцилятор для квантових обчислень. Кубіти в такому разі подаються власними станами енергії |*n*>. Як тоді реалізувати оператор CNOT? Нагадаємо, що дія цієї операції на двокубітові базисні стани має вигляд:

$$|00\rangle_L \rightarrow |00\rangle_L$$
$$|01\rangle_L \rightarrow |01\rangle_L$$
$$|10\rangle_L \rightarrow |11\rangle_L$$
$$|11\rangle_L \rightarrow |10\rangle_L$$

Індекс *L* говорить про те, що це є логічними станами. Ми можемо закодувати ці два кубіти наступним чином:

$$|00\rangle_L = |0\rangle$$
$$|01\rangle_L = |2\rangle$$
$$|10\rangle_L = (|4\rangle + |1\rangle)/\sqrt{2}$$
$$|11\rangle_L = (|4\rangle - |1\rangle)/\sqrt{2}.$$

Нехай в момент часу $t=0$ стан системи є лінійною комбінацією векторів |0>, |1>, |2>, |4>, а система еволюціонує на проміжку часу $t=\pi/\hbar\omega$. При цьому власні стани системи перетворюються за законом: $|n\rangle=(-1)^n|n\rangle$. Тоді $|0\rangle=(-1)^0|0\rangle=|0\rangle$; $|1\rangle=(-1)^1|1\rangle=-|1\rangle$; $|2\rangle=(-1)^2|2\rangle=|2\rangle$; $|4\rangle=(-1)^4|4\rangle=|4\rangle$, звідки видно, що стани |0>, |2>, |4> лишаються незмінними, а стан |1> - змінює знак. У результаті для логічних станів отримаємо потрібне нам перетворення CNOT.

Отже, бачимо, що у такий спосіб можна реалізувати практично довільний набір квантових операцій з довільним числом кубітів. Може здатися, звичайно, що за допомогою такої квантової системи можна реалізувати квантовий комп’ютер. Однак, не все так просто!

Недоліки

Очевидними недоліками запропонованої схеми є те, що кубіти подаються як рівні енергії багаторівневої квантової системи. Це означає, що: а) це аналоговий спосіб подання інформації, тоді як усі квантові алгоритми оперують із цифровим поданням; б) таке подання інформації (енергетичними рівнями та їх комбінаціями) не може бути застосоване для довільного квантового оператора, оскільки часто їх спектр невідомий.

Квантовий комп’ютер на фотонах

Однією з найцікавіших фізичних систем для представлення квантового біта є оптичний фотон. Фотони є нейтральними частинками, які досить слабко взаємодіють один з одним та оточуваним середовищем. Їх можна практично без втрат переносити на великі відстані за допомогою оптичного кабелю, змінювати фазу за допомогою оптичних пристроїв та створювати стан суперпозиції за допомогою розділювачів. Фотони демонструють яскраві квантові ефекти, наприклад, інтерференцію на двох щілинах. Крім того, у нелінійних середовищах може спостерігатися фотон-фотонна взаємодія, яке виникає внаслідок нелінійності взаємодії фотонів з речовиною. Проаналізуємо фотонну модель квантового

комп’ютера, її архітектуру та деталі.

Фізична апаратура

Одним з експериментальних способів генерування одиничних фотонів є зменшення інтенсивності лазерного випромінювання. Лазер випромінює так зване когерентне випромінювання, імпульс якого містить n фотонів. У результаті зменшення інтенсивності пакет зменшує середню енергію, що дає змогу з великою ймовірністю отримати однофотонний стан.

Існує також достатньо багато способів детектування одиничних фотонів у широкому спектральному діапазоні з великою квантовою ефективністю, наприклад, за допомогою фотопомножувачів. На практиці на ці процеси сильно впливає недосконаліть детектора: час відгуку, смуга пропускання, шумові та темнові характеристики.

Експериментальна техніка для керування станами фотонів складається з трьох важливих компонентів: дзеркал, фазообертача та розділювача світла. На сьогодні дзеркала, у яких втрачається лише 0,01% фотонів є цілком доступними. Фазообертач являє собою просто прозору пластинку з показником заломлення, відмінним від одиниці. Наприклад, звичайне боро-силікатне скло має показник заломлення приблизно n=1,5. Зрозуміло, що при проходженні фотона крізь пластинку товщини L, його фаза буде змінюватися на exp(ikL), де $k=n\omega/c_0$, c_0 — швидкість світла у вакуумі.

Розділювач світла являє собою скло, вкрите тонким шаром срібла, з коефіцієнтом відбивання R та коефіцієнтом пропускання 1-R.

Квантові обчислення

Зручно описувати розділювач світла за допомогою кута θ, уведеного як $\cos(\theta)=R$. У такому разі цей кут характеризує ступінь відбиття та, у загальному випадку, не має жодного стосунку з геометрією розділювача.

Якщо ми маємо два входи та два виходи розділювача, інтенсивність на них пов’язана такими співвідношеннями:

$$a_{вих} = a_{вх} \cos\theta + b_{вх} \sin\theta,$$
$$b_{вих} = - a_{вх} \sin\theta + b_{вх} \cos\theta,$$

де a та b — класичні амплітуди електромагнітного поля двох променів. Якщо ж нам треба отримати розділювач 50/50, маємо $\theta=45^o$.

Кубіти найчастіше представляються одиничними фотонами, які можуть перебувати на двох модах: |01> та |10>. Зміну квантового стану реалізують за допомогою ефекту Керра [36], коли у речовині під дією зовнішнього постійного або змінного електричного поля спостерігається подвійне променезаломлення внаслідок зміни показника заломлення. Ефект Керра зумовлений, головним чином, переполяризацією середовища внаслідок деформації електронних орбіталей атомів та молекул, або їхньої переорієнтації. Ефект Керра дуже швидкий, оскільки у твердих тілах може відбутися лише деформація електронної хмари атомів.

Зрозуміло, що й тут є свої недоліки, головний з яких — поглинання та розсіювання світла у різних оптичних структурах, внаслідок чого ми не можемо застосувати оптичні канали будь-якої довжини.

Основні недоліки

Представлення кубіти за допомогою одиничних фотонів дуже привабливе, оскільки їх порівняно легко генерувати та детектувати. У двомодовому представленні можна реалізувати довільний однокубітовий квантовий оператор. На жаль, забезпечити взаємодію між фотонами значно складніше: взаємодія, навіть у найкращих керрівських середовищах, значно слабша, щоби забезпечити фазову модуляцію порядку π між однофотонними станами. Крім того, оскільки нелінійність, як правило, відбувається поблизу оптичного резонансу, ефект Керра практично завжди буде супроводжуватися поглинанням світла. Теоретичні оцінки вказують на те, що на один фотон, який пройшов крізь середовище, припадає приблизно 50 поглинутих фотонів. Це означає, що у рамках сучасної нелінійної оптики побудова квантового комп’ютера має дуже мало шансів на успіх.

Тим не менше, обговорення квантового однофотонного комп’ютера надало нам знання про те, як би міг виглядати реальний лабораторний квантовий комп’ютер.

