УДК **681.3**

Завадський І. О.

КВАНТОВИЙ КОМП'ЮТЕР: ПРОБЛЕМИ І ПЕРСПЕКТИВИ

Мета праці - ознайомити з основами теорії та практики квантових обчислень науковців і програмістів, які не є фахівцями в даній галузі. Розглядаються сучасні досягнення і проблеми на шляху до створення квантового комп 'ютера.

Закони квантового світу не мають аналогів у світі макроскопічному. У «звичний» спосіб квантові частки поводять себе лише тоді, коли ми «підглядаємо» за ними, тобто визначаємо їх стани. Достатньо нам лише перервати спостереження – і квантова частка перейде з певного визначеного стану в нескінченну кількість різних станів. Тобто електрон, фотон або будь-який інший квантовий об'єкт частково перебуватиме в одній точці простору, частково в іншій, а частково ще в іншій тощо. Проте в результаті вимірювання електрон неодмінно буде знайдено «цілим і неушкодженим» у певній одній точці простору. Постає питання: чи завжди можна змоделювати на комп'ютері поведінку систем, що складаються з таких «непередбачуваних» часток?

Уперше гіпотезу про те, що деякі квантомеханічні операції не можна точно відтворити на класичному комп'ютері, у 1980 р. висловив Ю. І. Манін, а у 1982 р.– Р. Фейнман. Цим моментом прийнято датувати початок досліджень у галузі квантових обчислень. Зі спостереження Фейнмана випливало, що, можливо, обчислення стануть продуктивнішими, якщо їх здійснювати за допомогою квантових операцій. Проте створення квантової обчислювальної машини виявилося надто складною задачею, до того ж не було впевненості у тому, що квантові ефекти прискорять обчислення. Тому спочатку інтенсивність досліджень у цій сфері була досить низькою. Так тривало до 1994 р., коли П. Шор винайшов квантовий алгоритм факторизації цілих чисел, часова складність якого приблизно квадратично залежить від довжини вхідних даних [3].

Усі відомі класичні алгоритми факторизації, або розкладу на множники цілих чисел, мають експоненціальну часову складність відносно довжини вхідних даних. *Тобто розкласти на множники число, яке містить декілька сотень* цифр, за допомогою таких алгоритмів практично неможливо. Зокрема, за приблизною оцінкою розклад на множники 1000-знакового числа за найкращим на сьогодні класичним алгоритмом факторизації відбуватиметься протягом 10^{25} років (що значно перевищує вік Всесвіту). Факторизація 1000-знакового числа за допомогою алгоритму Шора потребуватиме виконання лише кількох мільйонів елементарних операцій, тобто займатиме не більше кількох годин. Це означає, що криптосистеми з відкритим ключем, які базуються на факторизації, можуть бути зламані на квантовому комп'ютері.

Саме з моменту відкриття Шора галузі квантових обчислень почали приділяти належну увагу з боку фізики і математики усього світу. На сьогодні дослідження в цій галузі стали пріоритетними в багатьох університетах і науково-дослідних центрах Західної Європи та США.

Найменшою одиницею інформації у квантових комп'ютерах є квантовий біт, або *кубіт*. Фізично кубіт моделюється, як правило, однією квантовою часткою – фотоном, електроном тощо. Якщо припустити певні спрощення, то стан такої частки можна описати вектором одиничної довжини у двовимірному комплексному просторі: $\Psi = \alpha|\rightarrow\rangle + \beta|\uparrow\rangle$ (рис. 1). Наведений вираз називається хвильовою функцією, де α і β – деякі комплексні числа, *амплітуди*, $|\alpha|^2 + |\beta|^2 = 1$, $|\rightarrow\rangle$ та $|\uparrow\rangle$ – базисні вектори.

