Issue 17, 2025

https://doi.org/10.23939/sisn2025.17.248

УДК 004.94:530.145

АНАЛІЗ МАТЕМАТИЧНИХ МОДЕЛЕЙ КВАНТОВОГО ПАРАЛЕЛІЗМУ

Петро Кравець
Національний університет „Львівська політехніка”,
кафедра інформаційних систем та мереж, Львів, Україна
E-mail: Petro.O.Kravets@lpnu.ua, ORCID: 0000-0001-8569-423X

У цій статті виконано аналіз математичних моделей квантового паралелізму, основаного на переведенні квантової системи у стан суперпозиції. Обґрунтовано принципи квантового паралелізму та його математичні засади. Для демонстрації квантової переваги проаналізовано математичні моделі фундаментальних квантових алгоритмів Дойча-Йожи та Гровера, які ілюструють ефективність квантових обчислень у порівнянні з класичними методами.

Розглянуто алгоритм Дойча-Йожи, який узагальнює задачу визначення виду бінарної функції, розширюючи її на множину аргументів, записаних у квантовому регістрі. Цей алгоритм дозволяє визначити, чи є функція постійною або збалансованою за один квантовий виклик, тоді як у класичних обчисленнях для цього потрібен експоненційний час. Відзначено, що хоча алгоритм Дойча-Йожи демонструє можливості паралельних квантових обчислень, проте має переважно теоретичне значення.

Алгоритм Гровера реалізує квантові паралельні обчислення для практичної задачі пошуку елемента у невпорядкованій базі даних. Він заснований на ітераційному підсиленні амплітуди стану, що відповідає шуканому елементу, та забезпечує квадратичне прискорення порівняно з класичними алгоритмами. Крім пошуку в базі даних, алгоритм Гровера може бути адаптований для розв’язання інших задач оптимізації.

Роботу розглянутих алгоритмів проілюстровано числовими прикладами, що спрощує розуміння їхніх принципів та сприяє подальшому методологічному розвитку паралельних квантових обчислень.

У статті також окреслено переваги квантового паралелізму над класичними обчисленнями та визначено перспективи застосування паралельних квантових алгоритмів.

Ключові слова – квантова система, суперпозиція станів, вимірювання квантових станів, унітарний оператор, алгоритм Дойча-Йожи, алгоритм Гровера.

Постановка проблеми

Розвиток квантових обчислень є одним із найперспективніших напрямів сучасної науки та технологій, оскільки квантові комп’ютери здатні розв’язувати задачі, які є обчислювально складними або навіть недоступними для класичних комп’ютерів. Однією з ключових концепцій, що забезпечує перевагу квантових обчислень, є квантовий паралелізм. Завдяки принципу суперпозиції квантові системи можуть одночасно опрацьовувати множину станів, що суттєво розширює їх обчислювальні можливості у порівнянні з традиційними алгоритмами.

Актуальність математичного моделювання та аналізу квантового паралелізму зумовлена як теоретичними, так і практичними чинниками. З теоретичної точки зору, формалізація квантових алгоритмів та їх математичних моделей є необхідною для розуміння принципів роботи квантових комп’ютерів, оцінки їхньої ефективності та визначення обмежень їх застосування. Одним із перших фундаментальних алгоритмів, що демонструє можливості квантового паралелізму, є алгоритм Дойча,

який дозволяє встановити тип бінарної функції за один квантовий виклик, тоді як класичні алгоритми потребують двох викликів. Узагальнення цього алгоритму в алгоритмі Дойча-Йожи демонструє ще більшу ефективність квантових обчислень у порівнянні з класичними підходами.

З практичної точки зору, математичне моделювання квантового паралелізму є основою для розробки квантових алгоритмів, які можуть знайти застосування в оптимізаційних задачах, криптографії, моделюванні складних фізичних та хімічних процесів, а також у машинному навчанні. Наприклад, алгоритм Гровера, який використовує квантовий паралелізм та принципи квантової інтерференції, дозволяє виконувати пошук у невпорядкованій базі даних із квадратичним прискоренням у порівнянні з класичними методами. Це відкриває перспективи для ефективного розв'язання широкого класу задач у сфері інформаційних технологій, кібербезпеки та логістики.

Окремо варто зазначити, що стрімкий розвиток квантових процесорів та апаратного забезпечення підсилює потребу в математичних дослідженнях, які дозволяють оцінити ефективність квантових обчислень, формалізувати основні принципи роботи квантових алгоритмів та визначити шляхи їх подальшого вдосконалення. Сучасні квантові комп'ютери вже демонструють експериментальні результати, що підтверджують їхню перевагу над класичними методами в певних обчислювальних задачах. Це робить дослідження квантового паралелізму особливо актуальним для подальшого розвитку квантових технологій та їхнього практичного впровадження.

Отже, математичне моделювання та аналіз квантового паралелізму є важливим напрямом досліджень, який сприяє поглибленню розуміння фундаментальних принципів квантових обчислень, розробленню ефективних алгоритмів та оцінюванню їхнього потенціалу у реальних застосуваннях. Таке дослідження є не лише теоретично значущим, але й має прикладне значення, оскільки формує наукову основу для подальшого розвитку квантових технологій, які у майбутньому можуть кардинально змінити підходи до обчислень у різних сферах науки і техніки.

Аналіз останніх досліджень та публікацій

Розвиток математичних моделей квантового паралелізму має глибокі теоретичні основи, що сформувалися внаслідок багаторічних досліджень у сфері квантової механіки, квантової інформатики та алгоритмічного аналізу. У цьому огляді розглядається хронологія розвитку концепції квантового паралелізму, внески провідних науковців у формування математичних моделей квантових обчислень та перспективи подальших досліджень.

Поняття квантового паралелізму бере свій початок із засад квантової механіки, розроблених у першій половині XX століття. Основоположні роботи Е. Шредінгера (Schrödinger, 1926) та П. Дірака (Dirak, 1930) заклали фундамент квантової теорії станів та принципу суперпозиції, який є ключовим для квантового паралелізму. Саме принцип суперпозиції дозволяє квантовій системі одночасно перебувати в експоненційно великій кількості станів, що і забезпечує потенційну перевагу квантових обчислень над класичними.

Концепцію квантових обчислень вперше запропонував Р. Фейнман (Feynman, 1982), висловивши гіпотезу, що квантові системи можна ефективніше моделювати за допомогою квантових пристроїв, ніж класичних комп'ютерів. Подальший розвиток цієї ідеї здійснив Д. Дойч, який запропонував перший квантовий алгоритм – алгоритм Дойча (Deutsch, 1985). Цей алгоритм продемонстрував можливість одночасного обчислення значень функції для двох вхідних двійкових значень усього за один квантовий виклик, що неможливо у класичній схемі обчислень. Пізніше Д. Дойч разом з Р. Йожою узагальнили цей алгоритм (алгоритм Дойча-Йожи), який ще виразніше ілюстрував квантовий паралелізм і його переваги (Deutsch, & Jozsa, 1992).

Згодом П. Шор (Shor, 1994) запропонував алгоритм факторизації цілих чисел на квантовому комп'ютері, який використовує квантовий паралелізм та квантове перетворення Фур'є. Це стало значним проривом, оскільки алгоритм Шора здатний розв'язувати задачу факторизації експоненційно швидше, ніж найкращі класичні алгоритми, що має фундаментальне значення для криптографії та криптоаналізу.

Подальші дослідження привели до появи алгоритму Гровера, побудованому на основі методу амплітудного підсилення (Grover, 1996, 1997). Цей алгоритм дозволяє значно прискорити процес пошуку елементів у невпорядкованих базах даних, даючи квадратичне прискорення порівняно з класичними методами пошуку. Алгоритм Гровера є прикладом використання квантової інтерференції, що разом із суперпозицією є ключовим механізмом квантового паралелізму (Kozhukhivskyi, Gaidur, & Kozhukhivska, 2022).

У наступні десятиліття науковці зосередилися на формалізації математичних моделей квантових обчислень. У 2000-х роках основний тренд дослідження полягав у моделюванні квантових схем, оптимізації квантових алгоритмів та оцінці їхньої складності. Зокрема, роботи М. Нільсена та І. Чуанга (Nielsen, & Chuang, 2000) сформували стандартний підхід до квантових обчислень та їх математичного моделювання. Вони систематизували основи квантової теорії обчислень, що сприяло розвитку квантових алгоритмів і теоретичних моделей у галузі квантових обчислень. Ця робота стала однією з ключових у цій сфері і заклала основи для подальших досліджень та практичних розробок.

Дослідження, проведені у 2010-х роках, зосереджувалися на розробленні алгоритмів для квантових процесорів та застосуванні квантового паралелізму у машинному навчанні та оптимізаційних задачах. Так, у 2018 році компанія Google представила експериментальні результати, які підтверджують квантову перевагу, а саме виконання певних обчислень швидше, ніж це можливо на найпотужніших класичних суперкомп'ютерах (Arute et al., 2019).

