

ПЕРСПЕКТИВИ РОЗВИТКУ КВАНТОВИХ ОБЧИСЛЕНЬ

Ця стаття дає уявлення про квантові обчислення та комп'ютери — технології, що набули на поточний момент бурхливого розвитку. Наведено переваги над класичними обчисленнями та розглянуто основні проблеми на шляху реалізації квантових комп'ютерів.

Сучасний етап розвитку класичних електронних обчислювальних пристроїв практично досяг межі можливості підвищення швидкості обчислень за рахунок удосконалення елементарної бази пристроїв. Тому розв'язання нових задач ХХІ ст. потребує створення нових теоретичних принципів обчислень на новітніх елементах. Висвітленню одного з них — квантовим обчисленням з використанням квантових комп'ютерів — і присвячена ця стаття. Останнім часом з'явилося дуже багато публікацій, що описують різні аспекти квантових обчислень [1–5]. Охарактеризуємо основні з них.

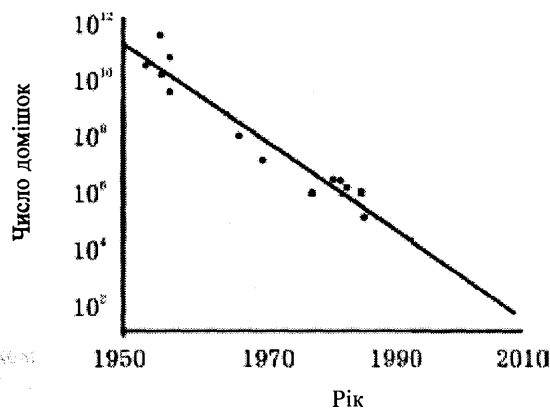


Рис. Зменшення з роками кількості електронів для збереження одного біта інформації

Почнемо з дослідження тенденції розвитку технологій виробництва мікросхем. На рисунку наведені результати отриманих у 1988 р. оцінок зміни з роками числа домішок у основах біполярних транзисторів, необхідних для логічних операцій [8]. Можна вважати, що цей графік показує число електронів, необхідне для збереження одного біта інформації. Ситуація, яку ми маємо сьогодні, цілком задовільняє залежностям на графіку. Екстраполяція графіка означає, що впродовж наступних двох десятиріч ми змогли б проводити обчислення на атомних відстанях. Але виявляється, що на малих відстанях закони класичної фізики, на яких засновані класичні комп'ютери, не діють.

На рубіжі ХІХ—ХХ ст. виникла фізична теорія, що описала властивості частинок та їх рух у мікросвіті — квантова фізика (механіка). Одним з поштовхів до цього була неможливість з точки зору класичної фізики описати спектр випромінювання абсолютно чорного тіла в короткохвильовій частині спектра, так звана "ультрафіолетова катастрофа". Зусиллями Планка, Н. Бора, Э. Шредингера, В. Гейзенберга було створено математичний апарат квантової механіки та розв'язані основні задачі про квантовий опис руху об'єктів мікросвіту: електронів, атомів, молекул та інших частинок [11].

На квантовому рівні світ описується рівнянням Шредингера:

$$i\hbar \frac{\partial |\Psi\rangle}{\partial t} = \hat{H} |\Psi\rangle.$$

Оператор $\hat{H}$ лінійний:

$$\hat{H}(a|\Psi_1\rangle + b|\Psi_2\rangle) = a\hat{H}|\Psi_1\rangle + b\hat{H}|\Psi_2\rangle,$$

наслідком чого є квантовий принцип суперпозиції станів. Якщо квантова система може існувати в станах $|\Psi_1\rangle$ та $|\Psi_2\rangle$, то вона може так само "законно" існувати і в станах їх суперпозиції:

$$a|\Psi_1\rangle + b|\Psi_2\rangle = |\Psi\rangle,$$

де a, b — комплексні амплітуди, $|a|^2 + |b|^2 = 1$.

