Vol. 4, No. 1, 2022

https://doi.org/.....

УДК 638.235.231; 530.145+621.142

Кособуцький П.С.
Національний університет Львівська політехніка

ФІЗИЧНІ ОСНОВИ КВАНТОВОЇ ІНФОРМАТИКИ: ВІД КВАНТОВОЇ МЕХАНІКИ, ЧЕРЕЗ КВАНТОВІ ОБЧИСЛЕННЯ ДО КВАНТОВОЇ КРИПТОГРАФІЇ

Зроблений методичний аналіз базової задачі, пов'язаний з квантовими обчисленнями параметрів фізичних систем. Зроблений акцент на фізичних принципах робота квантового комп'ютера з наголос на тому, що в квантових обчисленнях важливий одночасний доступ до усіх квантових станів, що дозволяє реалізувати одночасну зміну квантового стану із всіх суперпозицій в системі кубітів. Зроблено наголос на тому, що в квантових алгоритмах базовими є операції перетворення Фур'є і Адамара. Звернуто увагу читача на тому, що квантові обчислення перш за все реалізуються в квантових об'єктах із властивостями елементарних вентилів NOT і контрольованого CNOT, які можуть бути реалізовані на інтерферометрі Маха-Зендера з використанням явищами інтерференції фотона та обертання його вектора поляризації.

Незважаючи на прогрес звичайних комп'ютерів, потерба розвитку квантових обчислень зумовлена технологічним обмеженням із-за розмірного квантування електронного спектру та експоненційним зростанням часу обчислень класичними алгоритмами при збільшенні обсягу даних. Однак, широке застосування квантових комп'ютерів обмежене і рядом проблем. Це, перш за все, недостатня точність та висока чутливість до зовнішніх впливів, які здатні зруйнувати квантовий стан. Тому щоб підвищити точність обчислень на квантовому комп'ютері, алгоритм обчислення треба повторювати деяку кількість разів, а щоб уникнути руйнування квантових станів кубіту, застосовують низькі температури.

Ключові слова **- квантова інформація, квантові обчислення, квантова суперпозиція, заплутаність квантових об'єктів, квантовий комп'ютер.**

Вступ

Недавно [1], в Інституті кібернетики імені В.М. Глушкова НАН України (у межах Наукової ради з проблеми «Кібернетика») започатковано науковий семінар «Квантові обчислення». Перше засідання семінару відбулося в режимі онлайн 27 вересня 2022 року. Із доповіддю «Квантовий комп'ютер з точки зору фізика» виступив С. Шевченко (Харків, ФТІНТ). Він проаналізував сучасний стан проблеми створення квантового комп'ютера, та проаналізував роль в його роботи фундаментальних досліджень з квантової фізики. Квантовий комп'ютер – це засіб обчислювальної техніки, в основі якого покладені закони квантової механіки. В квантових комп'ютерах для обчислення використовуються квантові алгоритми, побудовані на квантово-механічних ефектах , як квантовий паралелелізм і квантова заплутаність.

Біти пам'яті в класичному комп'ютері, поділяються на ті, що язберігають інформацію і керовані біти, які обробляють інформацію. Керуючі біти реалізуються напівпровідниковими елементами (тригерами тощо) із двома стійкими станами такої висоти бар'єра між станами, щоб мінімізувати спонтанний перехід між ними. Ці два стани визначаються рівнями потенціалів транзисторних елементів - низький від -0.4 В до 0.4В відповідає логічному 0, а високий від 2.2В до 5.5В відповідає логічній 1 (у булевій алгебрі їм відповідають поняття «false» і «true»). Тому основний напрям розвитку мікропроцесорної техніки був пов'язаний із постійним зменшенням розмірів бар'єрних структур. Однак зменшення розмірів, супроводжувалось не лише зменшенням числа електронів, які потрібні для збереження одного біту інформації, але й підсиленням квантово-механічної поведінки електронів, що змусило змінювати алгоритмічну теорію обчислення

інформації [2] машиною Тьюрінга. Сам Тьюрінг довів, що не існує загального алгоритму, здатного визначити, завершить програма виконання поставленої задачі, чи зациклюючись буде працювати вічно. Для того, щоб це встановити, треба запустити саму программу [http://elliptic.space/]. Це пов'язано з тим, що для класичного комп'ютера із чітко визначеними детермінованими значеннями в комірках пам'яті,фазова траєкторія в координатах кількості вреалізацій 0 і 1 матиме вигляд замкнутої кривої другого порядку. В основу роботи процесора квантового комп'ютера покладена логіка квантової механіки. Тому принцип невизначеності формуватиме незамкнутий «пакет» фазових траєкторії ймовірністних значень реалізацій 0 і 1. На відміну від класичного комп'ютера, який оперує даними у двійкових розрядах із 0 та 1, квантовий комп'ютер використовує двохрівневі квантові біти (кубіти) із двома базовими станами 0 і 1, які можуть перебувати в стані суперпозиції. Стан суперпозиції представляє собою значення між 0 і 1, тому кубіт може приймати безмежно багато значень. Комірка пам'яті класичного комп'ютера об'ємом в 1 біт може лише перебувати в одному із двох станів 0 або 1. Тому якщо біт перебуває в стані 0, то він зберігає інформацію значенням 0, а якщо він перебуває в стані 1, то він зберігає інформацію значенням 1.

Квантово-механічну модель машини Тьюрінга першим запропонував в 1980 р. П.Беніофф, а С.Візнер [3] з 1970 р. понад десять років намагався опублікувати роботу, в якій обгрунтував концепцію квантового комп'ютера. В 1981 р. відомий фізик Р.Фейнман [4] сформулював фізичну основу квантових обчислень, в якій пропонує пристосувати для квантових обчислень елементарні логічні операції, що визначаються логічними зв'язками "і", "або", "ні", які в нових умовах отримали назву гейтів. Зокрема Фейнман розглядав такі гейти, як NOT, AND, EXCHANGE. З точки зору фон-нейманівської архітектури комп'ютера, в квантовому випадку принципово нової суті набуває процес вводу-виводу інформації. Елементами пам'яті є кубіти, а не біти, а логічні операції – це унітарні перетворення (унітара операція в квантовій механіці не змінює енергії), а не булеві операції класичних обчислень.Квантовий логічний елемент, ще відомий як квантовий вентиль, це базовий елемент квантового комп'ютера і використовується він для перетворення вхідних станів кубітів на вихідні за певним законом. Найпоширеніші квантові вентилі – це одинична матриця, матриця Паулі, квантове заперечення CNOT та оператор Адамара, який кубіт переводить в стан квантової суперпозиції.