Сучасні дослідження у сфері математичного моделювання квантового паралелізму зосереджені на таких напрямках, як дослідження топології квантових схем та розроблення нових методів оптимізації квантових алгоритмів; застосування квантових обчислень для моделювання фізичних систем, хімічних процесів та задач оптимізації; дослідження нових методів, що використовують квантовий паралелізм для покращення нейромережевих моделей; створення більш стійких квантових процесорів, здатних виконувати складні квантові алгоритми у стабільному середовищі. Один з основних напрямків майбутніх досліджень полягає в удосконаленні існуючих квантових алгоритмів для максимального використання квантового паралелізму. Наприклад, алгоритм Гровера, що демонструє квадратичне прискорення пошуку в невпорядкованих базах даних, може бути модифікований для ефективнішого використання ресурсів квантових процесорів. Існує також потреба в розробці нових варіантів квантових алгоритмів для вирішення практичних задач, таких як оптимізація функцій, машинне навчання та моделювання складних фізичних систем. Проблеми, що потребують уваги, включають питання стиснення кількості квантових операцій та зменшення кількості квантових бітів (кубітів) для забезпечення ефективності алгоритмів при обмежених ресурсах (Bodnarchuk, Zybin, & Vasilyuk-Zaytseva, 2024; Tomamichel, 2015).

Алгоритми квантової оптимізації використовують переваги квантових обчислень для швидшого розв'язання складних оптимізаційних задач, які є важкими для класичних комп'ютерів. Вони особливо корисні для задач у логістиці, фінансах, машинному навчанні та матеріалознавстві. До них належать алгоритм квантового відпалу, який використовується для розв'язання комбінаторних оптимізаційних задач і добре підходить для розв'язання NP-складних задач, таких як проблема комівояжера (Kadowaki, & Nishimori, 1998). Варіаційний квантовий алгоритм оптимізації (VQE – Variational Quantum Eigensolver), що поєднує класичні та квантові обчислення і використовується в квантовій хімії та матеріалознавстві (Peruzzo et al., 2014). Гібридний алгоритм квантової апроксимації (QAOA – Quantum Approximate Optimization Algorithm), що використовується для наближених розв'язків комбінаторних задач оптимізації і може застосовуватися у фінансових розрахунках, логістиці та аналізі графів (Farhi, Goldstone, & Gutmann, 2014). Квантове стохастичне моделювання для оптимізації стохастичних процесів, наприклад, фінансових ризиків (Matsakos, & Nield, 2024). Квантова оптимізація методом градієнтного спуску, що використовується для оптимізації параметрів моделей машинного навчання і дає можливість значного прискорення навчання нейронних мереж (Gaikwad, Torres, Ahmed, & Kockum, 2025).

Іншим важливим напрямком є розроблення більш складних математичних моделей для опису квантових систем, які б враховували всі аспекти квантового паралелізму, зокрема квантову інтерференцію та суперпозицію. У цьому контексті актуальними є роботи по моделюванню великих

систем кубітів, зокрема застосування методів квантової симуляції, які дозволяють вивчати поведінку фізичних систем, таких як молекули чи матеріали, з точністю, що недоступна класичним методам. Розроблення квантових симуляторів, наприклад, для моделювання простих молекулярних систем, є перспективним напрямком розвитку квантового паралелізму (Lloyd, 1996; Motta, 2022). Це дає змогу застосовувати квантовий паралелізм для розв'язування задач у хімії та фізиці, що має важливе значення для створення нових матеріалів та оптимізації хімічних реакцій.

Один із провідних напрямків розвитку квантових алгоритмів полягає в їх адаптації для вирішення практичних задач, таких як машинне навчання та штучний інтелект. Квантові алгоритми можуть забезпечити значне прискорення деяких процесів, зокрема, в таких завданнях, як класифікація даних, оптимізація та пошук у великих масивах інформації (Biamonte et al., 2017; Ramezani, Sommers, Manchukonda, Rahimi, & Amirlatifi, 2020).

У роботах (Beer, 2022; Pang, Li, & Wang, 2025) проаналізовано потенціал квантових алгоритмів для навчання нейронних мереж. Інші дослідження, такі як роботи (Gircha et al., 2023; Wu et al., 2025), спрямовані на створення гібридних квантово-класичних алгоритмів, що можуть значно покращити ефективність моделей глибинного навчання.

Існують також значні технічні виклики, пов'язані з практичним застосуванням квантового паралелізму. Оскільки квантові комп'ютери ще знаходяться на етапі раннього розроблення, питання корекції помилок та стабільності кубітів є ключовими для забезпечення їх ефективності на практиці. Вдосконалення квантових процесорів і квантових алгоритмів для стабільної роботи в реальних умовах вимагатиме вирішення численних проблем, зокрема, з контролем над декогерентністю кубітів та управлінням їх взаємодією (Shor, 1995; Zurek, 2003).

Дослідження, проведені Л. Гровером, який розробив алгоритм для пошуку в базах даних, та П. Шором, який створив алгоритм для факторизації чисел, показали теоретичні можливості значних переваг квантових обчислень. Проте існує необхідність в розробленні алгоритмів, здатних не тільки оптимізувати обчислення, а й знижувати імовірність помилок у процесі виконання. Одним з напрямків є роботи, що вивчають питання квантової декогерентності, створення стійких до помилок алгоритмів та корекції квантових помилок, що дозволяє значно підвищити стабільність квантових обчислень (Reichardt, & Grover, 2005; Wang, & Tang, 2024; Google Quantum AI and Collaborators, 2025).

Окремим важливим напрямком є розвиток квантових алгоритмів у сфері криптографії, зокрема, квантового шифрування та квантових цифрових підписів. Алгоритми на основі квантового паралелізму здатні зламувати традиційні криптографічні системи, такі як протоколи RSA та ECC, що зумовлює необхідність розроблення нових методів захисту на основі квантових алгоритмів. Принципи, проблеми та перспективи квантової криптографії окреслено у роботах (Kalyuzhny, 2015; Kosobutsky, 2022). Дослідження використання квантових методів для створення квантової криптографії та захисту інформації від потенційних загроз з боку квантових комп'ютерів розглянуто в (Easttom, 2022). Окремі роботи вказують на можливості комбінування класичних та квантових методів шифрування для забезпечення безпеки в нову еру квантових технологій (Ricci, Dobias, Malina, Hajny, & Jedlicka, 2024).

Математичне моделювання та аналіз квантового паралелізму відкривають величезні перспективи для розвитку обчислювальної техніки, що може призвести до значних досягнень у різних галузях – від фізики до криптографії та штучного інтелекту. Розвиток квантових обчислень і математичних моделей квантового паралелізму перебуває на передовій позиції наукових досліджень, відкриваючи нові можливості для вирішення складних задач, недоступних для класичних комп'ютерів. Однак, попри численні успіхи, існує низка важливих напрямків, які потребують подальшого вивчення та розвитку. Дослідження квантового паралелізму активно тривають у таких ключових напрямах, як удосконалення квантових алгоритмів, розроблення нових теоретичних моделей, а також вирішення технічних проблем, пов'язаних із квантовими процесорами.

Значний інтерес до проблем квантової механіки, квантової інформатики та квантових обчислень спостерігається також в навчально-освітній сфері. Квантові обчислення стали важливою складовою університетських курсів, що дозволяє готувати кваліфікованих фахівців та науковців у

галузі квантової механіки (Yukhnovsky, 2002; Tkachuk, 2011; Vakarchuk, 2012) та квантової інформатики (Karlash, 2018; Krokhmalskyi, 2018; Ostapov, & Dobrovolskyi, 2021). Перед ними стоїть завдання довести квантові комп'ютери до рівня практичного застосування, аналогічно з класичними обчислювальними системами. Для цього науковці та інженери працюють над створенням ефективніших квантових алгоритмів, удосконаленням квантових процесорів, розроблення методів корекції помилок і боротьби з декогерентністю. Важливим напрямом є інтеграція квантових і класичних обчислень для прикладних задач у криптографії, моделюванні матеріалів, фінансах та машинному навчанні. Розвиток цих технологій наближає квантові обчислення до широкого використання в науці та промисловості.

Отже, математичне моделювання квантового паралелізму залишається одним із ключових напрямів досліджень у квантовій інформатиці. Попри значний прогрес, актуальними залишаються питання оптимального використання квантового паралелізму та його адаптації до практичних обчислювальних задач. Це зумовлює подальші наукові дослідження, спрямовані на підвищення ефективності квантових алгоритмів і розширення їхніх застосувань.

Формулювання цілі статті

Метою цієї роботи є аналіз математичних моделей квантового паралелізму для ілюстрації квантової переваги над класичними методами обчислень.

Досягнення мети забезпечується вирішенням таких задач: 1) дослідити принципи квантового паралелізму та провести його математичне обґрунтування; 2) проаналізувати математичні моделі фундаментальних квантових обчислень, зокрема алгоритмів Дойча-Йожи та Гровера; 3) формалізувати математичний опис алгоритму Дойча-Йожи, що визначає вид бінарної функції; 4) описати принцип роботи алгоритму Гровера для пошуку в невпорядкованих структурах даних та оцінити його ефективність; 5) продемонструвати квантову перевагу шляхом порівняння квантових алгоритмів із класичними методами обчислень; 6) проілюструвати роботу квантових алгоритмів числовими прикладами для полегшення розуміння їхньої суті; 7) окреслити перспективи застосування квантового паралелізму та сучасні досягнення в розробці квантових комп'ютерів.