Взагалі кажучи, оптичні комп’ютери давно розглядалися як заміна електронним класичним комп’ютерам. Розроблялися експериментальні зразки оптичних процесорів та комп’ютерів у цілому [37]. Однак, пов’язані з ними надії, врешті решт, не справдилися, оскільки поки що не вдається отримати матеріали з високим ступенем нелінійності, а також тому, що складнощі з налаштуванням та енерговитрати не компенсують переваги у швидкості та можливості паралельних обчислень.

Не дивлячись на вказані недоліки оптичної реалізації квантового комп’ютера, формальна теорія, що його описує, є фундаментом для решти реалізацій. Далі ми розглянемо дещо інший варіант оптичного квантового комп’ютера, де використовується інше нелінійне середовище.

Квантовий комп’ютер на оптичних резонаторах

Тут розглядається задача про взаємодію окремих атомів з невеликою кількістю оптичних фотонів. Така взаємодія може бути реалізована в оптичних резонаторах з великою добротністю. Якщо в резонаторі існує всього одна=дві оптичних моди, а напруженість електричного поля достатньо велика, то взаємодія цих оптичних мод з дипольним моментом атома стає істотним. Відповідно, можливі процеси, коли фотон встигає багато разів вступити у взаємодію з атомом раніше, чим він вийде з резонатора. Така експериментальна техніка знаменита тим, що дозволяє вивчати окремі квантові системи та маніпулювати ними.

Зокрема, використання такої техніки дозволяє подолати основну перешкоду до реалізації оптичного квантового комп’ютера, тобто слабку взаємодію фотонів між собою.

Фізична апаратура

Реальна апаратура для такого роду процесів складається з двох компонентів: електромагнітний резонатор та атом. Процеси відбуваються у сильному електричному полі, тому зручно використовувати резонатор Фабрі-Перо [38]. Основною частиною резонатора Фабрі-Перо є напівпрозоре дзеркало, вкрите шаром срібла, на якому відбуваються багаторазові процеси відбивання та проходження променів світла. В результаті цих процесів промінь набуває додаткової фази, яка залежить від довжини шляху, що його він пройшов. У

резонаторі фотони (одиничні фотони) взаємодіють з одиничними (спеціально підібраними) атомами речовини, і змінюють при цьому свою фазу. Оскільки електричне поле досить сильне, то тут можна досягти значної взаємодії між однофотонними станами. Це робить описану техніку досить перспективною для створення оптичного квантового комп’ютера.

Подання квантової інформації

Тут можливі дві схеми подання квантової інформації: різними станами фотонів, а самий резонатор з атомами використовується для створення фотон-фотонної взаємодії; різними станами атомів, а власне фотони служать для передавання інформації між атомами. У першому випадку, так само, як і у попередній схемі однофотонного оптичного комп’ютера, як кубіт використовується один фотон, який може перебувати на двох модах |01>, |10> або з різними поляризаціями.

Довільний квантовий оператор можна реалізувати за допомогою фазообертачів, світло розділювачів та резонатора Фабрі-Перо, всередині якого утримуються кілька атомів, що взаємодіють з фотонними модами резонатора.

Початковий стан системи можна забезпечити, як і в попередньому випадку, генеруванням однофотонних станів шляхом, наприклад, зменшення інтенсивності лазерного променя.

Вимірювання остаточного результату досягається застосуванням фотопомножувачів для реєстрації одиничних фотонів.

Недоліки

Оскільки фотон-фотонна взаємодія зумовлена проміжною взаємодією з атомом, бажано збільшити ступінь зв’язку атома з електричним полем. Однак, в такому разі, зменшується час існування стану когерентності атомі, що, у свою чергу, обмежує час виконання квантових обчислень.

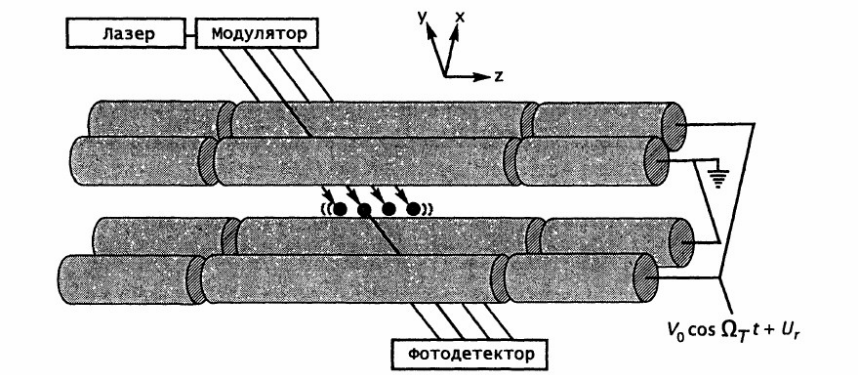
Йони у пастках

У цьому випадку до інших способів представлення кубіта, - атомних чи ядерних станів, наприклад, наприклад, електронного та ядерного спінів. І хоча спін — це досить дивне (хоча й реальне!) поняття, причому різниця енергій різних спінових станів, як правило, значно менша за решти характерних енергій (наприклад, кінетичної енергії атома при кімнатній температурі), однак, існує спеціальна експериментальна техніка, що дозволяє контролювати спінові стани. Для цього невелика кількість ізольованих йонізованих атомів утримується в електромагнітній пастці, після чого вони охолоджуються до такої температури, коли кінетична енергія стає меншою за спінові енергії. Вмикаючи зовнішнє резонансне електромагнітне поле, можна селективно впливати на кожну пару станів. Це й становить основу квантових обчислень методом йонів у пастці.

Фізична апаратура

Фізичне приладдя для такого роду експериментів складається з двох частин: електромагнітної пастки, обладнану лазерами та власне йонів. Основна частина,

електромагнітна пастка, складається з чотирьох циліндричних електродів, як це подано на рисунку.



Ці електроди утворюють в центрі пастки електричний потенціал, що утримує чотири йони, зображені чорними кульками. Пастку, як правило, розміщують у глибокому вакуумі (порядку 10^{-8} Па), а йони постачаються з розміщеного поруч джерела. Модульоване лазерне випромінювання потрапляє на йони крізь вікно вакуумної камери. Впливаючи ним на атомні стани, ми можемо виконувати квантові обчислення та читати результати.

Зрозуміло, що тут розглянуто дуже простий випадок усього чотирьох йонів у пастці. Зі збільшенням кількості йонів геометрія стає складнішою, утворюючи різні структури. Якщо така система добре ізольована й теплові флуктуації не руйнують стан системи, рух йонів починає квантуватися. Крім того, флуктуації електричного та магнітного полів, можуть викликати хаотичні рухи йонів, які ми назвемо шумом. Такий шум практично неминучий у цих системах, а його збільшення також призводить до руйнування квантового стану. Тим не менше, більшість завад може бути зменшено до такої величини, коли їх впливом за час експерименту можна знехтувати.