Квантові комп'ютери зможуть здолати багато обмежень, які мають звичайні комп'ютери. Вже зараз у побудові сучасних електронних систем ми оперуємо розмірами близько 500 атомних розмірів. Перепони на шляху поліпшення традиційних комп'ютерів будуть врешті-решт виникати з обмежень для класичної фізики на мініатюризацію (наприклад, тому що транзистори та електронні дроти неможливо зробити тоншими за розміри атома). Або вони можуть виникнути з практичних причин, що ймовірніше, тому що обладнання для виготовлення все більш потужних мікросхем буде ставати непомерно дорогим. Однак є всі підстави сподіватися, що квантові обчислення можуть вирішити обидві ці проблеми [5].

У чому ж полягають труднощі побудови класичної обчислювальної машини на таких малих відстанях? Одна з найбільш значних проблем мініатюризації звичайних комп'ютерів пов'язана з виділенням тепла.

Уже в 1961 р. Ландауер дослідив фізичні обмеження, що накладаються на обчислення дисипацією [9]. Неймовірно, але йому вдалося показати, що практично всі операції, що використовуються для обчислень, можуть бути проведені зворотним чином, тобто без дисипації тепла! Перша умова зворотності детермінованого пристрою полягає в тому, що вхідні та вихідні дані повинні єдиним чином відновлюватися одне з одного. Це називається логічною зворотністю. Якщо на додаток до логічної зворотності пристрій може реально діяти і у зворотному напрямку у часі, то він називається фізично зворотним, а другий закон термодинаміки гарантує, що він не розсіює тепло.

Праці з класичних зворотних обчислень заклали основи розвитку квантово-механічних комп'ютерів. На квантовому комп'ютері програми виконуються як унітарні еволюції вхідних даних, що описуються станом системи. Оскільки унітарні оператори U мають обернені та $U^\dagger = U^*$, то на квантовому комп'ютері обчислення завжди можна обернути.

Першою відмінністю квантових комп'ютерів від звичайних є спосіб кодування біта — фундаментальної одиниці інформації. У класичній цифровій обчислювальній машині стан біта може набувати тільки дискретних значень, що задаються однією цифрою 0 або 1. N -бітне бінарне слово в класичному комп'ютері відповідно описується послідовністю з n нулів та одиниць. Квантовий біт, що називається кубітом, міг би бути представлений атомом в одному з двох різних станів, що можна також позначати, як 0 або 1. Тоді два кубіта, так само як два класичних біта, мають чотири добре визначені стани (0 та 0, 0 та 1, 1 та 0, 1 та 1).

Принциповою відмінністю кубітів від класичних бітів є те, що перші можуть існувати одночасно в станах 0 та 1 з певною ймовірністю для кожного стану, заданою числовим коефіцієнтом, а не дискретно перебувати точно в 0 або точно в 1. Причому кожна ймовірність лише вказує на можливість знайти частинку в цьому стані (провівши спостереження), в той час як вона може перебувати в двох станах одночасно. Таким чином, трикубітний квантовий комп'ютер може з певним ступенем ймовірності перебувати у 8 станах одночасно. Взагалі n кубітів можуть перебувати у 2^n станах, що швидко стає множиною значних розмірів для великих значень n . Наприклад, якщо $n = 50$, тоді потрібно 10^{15} варіантів, щоб описати всі можливі стани квантової машини. Квантовий комп'ютер обіцяє безмежну потужність завдяки тому, що він може перебувати

у багатьох станах одночасно — явище, що називається суперпозицією, а також тому, що він може впливати на всі свої можливі стани одночасно.

Як уже було зазначено, в основі квантових обчислень лежить кубіт (квантовий біт) — квантова система, що, як і звичайний комп'ютерний біт, може мати два можливих стани, але на відміну від звичайного біта може перебувати у суперпозиції цих двох станів. Якщо біти можуть набувати лише два різних значення 0 та 1, кубіти не обмежені цими двома базисними станами, що позначаються $|0\rangle$ та $|1\rangle$, а можуть також існувати в таких станах, як $|0\rangle + |1\rangle$. Кубіт в цьому випадку не перебуває ані просто в стані $|0\rangle$ чи $|1\rangle$, ані в проміжному стані; скоріше кубіт перебуває в обох станах одночасно. Квантові логічні гейти $[]$ діють на кубіти так само, як класичні логічні операції діють на класичні біти, але квантові гейти також працюють з суперпозиціями і тому можуть виконувати багато операцій одночасно.