Виклад основного матеріалу

Математичне формулювання квантового паралелізму

Квантові паралельні обчислення основані на принципах квантової механіки, таких як суперпозиція, заплутаність і квантові оператори**.** Паралельність виконання квантових операцій полягає у можливості їх одночасного виконання над усіма можливими станами кубітів, що значно прискорює розрахунки порівняно з класичними обчисленнями.

На відміну від класичних обчислень, де кожен стан опрацьовується послідовно, квантові алгоритми працюють з усіма станами одночасно. Основними інструментами для цього є застосування унітарних операторів до суперпозиції.

Суперпозиція одного кубіта описується лінійною комбінацією базисних станів $|0\rangle$ та $|1\rangle$:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \tag{1}$$

де α, β – комплексні амплітуди імовірностей з умовою нормування: $|\alpha|^2 + |\beta|^2 = 1$.

Якщо система містить n кубітів, її загальний стан описується як:

$$|\Psi\rangle = \sum_{x=0}^{2^n-1} \alpha_x |x\rangle, \tag{2}$$

де $\sum_{x=0}^{n-1} |\alpha_x|^2 = 1$.

Наприклад, суперпозиція трьох кубітів буде складатися з $2^3 = 8$ станів:

$$|\Psi\rangle = \alpha_0|000\rangle + \alpha_1|001\rangle + \alpha_2|010\rangle + \alpha_3|011\rangle + \alpha_4|100\rangle + \alpha_5|101\rangle + \alpha_6|110\rangle + \alpha_7|111\rangle. \quad (3)$$

Це означає, що квантовий комп'ютер з регістром із n кубітів може опрацьовувати всі 2^n можливих вхідних станів одночасно, що визначає суть квантового паралелізму.

Нехай існує квантова схема $U_f\left(|x,y\rangle\right) = |x, y \oplus f(x)\rangle$, яка реалізує обчислення деякої бінарної функції $f(x)$. Тут $\oplus$ позначає операцію "сума за модулем 2". Щоб обчислити $f(x)$ на вхід необхідно подати значення $|x,0\rangle$:

$$U_f\left(|x,0\rangle\right) = |x, 0 \oplus f(x)\rangle = |x, f(x)\rangle. \quad (4)$$

Значення x можна задати в n-кубітному квантовому регістрі $\left(|x_0\rangle, |x_1\rangle, ..., |x_{n-1}\rangle, \right)$. Нехай початково $x_i = 0$ ($i = 0..(n-1)$). Якщо тепер до цього регістра застосувати оператор Адамара, то його кубіти перейдуть у стан суперпозиції. У цьому стані квантовий регістр одномоментно буде містити усі можливі значення n-розрядного цілого числа без знаку:

$$|\Psi\rangle = \frac{1}{\sqrt{2^n}}\left(|00...0\rangle + |00...1\rangle + ... + |11...1\rangle\right) = \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle. \quad (5)$$

Далі цей регістр разом з $y = 0$ подається на вхід квантової схеми U_f. Після застосування U_f отримаємо:

$$U_f\left(|\Psi\rangle, 0\right) = U_f\left(\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x,0\rangle\right) = \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}U_f|x,0\rangle = \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x, f(x)\rangle. \quad (6)$$

Це означає, що одночасно буде обчислено значення функції $f(x)$ для всіх x.

Однак, існує проблема їх вимірювання, адже це виведе систему зі стану суперпозиції і буде отримано тільки якесь одне значення функції. На сьогодні розроблено цілий клас квантових перетворень, які збільшують імовірність отримання потрібного результату на основі квантового паралелізму. Квантові алгоритми можуть маніпулювати станами перед вимірюванням, щоб отримати потрібну інформацію. Квантова томографія, інтерференція, амплітудна ампліфікація та квантове перетворення Фур'є дозволяють отримати інформацію про функцію, не вимагаючи прямого вимірювання всіх значень одночасно.

Алгоритм Дойча-Йожи

Алгоритм Дойча-Йожи є узагальнення алгоритму Дойча для бінарної функції $f: \{0,1\}^n \to \{0,1\}$. Алгоритм Дойча-Йожи є одним із перших квантових алгоритмів, який продемонстрував перевагу квантових обчислень над класичними та є одним із найпростіших прикладів використання квантового паралелізму. Він дозволяє визначити, чи функція $f(x)$ є постійною або збалансованою за один квантовий виклик, замість експоненційного значення у класичних обчисленнях. Нехай маємо функцію $f: \{0,1\}^n \to \{0,1\}$, яка приймає n-бітний вхід та повертає 0 або 1. Відомо, що $f(x)$ може бути або константною (повертає одне і те ж значення для всіх x), або збалансованою (повертає 0 рівно для половини значень x і 1 – для іншої половини).

Необхідно визначити, чи є $f(x)$ константною або збалансованою. У найгіршому випадку, щоб впевнено визначити вид функції, класичний алгоритм повинен обчислити $f(x)$ для $2^{n-1}+1$ різних входів. Алгоритм Дойча-Йожи використовує квантові суперпозиції та перетворення Адамара, що дозволяє визначити вид функції лише за один квантовий виклик. Для цього необхідно виконати такі кроки алгоритму.

1. Підготовка стану.

Необхідно підготувати квантовий регістр з такими значеннями:

$$|0\rangle^{\otimes n} \otimes |1\rangle, \tag{7}$$

де перші n кубітів – це нульові аргументи x функції $f(x)$, а останній допоміжний кубіт містить значення 1 і використовується для обчислення $f(x)$.

2. Перше перетворення Адамара.

Застосовуємо оператор Адамара $H^{\otimes(n+1)}$ до всіх кубітів:

$$H^{\otimes(n+1)}|0\rangle^{\otimes n} \otimes |1\rangle. \tag{8}$$

Це переводить стан у рівномірну суперпозицію:

$$|\psi\rangle = \frac{1}{\sqrt{2}} \sum_{x=0}^{2^n-1} |x\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}. \tag{9}$$

ДЕ $H|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$ – суперпозиція допоміжного кубіта.

3. Дія оракула.

Застосуємо оператор оракула до кожного базисного стану:

$$U_f\left(|x\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}\right). \tag{10}$$

Використаємо визначення оператора U_f:

$$U_f\left(|x, y\rangle\right) = |x, y \oplus f(x)\rangle. \tag{11}$$

Поширимо це перетворення на суперпозицію станів кубітів, замінивши другий кубіт $|y\rangle$ на $|y \oplus f(x)\rangle$:

$$\frac{1}{\sqrt{2}}\left(|x\rangle \otimes |0\rangle - |x\rangle \otimes |1\rangle\right) = \frac{1}{\sqrt{2}}\left(|x\rangle|0 \oplus f(x)\rangle - |x\rangle|1 \oplus f(x)\rangle\right). \tag{12}$$

Оскільки $0 \oplus f(x) = f(x)$, а $1 \oplus f(x) = 1 - f(x)$, отримуємо:

$$\frac{1}{\sqrt{2}}\left(|x\rangle|0 \oplus f(x)\rangle - |x\rangle|1 \oplus f(x)\rangle\right) = \frac{1}{\sqrt{2}}\left(|x\rangle|f(x)\rangle - |x\rangle|1 - f(x)\rangle\right). \tag{13}$$

Якщо $f(x) = 0$, то вираз $\frac{1}{\sqrt{2}}\left(|x\rangle|f(x)\rangle - |x\rangle|1 - f(x)\rangle\right) = |x\rangle\frac{|0\rangle - |1\rangle}{\sqrt{2}}$, а якщо $f(x) = 1$, то він стає $\frac{1}{\sqrt{2}}\left(|x\rangle|f(x)\rangle - |x\rangle|1 - f(x)\rangle\right) = |x\rangle\frac{|1\rangle - |0\rangle}{\sqrt{2}} = |x\rangle\left(-\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$, що просто додає фазовий множник.

Тобто отримуємо:

$$\frac{1}{\sqrt{2}}\left(|x\rangle|f(x)\rangle - |x\rangle|1 - f(x)\rangle\right) = (-1)^{f(x)}|x\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}. \tag{14}$$

Оскільки це відбувається для кожного x, то після застосування дії оракула отримуємо загальний стан:

$$|\psi'\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |x\rangle \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}. \tag{15}$$

Помічаємо, що що допоміжний кубіт залишився у тому ж самому стані, що й перед застосуванням оракула:

$$\frac{|0\rangle - |1\rangle}{\sqrt{2}}. \tag{16}$$

Це означає, що він не містить нової інформації про $f(x)$. Уся інформація про $f(x)$ тепер закодована у фазах основного регістра $|x\rangle$, оскільки його коефіцієнти набули множника $(-1)^{f(x)}$.

Оскільки останній кубіт залишається у фіксованому стані, він є незалежним від основного регістра, і його можна ігнорувати при подальшому опрацюванні. При вимірюванні основного регістра він не впливатиме на результат.

4. Друге перетворення Адамара.

Отже, після проходження оракула, стан системи виглядає так:

$$|\psi'_{\otimes n}\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |x\rangle. \tag{17}$$

Тепер повторно застосовуємо оператор Адамара $H^{\otimes n}$ до цього стану.
Оператор Адамара для одного кубіта діє так:

$$H|x\rangle = \frac{1}{\sqrt{2}} \sum_{z=0}^{1} (-1)^{x \cdot z} |z\rangle. \tag{18}$$

Для n кубітів цей оператор записується у вигляді:

$$H^{\otimes n}|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{z=0}^{2^n-1} (-1)^{x \cdot z} |z\rangle. \tag{19}$$

Тут $x \cdot z$ – це скалярний добуток двійкових представлень чисел x та z.