Для зменшення амплітуди коливань атомів використовують спеціальну техніку зниження їхньої температури, яка використовує ефект Доплера. Як ми знаємо, фотон володіє енергію та імпульсом. Подібно тому, як автомобільний сигнал від автомобіля, що наближається до спостерігача, має вищу частоту, ніж у автомобіля, що віддаляється від нього, атом, що рухається “до лазера”, має частоту переходу трохи вищу, ніж той, що рухається “від лазера”. Якщо підібрати частоту лазера так, щоби випромінювання поглиналося лише атомами, що наближаються, то атоми почнуть сповільнюватися, оскільки імпульс фотонів, що поглинаються, спрямований назустріч руху атома. Цей метод отримав назву доплерівського охолодження. Він дозволяє охолодити атоми до дуже низьких температур.

Подання квантових станів

Внутрішній стан йонів характеризується електронним спіном та ядерним, які в сумі утворюють повний спін атома. Внутрішній стан атома зручно описувати базовими квантовими станами повного кутового моменту атома.

Як приклад, розглянемо два спіни 1/2. У цьому випадку як базові стани можна взяти |00>, |01>, |10>, |11>. Але, як правило, використовують інші базові стани, оскільки пов’язують їх з повним спіном атома:

$$|0,0\rangle_J = \sqrt{2}(|01\rangle - |10\rangle),$$
$$|1,0\rangle_J = \sqrt{2}(|01\rangle + |10\rangle),$$

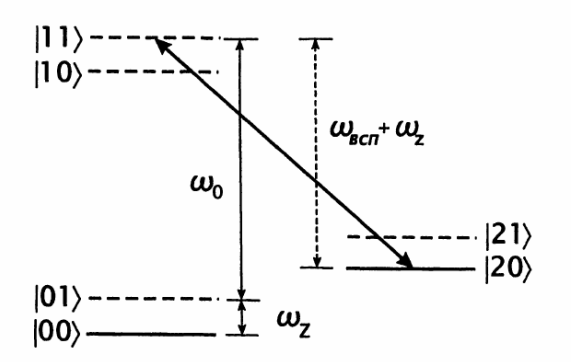
$$|1,1\rangle_J = |11\rangle,$$

$$|1,-1\rangle_J = |00\rangle.$$

Як довго може існувати суперпозиція різних спінових станів? Її час життя обмежується процесом спонтанного випромінювання, коли атом переходить зі збудженого стану до основного, випромінюючи фотон. Акт випромінювання відбувається у випадковий момент часу. На перший погляд може здатися дивним, що атом, який у вільному просторі без зовнішнього впливу може випромінити фотон. Насправді атом не перебуває у вільному просторі, оскільки на нього діє зовнішнє електричне поле. І саме взаємодія з ним спонукає атом до спонтанного випромінювання фотона.

Квантові обчислення

Зміну стану такої квантової системи можна ініціювати лазерним випромінюванням певної частоти. На рисунку видно, що перехід атома зі стану |10> до стану |11> відбувається лазерним імпульсом з частотою ω_0, а зі стану |00> до |01> - з частотою ω_Z тощо. Про обернені переходи можна судити за частотою фотона, що випромінюється атомом.



Взаємодія між кубітами відбувається засобами спільного фононного стану. Вимірювання кінцевого результату виконується вимірюванням заселеності квантових станів такої структури, що виконується за допомогою індукованої флуоресценції.

Недоліки

Основним недоліком такої системи є малий час існування збуджених станів атому і, відповідно, важким є приготування основного коливного стану системи.

Ядерний магнітний резонанс

Ми бачили, ядерні спіни були б ідеальною системою для реалізації квантових обчислень за умови, що спін-спінова взаємодія була би досить сильною та контрольованою. Принциповий недолік використання йонів у пастках був якраз у слабкості спін-спінової взаємодії, а також у швидкій втраті когерентності. Можна було би розташувати у пастці не атом а молекулу, де ця взаємодія значно сильніша, однак внаслідок наявності у спектрі молекули коливних мод, утримувати її у пастці та охолодити значно складніше.

З іншого боку, існує добре відпрацьований метод, що дозволяє маніпулювати ядерними спінами та вимірювати їх за допомогою радіочастотних імпульсів. Це — ядерний магнітний резонанс (ЯМР). Цей метод широко застосовується у різних галузях науки і

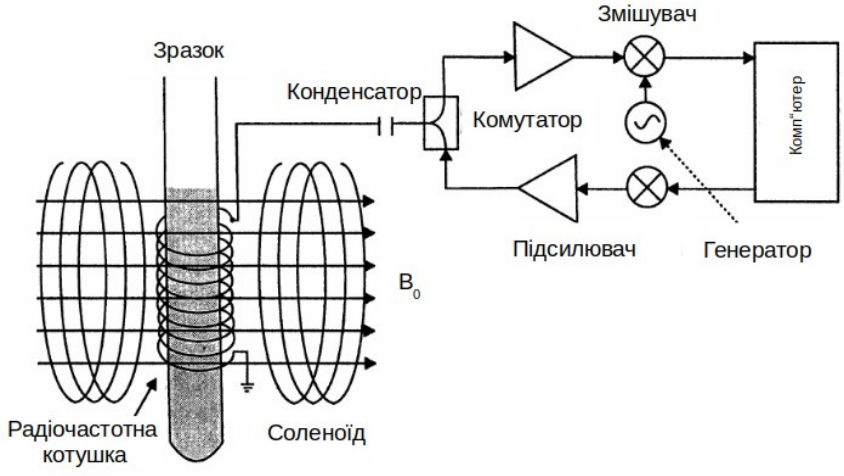
техніки, і дозволяє виконувати експерименти з контролю десятків, сотень і навіть тисяч ядер.

Однак, при використанні ЯМР для квантових обчислень виникають дві проблеми. По-перше, внаслідок малості величини ядерного магнітного моменту, необхідно використовувати зразки з великою кількістю (порядку 10^8 й більше) молекул. Це, у свою чергу, ставить питання, чи можемо ми використовувати результат усереднення по квантових системах? По-друге, ЯМР використовують при кімнатних температурах. Це значить, що початковий стан системи близький до невпорядкованого. Постає питання: чи можна виконувати квантові обчислення над системою у змішаному початковому стані та має велику ентропію?