Незважаючи на те, що перший квантовий алгоритм, був запропонований в [5], квантовий алгоритм для розв'язування задачі, що не мала класичного розв'язку ймовірнісним методом, був запропонований в роботі [6]. Однак, лише квантовий алгоритм П.Шора [7], відомий як алгоритм квантової факоризації, став поштовхом до подальшого розвитку квантових обчислень. Власне Шор продемонстрував набір математичних операцій для квантового комп'ютера, спроможний розкладати на прості множники великі числа майже миттєво, тобто набагато швидше, ніж це робив класичний комп'ютер. Розробивши схему кодування квантових станів, Шор також запропонував алгоритм корекції помилок.

Квантовий алгоритм факторизації став важливим із трьох причин. По-перше, саме даний алгоритм свідчив про те, що квантові комп'ютери більш ефективні, ніж класичні. По-друге, задача факторизації цікава сама по собі, так що будь-який новий алгоритм для її вирішення, чи то класичний, чи квантовий, представляє інтерес. По-третє, алгоритм факторизації дозволяв зламувати криптосистеми з відкритим ключем. Сьогодні, алгоритм Шора найвідоміший із алгоритмів для квантових технологій обробки інформації [8-9]. Відомі інші квантові алгоритми, як квантові версії Фур'є-перетворень, квантовий алгоритм Дойча, що поєднує квантовий паралелелізм із квантовою інтерференцією, алгоритми квантового пошуку і моделювання квантових систем.

Таким чином, стали формуватись основні напрямки квантової інформатики, як квантові обчислення (quantum calculating), квантові комп'ютери (quantum computing) та квантова криптографія (quantum cryptography). Квантова інформатика, на відміну від класичної інформатики, стала оперувати квантовими поняттями, досліджувати їх властивості та можливості застосування для квантових обчислень, як першочергового завдання опрацювання даних про квантові системи, в яких об'єктами досліджень єбули фізичні стани самих квантових об'єктів [10-11]. Для потреб квантової інформатики, квантові об'єкти мусять мати проявляти такі квантові властивості:

1. Мати визначені квантові стани із двома граничними рівнями (класичний аналог герба та цифри при підкиданні монети);

2. Перебувати в стані суперпозиції своїх станів до моменту вимірювання;

3. Заплутуватись (entangled states) з іншими квантовими об'єктами для створення квантової системи; Це стан квантової системи, в якому існує сильна кореляція між квантовихоб'єктами, навіть коли вони просторово розділені.

4. Задовольняти теорему про заборону клонування, що не давало можливості копіювати стан квантового об'єкту.

На відміну від класичного комп'ютера, в якому інформація зчитується методом послідовної вибірки, в квантовому випадку, зміна квантового стану одного із кубітів супроводжується миттєвою зміною станів решта кубітів, що забезпечує експоненціальне зростання швидкості виконання операцій від їх числа і вже 2019 році, компанія Google продемонструвала, що квантовий комп'ютер обчислив задачу приблизно за 200 секунд, для якої на класичному цифровому суперкомп'ютері треба було затратити понад 10 000 років.

Дана робота присвячена методологічному аналізу задач квантової інформатики в ракрусі від квантової механіки, через квантові обчислення до квантової криптографії. Такий виклад матеріалу розрахований на читачів, які вивчали обмежені ресурси з квантової механіки, квантової статистики, та інші, тобто в основу фахової підготовки кого покладені переважно комп'ютерні науки, інформатика, програмування, тощо.

Результати дослідження та їх обговорення

Сформульована задача актуальна, адже в 2022 році Нобелівська премія з фізики була присуджена А.Аспект, Д.Клаузер та А.Зайлінгер саме за досягнуті успіхи в розвитку квантової інформатики із формулюванням: *"за експерименти із заплутаними фотонами, встановлення порушення нерівностей Белла та новаторську квантову інформатику"* [12]. Тому спершу зробимо методичний аналіз базових представлень квантової механіки для задачі квантової інформатики, які в класичній ймовірнісній інтерпретації формулюються у вигляді таких постулатів:

1.Стан ізольованої системи моделюється вектором Дірака $|\psi\rangle$ та для скінченого числа станів умовою нормування $\langle\psi|\psi\rangle = 1$. Фізичний зміст цього квантового стану полягає в тому, що для нього справджується принцип лінійності, тобто якщо система може перебувати у двох різних станах, то вона може перебувати в стані, що представляє їх суперпозицію.

2.Фізичні величини, що піддаються вимірюванням, представляються операторами у відповідному просторі.

3. Еволюція ізольованої системи унітарна і обернена.

4. Операція вимірювання відбувається у відповідності до принципу невизначенності Гейзенберга. Вимірювання перетворює квантово механічну систему і оператор перетворення не унітарний, і не обернений. Адже квантовий стан може змінювати в часі лише двома прінциповими методами, унітарною квантовою операцією (квантовий вентиль (*quantum gate*)) та вмірюванням.

Насправді це не повний перелік важливих формулювань квантової механіки, однак наведені достатні для опису основних ідей квантової теорії інформації.

Початкові квантові поняття були введені ще М.Планком [13]. Планк вивчав теоретичні закономірності випромінювання абсолютно чорного тіла і довів, що отримані ним висновки теоретичних досліджень, найкраще узгоджуються з експериментальними результатами, якщо прийняти ідею про дискретний характер процесу випромінювання порціями з енергією

$$W = h\nu, \qquad (1)$$

де ν — частота хвилі, а h - деякий коефіцієнт пропорційності із значенням $h = 6.62\times10^{-34}$ Дж·с, який в подальшому названий сталою Планка, а дискретна порція енергії $h\nu$ квантом енергії електромагнітної хвилі. Тому з квантової точки зору, світло поглинається та випромінюється квантами, які ще звуться фотонами. Хоч фотонна модель краще пояснює явища, пов'язані з фотоефектом, однак хвильова модель світла частіше використовується для пояснення явищ дифракції та інтерференції. Це відомий у фізиці корпускулярно-хвильовий дуалізм.