Застосуємо $H^{\otimes n}$ до суперпозиції:

$$H^{\otimes n} \frac{1}{\sqrt{2^n}} \sum_{z=0}^{2^n-1} (-1)^{f(x)} |x\rangle = \frac{1}{\sqrt{2^n}} \sum_{z=0}^{2^n-1} (-1)^{f(x)} \left(\frac{1}{\sqrt{2^n}} \sum_{z=0}^{2^n-1} (-1)^{x \cdot z} |z\rangle \right) = \frac{1}{2^n} \sum_{z=0}^{2^n-1} (-1)^{f(x)} \left(\sum_{z=0}^{2^n-1} (-1)^{x \cdot z} |z\rangle \right). \tag{20}$$

Змінивши порядок підсумовування, отримаємо:

$$|\psi''_{\otimes n}\rangle = \frac{1}{2^n} \sum_{z=0}^{2^n-1} \left(\sum_{x=0}^{2^n-1} (-1)^{f(x)+x \cdot z} \right) |z\rangle. \tag{21}$$

Перейдемо до аналізу амплітудних коефіцієнтів стану суперпозиції $|\psi''_{\otimes n}\rangle$.

5. Для $z = 0$ отримаємо n-кубітний стан $|0\rangle^{\otimes n}$:

$$\frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{f(x)}. \tag{22}$$

Ця сума складається з усіх значень функції $f(x)$.

Якщо $f(x)$ константна, то всі $(-1)^{f(x)}$ однакові, тобто вони всі або дорівнюють $(-1)^0 = 1$, або $(-1)^1 = -1$. У такому випадку підсумовуємо 2^n однакових значень:

$$\frac{1}{2^n}(\pm 2^n) = \pm 1. \tag{23}$$

Це означає, що коефіцієнт перед $|0\rangle^{\otimes n}$ дорівнює ± 1, і після вимірювання буде отримано стан $|z\rangle = |0\rangle^{\otimes n}$.

Якщо $f(x)$ збалансована, то половина значень $(-1)^{f(x)} = 1$, а інша половина $(-1)^{f(x)} = -1$.

Тобто, сума:

$$\sum_{x=0}^{2^n-1}(-1)^{f(x)} = 0. \tag{24}$$

Це означає, що коефіцієнт перед $|0\rangle^{\otimes n}$ дорівнює нулю, і після вимірювання отримаємо будь-який інший стан $|z\rangle$, окрім $|0\rangle^{\otimes n}$.

6. Вимірювання перших n кубітів.

Якщо функція $f(x)$ константна, то після другого перетворення Адамара система переходить у стан $|0\rangle^{\otimes n}$, і вимірювання завжди дає 0.

Якщо $f(x)$ збалансована, то після другого перетворення Адамара система знаходиться у суперпозиції станів $|z\rangle$, де $z \neq 0$, і вимірювання дає будь-який інший стан, окрім $|0\rangle^{\otimes n}$.

На відміну від класичного підходу, який вимагає до $2^{n-1}+1$ обчислень функції, квантовий алгоритм Дойча-Йожи використовує лише один виклик оракула U_f, що є експоненційним прискоренням у порівнянні з класичними алгоритмами.

Це демонструє експоненційну квантову перевагу квантового алгоритму, оскільки складність класичного алгоритму є $O(2^n)$, тоді як квантовий виконує завдання за $O(1)$ операцій.

Варто зазначити, що алгоритм Дойча-Йожи є повністю детермінованим, тобто він повертає правильну відповідь у 100% випадків (на відміну багатьох квантових алгоритмів, заснованих на імовірнісному визначенні кубітів).

Отже, алгоритм Дойча-Йожи є одним із перших алгоритмів, що показав силу квантових обчислень. Він доводить, що квантові обчислення можуть вирішувати певні задачі експоненційно швидше, ніж класичні методи. Хоча алгоритм Дойча-Йожи має переважно теоретичне та освітнє значення через обмежене практичне застосування, він є фундаментальним у квантовій інформатиці та слугує основою для розробки більш складних квантових алгоритмів.

Приклад застосування алгоритму Дойча-Йожи

Розглянемо алгоритм Дойча-Йожи на прикладі квантової системи $n = 4$ кубітів: трьох вхідних кубітів $|x_1 x_2 x_3\rangle$ та одного допоміжного кубіта $|y\rangle$.

Початковий стан системи:

$$|000\rangle \otimes |1\rangle. \tag{25}$$

Застосовуємо оператор Адамара до кожного кубіта. Оператор Адамара H переводить кожен кубіт у стан суперпозиції:

$$H|0\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right),\ H|1\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right). \tag{26}$$

Застосовуємо $H^{\otimes 4}$ до всіх кубітів. Для вхідних кубітів

$$H^{\otimes 3}|000\rangle = \frac{1}{\sqrt{8}}\sum_{x=0}^{7}|x\rangle = \frac{1}{\sqrt{8}}\left(|000\rangle + |001\rangle + |010\rangle + ... + |111\rangle\right). \tag{27}$$

Для допоміжного кубіта:

$$H|1\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right). \tag{28}$$

Отже, загальний стан системи після оператора Адамара:

$$|\psi\rangle = \frac{1}{\sqrt{8}}\sum_{x=0}^{7}|x\rangle \otimes \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right). \tag{29}$$

Тепер застосуємо оператор оракула:

$$U_f|x\rangle|y\rangle = |x\rangle|y + f(x)\rangle. \tag{30}$$

Оскільки допоміжний кубіт знаходиться у стані $\frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)$, операція змінює його фазу:

$$|\psi'\rangle = \frac{1}{\sqrt{8}}\sum_{x=0}^{7}(-1)^{f(x)}|x\rangle \otimes \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right). \tag{31}$$

Допоміжний кубіт відокремлюється (його стан не змінився після дії оракула), тому стан регістра кубітів спрощується до такого:

$$\frac{1}{\sqrt{8}}\sum_{x=0}^{7}(-1)^{f(x)}|x\rangle. \tag{32}$$

Повторно застосовуємо оператор Адамара $H^{\otimes 3}$ до перших трьох кубітів. Використавши рівність:

$$|\psi''_{\otimes n}\rangle = H^{\otimes n}|x\rangle = \frac{1}{2^n}\sum_{z=0}^{2^n-1}\sum_{x=0}^{2^n-1}(-1)^{f(x)+x\cdot z}|z\rangle, \tag{33}$$

отримаємо:

$$|\psi''_{\otimes 3}\rangle = H^{\otimes 3}|x\rangle = \sum_{z=0}^{7}\left(\frac{1}{8}\sum_{x=0}^{7}(-1)^{f(x)+x\cdot z}\right)|z\rangle = \sum_{z=0}^{7}C_z|z\rangle, \tag{34}$$

де $C_z = \frac{1}{8}\sum_{x=0}^{7}(-1)^{f(x)+x\cdot z}$ – амплітудний коефіцієнт стану $|z\rangle$.

Якщо $z=0$, то коефіцієнт біля стану $|000\rangle$ приймає значення:

$$C_0 = \frac{1}{8}\sum_{x=0}^{7}(-1)^{f(x)}. \tag{35}$$

Якщо $f(x)$ є константною функцією, то $C_0 = \pm 1$. У цьому випадку імовірність вимірювання стану $|000\rangle$ дорівнює 1.

Якщо $f(x)$ є збалансованою функцією, то $C_0 = 0$, і вимірювання дає випадковий стан $|z\rangle \neq |000\rangle$.

Алгоритм Гровера

Значно ширше практичне застосування, ніж алгоритм Дойча-Йожи, має алгоритм Гровера.

Алгоритм Гровера – це квантовий пошуковий алгоритм, який використовується для знаходження заданого елемента в невпорядкованій базі даних із квадратичним прискоренням порівняно з класичними алгоритмами. Він був запропонований Л. Гровером у 1996 році і є одним із найважливіших квантових алгоритмів поряд із алгоритмом Шора для квантової факторизації великих чисел.

Основні операції алгоритму включають:

1. Створення рівномірної суперпозиції всіх можливих станів.
2. Оператор оракула, що змінює знак амплітуди (фазу) шуканого елемента.
3. Оператор амплітудної інверсії для підсилення імовірності правильного результату.
4. Повторення цих кроків для досягнення максимального підсилення імовірності.

Вхідними даними алгоритму є:

1. Функція $f(x)$, яка повертає 1, якщо x є шуканим елементом, і 0 в іншому випадку.
2. Невпорядкований набір N записів бази даних.
3. Квантовий комп'ютер із n кубітами, де $N = 2^n$.

Алгоритм Гровера складається з таких основних кроків.

1. Початкове перетворення (ініціалізація)

Спочатку створюємо рівномірну суперпозицію всіх можливих станів бази даних, де кожен стан має однакову імовірність бути виміряним. Це досягається застосуванням операторів Адамара $H^{\otimes n}$ до кожного з n кубітів:

$$|\psi_0\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle, \tag{36}$$

де $|x\rangle$ – квантовий стан, що представляє елемент x з бази даних; $N = 2^n$ – загальна кількість елементів у базі даних, де n – кількість кубітів.