Одну з найпростіших квантових систем, в якій є два рівні, являє собою частинка зі спіном $\frac{1}{2}$. Її базисні стани, спін вниз $|\downarrow\rangle$ та спін вгору $|\uparrow\rangle$, можуть бути перевизначені для представлення двійкових нуля та одиниці, тобто відповідно $|\downarrow\rangle$ та $|1\rangle$. Хвильова функція $\psi = \alpha|0\rangle + \beta|1\rangle$ показує, що процесор перебуває в двох станах одночасно. Якщо буде проведено вимірювання, що виділяє певний стан, то він буде спостерігатись з відповідною ймовірністю. Відмітимо, що коефіцієнти α та β — комплексні. Квадрати модуля комплексних коефіцієнтів $|\alpha|^2$ та $|\beta|^2$ задають ймовірності знайти частинку у відповідних станах. Узагальнюючи це на набір з n частинок спіну $\frac{1}{2}$, отримуємо 2^n базисні стани (квантово-механічні вектори, що утворюють гільбертовий простір), які відповідають 2^n можливим послідовностям довжини n . Наприклад, $|19\rangle = |10011\rangle = |\uparrow\downarrow\downarrow\uparrow\uparrow\rangle$ — один з таких станів для $n = 5$.

Розмірність гільбертового простору зростає експоненційно зі збільшенням n .

Нині не існує процесорів, що добре описуються такою хвильовою функцією. Сучасні процесори повністю задовольняють умовам класичної фізики. Але якщо розміри бітів скоротяться до атомних розмірів, то квантовий опис стану бітів і динаміки процесора може виявитись дуже корисним.

Одним з прикладів, де квантовий комп'ютер дає результат кращий, ніж може дати будь-який алгоритм на класичному комп'ютері, є пошук певного запису у невпорядкованій базі даних, де такий елемент є унікальним. Якщо вважати за один крок вибір певного елемента бази даних та перевірку його на відповідність певному критерію, то найкращий алгоритм на класичному процесорі зробить

в середньому $O(N/2)$ кроків. У 1996 р. Гровер показав [4], що на квантовому процесорі це можливо зробити за $O(\sqrt{N})$ квантово-механічних кроків. Кожен квантово-механічний крок складається з елементарної унітарної операції.

Квантовий алгоритм пошуку починається з переведення системи у суперпозицію станів, що відповідають всім N елементам, серед яких проводиться пошук. Якщо одразу запрограмувати виведення правильного об'єкта, то він буде виведений з ймовірністю $1/N$, тому що тільки один з N об'єктів відповідає вимогам. Якщо замість цього провести серію квантових операцій, то врешті-решт шуканий елемент буде виведено з достатньо високим ступенем ймовірності. Прискорення отримується як за рахунок квантового паралелізму, так і внаслідок того, що ймовірність у квантовій теорії є квадратом амплітуди — алгоритм Гровера впливає на початковий стан, у якому всі N класичних записів представлені з амплітудою $1/\sqrt{N}$, і приводить початковий стан за $\sqrt{N}$ кроків до стану, де шуканий запис представлений з амплітудою порядку одиниці.

Щоб уявити квантовий паралелізм, розглянемо нескладний квантово-механічний експеримент, що описує це явище [6]. Нехай маємо дві щілини та джерело світла. Джерело випромінює фотони, електрони та інші частинки, що досягають пари щілин. Частинки проходять через унітарну еволюцію і врешті-решт ми бачимо інтерференційну картину. Ця картина має місце тільки тоді, коли обидві щілини відкриті, і зникає, коли одна з них зачинена. У певному розумінні частинки проходять крізь обидві щілини паралельно. Якщо б така унітарна еволюція була обчисленням або деякою операцією в рамках обчислення, то квантова система виконувала б обчислення паралельно. Тобто, іншими словами, ми отримали квантовий паралелізм “безкоштовно”. Результат, отриманий на виході цієї системи, є інтерференцією результатів паралельних обчислень.