Фізична апаратура

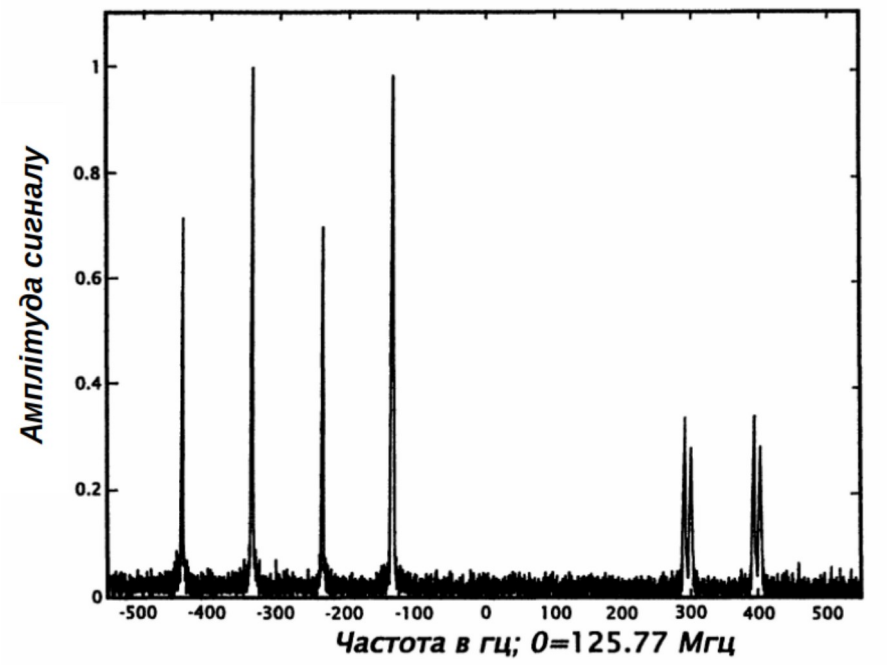
Імпульсне ЯМР-приладдя для рідких зразків складається зі спектрометру та власне зразку. Молекули, у яких спостерігається ЯМР, як правило, містять деяку кількість протонів зі спіном 1/2 (наприклад, ^{13}C, ^{19}F, ^{15}N, ^{31}P). У магнітному полі порядку 12 Тл протони мають частоту резонансу приблизно 500 МГц. Резонансні частоти для різних ядер певної молекули можуть відрізнятися на величину до кількох сотень кілогерц. Молекули ці знаходяться у розчині, так що їх концентрація дуже мала, тож їхньою взаємодією можна знехтувати. Тому систему таких молекул можна описати як ансамбль багатокубітових квантових обчислювачів.

ЯМР-спектрометр принципово складається з радіочастотних котушок та великого надпровідного магніту, де як сердечник розміщено зразок у скляній пробірці, як це показано на рисунку. Постійне магнітне поле B_0, напрямлене перпендикулярно до зразку, налаштовується так, що у межах зразку його неоднорідність не перевищує 10^{-9}. Розміщені перпендикулярно до магніту котушкі Гельмгольца формують слабке змінне магнітне поле у площині зразка. Це поле можна швидко вмикати та вимикати, що дозволяє маніпулювати ядерними спінами. Ті ж котушки використовують також для приймання радіочастотного сигналу від прецесії ядерних спінів подібно до того, як магніт, що обертається, створює змінний індукційний струм у котушці.



Типовий експеримент починається з етапу очікування для того, щоби ядра досягли стану термодинамічної рівноваги. Цей час може складати кілька хвилин. Після чого класичний комп’ютер створює послідовність радіочастотних імпульсів, які виконують потрібні перетворення над станами ядер. Далі потужні підсилювачі, які формували імпульси, вимикаються і вимірюється кінцевий стан спінів за допомогою високочутливого

підсилювача. До отриманого сигналу застосовується перетворення Фур’є, за результатами якого, обчислюючи площу піків у спектрі частот, можна визначити поточний стан ядерних спінів.



Як приклад, на рисунку подано вуглецевий спектр ЯМР трихлоретилену (^{13}C). Чотири лінії ліворуч належать ядру вуглецю, яке є сусідом протона. Їх чотири внаслідок спарювання з протоном та другим ядром вуглецю. Чотири лінії праворуч — сигнал від другого ядра вуглецю. Воно знаходиться далі від протону, ніж перше, тому спарювання слабше.

Квантові обчислення

Основною проблемою виконання квантових обчислень за допомогою ЯМР є те, що ми тут працюємо з ансамблем ядер. Тому результатом квантових обчислень буде якесь середнє значення, тоді як нам треба отримати результат строго одного квантового обчислювача. І тут ми стикаємося з наступною проблемою, яку простіше усього продемонструвати на прикладі алгоритму Шора. У цьому випадку квантовий алгоритм повинен дати число c/r, де c — невідоме ціле число, а r — цілий показник ступеня, який нас і цікавить. Далі, використовуючи класичний алгоритм розкладання у ланцюговий дріб, можна з великою ймовірністю визначити число r, після чого можна визначити, чи є r дільником, а якщо ні, - виконуємо весь алгоритм спочатку. На жаль, у випадку вимірювань на ансамблі, ми можемо отримати лиш середнє значення $<c/r>$, з якого жодної інформації про r отримати неможливо.

Виходом з такої ситуації є наступне. Необхідно включити усі класичні обчислення, які завершують роботу алгоритму, до його квантової частини. Нехай кожен квантовий обчислювач, що входить до ансамблю (тобто кожна молекула), виконує розкладання до ланцюгового дробу, знаходить r та перевіряє, чи є він дільником. Далі, можна модифікувати алгоритм так, що внесок до підсумкового сигналу нададуть лише ті молекули, де обчислення дільника пройшло успішно. Тепер ми зможемо взяти середнє за ансамблем як остаточний результат, вимірюючи сигнал індукції, який виникає при прецесії магнітного моменту ядер.

Недоліки

Основним недоліком квантових систем на основі ЯМР у випадку, коли поляризація спінів у початковому стані не дуже висока, є те, що вихідний сигнал зменшується експоненційно зі збільшенням кількості кубітів.

Як видно з наведених принципів реалізувати квантовий комп’ютер — надзвичайно нетривіальне завдання, оскільки необхідно врахувати багато майже протилежних вимог. Усі запропоновані варіанти реалізації є незадовільними в тому розумінні, що на їхній основі у найближчому майбутньому не можна побудувати багатокубітовий квантовий комп’ютер. Тим не менше, це ще не означає що дана задача не має вирішення, оскільки існує багато інших варіантів реалізації.

З таблиці на початку розділу зрозуміло, що практично будь-яка фізична величина, що квантується, може представляти кубіти. В той же час, фундаментальні фізичні квантові об’єкти, такі як фотон та спін, є найбільш привабливими представленнями кубіта.

Існує ще одна фундаментальна величина, придатна для ролі кубіта. Це електричний заряд. Сучасна електроніка надає нам можливість створювати, контролювати та вимірювати заряд навіть в одноелектронному режимі. Наприклад, у квантових точках, виготовлених з напівпровідників, металів, чи навіть, з невеликих молекул, можуть локалізуватися заряди у тривимірних потенціальних ямах. На відміну від фотонів, заряди не можуть народжуватися та знищуватися, вони можуть лише мігрувати по системі. Таким чином, у представленні кубіта зарядовим станом ми маємо використовувати, наприклад, локалізації в одній з двох квантових точок чи двом станам електрона в одній точці.

Однокубітові операції можна реалізувати за допомогою електростатичні затвори, спеціальні двоканальні розсіювачі, тунельні контакти між квантовими точками. Використовуючи кулонівською взаємодією, можна реалізувати операції над кубітами. Як вимірювачі, можуть використовуватися, наприклад, одноелектронні транзистори. На жаль, неконтрольований рух віддалених зарядів призводить, внаслідок їхньої взаємодії з системою, до втрати когерентності. Разом з електрон-фононною взаємодією це зменшує час когерентності зарядових станів відносно малим: від сотень пікосекунд до сотень фемтосекунд.