2. Застосування оператора оракула U_f

Оракул – це унітарний оператор U_f, який інвертує знак амплітуди тільки для шуканого (цільового) елемента x^*:

$$U_f |x\rangle = (-1)^{f(x)} |x\rangle. \tag{37}$$

Якщо $x = x^*$, то $f(x) = 1$ і знак амплітуди інвертується. Якщо $x \neq x^*$, то стан не змінюється.

Після дії оракула стан системи змінюється на такий:

$$|\psi_1\rangle = \frac{1}{\sqrt{N}} \left(-|x^*\rangle + \sum_{x=0\ (x \neq x^*)}^{N-1} |x\rangle \right). \tag{38}$$

Отже, після застосування оракула, зміниться фаза стану тільки для цільового елемента у вигляді інверсії знаку амплітуди імовірності.

3. Застосування оператора амплітудної інверсії (дифузії)

Амплітудна інверсія є важливою частиною алгоритму. Вона підсилює імовірність правильного результату. Оператор амплітудної інверсії віддзеркалює всі амплітуди відносно середнього значення:

$$U_{diff} = 2|\psi\rangle\langle\psi| - I\,, \tag{39}$$

де $|\psi\rangle$ – це рівномірна суперпозиція всіх базисних станів, а I – одиничний оператор.

Всі необхідні для цього дії є закладені в оператор U_{diff}. Так, оператор $|\psi\rangle\langle\psi|$ знаходить середнє значення амплітуд. Матричний добуток $|\psi\rangle\langle\psi|$ є проєктором на рівномірний стан. Його застосування до вектора стану дає результат, в якому кожна амплітуда замінюється середнім значенням усіх амплітуд. Оператор $2|\psi\rangle\langle\psi| - I$ виконує інверсію відносно середнього. Подвоєння цього проєктора і віднімання одиничної матриці автоматично реалізує операцію відображення амплітуд відносно середнього.

Отже, дифузійний оператор U_{diff} виконує всі необхідні дії: обчислює середнє значення амплітуд, виконує відображення амплітуд відносно цього середнього, підсилює амплітуди шуканих станів і зменшує амплітуди інших.

Практично дифузійний оператор можна реалізувати як:

$$H^{\otimes n}\left(2|0\rangle\langle 0| - I\right)H^{\otimes n}. \tag{40}$$

Це еквівалентно послідовному застосуванню таких операцій: застосування операторів Адамара $H^{\otimes n}$, фазового зсуву Z та повторне застосування операторів Адамара $H^{\otimes n}$.

Оператор Адамара $H^{\otimes n}|0\rangle$ перетворює $|0\rangle$ у рівномірну суперпозицію. Вираз $2|0\rangle\langle 0| - I$ реалізується через Z-оператор.

Амплітудне посилення можна розглядати геометрично у двовимірному просторі, де вектор суперпозиції обертається у напрямку вектора, що відповідає шуканому стану, а кожна ітерація алгоритму виконує обертання на кут, що наближає стан до правильного.

Виконання амплітудної інверсії дає змінений стан:

$$|\psi_1'\rangle = U_{diff}|\psi_1\rangle = \left(2|\psi_0\rangle\langle\psi_0| - I\right)|\psi_1\rangle = 2|\psi_0\rangle\langle\psi_0|\psi_1\rangle - I|\psi_1\rangle. \tag{41}$$

4. Нормування амплітуд

Після інвертування амплітуд потрібно провести їх нормування. Нормування проводиться так, щоб сума квадратів амплітуд дорівнювала 1:

$$\bar{\alpha}_i = \frac{\alpha_i}{\sqrt{\sum_{k=1}^{N} |\alpha_k|^2}}. \tag{42}$$

Після нормування отримаємо новий стан квантового регістра:

$$|\psi_2\rangle = \bar{\alpha}^*|x^*\rangle + \bar{\alpha}_x \sum_{x=0\ (x\neq x^*)}^{N-1} |x\rangle. \tag{43}$$

5. Ітерації підсилення амплітуд

Основна ідея алгоритму Гровера полягає в тому, щоб підсилити амплітуду α^* шуканого елемента через кілька ітерацій. Після застосування оператора оракула U_f і оператора амплітудної інверсії U_{diff} отримаємо новий квантовий стан, який наближається до шуканого елемента. Ітераційний процес повторюється доти, поки зростає імовірність цільового стану.

6. Умова зупинки обчислень

Імовірність цільового стану в алгоритмі Гровера змінюється циклічно. Якщо продовжити ітерації після досягнення максимальної імовірності, то вона може зменшитися, а потім знову зрости (якщо у результаті перетворень не досягнуто одного із базисних станів). Це відбувається через періодичний характер відображення Гровера, яке можна розглядати як обертання в певному підпросторі гільбертового простору.

Імовірність знайти цільовий стан після k ітерацій виражається формулою:

$$p_k = \sin^2((2k+1)\theta), \tag{44}$$

де кут обертання θ визначає відхилення вектора стану на кожній ітерації алгоритму Гровера.

Обертання стану в певному напрямку реалізують оракул, що інвертує амплітуду цільового стану, та дифузійний оператор, який діє як відбиття щодо середнього значення амплітуд.

Після кожної ітерації стан обертається на кут θ, збільшуючи імовірність знайти цільовий стан. Коли обертання досягає максимуму, імовірність знаходження цільового стану максимальна. Після цього, якщо продовжувати ітерації, стан починає відхилятися назад, зменшуючи імовірність вимірювання цільового стану.

Якщо система має N можливих станів, а серед них є M розв'язків, то кут θ визначається як:

$$\sin\theta = \frac{\sqrt{M}}{\sqrt{N}}. \tag{45}$$

Для малих M / N, тобто якщо $M << N$, можна використати апроксимацію $\sin x \approx x$ для малих x, що дає:

$$\theta \approx \frac{\sqrt{M}}{\sqrt{N}}. \tag{46}$$

Як видно з формули (46), імовірність змінюється за законом синуса, тобто вона спочатку зростає, досягає максимуму, а потім починає спадати.

Оптимальна кількість ітерацій, яка дає максимальну імовірність цільового стану визначається за формулою:

$$k_{opt} = \left\lfloor \frac{\pi}{4\theta} \right\rfloor, \tag{47}$$

де $\lfloor \cdot \rfloor$ означає округлення до нижнього цілого. Якщо продовжувати виконувати більше ітерацій, імовірність знову почне спадати через періодичність.

Для малих значень θ можна записати:

$$k_{opt} = \left\lfloor \frac{\pi}{4} \cdot \frac{\sqrt{N}}{\sqrt{M}} \right\rfloor. \tag{48}$$

7. Вимірювання

Після того як алгоритм виконується достатню кількість разів, виконується вимірювання квантового стану. Оскільки амплітуда шуканого елемента була підсилена, імовірність виміряти шуканий елемент найбільша, що дозволяє з великою імовірністю знайти цільовий елемент x^*.

Як відомо, вимірювання призводить до руйнування квантового стану. Стан суперпозиції колапсує до одного із базисних станів, як правило до того, який має найбільшу амплітуду імовірності. Це особливо важливо в контексті алгоритму Гровера: після кількох ітерацій алгоритму амплітуда цільового стану посилюється, збільшуючи імовірність його вибору при вимірюванні. Тому вимірювання імовірності стану, як квадрат його амплітуди, потрібно проводити в кінці останньої ітерації квантового алгоритму.

Визначення імовірностей станів

Імовірності станів визначаються у після їх вимірювання як квадрати модулів їх амплітуд. Так, імовірність цільового стану можна обчислити так:

$$\Pr(x^*) = \left|\left\langle x^* \middle| \psi_2 \right\rangle\right|^2 = \left|\left\langle x^* \middle| \left(\bar{\alpha}^* \middle| x^* \right\rangle + \bar{\alpha}_x \sum_{x=0\,(x\neq x^*)}^{N-1} \middle| x \right\rangle\right)\right|^2 = |\,\bar{\alpha}^*\,|^2. \tag{49}$$

Аналогічно обчислюються імовірності всіх інших станів для $x \neq x^*$:

$$\Pr(x) = \left|\left\langle x \middle| \psi_2 \right\rangle\right|^2 = |\,\bar{\alpha}_x\,|^2. \tag{50}$$

Часова складність

Алгоритм Гровера потребує $O\left(\sqrt{N}\right)$ операцій для знаходження елемента у базі даних, де N – кількість елементів у базі даних. Це є значним прискоренням порівняно з класичними алгоритмами, які потребують $O(N)$ операцій для такого ж завдання.

Алгоритм Гровера показує, як квантові обчислення можуть значно прискорити розв'язання задач, що вимагають пошуку в невпорядкованих наборах даних. Крім цього він може бути адаптований для розв'язання багатьох інших задач, наприклад, вимірювання домінантного стану квантової системи, вирішення задач криптоаналізу тощо.

Алгоритм Гровера є ефективним методом пошуку, що використовує квантові переваги для прискорення обчислень. Він демонструє квадратичне прискорення порівняно з класичними алгоритмами, що робить його важливим інструментом для майбутніх квантових обчислень.

