УДК 004.058

В.О. Ковальчук

КВАНТОВІ ОБЧИСЛЕННЯ ТА КВАНТОВІ КОМП'ЮТЕРИ ЇХ ВПЛИВ НА РОЗВИТОК СУЧАСНИХ ТЕХНОЛОГІЙ

Вінницький національний технічний університет

Анотація

Квантові обчислення та квантові комп'ютери є перспективною галуззю сучасної інформаційної технології, яка обіцяє революційно змінити підхід до обробки інформації. Їх вплив на розвиток сучасних технологій є значним, сприяючи швидкішому розвитку обчислювальної сили та можливостей зберігання та обробки даних. Ця доповідь досліджує основні принципи квантових обчислень, їх потенційні застосування та вплив на сучасні технології.

Ключові слова: квантові обчислення, квантові комп'ютери, розвиток технологій.

Abstract

Quantum computing and quantum computers are a promising field of modern information technology that promises to revolutionize the approach to information processing. Their impact on the development of modern technologies is significant, contributing to faster advancements in computing power and capabilities for data storage and processing. This presentation explores the basic principles of quantum computing, their potential applications, and their influence on contemporary technologies.

Keywords: quantum computing, quantum computers, development of technologies.

Вступ

Що таке квантові обчислення? Квантові обчислення - це тип обчислень, який використовує квантово-механічні явища, такі як суперпозиція та заплутаність, для виконання операцій над даними. Він базується на принципах квантової механіки, яка описує поведінку матерії та енергії на дуже малих масштабах, наприклад, на рівні атомів і субатомних частинок.

У традиційних обчисленнях основною одиницею інформації є біт, який може бути як 0, так і 1. На відміну від них, квантові обчислення використовують кубіти (квантові біти), які можуть представляти як 0, так і 1 одночасно - стан, відомий як суперпозиція. Ця властивість дозволяє квантовим комп'ютерам виконувати певні типи обчислень набагато швидше, ніж класичні комп'ютери.

Квантові обчислення мають велике значення для майбутнього обчислювальних систем, оскільки вони можуть революціонізувати спосіб обчислення та обробки інформації.

Зараз розглянемо деякі аспекти їх важливості та потенціалу для сучасних обчислювальних систем:

Висока обчислювальна швидкість.

Квантові комп'ютери можуть виконувати обчислення набагато швидше, ніж навіть найпотужніші класичні комп'ютери. Особливо це стосується завдань, які вимагають інтенсивних обчислень або оптимізації.

Обробка складних проблем.

Багато складних проблем, які наразі недоступні для класичних комп'ютерів через їх обчислювальну складність, можна вирішити за допомогою квантових алгоритмів. Це включає об'ємний аналіз, оптимізацію складних систем, моделювання складних хімічних процесів тощо.

Величезний потенціал у сфері штучного інтелекту

Квантові обчислення можуть значно покращити можливості машинного навчання та штучного інтелекту, дозволяючи набагато ефективніше обробляти та аналізувати великі обсяги даних, а також вирішувати складніші проблеми в цій галузі.

поле.

Перегляд криптографічних стандартів

Розвиток квантових обчислень може призвести до перегляду криптографічних стандартів. Традиційні методи шифрування можуть стати безладними через здатність квантових комп'ютерів обчислювати великі числа швидше, ніж класичні комп'ютери.

Ефективне моделювання складних систем

Квантові обчислення можуть допомогти моделювати складні системи, такі як хімічні реакції чи молекулярні структури, що сприятиме розробці нових матеріалів, ліків, каталізаторів тощо.

Передача та обробка великих обсягів даних

Квантові обчислення можуть ефективно обробляти великі обсяги даних, які важко або неможливо отримати за допомогою класичних методів, що робить його корисним для аналітичних завдань і керування великими обсягами даних.

Основи квантових обчислень

Для того щоб краще зрозуміти що таке квантові обчислення розберем базові поняття цієї галузі.

Квантові обчислення - це вузькоспеціалізована галузь, яка вимагає знань у квантовій механіці, комп'ютерних науках та електротехніці.

Ось загальний огляд того, як працюють квантові обчислення:

Квантові біти (кубіти): Квантові обчислення використовують кубіти, які схожі на класичні біти в тому, що вони представляють інформацію, але з важливою відмінністю. У той час як класичні біти можуть мати лише значення 0 або 1, кубіти можуть існувати в обох станах одночасно.