Для представлення кубітів також пропонувалося використовувати носії заряду у надпровідниках, які об’єднуються у так звані куперівські пари. Їх також можна локалізувати у квантових точках. Однокубітові операції реалізуються за допомогою електростатичних зарядів, що впливають на пару, та джозефсонівських контактів, що можуть з’єднувати локалізації різних пар. Їх також можна використовувати для реалізації взаємодії між кубітами, причому силу цієї взаємодії можна змінювати зовнішнім магнітним полем за допомогою надпровідних квантових інтерферометрів. Вимірювання кубітів в такому разі — це просто вимірювання електричного заряду. Кубіти, що представлені куперівськими парами, відносно стійкі; оцінки показують, що час когерентності може перевищувати одну мікросекунду. На жаль, зовнішній електростатичний та електромагнітний фон обмежують час існування когерентності і у цьому випадку.

Короткодіюча магніто-дипольна взаємодія спонукає нас звернути увагу на представлення кубітів спінами у напівпровідникових системах. Наприклад, квантова точка,

яка містить багато електронів, може поводити себе як спін 1/2, якщо кількість електронів непарна. Відповідний стан можна приготувати, якщо розмістити квантову точку у сильному магнітному полі при низьких температурах. Маніпулювати спінами можна імпульсними магнітними полями. Вимірювати спінові стани можна, наприклад, надаючи електронам можливості тунелювати у сусідню “вимірювальну” квантову точку. Однак, сучасні технології поки що не дозволяють вимірювати спін у напівпровідниках з потрібною точністю.

Аналогічні “конструкції” можна запропонувати для ядерних спінів, а не лише для електронних.

Отже, найбільш перспективними з технологічної точки зору, вважаються сьогодні схеми, що ґрунтуються на твердотільних системах.

Можливо, будуть запропоновані й зовсім інакші, за принципом дії, платформи для реалізації квантового комп’ютера, однак це — напевне, справа майбутнього.

Лабораторний практикум

І. Загальний опис лабораторного практикуму

Квантові мови програмування розвиваються, як мінімум, два десятки років, але вони були, в основному, теоретичними, оскільки не існувало необхідного апаратного забезпечення. Тепер квантові комп'ютери є реальністю, яка дозволяє будь-кому, хто має доступ до Інтернету, використовувати їх. Ці комп'ютери поки що невеликі, зашумлені і не такі потужні, як сучасні класичні комп'ютери. Але вони зароджуються, неухильно зростають і обіцяють надзвичайно великі обчислювальні потужності для завдань хімії та медицини, машинного навчання та задач оптимізації, передбачень зміни клімату та природних катаклізмів тощо. Ці пристрої є випробувальним стендом для підготовки наступного покоління квантових інженерів-програмістів для вирішення існуючих в даний час класично складних завдань обчислювальної техніки. Дійсно, хмарні квантові обчислення вже використовувалися для розрахунку енергії зв'язку дейтрона і тестових процедур в алгоритмах машинного навчання.

Природно, що відбувається й бурхливе зростання програмного забезпечення для квантових обчислень на широкому наборі класичних комп'ютерних мов. Величезна кількість фреймворків, що позитивно відображає стрімке зростання галузі, ускладнює студентам і дослідникам приймати обгрунтоване рішення про використання того чи іншого програмного забезпечення, тому тут буде наведено короткий огляд інструментарію для квантових обчислень та платформ загального призначення, на яких це можна реалізувати.

З довгого списку було обрано наступні: три, які надають користувачу можливість підключатися до реальних квантових пристроїв - ***Cirq*** від Google, який обіцяє в майбутньому перехід до справжнього квантового комп'ютера; ***QISKit*** від IBM і ***ProjectQ*** від ETH Zurich (де доступ до реального комп'ютера надається вж зараз), - і один з аналогічною функціональністю, але з підключенням через ***PyQuil*** до квантового комп'ютера Rigetti, а також емулятор квантового комп'ютера ***QuTIP***.

Пропонований лабораторний практикум розрахований на магістрів галузі 12 – Інформаційні технології та побудований на принципах вільного вибору середовища розробки та мови програмування. Він може виконуватися як на справжньому квантовому комп’ютері, який надається у користування провідними компаніями, так і за допомогою емуляторів.

Тематика лабораторного практикуму.

Лабораторна робота №1. Знайомство з інструментами квантових розрахунків. Вибір та встановлення обраного інструментарію.

Лабораторна робота №2. Реалізація простих однокубітних обчислень.

Лабораторна робота №3. Реалізація багатокубітних обчислень.

Лабораторна робота №4. Реалізація алгоритму квантової телепортації.

Лабораторна робота №5. Реалізація алгоритму Дойча-Джози.

Лабораторна робота №6. Алгоритм Гровера.

Лабораторна робота №7. Алгоритм Шора. Квантове перетворення Фур'є.

На допомогу для кращого розуміння квантового коду рекомендуємо використовувати книги [39] - [40]

II. Опис інструментарію

1 ***Cirq*** від Google – фреймворк для квантових обчислень з відкритим кодом для NISQ-комп'ютерів (анонсовано 50-100-кубітні варіанти з високоякісними квантовими вентилями). Проєкт швидко розвивається, тому можливі неприємні для розробників ефекти, коли розроблений код не буде працювати на нових версіях фреймворку. Позиціонується як основний інструмент для майбутньої роботи з реальним квантовим комп'ютером від Google, однак сьогодні – це лише симулятор, який володіє відмінним набором простих прикладів: «quantum hello world», «a+b on quantum», нерівність Белла, алгоритм Гровера, квантове перетворення Фур'є та інші.

2 ***QisKit –*** фреймворк з відкритим кодом для роботи із зашумленим квантовим комп'ютером. Має хорошу документацію і дозволяє працювати з реальним квантовим комп'ютером від IBM. QisKit має хороші бібліотеки квантових алгоритмів:

2.a QisKit Aqua, яка дозволяє виконувати квантові обчислення з хімії, штучного інтелекту, моделювання фінансових потоків тощо.

2.b QisKit Aer – високопродуктивний фреймворк для моделювання квантових кіл на симуляторі квантового комп'ютера.

2.c QisKit Terra – основний пакет QisKit, який має набір інструментів для розробки квантових програм на рівні схем та імпульсів з можливістю оптимізації для певного фізичного квантового процесора та керуванням пакетного виконання при віддаленому доступі.

3 ***ProjectQ*** – програмне забезпечення з відкритим кодом для квантових обчислень. Перший випуск містив фреймворк компілятора, що здатен орієнтуватись на різні типи обладнання, високопродуктивний симулятор та модулі компілятора для креслення квантових схем та оцінки ресурсів. Фреймворк працює в Python і дозволяє тестувати квантові алгоритми за допомогою моделювання і працювати з реальним квантовим комп'ютером IBM Quantum Experience за допомогою внутрішнього підключення. Можна розробляти плагіни для оптимізації та синтезу вентилів. Має відмінний набір прикладів, в тому числі й тих, які описують способи підключення до реального квантового комп'ютера від IBM.

4 ***pyQuil*** – Python-бібліотека, представник SDK Forest від Rigetti, для роботи з 8-бітовим квантовим комп'ютером Rigetti засобами цієї популярної мови програмування.