Приклад роботи алгоритму Гровера

Розглянемо приклад роботи алгоритму Гровера для пошуку одного елемента у невпорядкованому масиві з чотирьох елементів, тобто $N = 4$. Нехай шуканим елементом є $x^* = 2$. Це означає, що потрібно знайти елемент, для якого $f(x^*) = 1$, а для всіх інших елементів $f(x) = 0$.

Для представлення $N = 4$ можливих станів необхідно $n = 2$ кубіти: $2^n = 2^2 = 4$. Початковий стан для двох кубітів:

$$\left|\psi_0\right\rangle = H^{\otimes 2}\left|00\right\rangle = \frac{1}{\sqrt{4}}\left(\left|00\right\rangle + \left|01\right\rangle + \left|10\right\rangle + \left|11\right\rangle\right) = \frac{1}{2}\left(\left|00\right\rangle + \left|01\right\rangle + \left|10\right\rangle + \left|11\right\rangle\right). \tag{51}$$

Це рівномірна суперпозиція всіх можливих станів.

Застосуємо до стану $\left|\psi_0\right\rangle$ оператор оракула, який інвертує знак тільки для шуканого елемента. Оскільки цільовим елементом є $x^* = 2 = (10)_2$, то оракул змінює знак лише для стану $\left|10\right\rangle$. Після застосування оракула, стан буде виглядати так:

$$\left|\psi_1\right\rangle = \frac{1}{2}\left(\left|00\right\rangle + \left|01\right\rangle - \left|10\right\rangle + \left|11\right\rangle\right). \tag{52}$$

Тепер застосуємо дифузійний оператор для амплітудної інверсії і підсилення амплітуди шуканого елемента:

$$U_{diff}\left|\psi_1\right\rangle = 2\left|\psi_0\right\rangle\left\langle\psi_0 \middle| \psi_1\right\rangle - I\left|\psi_1\right\rangle. \tag{53}$$

Обчислимо скалярний добуток:

$$\langle\psi_0||\psi_1\rangle=\frac{1}{2}\left(|00\rangle+|01\rangle+|10\rangle+|11\rangle\right)\frac{1}{2}\left(|00\rangle+|01\rangle-|10\rangle+|11\rangle\right)=\frac{1}{4}(1+1-1+1)=\frac{2}{4}=\frac{1}{2}. \quad (54)$$

Знайдемо $I|\psi_1\rangle=I\frac{1}{2}\left(|00\rangle+|01\rangle-|10\rangle+|11\rangle\right)=\frac{1}{2}\left(|00\rangle+|01\rangle-|10\rangle+|11\rangle\right)$. Підставимо знайдені значення у формулу $U_{diff}|\psi_1\rangle$:

$$U_{diff}|\psi_1\rangle=2\cdot\frac{1}{2}\cdot\frac{1}{2}\left(|00\rangle+|01\rangle+|10\rangle+|11\rangle\right)-\frac{1}{2}\left(|00\rangle+|01\rangle-|10\rangle+|11\rangle\right)=\frac{1}{2}\left(2|10\rangle\right)=|10\rangle. \quad (55)$$

Отже, після застосування цього оператора новий стан буде таким:

$$|\psi_2\rangle=|10\rangle. \quad (56)$$

Оскільки у ході перетворень досягнуто один зі стандартних базисних станів, то його вимірювання у двокубітному стандартному базисі відбудеться з одиничною імовірністю. Дальше продовження ітерацій алгоритму недоцільне. Для знаходження оптимальної кількості ітерацій в алгоритмі Гровера можна використовувати таку формулу для імовірності успіху після k ітерацій:

$$p(k)=\sin^2((2k+1)\cdot\theta), \quad (57)$$

де θ – це кут зміни вектора квантового стану на кожній ітерації.

Для системи з одним цільовим станом ($M=1$) кут θ обчислюється як:

$$\theta=\arcsin\left(\sqrt{N}\right)^{-1}, \quad (58)$$

де N – кількість можливих станів.

Для $N=4$ маємо:

$$\theta=\arcsin\left(\sqrt{4}\right)^{-1}=\arcsin 2^{-1}=\frac{\pi}{6}. \quad (59)$$

Оптимальна кількість ітерацій k_{opt} для досягнення максимальної імовірності вимірювання цільового стану для $N=4$ розраховується як:

$$k_{opt}=\left\lfloor\frac{\pi}{4\theta}\right\rfloor=\left\lfloor\frac{\pi}{4}\cdot\frac{6}{\pi}\right\rfloor=\left\lfloor\frac{6}{4}\right\rfloor=\lfloor 1.5\rfloor=1. \quad (60)$$

Отже, для $N=4$ оптимальна кількість ітерацій дорівнює 1.

Підставимо $k=1$ і $\theta=\frac{\pi}{6}$ у формулу для імовірності успіху:

$$p(1)=\sin^2\left((2\cdot1+1)\cdot\frac{\pi}{6}\right)=\sin^2\left(\frac{3\pi}{6}\right)=\sin^2\left(\frac{\pi}{2}\right)=1. \quad (61)$$

Отже, імовірність успіху після першої ітерації буде 1 (тобто, 100 %). Імовірність вимірювання стану, досягнутого після дії оператора дифузії U_{diff}, обчислюється як квадрат модуля амплітуди цього стану:

$$\Pr(10)=\left|\langle 10||\psi_2\rangle\right|^2=\left|\langle 10||10\rangle\right|^2=(0\quad 0\quad 1\quad 0)\cdot(0\quad 0\quad 1\quad 0)^{\mathrm{T}}=1^2=1. \quad (62)$$

Отже, після першої ітерації гарантовано отримаємо правильний розв'язок $x^*=2$, що відповідає стану $|10\rangle$.

Переваги квантового паралелізму обчислень над класичними обчисленнями

Квантовий паралелізм забезпечує значні переваги над класичними послідовними і паралельними обчисленнями завдяки використанню принципів квантової механіки: суперпозиції, квантової заплутаності та інтерференції.

У послідовних обчисленнях класичний процесор виконує операції поетапно, обробляючи один стан за раз. Класичний паралелізм досягається завдяки множинним процесорам або потокам кодів, які виконують різні частини задачі одночасно.

У класичних обчисленнях паралельне виконання можливе лише на обмеженій кількості процесорів чи потоків. У квантових обчисленнях квантовий регістр з n кубітів може одночасно перебувати в суперпозиції всіх 2^n можливих станів, дозволяючи обробляти експоненційно велику кількість комбінацій одночасно.

Квантовий комп'ютер може одночасно обробляти всі можливі стани завдяки суперпозиції, що призводить до експоненційного прискорення для певних задач. Наприклад, алгоритм Шора для факторизації чисел працює експоненційно швидше за найкращі класичні алгоритми. Алгоритм Гровера забезпечує квадратичне прискорення для пошуку у невпорядкованій базі даних.

У класичних послідовних обчисленнях кожен можливий стан обчислюється окремо. У класичних паралельних обчисленнях ці стани розподіляються між потоками, що прискорює процес, але все одно не дає експоненційного прискорення, як у квантових обчисленнях. Багато квантових алгоритмів використовують паралельну обробку шляхом квантового втручання (квантової інтерференції), що дозволяє швидко знаходити оптимальні рішення за рахунок пісилення або послаблення певних станів. У квантовій системі можливі результати комбінуються за допомогою квантової інтерференції, що дозволяє відкидати неправильні відповіді та підсилювати правильні.

Заплутані кубіти дозволяють реалізовувати квантову заплутаність та нестандартні кореляції між даними, що неможливо в класичних системах. Це забезпечує переваги в комунікаційних протоколах (квантова телепортація, квантова криптографія). У квантових обчисленнях є менші вимоги до обсягів пам'яті. Так, для представлення 2^n станів у класичній системі потрібен експоненційний обсяг пам'яті. У квантовій системі такий самий обсяг інформації кодується в n кубітах. Класичні обчислення неефективні для моделювання квантових систем через експоненційне зростання обсягу обчислень. Квантові комп'ютери можуть природним чином обробляти складні квантові явища, такі як молекулярні взаємодії, квантову хімію чи фізичні процеси на атомному рівні. Отже, квантовий паралелізм відкриває нові можливості для вирішення задач, які неможливо або вкрай складно вирішити класичними методами. Основна перевага полягає в тому, що квантові обчислення можуть працювати з експоненційно великою кількістю станів одночасно, що дає значний приріст продуктивності в певних задачах, таких як факторизація, оптимізація та симуляція квантових систем.

Попри значний потенціал квантових обчислень, класичні обчислення все ще мають суттєві переваги над квантовими в багатьох. Класичні обчислення характеризуються технологічною зрілістю та надійністю. Класичні комп'ютери добре розвинені, масово виробляються, мають стабільну архітектуру та надійне збереження інформації. Сучасні класичні алгоритми ефективні і добре оптимізовані для широкого спектра задач. У квантових системах присутні декогеренція (втрата квантової інформації) та шум, що ускладнює їх використання.

