Ватолкін Д.П., Гусєва Ю. І.
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Київ, пр.Берестейський 37,
email: vatolkin.dmytro@lll.kpi.ua

ВИКОРИСТАННЯ КВАНТОВИХ ОБЧИСЛЕНЬ У НАУКОВИХ ДОСЛІДЖЕННЯХ

Анотація. *Представлено базову інформація щодо устрою квантового комп'ютера, його переваги та недоліки. Проаналізовано можливість використання квантових обчислень у наукових сферах та надано перелік Українських науковців, які присвячують свою діяльність дослідженням із теми квантових обчислень.*

Abstract. *Basic information about the quantum computer device and its advantages and disadvantages is presented. The possibility of using quantum computing in scientific fields is analyzed and a list of Ukrainian researchers who devote their activities to research on the topic of quantum computing is provided.*

Ключові слова: *квантовий комп'ютер, квантові технології, кубіт, квантові обчислення.*

Key words: *quantum computer, quantum technologies, qubit, quantum calculations.*

Одним із напрямів дослідження сучасної фізики є створення квантових технологій, які забезпечать проривні результати в багатьох сферах суспільного життя: від криптографії до моделювання масштабних систем, опису та передбачення перебігу надскладних процесів. Актуальність цих досліджень зросла в рази після присудження Нобелівської премії з фізики французу Сержу Арошу (Serge Haroche) і американцю Девіду Вайнленду (David Wineland) за розроблені ними новаторські експериментальні методики, які дали можливість вимірювати окремі квантові системи та маніпулювати ними («for ground-breaking experimental methods that enable measuring and manipulation of individual quantum systems»). [1]

Квантовим комп'ютером вважається обчислювальний пристрій, функціонування якого ґрунтується на принципах квантової механіки, зокрема, принципі суперпозиції та явищі квантової заплутаності [3].

Принципова відмінність квантового комп'ютера від класичного полягає у роботі з даними. Якщо класичний комп'ютер оперує даними записаними у бітах (кожен із яких зберігає одне з двох можливих значень), то квантовий комп'ютер оперує даними, що зберігаються у кубітах, де кожен із них одночасно знаходиться у суперпозиції між двома можливими значеннями.

Для позначення стану кубіта прийнято використовувати нотацію бракет, запропоновану Полем Діраком:

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle,$$

де Ψ - хвильова функція, 0 і 1 - можливі стани системи, α, β - вірогідності того, що система знаходиться в зазначеному стані (що є деяким спрощенням, адже фізично система знаходиться одночасно у двох станах, тобто у їх суперпозиції) [4].

Поки йдеться лише про один кубіт – його відмінність не є показовою. Адже будь-який алгоритм можна було б обчислити окремо для кожного із двох варіантів значень. Принциповою особливістю квантового комп'ютера є можливість подати на вхід алгоритму набір заплутаних кубітів, і тим самим обчислити алгоритм одночасно для всіх можливих початкових даних. Однак, ще однією відмінністю квантового комп'ютера є неможливість отримати відповідь у формі кубітів. При читанні значення із кубіта, він, із вірогідностями α, β (що задають його стан) перетворюється у біт 0 або 1. Тому, для того щоб отримати відповідь, доводиться запускати обчислення багато разів, і накопичувати статистику.

Типовим використанням квантового комп'ютера є виконання задач пошуку оптимального значення.

Приклад розшифровування криптографічного хешу є дуже показовим для демонстрації "квантової переваги". Алгоритм бере всі можливі значення паролю, проводить їх через алгоритм хешування, і перевіряє, чи співпав хоч один із них після цього із відомим хешем (котрий плануємо зламати). І якщо співпав, то замінює будь-який кубіт на зафіксоване значення (0 або 1), і повторює крок підбору. А якщо ні – повертається на крок назад і бере протилежне значення тому біту). Таким способом за лінійну швидкість обчислень зламається криптографічний хеш, хоча вся ідея криптографічних хешів полягає в тому що їх практично неможливо обрахувати у зворотньому напрямку.

Важливо підкреслити, що криптографи знають про таку можливу загрозу для безпеки і визначили принципові недоліки квантових комп'ютерів. Враховуючи недоліки, дослідники переробили алгоритми так, щоб ні сучасні ні квантові комп'ютери майбутнього не могли легко зашкодити безпеці. Тому зазначений варіант використання квантового комп'ютера вже не є доцільним на практиці.

З’ясуємо питання доцільності використання квантових комп'ютерів у науковій сфері.