Етапи еволюції корпускулярно-хвильового дуалізму приведені на рис.1. Ліворуч зверху зображений дослід Юнга із двома щілинами, який свідчить про те, що з картинкою на екрані спостереження можна пов'язати хвильовий процес. Теж саме проявляється, коли потік інших квантових частинок електронів пропускати також крізь дві щілини. В обох випадках проявляється

інтерференційна картина, хоч насправді електрони – це квантові (дискретні) частинки, як і фотони світла. Але якщо класична механіка для аналізу динаміки руху приймає до уваги індивідуальні властивості частинок, то квантова механіка від такого підходу відмовилась в принципі. Прояв закономірностей з точки зору квантової механіки має ймовірнісний характер, тому фізичний зміст мають їх усереднені характеристики.

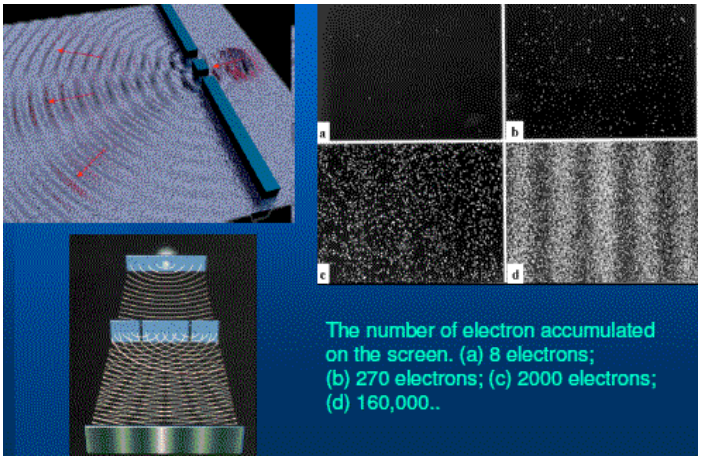

Рис. 1. Етапи еволюції корпускулярно-хвильового дуалізму

Важливий наступний крок зробив В. Гейзенберг. Він першим дійшов висновку про те, що такі класичні ньютонівські поняття як координата та швидкість, не повинні використовуватись для опису фізичних станів мікрочастинок. Гейзенберг сформулював відомі співвідношення невизначеностей які в координатному представленні мають вигляд:

$$\Delta x \cdot \Delta p_x \geq h;\ \Delta y \cdot \Delta p_y \geq h;\ \ \Delta z \cdot \Delta p_z \geq h\,. \qquad (2)$$

У відповідності до (2), в мікросвіті фраза ”імпульс частинки в точці простору з координатою x має значення p_x” не має фізичного змісту. Іншими словами, відсутні ансамблі квантових частинок, які б мали чітко визначені значення імпульсу і координати одночасно. Як переконаємось далі, співвідношення (2) фундаментальні і для квантової криптографії. Адже саме принцип невизначеності дозволяє виявити несанкціонований доступ до інформації в процесі її передачі.

Геометрична ілюстрація ролі принципу невизначеностей, зображена на рис.2 у вигляді фазового портрету динамічного стану мікрочастинки в площині декартових координат $m\dfrac{dx}{dt}, x$. Тут добуток $\Delta x \cdot \Delta p_x$ виражає площу, мінімальне значення якої дорівнює кванту дії, рівному сталої Дірака $\eta = \dfrac{h}{2\pi}$ (рис.2a). Тоді якщо в класичній фізиці траєкторію руху можна визначити як завгодно точно, тобто $S_{\min} \to 0$, то в квантовій механіці найменше значення $S_{\min}$ буде обмеженим значенням η (рис.2b).

Як ідея про кванти, так принцип невизначеностей, були використані Луї де Бройлем для обгрунтування ідеї про хвильові властивості мікрочастинок із ненульовою масою спокою. Він записав формулу

$$p_D \cdot \lambda_D = h\,, \qquad (3)$$

що пов’язує імпульс частинки з ненульовою масою спокою m_0, з довжиною хвилі де Бройля λ_D. Тому в мікросвіті, однаково важливі обидва квантові закони

$$W = h\nu \ \text{і}\ p = \eta k\,, \qquad (4)$$

які пов’язують між собою корпускулярні W, p та хвильові $\omega, \vec{k}$ властивості квантового об’єкту. Саме для рухомої мікрочастки із ненульовою масою спокою, де Бройль ввів комплексну

псі-функцію координат і часу $\Psi(\vec{r},t)=\Psi_0 e^{-\frac{i}{\eta}(W\cdot t-\vec{r}\cdot\vec{p})}$, де множник Ψ_0 обчислюється із умови нормування $\int \Psi\cdot\Psi^* dV=1.$

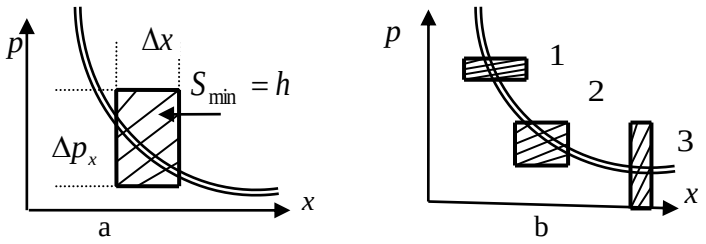

Рис. 2. Геометрична ілюстрація ролі принципу невизначеностей

Ймовірнісну інтерпретацію функції $\Psi(x,y,z,t)$ дав М.Борн. За Борном: *Хвильова псі-функція не фізичне поле, а поле інформації, а її квадрат* $|\Psi|^2=\frac{dP}{dV}$ *визначає густину ймовірності* dP *перебування мікрочастинки в деякому околі* dV *заданої точки простору.* Отже, псі-функція – це функція інформації, а фізичний зміст має її квадрат $|\Psi(x,y,z,t)|^2$ - ймовірність локалізації частинки в квантовому стані:

$$d\mathrm{P}=|\Psi(x,y,z,t)|^2\,dxdydz\,. \tag{5}$$

В (5), функція $\Psi(x,y,z,t)$ записана в просторово-часовому представленні, а для стаціонарного стану, вона має вигляд $\psi(x,y,z)$. Хвильова функція – це хвиля інформації, тому фізичний зміст має її квадрат. На відміну від самої псі-функції, її квадрат $|\Psi|^2$, як фізична величина, виражає достовірність спостережуваної події і завжди додатна, тоді як сама ψ може бути і від'ємною. Наявність уявної одиниці "i" не викликає протиріччя, оскільки ймовірність частинку в об'ємі V дорівнює інтегралу $\mathrm{P}=\int_V d\mathrm{P}=\int_V |\Psi|^2 dV$. Ймовірнісний характер псі-функції дозволяє обчислювати середні значення фізичних величин як

$$\langle \mathrm{A}\rangle=\int|\psi(r)|^2\,\mathrm{A}(r)d^3r=\int\psi\psi\cdot\mathrm{A}(r)d^3r=\int\psi\cdot\mathrm{A}(r)\psi d^3r\,. \tag{6}$$