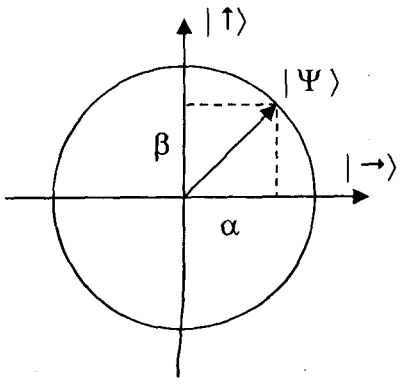

Рис. 1. Математичне зображення квантового біту

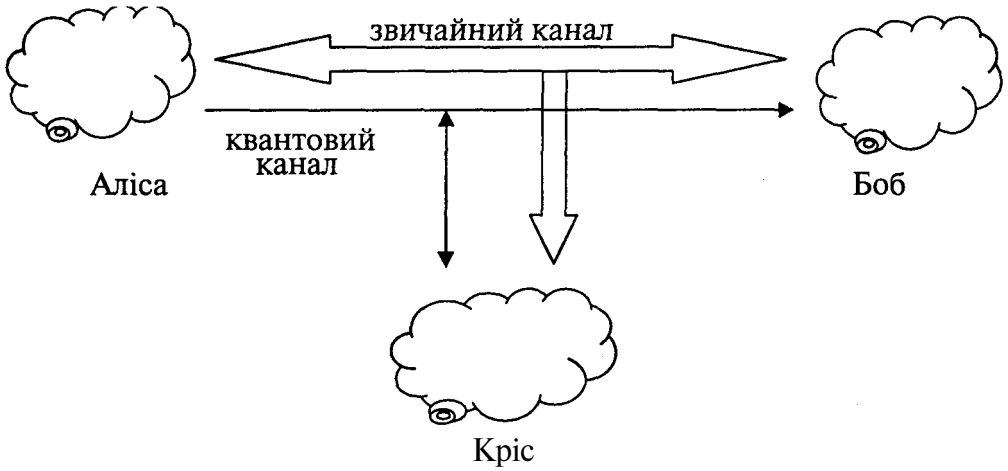

Рис. 2. Канали зв'язку в протоколі Беннета - Брассарда

Найважливішою властивістю квантової частки є те, що в результаті вимірювання вона неодмінно опиниться в одному з базисних станів: $|\rightarrow\rangle$ або $|\uparrow\rangle$. При цьому величини $|\alpha|^2$ та $|\beta|^2$ дорівнюють імовірностям віднайти частку в стані $|\rightarrow\rangle$ або $|\uparrow\rangle$ відповідно. Дізнатися значення амплітуд, маючи лише один екземпляр квантової частки, неможливо. Неможливо також і відтворити, або скопіювати квантову частку. Зазначимо також, що для зображення станів частки можна обрати довільний ортонормований базис. У квантовій механіці кожен вимірювальний пристрій характеризується власним базисом, на один із векторів якого і перетворюється стан квантової частки під час вимірювання.

Розглянуті властивості квантових часток надали можливості їх застосування у криптографії. У 1984 р. Беннет і Брассард вперше описали квантову схему протоколу передачі ключа [4].

Припустимо, Аліса і Боб для ведення переговорів хочуть спільно використовувати секретний ключ, тобто інформаційне повідомлення, зміст якого знатимуть лише вони вдвох. Як їм передати таке повідомлення одне одному? Адже зловмисник, назвемо його Крісом, прослуховує всі канали зв'язку між Алісою та Бобом. Сьогодні Аліса і Боб можуть вирішити цю проблему за допомогою процедури шифрування з відкритим ключем. Але така процедура не буде надійною, якщо у Кріса є квантовий комп'ютер. У цьому випадку Алісі й Бобу слід застосувати «квантовий захист» від озброєного квантовими інструментами зламування зловмисника, адже подібне нейтралізується подібним.

У протоколі Беннета і Брассарда зв'язок між Алісою і Бобом здійснюється за двостороннім звичайним та одностороннім квантовими каналами. Обидва ці канали прослуховуються зловмисником Крісом (рис. 2).

Квантовий канал дає змогу Алісі пересилати окремі частки (наприклад, фотони) Бобу, який може виміряти їхні стани. Кріс також може спробувати виміряти стани цих часток та переслати їх Бобу. Передавання секретного ключа відбувається в декілька етапів.

1. Аліса формує довільну послідовність бітів і кодує кожен із них квантовим станом фотона. Для кожного біта випадково обирається один із двох способів кодування:

1) нуль кодується станом $|\uparrow\rangle$, а одиниця – станом $|\rightarrow\rangle$;

2) нуль кодується станом $|\nwarrow\rangle$, а одиниця – станом $|\nearrow\rangle$.

Набір фотонів Аліса надсилає Бобу.