Класичні біти зберігають інформацію надійно, тоді як кубіти через квантову природу можуть швидко руйнуватися. У класичних системах немає проблем з квантовими помилками та потребою в корекції помилок, що є критичним викликом для квантових комп'ютерів. Класичні комп'ютери енергоефективні, тоді як квантові системи вимагають наднизьких температур та спеціального обладнання для підтримки когерентності. Створення великих квантових процесорів потребує значних витрат електроенергії та складної інфраструктури. У класичних обчисленнях можна зчитувати дані на будь-якому етапі без руйнування обчислювального процесу. У квантових системах вимірювання руйнує суперпозицію, тому проміжні результати неможливо зчитати без втрати інформації. Класичні комп'ютери придатні для будь-яких обчислювальних задач, тоді як квантові

підходять лише для специфічних алгоритмів (факторизація, пошук, квантова хімія). Більшість прикладних задач не потребують квантового прискорення, оскільки класичні алгоритми вже оптимізовані. Класичні процесори легко масштабуються за рахунок багатоядерності та розподілених обчислень. Масові обчислення (хмарні сервіси, дата-центри) легко реалізувати на класичних суперкомп'ютерах, тоді як квантові комп'ютери поки що не мають аналогічних інфраструктур.

Для класичних комп'ютерів існує величезна база програмного забезпечення та алгоритмів, які не можна легко адаптувати до квантових комп'ютерів. Квантове програмування вимагає спеціальних мов та підходів, які поки що не є масовими. До таких мов належать: Qiskit (Python) від IBM, Cirq (Python) від Google, Quipper (Haskell) від Microsoft Research, Q# від Microsoft, PennyLane (Python) від Xanadu. Сучасні платформи, такі як IBM Quantum, Google Quantum AI та інші, дозволяють реалізовувати квантові алгоритми на реальних квантових комп'ютерах. Це сприяє розвитку практичних навичок у написанні квантових програм мовою Qiskit, Cirq, PennyLane, розробці та тестуванні квантових алгоритмів, аналізі помилок та шумостійких реалізацій квантових алгоритмів. У навчальному процесі це допомагає студентам перейти від теорії до реальних квантових обчислень. Попри значний потенціал квантового паралелізму, класичні обчислювальні системи ще тривалий час залишатимуться основою для розв'язування більшості практичних задач.

Застосування квантового паралелізму на практиці все ще стикається з низкою технічних і теоретичних викликів. Квантові комп'ютери ще не досягли достатнього рівня надійності та потужності для вирішення реальних задач в промислових масштабах. З розвитком квантових технологій, таких як стабільні кубіти, квантова корекція помилок та масштабування квантових систем, в перспективі квантовий паралелізм може змінити парадигму обчислень і привести до значних проривів у багатьох науках і галузях. Водночас його реальне застосування потребує подолання значних технічних перешкод, але це вже вказує на можливості для розвитку нових ідей і підходів до вирішення сучасних та майбутніх задач.

Перспективи застосування квантового паралелізму

Квантовий паралелізм – це одна з основних переваг квантових обчислень, яка дозволяє здійснювати обчислення над великою кількістю можливих станів одночасно завдяки явищу квантової суперпозиції. Це принципова відмінність від класичних обчислень, де кожне значення обчислюється окремо. Оскільки квантові системи можуть одночасно виконувати багато операцій, це відкриває широкі можливості для розв'язування складних задач, які на класичних комп'ютерах займають величезну кількість часу. Зараз квантовий паралелізм в основному застосовується в таких сферах, як пошук, оптимізація та розв'язування математичних задач. Одним з найбільш перспективних напрямів є використання квантових алгоритмів для вирішення задач пошуку, таких як алгоритм Гровера. Цей алгоритм дозволяє зменшити складність пошуку в невпорядкованій базі даних, що містить N елементів, з класичного $O(N)$ до квантового $O(\sqrt{N})$. Це може значно прискорити обчислення в таких галузях, як криптографія, штучний інтелект, біоінформатика та вивчення матеріалів.

Ще одним важливим напрямком є використання квантових обчислень у симуляціях квантових систем. Квантові комп'ютери здатні моделювати поведінку молекул та матеріалів на атомарному рівні значно ефективніше, ніж класичні комп'ютери, що дозволяє прискорити розробку нових ліків, матеріалів і технологій. Наприклад, в хімії та фармацевтиці квантові обчислення можуть суттєво спростити процес моделювання молекул, що дозволить швидше знаходити нові лікарські засоби та оптимізувати процеси їх синтезу. Іншим важливим аспектом є використання квантового паралелізму для вирішення складних задач оптимізації. Оскільки багатофакторні оптимізаційні задачі (наприклад, задача комівояжера або задача складання розкладу) мають величезну кількість можливих варіантів рішень, квантові алгоритми можуть значно скоротити час, необхідний для знаходження оптимального розв'язку. Це може мати великий вплив на логістику, виробництво, фінанси та інші сфери, де важливі ефективність і швидкість прийняття рішень.

Окрім традиційних застосувань квантового паралелізму, не менш перспективним є використання квантових обчислень у галузі машинного навчання та штучного інтелекту. Квантові нейромережі, або квантові алгоритми для машинного навчання, можуть радикально змінити підходи до обробки даних, тренування моделей і вирішення складних завдань. Квантові нейромережі використовують принципи квантової механіки для реалізації алгоритмів навчання, що може дозволити значно скоротити час опрацювання та підвищити ефективність порівняно з класичними методами. Зокрема, квантові нейромережі здатні виконувати паралельне навчання над величезними наборами даних завдяки квантовому суперпозиційному стану. Це може бути особливо корисним для таких складних задач, як обробка великих обсягів даних, розпізнавання образів, прогнозування, класифікація та кластеризація. Квантові алгоритми можуть забезпечити ефективне розв'язування задач, для яких класичні нейромережі стикаються з обмеженнями через величезні обсяги даних або високі вимоги до обчислювальних потужностей. Наприклад, застосування квантових алгоритмів для класифікації та кластеризації виводить машинне навчання на новий рівень, дозволяючи здійснювати швидший пошук по багатовимірних просторах, що часто є надзвичайно складним для класичних підходів.

Однією з основних переваг квантових нейромереж є здатність обробляти складні нелінійні взаємозв'язки між величезними обсягами даних. Це дає можливість застосовувати квантові нейромережі в складних задачах, таких як обробка природного мовлення, рекомендаційні системи, фінансові прогнози, діагностика та персоналізоване лікування у медицині. Незважаючи на те, що квантові обчислення ще знаходяться на стадії розвитку, їхні можливості вже зараз виглядають дуже перспективними. Квантовий паралелізм, поряд із квантовими нейромережами та машинним навчанням, має потенціал для революційних змін у багатьох наукових і технологічних галузях, таких як пошук, оптимізація, моделювання квантових систем, а також в обробці великих даних і штучному інтелекті. У майбутньому, з розвитком квантових технологій, ці застосування можуть відкрити нові горизонти для наукових досліджень і промислових інновацій. Квантовий паралелізм має величезний потенціал для прогресивних змін багатьох сфер науки та технологій.

Висновки

Розглянуті математичні моделі квантового паралелізму підтверджують квантову перевагу над класичними обчислювальними методами, оскільки дозволяють виконувати обчислення над всіма можливими значеннями аргументів одночасно завдяки принципу суперпозиції. Перетворення квантових станів здійснюється унітарними операторами, що забезпечує зворотність операцій та відсутність інформаційних втрат, що є ключовою відмінністю квантових обчислень від класичних.

Розширений алгоритм Дойча-Йожи демонструє квантову перевагу, оскільки дозволяє встановити вид функції для множини аргументів за один квантовий виклик, тоді як класичний алгоритм потребує експоненційної кількості обчислень. Алгоритм Гровера реалізує ефективний квантовий пошук у невпорядкованій базі даних, що дозволяє знаходити потрібний елемент за кількість ітерацій, пропорційну квадратному кореню з кількості елементів, тоді як класичні алгоритми потребують лінійного часу.

Числові приклади роботи алгоритмів підтверджують можливості квантового паралелізму, оскільки демонструють зменшення кількості обчислень порівняно з класичними методами. Огляд фундаментальних квантових алгоритмів вказує на перспективність паралельних квантових обчислень, однак їх практичне застосування поки що обмежене через нестабільність квантових станів та технічні виклики реалізації масштабованих квантових процесорів.

Подальші дослідження у сфері квантового паралелізму можуть сприяти розвитку нових алгоритмів, що знайдуть застосування у криптографії, оптимізації, штучному інтелекті та інших сферах квантових обчислень.