В подальшому, завдяки ідеї Луї де Бройля про хвильові властивості мікрочастинок із ненульовою масою спокою, Е.Шредінгер сформулював хвильове рівняння, в якому стан мікрочастинки описується хвильовою псі-функцією $\Psi(x,y,z,t)$. Шредінгер аналізуючи процес квантово механічного вимірювання, формулює чотири основні положення про стан об'єктів квантового світу із такими властивостями:

1. *Суперпозиція квантових станів*. Стани описуються лінійною суперпозицією базисних векторів.

2. *Інтерференція квантових станів.* Результат вимірювань від відносних фаз амплітуд в цій суперпозиції.

3. *Entanglement ("заплутування") квантових станів*. Це таке квантово-механічне явище, при якому квантові стани двох або більшої кількості об'єктів є взаємозалежними. Такий взаємовлив зберігається навіть якщо квантові об'єкти просторово рознесені. Вимірювання параметру одного квантового стану миттєве руйнує усі сплутані квантові стани. Така поведінка не узгоджується з принципом локальності, проте не порушує теорії відносності, оскільки при цьому не відбувається передавання інформації із груповою швидкістю, що перевищує швидкість світла. Із-за складності розуміння цього квантового явища, обмежились дві моделями заплутаності. Перший метод її моделювання – це коли квантові об'єкти просторово розділені так, що причинно-настідковий зв'язок мінімізується. Цей підхід відомий як модель тензорного добутку. Але не завжди можна переконатись, що така ізоляція реалізована. Тому був запропонований інший метод моделювання заплутаності, в якіому вважається, що вона існує, коли властивості ізольованих квантових частинок

корелюють, але послідовність поведення вимірювань не відіграє ролі. Ця модель ще називається заплутаністю із комутуючим оператором.

4. *Неклонованість та невизначеність*. Неможливість клонування невідомого квантового стану була доказана теоремою в [14], яка виявила зв'язок із неможливістю миттєвої передачі інформації. З іншої сторони, якщо б було можливе клонування, то існувала б суперечність між квантовою механікою та спеціальною теорією відносності.

Невідомий квантовий стан не можна клонувати, та спостерігати без його зміни. Якщо перші два положення досить широко обговорювались в квантовій механіці, то на третє третє та четверте положення звернуто увагу лише при дослідженні парадоксу Ейнштейна-Подольского-Розена [15], пов'язаного з квантовими кореляціями між квантовими станами та пов'язаної з парадоксом нерівності Белла [16]. В 1960-тих роках фізик Д. Белл придумав перевірку у вигляді ігри, результат якої дозволяв дати відповідь на питання, чи заплутаність – це реальне фізичне явище, чи це прсто теоретична ідея. Це так звані «нелокальні» ігри.

Порушення нерівностей Белла було підтверджене дослідами Аспекта [17], що зняло підозру про невиконання базових постулатів квантової механіки. Вияснилось, що необхідною умовою порушення нерівності Белла є неможливість факторизації квантового стану із-за їх заплутаності. Адже на відміну від класичних бітів, між кванновими бітамм існує зв'язок – квантова кореляція, завдяки якій нема потреби використовувати в квантових обчисленнях експоненціально зростаючих розмірів матриці.

Важливе у квантовій фізиці поняття про ймовірність було введено ще Максвеллом в роботі "Пояснення до динамічної теорії газів" (1860 р.). В ній методом найменших квадратів, Максвелл обгрунтував ймовірнісний закон розподілу молекул за швидкостями та дійшов висновку, що "швидкості розподіляються між частинками за тим самим законом, за яким розподіляються похибки між даними спостережень та результатами теоретичних розрахунків. Пізніше ці ідеї використав Больцман для обгрунтування ймовірнісної суті ентропії, поняття про яку К.Шеннон [2] використав в 1948 році в статті "*A Mathematical Theory of Communication*" для кількісного опису інформації:

$$H = -\log_2 P. \qquad (7)$$

В підході (7), інформаційна ентропія - це міра зняття невизначенності, ще відома як 'неентропія'. Інформаційна за Шеннонном ентропія, була Сциллардом узагальнена на фізичні системи. За одиницю інформаційної ентропії, Шеннон взяв невизначеність при киданні монети, яку назвав *біт* (bit - абревіатуре від binary digit), оскільки бінарна подія з рівноймовірними результатами має ентропію $\log_2 2=1$ *біт*. Подібно цьому, можна розглянути один *трiт* із рівно імовірними значеннями $\log_2 3 \sim 1.58496$ *бітів* інформації, як одне з трьох значень. Логарифмічна оцінка кількості інформації, дозволяє кількість інформації від кількох об'єктів складати адитивно. Адже якщо декілька об'єктів розглядати як один, то кількість можливих станів $C=2^N$ перемножується і не важливо, чи йде мова про випадкові величини в математиці, чи про регістри цифрової пам'яті в техніці чи про квантові системи у фізиці. Тепер коротко розглянемо класичне і квантове представлення бітових станів та базових операцій над ними.

Класичні комп'ютери оперують із бітами інформацій, а квантові комп'ютери оперують із квантовими бітами (кубітами). Кубіт – це квантовий елемент із дворівневою системою, який може існувати в станах, що відповідають логічним 0 або 1, але й в змішаному із них. Це стан так званої квантової суперпозиції, завдяки якому в системі між двома і більше кубітами, виникає своєрідний зв'язок між ними - так звана заплутаність квантових станів. Фізичним об'єктом, яккий би відповідав двом граничним станам кубіту, може бути основний та збуджений стан атома, спин атомного ядра, (спин за полем – логічний 0 або проти поля – логічний 1), поляризований стан фотона,фотон в ловушці, напрямок струму в надпровідному кільці [18]. Так, якщо фізичним носієм кубіта є поляризація фотона, то випадкова двійкова послідовність символів 0 і 1 кодується напрямками поляризації одиночного фотона,якими можна керувати та вимірювати. У прямокутному базиці 0 або 1 кодується горизонтальним та вертикальним напрямками поляризації фотона, а в діагональному – з нахилом підкутом 45^0 та 135^0 . До вимірювання, інформація знаходиться у кубітах і лише після вимірюваня перетворюється у звичайні біти.