2. Боб вимірює стани фотонів. Будь-який квантомеханічний пристрій, що вимірює двовимірну систему (наприклад, фотон), характеризується двома базисними станами. Вимірювання фотона приводить до того, що він опиняється в одному з двох базисних станів вимірювального пристрою. Отже, Боб у випадковий спосіб добирає для кожного вимірювання один з тих двох базисів, які використовувались Алісою: $(|\uparrow\rangle, |\rightarrow\rangle)$ або $(|\nwarrow, |\nearrow\rangle)$.

3. Аліса і Боб повідомляють одне одному через звичайний канал зв'язку, які базиси вони використали. Якщо для кодування й розкодування певного біта були використані однакові базиси, біт передано правильно. Базиси збігатимуться приблизно в 50 % випадків, тому приблизно 50 % бітів повідомлення будуть передані правильно. Ці біти складатимуть ключ, а решту бітів можна відкинути.

Розглянемо можливі дії зловмисника. Припустимо, Кріс хоче залишити в себе копії фо-

тонів, що передаються квантовим каналом, а згодом, прослухавши розмову Аліси і Боба по звичайному каналу, виміряти ці скопійовані фотони в правильних базисах. Ця атака не вдасться, оскільки невідомий стан квантової частки скопіювати неможливо, а при вимірюванні цей стан втрачається.

Тепер припустимо, що Кріс вимірює стани фотонів, які передає Аліса, і хоче переслати Бобу нові фотони з цими самими станами. Оскільки Кріс не знає, яким саме способом було закодовано той чи інший біт, то приблизно для половини вимірювань він використає хибні базиси, а отже, не зможе відновити без спотворень стани фотонів, переданих Алісою. У результаті такого втручання приблизно 25 % бітів ключа в Аліси і Боба відрізнятимуться. Аліса і Боб можуть легко встановити факт прослуховування, порівнявши невелику кількість бітів секретного повідомлення.

Квантовий протокол передавання ключа було апробовано на відстані 24 км з використанням стандартних оптоволоконних кабелів і на відстані 0,5 км при передаванні в повітрі.

Оперування окремими квантовими частками має декілька цікавих застосувань, проте справжня, «експоненціальна» потужність квантових обчислень проявляється при дослідженні систем з n квантових часток. Уявімо макроскопічний об'єкт, що розбивається на n частин, які розлітаються в різних напрямках. Для того, щоб описати стан такої системи, достатньо описати стан кожної її складової частини. Квантова система, що складається з n часток, має досить дивну й неочевидну властивість: для того, щоб повністю описати її стан, у загальному випадку недостатньо описати стани її складових. Якщо стан кожної частки задається вектором у двовимірному просторі, то в класичній фізиці множина станів системи з n часток утворюватиме $2n$-вимірний простір. У квантовій системі розмірність простору станів становитиме 2^n. Саме це експоненціальне зростання розмірності простору станів дає експоненціальну перевагу в швидкості обчислень на квантових комп'ютерах порівняно з класичними.

Отже, стан n-розрядного квантового регістра в загальному випадку описується 2^n-вимірним вектором. Важливим є також те, що операція над одним або двома кубітами може спричинити зміну експоненціальної кількості компонент вектора амплітуд квантового регістра. Враховуючи ці факти, опишемо типову схему квантового алгоритму.

1. Набір з m квантових часток приводиться до стану $|\uparrow\uparrow\ldots\uparrow\rangle$, що в математичному записі означає $|0\,0\ldots0\rangle$.

2. До n кубітів квантового регістру ($n<m$) застосовується перетворення Уолша – Адамара H, яке перетворює стан $|0\,0\ldots0\rangle$ на стан $1/2^n(|0\,0\ldots0\rangle|0\rangle+|0\,0\ldots0\,1\rangle|0\rangle+\ldots+|1\,1\ldots1\rangle|0\rangle)$. Останні $m-n$ кубітів, що їх умовно було позначено символами $|0\rangle$, будуть використані для запам'ятовування значень функцій, аргументами яких будуть перші n кубітів.