5 ***QuTIP – Qu***antum ***T***oolBox ***I***n ***P***ython, квантовий емулятор для роботи з квантовими алгоритмами на мові Python. Підтримує програмування одно- і багатокубітних квантових вентилів (Тоффолі, Адамара тощо), квантове перетворення Фур'є, алгоритм Дойча-Джози та багато іншого.

III. Методичні вказівки до лабораторних робіт.

Лабораторна робота №1
Знайомство з інструментами квантових розрахунків. Вибір та встановлення обраного інструментарію.

Мета: ознайомитися з інструментарієм для здійснення квантових розрахунків; обрати та встановити обраний фреймворк.

Обладнання: персональний комп'ютер, будь-яка мова програмування.

Завдання:

1 Ознайомитися з рекомендованими інструментами для виконання квантових обчислень.
2 Встановити необхідні бібліотеки як доповнення до бажаної мови програмування.

Теоретична частина

Ознайомтесь з можливостями, методами встановлення та роботи фреймворків для квантових обчислень, поданих у частині II – Опис інструментарію. Детальний опис кожного можна прочитати за посиланнями:

1 ***Cirq*** - https://ai.googleblog.com/2018/07/announcing-cirq-open-source-framework.html; Тут подано загальний опис фреймворку. Документацію можна вивчити за посиланням: https://cirq.readthedocs.io/en/latest/index.html; Код простих прикладів - тут: https://github.com/quantumlib/Cirq/tree/master/examples
2 ***QisKIT*** – сайт проєкту: https://qiskit.org/; хороша документація: https://x-team.com/blog/quantum-computation-python-javascript/; стаття з прикладами: https://hackernoon.com/exploring-quantum-programming-from-hello-world-to-hello-quantum-world-109add25305f;
3 ***ProjectQ*** **–** сайт проєкту: https://projectq.ch/; проста документація: https://dataespresso.com/en/2018/07/22/Tutorial-Generating-random-numbers-with-a-quantum-computer-Python/#comments; приклади написання коду: https://github.com/ProjectQ-Framework/ProjectQ/tree/master/examples
4 ***PyQuil*** **–** проста документація для початківців: https://medium.com/rigetti/how-to-write-a-quantum-program-in-10-lines-of-code-for-beginners-540224ac6b45;
5 ***QuTIP*** **–** хороший tutorial: http://qutip.org/tutorials.html;

Практична частина

1 Використовуючи знання, набуті при вивченні теоретичної частини, оберіть потрібний Вам фреймворк, який: а) придатний для виконання усіх лабораторних робіт; б) відповідає Вашим уподобанням щодо робочої мови програмування.
2 Встановіть обраний інструментарій на Ваш комп'ютер та протестуйте його працездатність за допомогою простих прикладів, наведених в документації.
3 Складіть звіт з лабораторного практикуму з використанням Colab-блокноту або

іншим чином. Дайте відповіді на контрольні запитання.

4 Захистіть лабораторну роботу у викладача.

Контрольні запитання

1 Обгрунтуйте Ваш вибір квантового інструментарію та мови програмування. Чому Ви вважаєте, що обраний Вами інструментарій дозволить виконати лабораторний практикум?

2 Продемонструйте працездатність обраного інструментарію на простих контрольних прикладах з документації.

3 Охарактеризуйте особливості, переваги та недоліки обраного Вами квантового інструментарію.

Лабораторна робота №2
Реалізація простих однокубітних обчислень

Мета: використовуючи знання, набуті у попередній лабораторній роботі, навчитись реалізовувати у програмному коді прості однокубітні квантові операції.

Обладнання: персональний комп’ютер, будь-яка мова програмування.

Завдання:

1 Ознайомитися з теоретичними відомостями про однокубітні квантові операції.
2 Реалізувати прості квантові однокубітні операції в програмному коді, використовуючи встановлений інструментарій.
3 Виконати розроблений програмний код на реальному квантовому комп'ютері (емуляторі квантового комп'ютера).

Теоретична частина

Ознайомтесь з простими однокубітними операціями, прочитавши розділ «Прості операції над кубітами». До простих квантових операцій будемо відносити тотожну операцію (*I*), заперечення (*NOT*) та гейт Адамара (*H*).

Практична частина

1 Реалізуйте в програмному коді прості однокубітні квантові операції: тотожну операцію, заперечення та гейт Адамара з використанням встановленого Вами фреймворку.
2 Запустіть розроблений Вами код на квантовому комп'ютері (емуляторі квантового комп'ютера).
3 Проаналізуйте отримані результати.
4 Дайте відповіді на контрольні запитання.
5 Опишіть протокол Ваших дій та дайте відповіді на контрольні запитання у Вашому Colab-блокноті.
6 Захистіть лабораторну роботу у викладача.

Контрольні запитання

1 Що таке кубіт? Чим він відрізняється від класичного біту? Наведіть приклади.
2 Опишіть прості операції з квантовими бітами. В чому полягає їх особливості?
3 Для чого найбільше використовують операцію Адамара?
4 Які висновки Ви можете зробити з цієї лабораторної роботи стосовно роботи квантових фреймворків?

Лабораторна робота №3
Реалізація багатокубітних обчислень

Мета: використовуючи знання, набуті у попередніх лабораторних роботах, навчитись реалізовувати у програмному коді багатокубітні квантові операції.

Обладнання: персональний комп’ютер, будь-яка мова програмування.

Завдання:

1 Ознайомитися з теоретичними відомостями про багатокубітні квантові операції.
2 Реалізувати багатокубітні квантові операції в програмному коді, використовуючи встановлений інструментарій.
3 Виконати розроблений програмний код на реальному квантовому комп'ютері (емуляторі квантового комп'ютера).

Теоретична частина

Ознаййомтесь з багатокубітними квантовими операціями, прочитавши розділ «Багатокубітні операції». До багатокубітних квантових операцій будемо відносити контрольоване заперечення (*CNOT, Controlled NOT*), гейти Тоффолі та Фредкіна.

Практична частина

1 Реалізуйте в програмному коді обрані Вами багатокубітні квантові операції з використанням встановленого Вами фреймворку.
2 Запустіть розроблений Вами код на квантовому комп'ютері (емуляторі квантового комп'ютера).
3 Проаналізуйте отримані результати.
4 Дайте відповіді на контрольні запитання.
5 Опишіть протокол Ваших дій та дайте відповіді на контрольні запитання у Вашому Colab-блокноті.
6 Захистіть лабораторну роботу у викладача.

Контрольні запитання

1 Опишіть обрані Вами для дослідження багатокубітні операції. Скільки кубітів потрібно для їх реалізації?
2 Які класичні логічні операції можна реалізувати з використанням багатокубітних квантових операцій? Продемонструйте це.
3 Які висновки Ви можете зробити з виконаної лабораторної роботи?
4 Наскільки можливості обраного Вам фреймворка відповідають потребам цієї лабораторної роботи?
5 Які додаткові можливості фреймворка можна використати для реалізації багатокубітних операцій?