Кубіт можна визначити як вектор одиничної довжини в двовимірному гільбертовому просторі. В ньом для запису двох станів кубіту використовують вектори Дірака - кет-вектори (половинка від англійського слова «дужка $(braket = \langle bra | + | ket \rangle)$ », який ще в квантовій механіці

ототожнюють із вектором-стовпцем. Таким чином, кет вектор $|0\rangle$ описує нульовий стан кубіту, а кет-вектор $|1\rangle$ описує одиничний стан кубіту: $|0\rangle = \begin{bmatrix}1\\0\end{bmatrix}$ і $|1\rangle = \begin{bmatrix}0\\1\end{bmatrix}$. Це так звані чисті, базисні стани кубіту.

Однак кубіт, як одиниця вимірювання в квантовій інформатиці, може перебувати в стані суперпозиції, хвильова функціяя кубіта в якому може бути записана як кет-вектор у вигляді лінійної комбінації $|0\rangle$ і $|1\rangle$:

$$|\psi\rangle = c_0|0\rangle + c_1|1\rangle,\ |c_0|^2 + |c_1|^2 = 1. \tag{8}$$

де $|c_0|^2 + |c_1|^2 = 1$ - умова нормування для обчислення множників $c_{0,1}$, доданки якої виражають ймовірності знайти кубіт у відповідному граничному стані, тобто або $|0\rangle$, або $|1\rangle$. Тому результат вимірювань є $|0\rangle$, або $|1\rangle$ з відповідними ймовірностями. В стані суперпозиції кубіт перебуває лише до його вимірювання. Після вимірювання на кінцевому етапі квантових обчислень, ми маємо можливість отримати відповідь на питання, з якою ймовірністю ми матиме нулі чи одиничи. Так, якщо кубіт перебуває в квантовому стані $|\psi\rangle = \frac{4}{3}|0\rangle + \frac{\sqrt{7}}{3}|1\rangle$, то ймовірність одержати при вимірюванні нульове значення дорівнює: $\left|\frac{3}{4}\right|^2 = \frac{9}{16} \cong 51\%$, а одиницю - $\left|\frac{\sqrt{7}}{3}\right|^2 = \frac{7}{16} \cong 49\%$. Тому, якщо під час вимірювання кубіту нульове значення одержано з ймовірністю $\cong 51\%$, то оскільки процесом вимірювання даний стан зруйнований, то кубіт переходить у новий квантовий стан $1\cdot|0\rangle + 0\cdot|1\rangle$ і при повторному вимірюванні кубіту, нульове значення вже одержимо із 100% ймовірністю.

Часто для геометричної ілюстрації просторового уявлення про векторні стани кубіту використовують так звану сферу Блоха (рис.3), для якої представлення (8) запишеться як:

$$|\psi\rangle = cos(\theta/2)|0\rangle + e^{i\varphi}\sin(\theta/2)|1\rangle,\ |cos(\theta/2)|^2 + |\sin(\theta/2)|^2 = 1,\quad 0 \langle \pi,\quad 0 \le \varphi\langle\pi \tag{9}$$

де $e^{i\varphi}$ - фазовий множник, який на квантовий стан кубіту і на результати вимірювань не впливає, тому ним інколи нехтують. На полюсах поверхні сфери локалізовані чисті стани кубіту $|0\rangle$ і $|1\rangle$. Коли кубіт перебуває в стані суперпозиції, то на сфері Блоха цьому стану відповідає вектор, що відхилений на кут θ. Обертання навколо осі Z описується кутом φ, і відповідає він за зміну фази кубіту φ. Таким чином окремому стану кубіту відповідає окрема точка на поверхні сфери.

Решта поверхні сфери Блоха недоступна класичному біту. Тому квантові стани кубіту представляються матрицями:

$$|0\rangle = \begin{bmatrix}1\\0\end{bmatrix},\qquad |1\rangle = \begin{bmatrix}0\\1\end{bmatrix},\qquad \begin{bmatrix}1/\sqrt{2}\\1/\sqrt{2}\end{bmatrix},\qquad \begin{bmatrix}1/\sqrt{2}\\-1/\sqrt{2}\end{bmatrix},\qquad \begin{bmatrix}1/\sqrt{2}\\i/\sqrt{2}\end{bmatrix}. \tag{10}$$

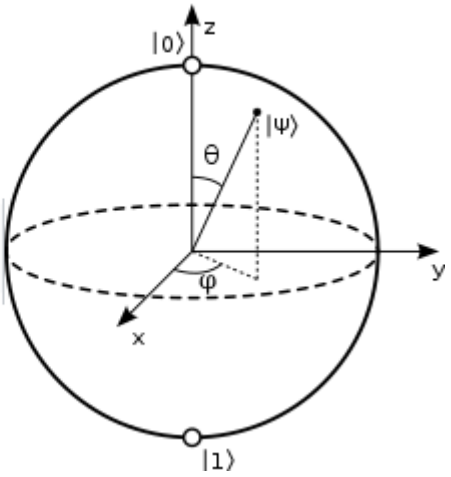

Рис. 3. Сфера Блоха

Операції з матрицями відповідають повороту вектора на сфері, а матриці, що відповідають операціям над кубітами, називаються унітарними. Унітарність – це операція, для якої існує обернена операція, яка з точки зору повертання вектору означає, що завжди вектор можна повернути у вихідний стан. Тому квантові ґейти мають бути оборотними. Щоб створити стан суперпозиції двох квантових станів $|0\rangle$ і $|1\rangle$, кожний із яких є носієм 1 біту інформації (8), використовують відомий унітарний гейт Адамара $H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$. Дія оператора H приводить кубіт в стан суперпозиції,в якому він рівноймовірно може перейти в один із станів:

$$\begin{cases} H \cdot |0\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) = |+\rangle \\ H \cdot |1\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}\begin{bmatrix} 0 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right) = |-\rangle \end{cases}, \text{ де } |c_0|^2 = |c_1|^2 = \frac{1}{2}. \qquad (11)$$

Якщо гейт Адамара застосувати двічі, то отримаємо вихідний стан. Отже, дія оператора Адамара на кубіт в стані $|0\rangle$, переводить його в стан $|+\rangle$ між станами $|0\rangle$ і $|1\rangle$ в одній половині сфери, а дія оператора Адамара на кубіт в стані $|1\rangle$, переводить його в стан $|-\rangle$ між станами $|0\rangle$ і $|1\rangle$ в іншій половині сфери. У першому випадку, векто повертається проти годинникової стрілки на 90^0 в площині ZX, а в другому – симетрично за годинниковою стрілкою.