3. Тепер значення перших n кубітів можна використати як аргументи певної обчислювальної схеми. Кожен елемент такої схеми реалізовуватиме деяку булеву функцію від двох (можливо, одного або трьох) аргументів. Результат роботи схеми записується в останні $m-n$ кубітів. Найважливішим є те, що значення булевої функції обчислюється одночасно для 2^n наборів аргументів, ця властивість називається *квантовим паралелізмом*. Отже, квантовий регістр набуває вигляду

$$\sum_{u=0}^{2^n-1}\alpha_u|u\rangle|f(u)\rangle$$

де α_u – комплексні амплітуди, $\sum_{u=0}^{2^n-1}|\alpha_u|^2=1$.

4. Застосувавши квантовий паралелізм, можна виконувати подальші перетворення над групами бітів квантового регістра. Як правило, мета таких перетворень полягає у підвищенні ймовірності отримання потрібного результату під час останньої дії – вимірювання.

5. Виконується вимірювання, в результаті якого з тою чи іншою імовірністю отримаємо той чи інший набір значень m кубітів.

Як і у звичайних імовірнісних алгоритмах, для розв'язання конкретної задачі означена вище процедура застосовується багаторазово. Це пояснюється тим, що потрібний результат отримується лише з певною імовірністю, і для підвищення його достовірності обчислення слід повторити.

Однак для того, щоб використати потенційні переваги квантових обчислень, доводиться долати численну кількість проблем, як алгоритмічних, так і фізичних. Ситуація, коли квантові частки є ізольованими від впливів зовнішнього середовища, а їх стани стабільні у часі, є надто ідеалізованою. Насправді квантова система є надзвичайно чутливою через її вкрай малі розміри. Взаємодія часток, що відповідають кубітам, із зовнішнім середовищем, збурює

стан квантової системи і перетворює його у непередбачуваний спосіб. Певний час навіть були сумніви щодо можливості фізично реалізувати квантові алгоритми. Адже похибки, які виникають при спробі виконати алгоритм Шора із числами, що містять 130 десяткових розрядів, у будь-якій із наявних моделей квантового комп'ютера приблизно на 7 порядків перевищують допустиму величину. Але, на щастя, вдалося побудувати квантові коригуючі коди, що, як і класичні коди, дають змогу виправити досить широкий клас помилок за допомогою збільшення довжини інформаційного повідомлення [5].

На сьогодні запропонована численна кількість і власне фізичних способів нівелювання впливу зовнішнього середовища на квантову систему. Найвідомішими з них є використання іонних пасток та ядерного магнітного резонансу.

У квантових комп'ютерах з іонною пасткою лінійна послідовність іонів, які відповідають кубітам, обмежена електричним полем. Для того, щоб виконати однокубітові квантові операції, лазери спрямовуються на окремі іони. Двохкубітові операції здійснюються за допомогою лазера, що спрямовується на окремий кубіт для створення коливання, що поширюється вздовж послідовності іонів до другого кубіта, де інший лазер зупиняє це коливання, а отже, завершує виконання операції. Даний метод вимагає, щоб іони перебували в чистому вакуумі при максимально низьких температурах.

Переваги методу ядерного магнітного резонансу пояснюються тим, що його можна застосовувати при кімнатній температурі. Ця технологія вже досягла певних успіхів. Сутність методу полягає в тому, щоб використати макроскопічну кількість матерії і закодувати квантовий біт середнім станом спинів багатьох ядер. Станами спинів можна керувати за допомогою магнітних полів, а спеціальна техніка ядерного магнітного резонансу дає змогу вимірять середній стан спинів.

Складність теоретичної побудови ефективних квантових алгоритмів пов'язана насамперед з такими особливостями квантових обчислень:

1. Оскільки вимірювання руйнує стан квантової системи, у процес квантового обчислення не можна «втрутитись», тобто вимірять проміжні результати і, проаналізувавши їх, спрямувати обчислювальний процес в тому чи іншому напрямку. Квантове обчислення має відбуватися безперервно від введення вхідних даних до вимірювання результатів, будучи для зовнішнього спостерігача певною «чорною скринькою».

2. Над системою квантових бітів можна виконувати не довільні перетворення, а лише ті, які задаються унітарними операторами в просторі станів квантової системи, що є гільбертовим простором.

3. Під час вимірювання стану квантової системи, який визначається 2^n-вимірним вектором, можна отримати лише один n-розрядний результат. При цьому не можна визначити наперед, який саме результат буде отримано, оскільки квантове обчислення є імовірнісним.