Квантові ворота: Квантові вентилі - це операції над кубітами, які дозволяють маніпулювати станом кубітів. Вони є аналогом класичних логічних вентилів, але з деякими важливими відмінностями, зумовленими природою квантової механіки. Квантові ворота - це операції, що виконуються над кубітами, які дозволяють маніпулювати станом кубітів. На відміну від класичних вентилів, квантові вентилі можуть оперувати з кубітами в суперпозиції.

Квантові схеми*:* Подібно до класичних схем, квантові схеми складаються з серії вентилів, які оперують з кубітами. Однак, на відміну від класичних схем, квантові схеми можуть оперувати кількома кубітами одночасно завдяки властивості заплутаності.

Квантові алгоритми: Квантові алгоритми - це алгоритми, розроблені для запуску на квантових комп'ютерах. Вони, як правило, використовують унікальні властивості кубітів і квантових воріт для виконання обчислень більш ефективно, ніж класичні алгоритми.

"Квантове обладнання": Квантове обладнання - це фізична реалізація квантового комп'ютера. Наразі існує кілька різних типів квантового обладнання, включаючи надпровідні кубіти, кубіти з іонними пастками та топологічні кубіти.

Принципи квантових обчислень

Квантові обчислення базуються на кількох фундаментальних принципах квантової механіки. Ось деякі з ключових принципів, які лежать в основі квантових обчислень:

Накладання: У квантовій механіці частинки можуть існувати в декількох станах одночасно. У квантових обчисленнях кубіти (квантові біти) можуть існувати в суперпозиції 0 і 1, що дозволяє виконувати кілька обчислень одночасно.

Заплутаність: Заплутаність - це явище, при якому дві або більше частинок можуть стати корельованими таким чином, що їхні квантові стани пов'язані між собою. У квантових обчисленнях заплутані кубіти можна використовувати для виконання певних обчислень набагато швидше, ніж класичні комп'ютери.

Принцип невизначеності: Принцип невизначеності стверджує, що неможливо знати положення та імпульс частинки з повною точністю. Цей принцип має важливе значення для квантових обчислень, оскільки означає, що вимірювання на кубітах можуть змінювати їхній стан.

Вимірювання: Вимірювання є фундаментальною частиною квантової механіки, оскільки воно згортає суперпозицію частинок у певний стан. У квантових обчисленнях вимірювання використовуються для вилучення інформації з кубітів, але вони також руйнують стан суперпозиції кубітів.

Мови програмування квантових комп’ютерів

Квантові комп’ютери, що використовують кубіти замість бітів, можуть значно прискорити розв’язання складних завдань, які класичні комп’ютери не в змозі вирішити в розумний час.

Для програмування таких комп’ютерів було розроблено спеціальні мови програмування. Розглянемо кілька найпопулярніших мов.

- Twist – це відкрита мова програмування квантових комп’ютерів, яку було розроблено у 2018 році. Вона заснована на Python і використовує відкритий вихідний код. Twist підтримує симуляцію квантових обчислень і їх реалізацію на реальних квантових пристроях.
- Qiskit – це відкритий набір інструментів для розробки квантових алгоритмів, створений компанією IBM. Він містить у собі мову програмування Qiskit, яка заснована на Python і дає змогу створювати і симулювати квантові алгоритми, а також реалізовувати їх на реальних квантових пристроях.
- Cirq – це відкрита мова програмування квантових обчислень, розроблена компанією Google. Заснована на мові Python і надає інструменти для створення квантових алгоритмів та їх реалізації на реальних квантових пристроях.
- Quil – це мова програмування квантових обчислень, розроблена компанією Rigetti. Вона дає змогу створювати квантові алгоритми та реалізовувати їх на реальних квантових пристроях. Quil використовує спеціальний синтаксис, який нагадує асемблерний код.
- Microsoft Q# – це мова програмування квантових обчислень, створена компанією Microsoft. Вона заснована на мові C# і дає змогу створювати квантові алгоритми, симулювати їх і реалізовувати на реальних квантових пристроях.

Усі ці мови програмування мають свої переваги та недоліки, і вибір тієї чи іншої мови залежить від конкретного завдання та уподобань програміста.