В квантовій інформатиці, перетворення Адамара ще називають вентилем Адамара. На ньому побудована математична модель роботи генератора випадкових чисел. Для цього створюється кубіт в стані $|0\rangle$, потім до нього застосовується перетворення Адамара, після чого при вимірюванні даного кубіту значення $|0\rangle$ або $|1\rangle$ з'являться з однаковими ймовірностями. Повторивши процес n разів, ми отримаємо випадкове число в межах від 0 до $2^n - 1$, ще відоме як число Мерсена. Отже, якщо в класичному комп'ютері випадковість імітується детермінованим обчисленням, то в квантовому випадку вона пов'язана з фізикою самого обчислювача. Так, квантова механіка за своєю природою ймовірністна, а вимірювання – це єдиний засіб для одержання даних про квантовий стан кубіту. Тому в результаті вимірювання кубіт миттєво колапсує і будуть втрачені коефіцієнти, якими характеризують його попередній стан.

З іншої сторони, кубіт із двома ортогональними станами $|0\rangle$, $|1\rangle$ представляє собою дворівневу квантову систему. В класичних комп'ютерах на транзисторних схемах, реалізується нелінійна залежність між вхідною та вихідною напругами, на яких формується бістабільний

елемент. Так, якщо низькій вхідній напрузі співставити логичний "0", то високій вхідній напрузі відповідатиме логічна "1" і навпаки. У випадку дворівневої квантової системи, стану з енергією $W_0, |\psi_0\rangle$ можна приписати логічному $0 \equiv |0\rangle$, а збудженому стану $W_1, |\psi_1\rangle$ відповідатиме логічна $1 \equiv |1\rangle$. Отже, бістабільному переходу $0 \to 1$ в транзисторній схемі, в квантовій відповідатиме перехід між квантовими рівнями.

Квантова суперпозиція квантових станів системи бістабільних кубітів заплутує їх, як це записано для двох кубітів (12). Суть цього полягає в тому, що кожний із кубітів в системі вже не можна розглядати окремо, так як стан тепер спільний. Суть цього полягає в тому, що окрім квантової інтерференції, як фізичної основи існування одинокого кубіту (8), в системі кубітів виникає явище заплутаності між квантовими станами. Так, якщо є два кубіти із початковими векторами $|0\rangle$ та $|1\rangle$, після вимірювання кубіти можна виявити в чотирьох різних комбінаціях із ймовірностями $|c_{00}|^2, |c_{01}|^2, |c_{10}|^2, |c_{11}|^2$:

$$|\psi\rangle = c_{00}|00\rangle + c_{01}|01\rangle + c_{10}|10\rangle + c_{11}|11\rangle,\ |c_{00}|^2 + |c_{01}|^2 + |c_{10}|^2 + |c_{11}|^2 = 1, \qquad (12)$$

де $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ базисні орти двокубітної системи. В стані $|00\rangle$ обидва кубіти при вимірюванні дають результат $|0\rangle$. В стані $|01\rangle$ - перший кубіт при вимірюванні дає значення $|0\rangle$, а другий - $|1\rangle$; $|10\rangle$ - перший кубіт при вимірюванні дає значення $|1\rangle$, а другий при вімірюванні дає значення $|0\rangle$; $|11\rangle$ - обидва кубіти при вимірюванні дають результат $|1\rangle$. Кількість проміжних станів для системі із трьох кубітів вже дорівнює 2^3 і т.д.

Якщо квантовий регістр із двох кубітів перебуває в базовому стані $|0\rangle$, то подіявши перетворенням Адамара на перший кубіт, отримаємо стан регістру:

$$H|00\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) \times \left(1|0\rangle - 0|1\rangle\right) = \frac{1}{\sqrt{2}}\left(|00\rangle + |10\rangle\right). \qquad (13)$$

Так як кубіт представляє собою векторний простір, то в (13) використане тензорне перемноження, як спеціальна операція створення нового квантового стану двох і більше кубітів, що створює новий векторний простір із окремих векторних просторів перемножуваних між собою матриць (Microsoft Quantum бібліотеки дозволяють виконувати складні квантові алгоритми без необхідності детально вникати в відповідну математику).

Обидва кубіти в даному регістрі незалежні один від одного. Другий кубіт до цього часу перебуває в стані $|0\rangle$ і якщо ми його виміряємо, то все одно не одержимо інформації про стан першого кубіту, оскільки перший кубіт перебуває в змішаному стані суперпозиції. Приклад найпростішої квантової заплутаності двох кубітів має вигляд:

$$|\psi^+\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}},\ |\psi^-\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}},\ |\phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}},\ |\phi^-\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}}. \qquad (14)$$

Ці пари відомі як пари Ейнштейна-Подольского-Розена, авторів заплутаності, які в подальшому розвинув Белл.

Ефект заплутаності відображається в логічних операціях. Так, якщо однокубітна логічна операція NOT перетворює інформацію як:

$$NOT:\ |\psi\rangle \to NOT:\ (c_0|0\rangle + c_1|1\rangle) = c_0|1\rangle + c_1|0\rangle, \qquad (15)$$

тобто переставляє місцями вагові коефіцієнти і кванновим аналогом класичного NOT-гейта є матриця $X \equiv \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ то двокубітний контрольований гейт $CNOT$ (англ. *Controlled NOT*) заплутує стани кубітів за схемою:

$$|00\rangle \to |00\rangle, \quad |01\rangle \to |01\rangle, \quad |10\rangle \to |11\rangle, \quad |11\rangle \to |10\rangle. \tag{16}$$

Отже, якщо перший квантовий біт 1, то змінюється другий квантовий біт.