Ці алгоритмічні складнощі накладають суттєві обмеження на мову програмування для квантових комп'ютерів. Унітарні перетворення є зворотними, а отже, зворотними повинні бути всі операції над квантовими бітами. З цього, зокрема, випливає незаконність звичайного присвоєння: замість оператора $|a> = n$ має здійснюватися приростання значення початково рівної нулю змінної: $|a> = |a> + n$. З неможливості копіювання квантових бітів випливає неприпустимість присвоювань вигляду $|x> = |y>$. Оскільки програма може отримати доступ до квантової інформації після вимірювання, але не під час обчислювального процесу, кількість ітерацій циклів має бути незалежною від значень квантових змінних. Певні обмеження накладаються на структуру операторів умовного переходу тощо. На сьогодні розроблено декілька варіантів квантової мови програмування, проте всі вони потребують подальшого вдосконалення [6]. Для деяких мов створено інтерпретатори та симулятори квантового обчислювального процесу на класичних комп'ютерах.

Отже, способи експоненціального зменшення складності класичних обчислень є зовсім не очевидними. Управління квантовою системою не має класичних аналогів і потребує нетрадиційних прийомів програмування. Доведено, що неможливо винайти певний універсальний спосіб квантового прискорення класичних алгоритмів [7]. Таке прискорення насправді є рідкісним феноменом, своєрідним витвором техніки. Фактично, досі було винайдено лише два принципово різних методи отримання квантового прискорення. Перший було запропоновано у згаданому вище алгоритмі П. Шора. Авторство другого належить Л. Гроверу, який у 1996 р. запропонував алгоритм пошуку елемента із заданою властивістю в n-елементному невпорядкованому списку [8]. Кількість кроків в алгоритмі Гровера є пропорційною величині $\sqrt{n}$,

в той час як жоден класичний алгоритм не може виконати такий пошук швидше, ніж за n кроків.

Попри всі складнощі, прототипи квантових комп'ютерів створено вже сьогодні. Щоправда, поки що вдається зібрати лише невеликі квантові регістри, що складаються з кількох кубітів. Зокрема, нещодавно група американських фізиків з корпорації IBM оголосила про створення 7-бітового квантового комп'ютера. На жаль, наявні квантові системи ще не можуть гарантувати надійності обчислень, оскільки вони або недостатньо керовані, або недостатньо ізольовані від впливу шумів. Проте принципових фізичних «заборон» щодо побудови ефективного квантового комп'ютера немає, необхідно подолати лише технологічні труднощі. У цьому напрямі проводяться активні дослідження, і можна припустити, що потужний квантовий комп'ютер буде реалізовано у недалекому майбутньому — за 10—20 років.

1. *Риффель Э., Полак В.* Основы квантовых вычислений // Квантовый компьютер и квантовые вычисления.- Т. 1.— № 1.- 2000.- С. 4-57.
2. *Pittenger A. O.* An introduction to Quantum Computing Algorithms.- Birkhauser Boston, 2001.- 154 p.
3. *Shor P. W.* Algorithms for quantum computation: Discrete log and factoring // Proceedings of the 35th Annual Symposium on Foundations of Computer Science, November, 1994.— P. 124—134.
4. *Bennett C H., Brassard G.* Quantum public key distribution reinvented *I/* SIGA CT News (ACM Special Interest Group on Automata and Computability Theory), 18, 1987.
5. *Ауї/ E., Laflamme R.* A theory of quantum error-correcting codes *II* Physical Review, A 55.- 1997.- P. 900-911.
6. *Omer B.* Structured quantum programming, ph. d. thesis preprint.- Institute for Theoretical Physics, Technical University of Vienna, 2003,— 125 p.
7. *Ozhigov Y.* Limitation of computational resources as a physical principle */I* lanl e-print, http://xxx.lanl.gov/quant-ph/0303127
8. *Grover L. K.* A fast quantum mechanical algorithm for database search *U* Proceedings of the 28th Annual ACM Symposium on the Theory of Computing, Philadelphia, Pennsylvania, May, 1996.- P. 212-219.

I. O. Zavadskiy

QUANTUM COMPUTER: PROBLEMS AND PROSPECTS

The aim of the paper is to acquaint scientists and programmers with the basics of the quantum computations theory and practice. Last achievements and problems of quantum computer creating are discussed.