Лабораторна робота №4
Реалізація алгоритму квантової телепортації

Мета: використовуючи знання, набуті у попередніх лабораторних роботах, навчитись реалізовувати у програмному коді алгоритм квантової телепортації.

Обладнання: персональний комп’ютер, будь-яка мова програмування.

Завдання:

1 Ознайомитися з теоретичними відомостями про алгоритм квантової телепортації.
2 Реалізувати алгоритм квантової телепортації в програмному коді, використовуючи встановлений інструментарій.
3 Виконати розроблений програмний код на реальному квантовому комп'ютері (емуляторі квантового комп'ютера).

Теоретична частина

Ознайомтесь з алгоритмом квантової телепортації, прочитавши розділ «Квантова телепортація». Вивчіть також теоретичний матеріал, необхідний для ясного розуміння цього алгоритму: «Часткові вимірювання», «Переплутані стани», «Прості операції над кубітами» тощо.

Практична частина

1 За допомогою обраного Вами фреймворку реалізуйте алгоритм квантової телепортації.
2 Запустіть розроблений Вами код на квантовому комп'ютері (емуляторі квантового комп'ютера).
3 Проаналізуйте отримані результати.
4 Дайте відповіді на контрольні запитання.
5 Опишіть протокол Ваших дій та дайте відповіді на контрольні запитання у Вашому Colab-блокноті.
6 Захистіть лабораторну роботу у викладача.

Контрольні запитання

1 Опишіть алгоритм квантової телепортації та поясніть його призначення.
2 В чому полягає причина заборони клонування квантових станів?
3 Поясніть, будь ласка, вплив часткових вимірювань на квантові стани кубітів, що беруть участь у процесі квантової телепортації.
4 Для чого використовують ґейт Адамара при реалізації квантової телепортації?
5 Які висновки Ви зробили при виконанні цієї лабораторної роботи?

Лабораторна робота №5
Реалізація алгоритму Дойча-Джози

Мета: використовуючи знання, набуті у попередніх лабораторних роботах, навчитись реалізовувати у програмному коді алгоритм Дойча-Джози.

Обладнання: персональний комп’ютер, будь-яка мова програмування.

Завдання:

1 Ознайомитися з теоретичними відомостями про алгоритм Дойча-Джози.
2 Реалізувати алгоритм Дойча-Джози в програмному коді, використовуючи встановлений інструментарій.
3 Виконати розроблений програмний код на реальному квантовому комп'ютері (емуляторі квантового комп'ютера).

Теоретична частина

Ознайомтесь з алгоритмом Дойча-Джози, прочитавши розділ «Алгоритм Дойча». Вивчіть також теоретичний матеріал, необхідний для ясного розуміння цього алгоритму: «Часткові вимірювання», «Переплутані стани», «Прості операції над кубітами» тощо.

Практична частина

1 За допомогою обраного Вами фреймворку реалізуйте алгоритм Дойча-Джози.
2 Запустіть розроблений Вами код на квантовому комп'ютері (емуляторі квантового комп'ютера).
3 Проаналізуйте отримані результати.
4 Дайте відповіді на контрольні запитання.
5 Опишіть протокол Ваших дій та дайте відповіді на контрольні запитання у Вашому Colab-блокноті.
6 Захистіть лабораторну роботу у викладача.

Контрольні запитання

1 Опишіть алгоритм Дойча-Джози, користуючись матеріалами теоретичної частини.
2 В чому полягає суть квантового прискорення обчислень і як це демонструє алгоритм Дойча-Джози?
3 Які прості операції над кубітами використано в цьому алгоритмі?
4 Які багатокубітні операції використано в цьому алгоритмі?
5 Як часткові вимірювання впливають на квантовий стан кубітів в алгоритмі Дойча-Джози?
6 Які висновки Ви зробили з цієї лабораторної роботи?

Лабораторна робота №6
Реалізація алгоритму Л.Гровера

Мета: використовуючи знання, набуті у попередніх лабораторних роботах, навчитись реалізовувати у програмному коді алгоритм швидкого пошуку у невпорядкованому масиві Лова Гровера.

Обладнання: персональний комп’ютер, будь-яка мова програмування.

Завдання:

1 Ознайомитися з теоретичними відомостями про алгоритм Гровера.
2 Реалізувати алгоритм Гровера в програмному коді, використовуючи встановлений інструментарій.
3 Виконати розроблений програмний код на реальному квантовому комп'ютері (емуляторі квантового комп'ютера).

Теоретична частина

Ознайомтесь з алгоритмом Дойча-Джози, прочитавши розділ «Алгоритм Гровера». Вивчіть також теоретичний матеріал, необхідний для ясного розуміння цього алгоритму: «Часткові вимірювання», «Переплутані стани», «Прості операції над кубітами» тощо.

Практична частина

1 За допомогою обраного Вами фреймворку реалізуйте алгоритм Гровера.
2 Запустіть розроблений Вами код на квантовому комп'ютері (емуляторі квантового комп'ютера).
3 Проаналізуйте отримані результати.
4 Дайте відповіді на контрольні запитання.
5 Опишіть протокол Ваших дій та дайте відповіді на контрольні запитання у Вашому Colab-блокноті.
6 Захистіть лабораторну роботу у викладача.

Контрольні запитання

1 В чому полягає суть квантового алгоритму швидкого пошуку у невпорядкованому масиві Л.Гровера?
2 Обґрунтуйте загрози, що їх несе алгоритм Л.Гровера для класичних криптографічних алгоритмів.
3 Що необхідно зробити для блокування зазначених Вами загроз? Які рекомендації щодо цього надає Національний інститут стандартів і технологій США?
4 Які квантові операції використано при реалізації алгоритму Гровера?
5 Які висновки щодо обраного інструментарію Ви зробили після виконання цієї лабораторної роботи?

Лабораторна робота №7
Реалізація алгоритму П.Шора. Квантове перетворення Фур'є.

Мета: використовуючи знання, набуті у попередніх лабораторних роботах, навчитись реалізовувати у програмному коді алгоритм Шора та квантове перетворення Фур'є.

Обладнання: персональний комп’ютер, будь-яка мова програмування.

Завдання:

1 Ознайомитися з теоретичними відомостями про алгоритм Шора.
2 Реалізувати алгоритм Шора в програмному коді, використовуючи встановлений інструментарій.
3 Виконати розроблений програмний код на реальному квантовому комп'ютері (емуляторі квантового комп'ютера).

Теоретична частина

Ознайомтесь з алгоритмом П.Шора, прочитавши розділ «Алгоритм факторизації цілих чисел (алгоритм Шора)». Вивчіть також теоретичний матеріал, необхідний для ясного розуміння цього алгоритму: «Часткові вимірювання», «Переплутані стани», «Прості операції над кубітами» тощо.

Практична частина

1 За допомогою обраного Вами фреймворку реалізуйте алгоритм П.Шора.
2 Запустіть розроблений Вами код на квантовому комп'ютері (емуляторі квантового комп'ютера).
3 Проаналізуйте отримані результати.
4 Дайте відповіді на контрольні запитання.
5 Опишіть протокол Ваших дій та дайте відповіді на контрольні запитання у Вашому Colab-блокноті.
6 Захистіть лабораторну роботу у викладача.