В системі із двох вхідних кубітів на вході і двох кубітів на виході, один із пари кубітів називається контролюючим, а один із другої пари – контрольованим (або кубітом-мішенню). Тоді операції виконуться за такою схемою: якщо контролюючий кубіт перебуває в стані $|1\rangle$, то контрольований кубіт піддається квантовій операції NOT, інакше контрольований кубіт залишається без змін.

Квантові обчислення на квантових об'єктах із властивостями елементарного вентиля NOT і контрольованого CNOT, можуть бути реалізовані на інтерферометрі Маха-Зендера з використанням явищами інтерференції фотона та обертання його вектора поляризації. Нагадаємо, що для квантової інформатики фотон зручний тим, що вакуум, в якому він поширюється, не змінює його властивостей, перш за все для фотона у вакуммі відсутнє явище дисперсії, чого не можна сказати про навколишню атмосферу Землі. Детальніше, про заплутування фотонів для квантових обчислень, планується обговорити в окремій статті.

Квантовий алгоритм є класичним алгоритмом, що задає послідовність унітарних операцій із зазначенням кубитів, над якими їх треба здійснити. Квантовий алгоритм задається або у вигляді словесного опису таких команд, або за допомогою їхнього графічного запису у вигляді системи вентилів. Найбільш близьким класичним аналогом квантового обчислення є імовірнісне обчислення, тобто правильність результату роботи квантового алгоритму визначено з деякою ймовірністю. Для підвищення ймовірності правильного результату в квантових алгоритмах спеціально збільшується кратність операцій, які підбираються таким чином, щоб неправильні результати з великою ймовірністю взаємно знищувалися, і ймовірність правильного результату збільшувалася. Переваги квантових алгоритмів полягає в зниженні часу вирішення задачі за рахунок розпаралелювання операцій шляхом генерування заплутаних квантових станів та їх подальшого використання. Такі випадки називають квантовим паралелізмом.

Якщо кубіти перебувають в заплутаному стані, то вимірювання довільного із них супроводжується коллапсом іншого. Тому вимірявши стан одного із кубітів, ми миттєво отримуємо інформацію про стан іншого. Якщо система складається із n кубітів, то завдяки заплутаності одноактним вимірюванням, маємо можливість забезпечити одночасну обробку 2^n квантових станів. Цей колективний характер поведінки взаємодіючих кубітів є основою квантових обчислень, які не реалізуються в звичайному комп'ютері.

Результат роботи квантового комп'ютера має ймовірністний характер, тому для досягнення правильного результату з ймовірністю максимально наближеною до 100%, треба максимально заплутати квантові стани в системі кубітів. Це досягається шляхом повторювань однотипних квантових обчислень і одна з вимог до квантового комп'ютера полягає в тому, щоб як найдовше кубіт зберігав свій когерентний стан, тобто щоб як найменше піддавався зовнішнім впливам. Задовільним вважається квантовий стан, в якому когерентність зберігається на два порядки довше часу одної логічної операції.

Така принципова відмінність від класичного процесу вимірювання називається квантовим паралелізмом. Квантовий паралелізм трактують так: «Дані в процесі обчислення представляють собою квантову інформацію, яка по завершенні перетворюється в класичну шляхом вимірювання кінцевого стану квантового регістра. Виграш в квантових алгоритмах досягається тим, що при застосуванні одної квантової операції велика кількість коефіцієнтів суперпозиції квантових станів, які у віртуальній формі мають класичну інформацію, перетворюється одночасно».

Спрощена блок-схема квантового комп'ютера (процесора) приведена на рис.4. Квантовий процесор або кубітний процесор – це обчислювальний прилад, який виконує квантові логічні операції, що не руйнують квантову когерентність (суперпозицію) до завершення квантових обчислень. На початковому етапі всі кубіти переводяться у основний стан $|0\rangle$, тому система із n

кубітів в стані $|0\,0...0\rangle$ відіграє роль регістра пам'яті для запису вхідних даних та проведення обчислень. Регістр квантового комп'ютера являє собою набір деяким чином заплутаних кубітів, і цей взаємозв'язок забезпечує можливість виконання операцій одночасно над усіма станами кубітів, внаслідок чого при кожній зміні стану одного з декількох кубітів інші змінюються узгоджено з ним. Тому важливою властивістю регістра квантового процесора є забезпечення когерентної інтерференції між кубітами, тобто квантовий паралелізм. Саме квантовий паралелізм є головною відмінністю та перевагою квантових обчислень від класичних.

Після того, як кубіти переведені у початковий стан, над здійснюється унітарне перетворення, яке переводить кубіти в інший квантовий стан, який вимірюється на завершальному етапі квантового обчислення. Вимірювання квантового стану $|\psi\rangle$ кубіта полягає в обчисленні ймовірністних множників $c_0 = \left|\langle 0|\psi\rangle\right|$ і $c_1 = \left|\langle 1|\psi\rangle\right|$. Керування станами кубіта, здійснюється :

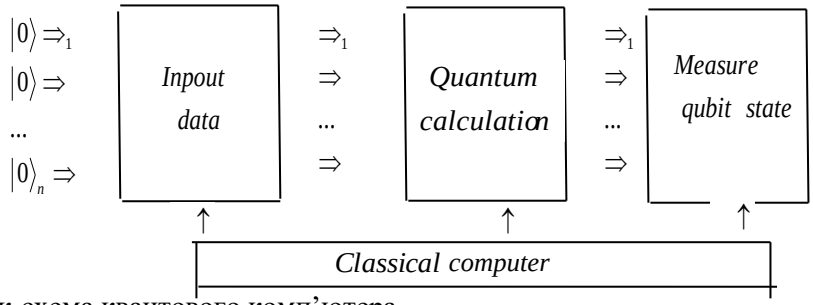

Рис. 4. Блок-схема квантового комп'ютера

генератором імпульсів класичного комп'ютера. Така концепція квантового процесора і квантових логічних операцій була запропонована ще в 1989 році Дойчем.