Нагадаємо, що квантова система визначається певною амплітудою, а квадрат амплітуди є ймовірністю появи системи в певному стані. Усі квантові операції мають бути унітарними, тобто вони повинні бути жорсткими поворотами амплітуд вектора станів у N вимірному просторі станів. Елементарні квантові операції — квантова дифузія та квантові повороти. Саме з цих двох операцій і складається квантовий алгоритм пошуку.

Квантова дифузія подібна до класичної, окрім того факту, що амплітуда, яка переноситься з одного стану до іншого, уявна. Якщо амплітуди системи в двох станах рівні, то амплітуда, що переноситься в кожному напрямі, та ж сама і сумарний перенос дорівнює нулю. Однак, якщо амплітуда в

одному стані повернена відносно амплітуди в іншому стані, то маємо сумарний перенос від одного стану до іншого. Як результат цього переносу кут між двома станами зменшується.

Спочатку система приводиться у однорідну суперпозицію всіх станів, потім після приблизно $O(\sqrt{N})$ застосувань операцій квантової дифузії та фазових поворотів система концентрується на шуканому стані. Це досягається за рахунок паралелізму квантових обчислень.

Опишемо просту модель квантового комп'ютера [10], що ґрунтується на класичному комп'ютері, який навчає машину керувати набором спінів. У цієї моделі є деякі внутрішні обмеження, що роблять реалізацію алгоритмів за допомогою мови програмування високого рівня досить складною. Нехай на початку частинки зі спіном $1/2$ перебувають у деякому визначеному стані, наприклад, усіма спінами вниз. Класична машина бере окремі спіни або пари спінів та схрещує їх (застосовуючи елементарну однобітну операцію або XOR-гейт). Це повторюється з різними парами спінів згідно з вказівками звичайної комп'ютерної програми. Програма в цьому випадку може виглядати як набір вказівок щодо часу та напрямку випромінювання радіочастотних імпульсів. У цьому полягає відмінність квантових обчислень від класичних — у останніх біти інформації мігрують через набір логічних гейтів, а в першому випадку кубіти знаходяться на місці, нікуди не рухаючись, а гейти ніби “надходять” для проведення поточної операції. Коли цикл маніпуляцій завершено, орієнтації спінів вимірюються.

Найбільш суттєві труднощі при написанні коду високого рівня виникають через те, що квантова інформація керується звичайним комп'ютером абсолютно всліпу без будь-якого доступу до значень цієї квантової інформації. Це означає, що програма не може використовувати скорочення, обумовлені значеннями квантових змінних. Зокрема, число ітерацій циклу повинно бути сталим, передчасний вихід з нього неможливий. До того ж кожна команда, що виконується над квантовими бітами, повинна мати логічно обернену.

Створення квантового комп'ютера буде важким завданням. Річ у тому, що майже будь-яка взаємодія з зовнішнім середовищем (наприклад, зіткнення двох атомів) призведе до того, що суперпозиція квантово-механічних станів сколапсує до одного дуже добре визначеного стану — того, що детермінується спостерігачем. Це явище, відоме як декогерентність, робить наступні квантові обчислення неможливими. Тому внутрішня працююча частина квантового процесора повинна бути якоюсь відокремлена від оточуючого середовища, щоб підтримати когерентність. Але вона повинна бути та-

кож легкодоступна, щоб обчислення могли бути виконані, а результати виведені.

Після того, як мине час, що дорівнює часу декогерентизації квантових станів системи кубітів, обчислювальний процес, що контролюється, припиниться, еволюція квантового процесора набуде випадкового (дифузійного) характеру. Час декогерентизації, як правило, буде менший за час, необхідний для виконання складного алгоритму, який складається з великої кількості ($\sim 10^9$) елементарних операцій.

Виходом з цієї ситуації є застосування методів корекції помилок, які добре відомі з теорії класичних комп'ютерів, наприклад методи, що застосовуються при передачі даних через Internet. Спільне в них те, що логічні 0 та 1 кодується більшим числом бітів; аналіз кодових комбінацій дозволяє знайти та виправити помилку. Багато експертів було вражено, коли Шор зі співавторами показали, що те ж саме може бути зроблено квантово-механічним методом [7]. Вважалося, що квантове виправлення помилок вимагає вимірювання стану системи, а значить, порушення когерентності. Виявилося, що квантові помилки можуть бути виправлені всередині комп'ютера, без втручання приладів, що зчитують помилку. Аналогічні методи були розроблені і для квантових обчислень, де помилки можуть бути фазовими та амплітудними.