Класичні алгоритми квантового комп’ютера дозволяють здійснювати пошук оптимальних значень можуть бути дуже корисними для фізичних симуляцій. Особливо корисними вони стають, якщо всередині фізичної симуляції є об’єкти із квантовою суперпозицією. Їх дуже легко розраховувати, якщо за стан такого об’єкту буде відповідати окремий кубіт із відповідним квантовим станом.

Так класичним прикладом розрахунків оптимальних параметрів квантової системи на квантовому комп’ютері є пошук стабільних квантових рівнів системи. Це може використовуватись наприклад для розрахунку хімічних характеристик ще не синтезованих молекул.

Нажаль більш складні фізичні симуляції ще залишаються недоступними науковцям, адже відмінною характеристикою квантового комп’ютера є:

- обмеженість у кількості кубітів, що може використовуватись (на противагу величезної кількості оперативної пам’яті у сучасних комп’ютерах).
- обмеженість у часі розрахунків, адже стан суперпозиції для кубіта не може зберігатися впродовж довгого часу.
- обмеженість у точності розрахунків. Спонтанне спотворення суперпозиції кубіта призводить до невірних відповідей. Частково це вирішується об’єднанням групи фізичних кубітів у 1 логічний кубіт, та багаторазовим повторенням обчислень.

Також треба зазначити, що квантові комп’ютери є надзвичайно дефіцитним і коштовним обладнанням, вимогливим до систем кріо-охолодження (до температур 20 мК). Все це у сукупності, нажаль, робить квантові комп’ютери недоступними для українських науковців. Проте міжнародна співпраця і робота із квантовими комп’ютерами через мережу інтернет дозволяє проводити відповідні дослідження.

Наведемо неповний список наукових центрів в Україні [2], що активно займаються дослідженнями квантових обчислень:

- Фізико-технічний інститут низьких температур ім. Б.І. Вєркіна АН України — Л.А. Пастур, О.М. Омельянчук, С.М. Шевченко та ін. вивчають твердотільні кубіти, заплутані стани;
- Інститут фізики НАН України — Л.П. Яценко, А.М. Негрійко, А.А. Чумак та ін. займаються динамікою квантових систем, квантовими логічними операціями, квантовою метрологією;
- Інститут теоретичної фізики ім. М.М. Боголюбова НАН України — група А.О. Семенова працює в галузі квантових комунікацій, неуніверсальних квантових обчислень, квантової оптики;
- Київський національний університет імені Тараса Шевченка — І.П. Пінкевич, І.М. Дмитрук створили освітньо-наукову програму «Квантові комп'ютери, обчислення та інформація»;
- Київський академічний університет — під керівництвом О.А. Кордюка започатковано Центр квантових матеріалів та технологій, у якому вивчають надпровідникові матеріали для реалізації кубітів і готують висококваліфіковані кадри;
- Інститут математики НАН України — В.Л. Островський, Ю.С. Самойленко, Д.Ю. Якименко та ін. створюють алгебраїчні структури для квантових протоколів;
- Львівський національний університет імені Івана Франка — група В.М. Ткачука займається симуляціями на квантовому комп'ютері; в університеті діє освітньо-наукова програма «Квантові комп'ютери та квантове програмування».

Отже тезисно сформулюємо висновки:

- Квантові комп'ютери, в силу своєї унікальної будови можуть бути оціненими у створенні комп'ютерних симуляцій фізичних систем.
- Наразі технічні характеристики таких комп'ютерів є незначними, а їх вартість високою для безпосереднього практичного використання.
- Дослідження можливостей квантових комп'ютерів активно проводяться в Україні, навіть за фізичної відсутності самих квантових комп'ютерів.

ЛІТЕРАТУРА

[1] Нобелівська премія — 2012 // Вісн. НАН України. — 2012. — № 12. — С. 89-95.
[2] Шевченко, С. М. (2022). Квантовий комп’ютер: стан проблеми у світі та в Україні: Стенограма доповіді на засіданні Президії НАН України 8 грудня 2021 року. Вісник НАН України, (2), 35–43. https://doi.org/10.15407/visn2022.02.035
[3] Quantum computers / T. D. Ladd et al. Nature. 2010. Vol. 464, no. 7285. P. 45–53. Режим доступу: https://doi.org/10.1038/nature08812.
[4] Quantum computing: A taxonomy, systematic review and future directions / S. S. Gill et al. Software: Practice and Experience. 2021. Vol. 52, no. 1. P. 66–114. Режим доступу: https://doi.org/10.1002/spe.3039