Контрольні запитання

1. Опишіть алгоритм Шора і його значення для класичної криптографії.
2. Для яких цілей використовується квантове перетворення Фур'є в алгоритмі Шора?
3. Охарактеризуйте рекомендації Національного інституту стандартів і технологій США стосовно блокування загроз, що їх несе алгоритм Шора для класичної криптографії.
4. Які квантові операції використано при реалізації алгоритму Шора?
5. Які висновки Ви зробили після виконання цієї лабораторної роботи?

Перелік використаної літератури

1.Закон Мура.Вікіпедія. Вільна енциклопедія. - https://en.wikipedia.org/wiki/Moore%27s_law (дата звернення: 02.07.2021).
2.Закон Амдала.Вікіпедія. Вільна енциклопедія. - https://en.wikipedia.org/wiki/Amdahl%27s_law (дата звернення: 02.07.2021).
3.Planck, M.//Verhandl. Dtsch. phys. Ges.,1900. -2. - 202-210
4.L. de BroglieOndes et quanta//Comptes rendus de l'Académie des sciences,1923. -177. - P.507-510.
5.Simon B., Functional Integration and Quantum Physics//Academic Press,1979. - 546.
6.Wiesner S. Conjugate coding//SIGACT News,1983. -Vol. 15, No. 1. - P.78-88.
7.Feynman, R.P. There's plenty of room at the bottom (data storage)//Journal of Microelectromechanical Systems,1992. -vol. 1, no. 1. - P. 60—66.
8.Toffoli T. Reversible computing// International Colloquium on Automata, Languages, and Programming, 1980. - P.632-644
9.Wootters W., Zurek W. H. A Single Quantum Cannot be Cloned//Nature,1982. -299. - P.802-803.
10.Bennett C. H., Brassard G. Quantum Cryptography: Public Key Distribution and Coin Tossing//Proceedings of International Conference on Computers, Systems & Signal Processing, Dec. 9-12, 1984, Bangalore, India,1984. - P.175.
11.Bennett C. and Wiesner S. Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states//Phys. Rev. Lett,1992. -69. - P.2881.
12.Bennett C. Quantum Cryptography Using Any Two Nonorthogonal States//Physical Review Letters,1992. -25.05. - P.3122.
13.Wolf R. de , Quantum Computing: Lecture notes//arXiv:1907.09415,2019. - 176 P.
14.Bennett C. H., Brassard G., Crépeau C., Jozsa R., Peres A., Wootters W. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels//Phys. Rev. Lett,1993. - V.70, N.13. - P.1895-1899.
15.Shor P. W. Algorithms for quantum computation: discrete logarithms and factoring//Foundations of Computer Science : Conference Publications,1994. - P.124-134.
16.Report on Post-Quantum Cryptography. NIST 9105 Draft Report. - https://csrc.nist.gov/csrc/media/publications/nistir/8105/final/documents/nistir_8105_draft.pdf (дата звернення: 03.07.2021).
17.Grover L.K. A fast quantum mechanical algorithm for database search//Proceedings, 28th Annual ACM Symposium on the Theory of Computing,1996. - P.212.
18.Quantum Copmuting: How D-Wave System Works.D-Wave: The Quantum Computing Company. - https://www.dwavesys.com/quantum-computing (дата звернення: 03.07.2021).
19.Фейнман Р., Лейтон Р., Сэндс М., Фейнмановские лекции по физике. Т.1-9.//М.: "Мир",1976.
20.Einstein A., Podolsky B., Rosen N.Einstein A., Podolsky B., Rosen N. Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?//Phys. Rev.,1935. -V.47, N.10. - P.777-780.
21.Bohm D., Quantum Theory//New York: Prentice Hall,1951. - 700 P.
22.Bell J.S. On the Einstein Podolsky Rosen Paradox//Phys. Phys. Fiz.,1964. -V.1, N.3. - P. 195-200
23.Bouwmeester D., Pan J-W., Mattle K., Eibl M., Weinfurter H. & Zeilinger A.Experimental quantum teleportation//Nature,1997. -390. - P. 575-579.
24.D. Boschi, S. Branca, F. De Martini, L. Hardy, and S. Popescu. Experimental Realization of Teleporting an Unknown Pure Quantum State via Dual Classical and Einstein-Podolsky-Rosen Channels//Phys. Rev. Lett.,1998. -80. - 1121.
25.Jacob F. Sherson, Hanna Krauter, Rasmus K. Olsson, Brian Julsgaard, Klemens Hammerer, Ignacio Cirac and Eugene S. Polzik. Quantum teleportation between light and matter//Nature,2006. -443. - P. 557-560.

26.Xian Min-Jin et al. Experimental free-space quantum teleportation//Nature Photonics,2010. -V. 4. - PP. 376–381.
27.Satellite-based photon entanglement distributed over 1,200 kilometers. EurekAlert!. - https://www.eurekalert.org/pub_releases/2017-06/uosa-spe061217.php (дата звернення: 05.07.2021).
28.The classical and quantum Fourier transform. Домашня сторінка P. де Вольфа. - https://homepages.cwi.nl/~rdewolf/qfourierintro.pdf (дата звернення: 05.07.2021).
29.Rabin M.O. Probabilistic Algorithm for Testing Primality//JOURNAL OF NUMBER THEORY ,1980. -12. - PP.128-138.
30.Gisin N., Ribordy G., Tittel W., Zbinden N. Quantum Cryptography//Rev. Mod. Phys., 2002. - V.74, N.1. - PP. 145-191.
31.Lydersen L. et al. Hacking commercial quantum cryptography systems by tailored bright illumination//Nature Photonics,2010. -4. - PP.686-689.
32.Ekert, A. K.Quantum Cryptography Based on Bell's Theorem//Physical Review Letters, 1991. - 67. - PP.661-663.
33.The Nobel Prize in Physics 2012. Веб-сайт Нобелівського комітету. - https://www.nobelprize.org/prizes/physics/2012/summary/ (дата звернення: 05.07.2021).
34.Нильсен М., Чанг И., Квантовые вычисления и квантовая информация//М.:Мир, 2006. - 824 С.
35.Баумейстер Д., Экрет А., Цайлингер А., Физика квантовой информации//М.: Постмаркет, 2002. - 376 С.
36.Ефект Керра. Вікіпедія. Відкрита енциклопедія. - https://en.wikipedia.org/wiki/Kerr_effect (дата звернення: 07.07.2021).
37.Оптичний комп'ютер. Вікіпедія. Вільна енциклопедія. - https://en.wikipedia.org/wiki/Optical_computing (дата звернення: 07.07.2021).
38.Fabry–Pérot interferometer. Вікіпелія: вільна енциклопедія. - https://en.wikipedia.org/wiki/Fabry%E2%80%93P%C3%A9rot_interferometer (дата звернення: 09.07.2021).
39.Химено-Сеговиа М., Хэрриган Н., Джонстон Э., Программирование квантовых компьютеров//O'Reilly, 2021. - 336 с.
40.Крохмальський Т., Вступ до квантових обчислень//Львів: ЛНУ, 2018. - 204 с.