Квантові алгоритми

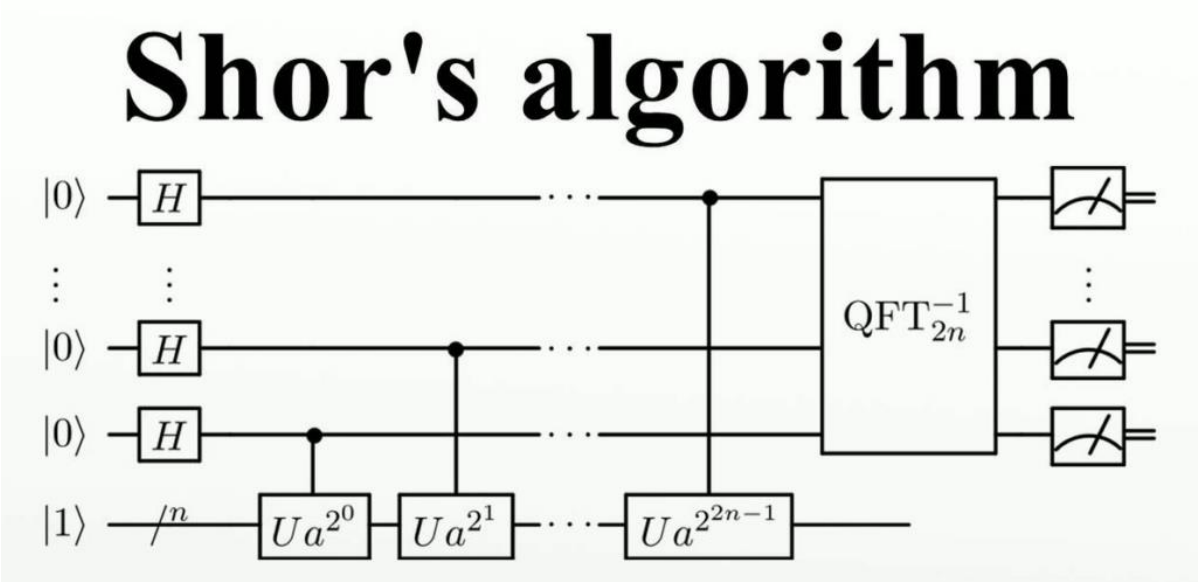
У цьому розділі розглянемо квантові алгоритми які використовуються для вирішення різних складних задач(факторизація цілих чисел, розв'язання систем лінійних рівнянь, оптимізацію, симуляцію квантових систем, тощо).

Програмування квантових комп’ютерів дає змогу створювати та використовувати квантові алгоритми для розв’язання задач. Ці алгоритми використовують кубіти і квантові обчислення, щоб забезпечити більш швидке і ефективне вирішення певних завдань, ніж класичні алгоритми. Перелічимо основні:

Алгоритм Шора

Це один із найвідоміших квантових алгоритмів, який використовується для факторизації великих чисел. Цей алгоритм дає змогу розв’язати задачу факторизації за поліноміальний час на квантовому комп’ютері, що є значним покращенням порівняно з класичними алгоритмами. Використання алгоритму Шора на квантовому комп’ютері може створити загрозу для криптографічних систем. Пояснимо, чому: алгоритм Шора дає змогу ефективно факторизувати (розкласти велике складене

число на прості множники) великі числа на квантовому комп’ютері. У криптографії факторизація використовується для створення криптосистем на основі задачі обчислення дискретного логарифма або факторизації великих чисел.



Однак, за допомогою алгоритму Шора можна легко розкласти велике складене число на прості множники, що може призвести до порушення безпеки криптографічних систем, заснованих на факторизації великих чисел. Наприклад, криптосистема RSA заснована на труднощах факторизації великих чисел, і якщо квантовий комп’ютер буде здатний ефективно розв’язувати це завдання, то RSA стане вразливою до атак.

Алгоритм Гровера

Це алгоритм пошуку в невпорядкованому списку елементів, який також може бути реалізований на квантових комп’ютерах. Цей алгоритм дає змогу знайти потрібний елемент у списку за O(√n) операцій, що в кілька разів швидше, ніж класичні алгоритми. Алгоритм Гровера може бути застосований у таких галузях, як машинне навчання, оптимізація і бази даних.

Квантова телепортація

Це явище дає змогу передавати квантовий стан через великі відстані. Цей процес заснований на використанні двох кубітів і класичного зв’язку. Квантова телепортація має великий потенціал для застосування в криптографії та комунікаціях.

Квантові симуляції

Ця галузь квантової інформатики займається симуляцією складних квантових систем. Квантові симуляції можуть бути використані для розв’язання багатьох наукових та інженерних завдань, таких як моделювання молекулярних систем і розробка нових матеріалів.