СПИСОК ЛІТЕРАТУРИ

1. Arute, F., Arya, K., Babbush, R. et al. (2019). Quantum supremacy using a programmable superconducting processor. Nature, 574, 505-510. https://doi.org/10.1038/s41586-019-1666-5.
2. Beer K. (2022). Quantum neural networks. arXiv: 2205.08154 [quant-ph]. https://doi.org/10.48550/arXiv.2205.08154.
3. Biamonte, J., Wittek, P., Pancotti, N. et al. (2017). Quantum machine learning. Nature, 549 (7671), 195-202. https://doi.org/10.1038/nature23474.
4. Bodnarchuk, O., Zybin, S., & Vasilyuk-Zaytseva, S. (2024). The effectiveness of quantum computers in solving complex problems (in Ukrainian), Information Technology and Society, 4 (15), 6-13. https://doi.org/10.32689/maup.it.2024.4.1.
5. Deutsch, D. (1985). Quantum theory, the Church-Turing principle and the universal quantum computer. Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences, 400(1818), 97–117. https://doi.org/10.1098/rspa.1985.0070.
6. Deutsch, D., & Jozsa, R. (1992). Rapid solution of problems by quantum computation. Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences, 439(1907), 553–558. https://doi.org/10.1098/rspa.1992.0167.
7. Dirac, P. A. M. (1930). The Principles of Quantum Mechanics. Oxford: Clarendon Press.
8. Easttom, C. (2022). Quantum Computing and Cryptography. In: Modern Cryptography, Applied Mathematics for Encryption and Information Security. Springer, Cham, 397-407. https://doi.org/10.1007/978-3-031-12304-7_19.
9. Farhi, E., G oldstone, J., & Gutmann, S. (2014). A Quantum Approximate Optimization Algorithm. arXiv: 1411.4028. https://doi.org/10.48550/arXiv.1411.4028.
10. Feynman, R. (1982). Simulating physics with computers. International Journal of Theoretical Physics, 21(6–7), 467–488. https://doi.org/10.1007/BF02650179.
11. Gaikwad, A., Torres, M.S., Ahmed, S., & Kockum, A.F. (2025). Gradient-descent methods for fast quantum state tomography, 1-20. arXiv: 2503.04526v1 [quant-ph].
12. Gircha, A.I., Boev, A.S., Avchaciov, K. et al. (2023). Hybrid quantum-classical machine learning for generative chemistry and drug design. Sci Rep, 13, 8250. https://doi.org/10.1038/s41598-023-32703-4.
13. Google Quantum AI and Collaborators. (2025). Quantum error correction below the surface code threshold. Nature 638, 920–926. https://doi.org/10.1038/s41586-024-08449-y.
14. Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. Proceedings of the 28th Annual ACM Symposium on Theory of Computing, 212–219. https://doi.org/10.1145/237814.237866.
15. Grover, L. K. (1997). Quantum mechanics helps in searching for a needle in a haystack. Physical Review Letters, 79(2), 325–328. https://doi.org/10.1103/PhysRevLett.79.325.
16. Kadowaki, T., & Nishimori, H. (1998). Quantum annealing in the transverse Ising model. Physical Review E, 58(5), 5355. https://doi.org/10.1103/PhysRevE.58.5355.
17. Kalyuzhny, I. G. (2015). Quantum cryptography: principles, problems and prospects (in Ukrainian), Information systems, mechanics and control, 13, 29–37. http://nbuv.gov.ua/UJRN/Ismk_2015_13_5.
18. Karlash, G. Yu. (2018). Quantum Information Systems. Textbook for the specialty “Applied Physics and Nanomaterials” (in Ukrainian), Kyiv: Faculty of Radiophysics, Electronics and Computer Systems of Taras Shevchenko National University of Kyiv.
19. Kosobutsky, P. S. (2022). Physical foundations of quantum informatics: from quantum mechanics, through quantum computing to quantum cryptography (in Ukrainian), Computer systems design: theory and practice, 4 (1), 33-47. DOI: https://doi.org/10.23939/cds2022.01.033.
20. Krokhmalskyi, T. E. (2018). Introduction to Quantum Computing: Textbook (in Ukrainian), Lviv: Ivan Franko National University of Lviv.
21. Kozhukhivskyi, A.D., Gaidur, G.I., & Kozhukhivska, O.A. (2022). Quantum search algorithm in unstructured database, Scientific notes of the State University of Information and Telecommunication Technologies (in Ukrainian), 1-2(2), 10-14. DOI: 10.31673/25187678.2022. 021014.
22. Lloyd, S. (1996). Universal quantum simulators. Science, 273(5278), 1073–1078.
23. https://doi.org/10.1126/science.273.5278.1073.
24. Matsakos, T. & Nield, S. (2024). Quantum Monte Carlo simulations for financial risk analytics: scenario generation for equity, rate, and credit risk factors. Quantum, 8(1306), 1-35. arXiv: 2303.09682v2. https://doi.org/10.22331/q-2024-04-04-1306.
25. Motta, M. (2022). Quantum simulations of molecular systems with intrinsic atomic orbitals. Phys. Rev. A, 106(022404). https://doi.org/10.1103/PhysRevA.106.022404.

26. Nielsen, M. A., & Chuang, I. L. (2000). Quantum Computation and Quantum Information. Cambridge University Press.
27. Ostapov, S. E., & Dobrovolskyi, Y. G. (2021). Quantum Informatics and Quantum Computing (in Ukrainian), Chernivtsi: ChNU.
28. Pang, X., Li, Y., & Wang, Z. (2025). Quantum neural network quantum state. Proc. SPIE 13545, Third International Conference on Algorithms, Network, and Communication Technology (ICANCT 2024), 1354504 (3 March 2025). https://doi.org/10.1117/12.3059735.
29. (2014 Peruzzo, A., McClean, J., Shadbolt, P., Yung, M.-H., Zhou, X.-Q., Love, P. J., Aspuru-Guzik, A., & O'Brien, J. L.). A variational eigenvalue solver on a q uantum processor. Nature Communications, 5, 4213. https://doi.org/10.1038/ncomms5213.
30. Ramezani, S. B., Sommers, A., Manchukonda, H. K., Rahimi, S., & Amirlatifi, A. (2020). Machine Learning Algorithms in Quantum Computing: A Survey. 2020 International Joint Conference on Neural Networks (IJCNN), Glasgow, UK, 1-8, https://doi.org/10.1109/IJCNN48605.2020.9207714.
31. Reichardt, B. W., & Grover, L. K. (2005). Quantum error correction of systematic errors using a quantum search framework. Phys. Rev. A, 72, 042326. arXiv:quant-ph/0506242. https://doi.org/10.48550/arXiv.quant-ph/0506242.
32. Ricci, S., Dobias, P., Malina, L., Hajny J., & Jedlicka, P. (2024). Hybrid Keys in Practice: Combining Classical, Quantum and Post-Quantum Cryptography. In IEEE Access, 12, 23206-23219. https://doi.org/10.1109/ACCESS.2024.3364520.
33. Schrödinger, E. (1926). Quantisierung als Eigenwertproblem. Annalen der phyzik, 18, 109-139.
34. Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. Proceedings 35th Annual Symposium on Foundations of Computer Science, 124–134. https://doi.org/10.1109/SFCS.1994.365700.
35. Shor, P. W. (1995). Scheme for reducing decoherence in quantum computer memory. Physical Review A, 52(4), R2493–R2496. https://doi.org/10.1103/PhysRevA.52.R2493.
36. Tkachuk, V. M. (2011). Fundamental Problems of Quantum Mechanics (in Ukrainian), Lviv: Ivan Franko National University of Lviv.
37. Tomamichel, M. (2015). Quantum Information Processing with Finite Resources: Mathematical Foundations, Springer.
38. Vakarchuk, I. O. (2012). Quantum Mechanics, 4th edition (added) (in Ukrainian), Lviv: Ivan Franko National University of Lviv.
39. Wang, Z., & Tang, H. (2024). Artificial Intelligence for Quantum Error Correction: A Comprehensive Review. arXiv: 2412.20380, 1-20. https://doi.org/10.48550/arXiv.2412.20380
40. Wu, H., Zhang, J., Wang, L. et al. (2025). A survey on qu antum deep learning. J Supercomput, 81(564). https://doi.org/10.1007/s11227-025-07083-3.
41. Yukhnovsky, I. R. (2002). Fundamentals of Quantum Mechanics. Textbook (second edition with additions) (in Ukrainian), Kyiv: Lybid.
42. Zurek, W. H. (2003). Decoherence, einselection, and the quantum origins of the classica. Reviews of Modern Physics, 75(3), 715–775. https://doi.org/10.1103/RevModPhys.75.715.

ANALYSIS OF MATHEMATICAL MODELS OF QUANTUM PARALLELISM

Petro Kravets
Lviv Polytechnic National University,
Information Systems and Networks Department, Lviv, Ukraine
E-mail: Petro.O.Kravets@lpnu.ua, ORCID: 0000-0001-8569-423X

This article analyzes mathematical models of quantum parallelism based on the transfer of a quantum system into a superposition state. The principles of quantum parallelism and its mathematical foundations are substantiated. To demonstrate the quantum advantage, mathematical models of fundamental quantum algorithms Deutsch-Joža and Grover are analyzed, which illustrate the efficiency of quantum computing compared to classical methods.

The Deutsch-Joshy algorithm is considered, which generalizes the problem of determining the type of a binary function by extending it to a set of arguments written in a quantum register. This algorithm allows determining whether a function is constant or balanced in a single quantum call, while in classical calculations this requires exponential time. It is noted that although the Deutsch-Joshy algorithm demonstrates the possibilities of parallel quantum computing, it is of mainly theoretical importance.

Grover's algorithm implements quantum parallel computing for the practical problem of searching for an element in an unordered database. It is based on iterative amplification of the amplitude of the state corresponding to the searched element and provides quadratic speedup compared to classical algorithms. In addition to database search, Grover's algorithm can be adapted to solve other optimization problems.

The work of the considered algorithms is illustrated by numerical examples, which simplifies the understanding of their principles and contributes to the further methodological development of parallel quantum computing.

The article also outlines the advantages of quantum parallelism over classical computing and identifies the prospects for the application of parallel quantum algorithms.

Keywords – quantum system, superposition of states, measurement of quantum states, unitary operator, Deutsch-Joža algorithm, Grover algorithm.