Виявилося, що коли ймовірність помилки при виконанні однієї елементарної операції нижче деякого порогового рівня, обчислення можуть проводитись як завгодно довго. Це означає, що операції квантової корекції помилок видаляють більше помилок, ніж вносять. Цей висновок досить важливий; по суті, він є теоремою про можливість побудови повномасштабного квантового комп'ютера.

Сьогодні квантові комп'ютери є справою не завтрашнього, а навіть післязавтрашнього дня. Так звані звичайні класичні комп'ютери навряд чи зникнуть з початком ери квантових обчислень. Зараз не існує алгоритмів, які б ефективно розв'язували більшість NP-повних та NP-важких задач на квантових комп'ютерах. Але все ж таки для деяких задач було знайдено такі алгоритми, за допомогою яких ці задачі розв'язуються на квантових комп'ютерах набагато швидше, ніж на звичайних. Прикладами таких алгоритмів служать алгоритм пошуку в неупорядкованій базі даних та алгоритм факторизації цілих чисел [7]. Останній розв'язує задачу розкладання числа на множники за поліноміальний час. Уже той факт, що завдяки квантовим обчисленням ми впритул наблизились до ефективного розв'язання NP-повних та NP-важких задач, гарантує прискіпливу увагу до цих технологій у майбутньому.

1. *Bazenco A., Bzun T. A., Schack R., Spiller T.* Effects of noise on quantum error correction algorithms *II Phys. Rev.*— 1977.— № 56— P. 1177—1188. <http://xxx.soton.ac.uk/ps/quant-ph/9612047>.
2. *Benioff P.* 1982. Quantum mechanical models of Turing machines that dissipate no energy *II Phys. Rev. Lett.* 48, 1581. <http://pks.bu.edu/qcl/pdf/benioffp19827563797d.pdf>.
3. *Bennett C. B., Bernstein E., Brassard G., Vazirani U.* 1997a. Strengths and weaknesses of quantum computing. <http://pks.bu.edu/qcl/pdf7bennettc19940807050c.pdf>.
4. *Grover L. K.* 1996. A fast quantum mechanical algorithm for database search. Proceedings, 28th ACM Symposium on Theory of Computation, 212.
5. *Gershenfeld N., Chuangl.* 1997. Bulk spin resonance quantum computation *II Science* 275, 350. <http://pks.bu.edu/qcl/pdf/gershenm1997017a7079.pdf>.
6. Encyclopedia of Applied Physics.— Update, WILEY—VCH, 1999.
7. *Shor P. W.* In Proc. 35th Annual Symposium on the Foundations of Computer Science. Ed. by Goldwasser S. *II IEEE Computer Society Press.*— Los Alamitos, California, 1994.— P. 124.
8. *Keyes R. W.* IBM//J. Res. Develop.— 1998.— Vol. 32.— № 24. <http://www.research.ibm.com/journal/rd/441/keyes.pdf>
9. *Landauer R.* The seminal paper in reversible computation *II IBM J. Res. Develop.*— 1961.— № 3.— P. 183.
10. *Shor P. W.*, presented at Quantum Computation 1994, Villa Gualino, Turin, Italy, October 1994, unpublished.
11. *Валиев К. А.* Квантовая информатика: компьютеры, связь и криптография // Вест. РАН.— 2000.— Т. 70.— № 8.— С. 688—695. <http://www.ibmh.msk.su/vivovoco/vv/journal/vran/qubit/qubit.htm>.

Boltenkov A. T., Vatolin D. O., Omeltchenko V. V.
OUTLOOK FOR THE DEVELOPMENT OF QUANTUM COMPUTATIONS

This paper covers the main aspects of quantum computations and computers — technologies that are being developed now with rapid speed. It considers the advantages over the classic computations and main difficulties on the way to realize quantum computers.