Застосування квантових обчислень

Ознайомившись з базовими поняттями в галузі квантових обчислень трішки поговоримо про реальні сфери її застосування:

- Криптографія: Квантові обчислення потенційно можуть зламати багато сучасних криптографічних алгоритмів, що використовуються для захисту комунікацій і транзакцій. Однак вони також можуть бути використані для розробки нових квантово-стійких методів шифрування, які будуть більш безпечними.
- Проблеми оптимізації: Багато реальних проблем пов'язані з пошуком оптимального рішення з великої кількості можливих варіантів. Квантові обчислення можуть бути використані для розв'язання цих оптимізаційних задач ефективніше, ніж класичні комп'ютери, дозволяючи отримувати швидші та точніші рішення.
- Матеріалознавство: Квантові обчислення можуть моделювати поведінку складних матеріалів на молекулярному рівні, уможливлюючи відкриття нових матеріалів з такими бажаними властивостями, як надпровідність або краще зберігання енергії.
- Машинне навчання: Квантові обчислення потенційно можуть покращити алгоритми машинного навчання, дозволяючи ефективно обробляти великі обсяги даних.

- Хімія: Квантові обчислення можуть моделювати хімічні реакції та поведінку молекул на квантовому рівні, що може допомогти у розробці більш ефективних медичних препаратів та матеріалів.
- Фінансове моделювання: Квантові обчислення можна використовувати для більш ефективного фінансового моделювання та аналізу ризиків, що дозволяє швидше і точніше прогнозувати фінансові результати.

Хоча це лише кілька прикладів, потенційні застосування квантових обчислень є широкими і різноманітними. Однак технологія все ще перебуває на ранніх стадіях розвитку, і потрібно подолати багато викликів, перш ніж її можна буде широко застосовувати на практиці.

Перспективи розвитку квантового обчислення та квантових комп'ютерів

Сьогодні квантові комп'ютери – справа не завтрашнього, а навіть післязавтрашнього дня. Малоймовірно, що так звані класичні комп'ютери зникнуть на зорі ери квантових обчислень. Наразі не існує алгоритму, здатного ефективно розв'язувати більшість NP-повних і NP-складних проблем на квантових комп'ютерах. Проте для деяких задач знайдено такі алгоритми, за допомогою яких вони квантово розв'язуються набагато швидше, ніж на звичайному комп'ютері. Прикладами таких алгоритмів є алгоритм невпорядкованого пошуку в базі даних і алгоритм цілочисельної факторизації. Останній вирішує задачу розкладання числа на множники за поліноміальний час. Фактично, завдяки квантовим обчисленням ми дуже близькі до ефективного вирішення NP-повних і NP-задач, що вимагає особливої уваги до цих технологій у майбутньому.

Висновок

Квантові комп'ютери стають не лише об'єктом майбутнього, але й реальністю нашого часу, відкриваючи шлях до нових можливостей у сфері обчислень. Незважаючи на те, що класичні комп'ютери залишаються важливим елементом сучасної технологічної інфраструктури, квантові обчислення надають швидші, більш ефективні методи розв'язання певних класів завдань. Знайдення ефективних алгоритмів для певних завдань, таких як невпорядкований пошук у базах даних чи цілочисельна факторизація, демонструє потенціал цих систем. З кожним днем ми наближаємося до ефективного вирішення складних проблем завдяки квантовим обчисленням, що робить їх важливим інструментом для майбутнього розвитку сучасних технологій.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Mindthegraph [Електронний ресурс] – Режим доступу до ресурсу: https://mindthegraph.com/blog/uk/%D1%89%D0%BE-%D1%82%D0%B0%D0%BA%D0%B5-%D0%BA%D0%B2%D0%B0%D0%BD%D1%82%D0%BE%D0%B2%D1%96-%D0%BE%D0%B1%D1%87%D0%B8%D1%81%D0%BB%D0%B5%D0%BD%D0%BD%D1%8F/
2. Foxminded [Електронний ресурс] – Режим доступу до ресурсу: https://foxminded.ua/kvantove-prohramuvannia/
3. Крохмальський Т. Є. «Вступ до квантових обчислень» 2018.
4. Джон Д. Хідарі «Квантові обчислення. Прикладний підхід» 2021.

Ковальчук Василь Олександрович – студент групи 2КІ-22б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: vasya.kovalchyk20@gmail.com

Kovalchuk Vasyl O. — Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email : vasya.kovalchyk20@gmail.com