На кубітних технологіях побудована квантова криптографія. Квантова криптографія – це розділ квантової інформатики, що вивчає методи захисту інформації шляхом використання квантових носіїв. Можливість подібного захисту забезпечується фундаментальною теоремою про неможливість клонування невідомого квантового стану. Формування цього напрямку квантової інформатики, розпочалось ще з досліджень С. Візнера [3] після того, як методи класичної криптографії вже стали не задовольняти зростаючим вимогам до швидкості передачі інформації, рівня її безпеки та захищеності. Перш за все виникла потреба мінімізувати несанкціонований сторонній доступ до інформації. В класичній криптографії, для цього застосовують шифрування інформації: повідомлення за допомогою деякого алгоритму комбінується з додатковою секретною інформацією (ключем), в результаті чого споживачеві передається криптограма. Тому для надійності, треба щоб ключ був відомий лише для шифрування і дешифрування повідомлення.

Тут ще раз доречно нагадати про обмеження, які квантова механіка накладає на маніпуляції з квантовими об'єктами. Фундаментальним є невизначеність Гейзенберга, яка постулює неможливість одночасного вимірювання координати та імпульсу частинки з довільною точністю. Постулат про редукування хвильового пакету, висунутий фон Нейманом, вказує на неможливість в загальному випадку вимірювання квантової системи без руйнування її стану. Відкритий у 1982 р. принцип квантової неклонованості стверджує, що неможливо створити копію (клон) квантової системи як завгодно близько до оригіналу. З практичної точки зору ці та подібні до них обмеження тривалий час мали негативний характер, показуючи, що при досягненні певної точності в роботі апаратури виникають додаткові складності, пов'язані з квантовою природою фізичних об'єктів, такі як «квантовий шум» оптичного каналу зв'язку, «квантовий шум» фотодетектора тощо.

У 1949 р. С. Шеннон, спираючись на розроблену ним теорію інформації, довів теорему, що криптосистема є абсолютно секретною, якщо секретний код істинно випадковий та використовується лише один раз. Однак на практиці проблематично створити та передати секретний код, адже його треба надавати кожного разу, коли надсилається нове повідомлення. Вирішити цю проблему можна за допомогою квантової фізики. Хоч в цьому напрямку перший крок зробив Візнер ще в 1970 році, розв'язати проблему захисту інформації вдалось лише Ч. Беннету та Ж. Бассарду [19-20], які запропонували протокол квантового розподілу ключа (quantum key distribution).

Квантовий розподіл ключа - це метод передачі ключа на основі квантового явища. Вони відкинули ідею створення алгоритмів на основі математичних законів, які завжди можна розшифрувати, а запропонували застосовувати для передачі сигналів квантові стани мікрочастинок, як фотон. Але детальніше, квантові алгоритми обчислень, квантове шифрування як і квантова телепортація, планується розглянути окремо. А зараз, на завершення приведемо порівняльний аналіз базових характеристик звичайних і квантових комп'ютерів, представлений в таблиці 1.

Таблиця 1. Порівняння між звичайним і квантовим комп'ютерами

	Звичайний комп'ютер	**Квантовий комп'ютер**
Логіка	0 / 1	a|0> + b|1>, a^2+b^2=1
Фізика	Напівпровідниковий транзистор	Квантовий об'єкт
Носій інформації	Рівні напруги	Поляризація, спін,…
Операції	NOT, AND, OR, XOR над бітами	Вентилі: CNOT, Адамара,… над кубітами
Взаємозв'язок	Напівпровідниковий чіп	Заплутаність станів
Алгоритми	Стандартні (Кнут)	Спеціальні (Шор, Гровер)
Принцип	Цифровий, детермінований	Аналоговий, ймовірнісний

З точки зору організації підготовки фахівців з квантової інформатики, автор погоджується з думкою доцільності організації навчальних курсів, як: - «Фізичні основи квантової інформатики»; – «Математичні основи квантової інформатики»; – « Квантові алгоритми та програмна реалізація», приймаючи до уваги практичні можливості, що представляються IBM Q Experience (quantum-computing.ibm.com), залучаючи для цього можлиовсті комп'ютерної математики SageMath на Jupyter Notebook у середовищі CoCalc https://cocalc.com/app).

Висновки

Квантові комп'ютери спроможні виконувати більш складніші обчислення параметрів фізичних систем, в тому числі із застосуванням методів Монте-Карло. Це зумовлено тим, що в квантових обчисленнях можливий одночасний доступ до усіх квантових станів, що дозволяє реалізувати одночасну зміну квантових станів всієї суперпозицій в системі кубітів. Квантові обчислення грунтуються перш за все на реалізаціях в квантових об'єктах властивостей елементарних вентилів NOT і контрольованого CNOT, які можуть бути реалізовані на інтерферометрі Маха-Зендера з використанням явища інтерференції фотона і обертання його вектора поляризації. Незважаючи на прогрес звичайних комп'ютерів, потерба розвитку квантових обчислень зумовлена технологічним розмірним квантуванням електронного спектру та експоненційним зростанням часу обчислень класичними алгоритмами при збільшенні обсягу даних.

Однак, широке застосування квантових комп'ютерів обмежене рядом проблем. Це недостатня точність та висока чутливість до зовнішніх вливів, які здатні зруйнувати квантовий стан. Щоб підвищити точність обчислень на квантовому комп'ютері, алгоритм обчислення повторюють потрібну кількість разів. Щоб уникнути руйнування квантових станів кубіту, застосовують низькі темпертури. Більш детально, читач може ознайомитись із базовими принципами організаціїї квантових обчислень, звернувшись до джерел інформації [21-30], в тому числі методичного плану. Однак, незважаючи на труднощі, є надія, що квантові обчислювальні технології призведуть до наступного технічного прориву. Адже за своєю суттю, вони є вершиною розвитку паралельних обчислень, тому здатні успішно вирішити задачі, що пов'язані з

моделюванням складних природних процесів, оптимізації молекулярних структур в фарамакології, квантових систем, тощо.

Для набуття практичних навиків управління квантовим комп'ютером та обчислень квантовими алгоритмами, можна скористатись ,інструментарієм SDK Qiskit від IBM (quantum-computing.ibm.com; qiskit.org). Відомі квантові алгоритми – алгоритм Шора, алгоритм Гровера, алгоритм Дойча-Йожи, та квантової телепортації можна реалізувати використовуючи бібліотеки Python із зверненнями до інструментарію Qiskit, Cirq, PennyLane, TensorFlow,Quantum. Популярність мови програмування Python не могла обійти популярний комплекс для розробки квантового забезпечення – Qiskit . Тому IBM запустила двотижневий курс The Qiskit Global Summer School 2021, який складається із 20 лекцій та 5 лабораторних робіт. Мінімальні вимоги - це знання базових операцій над матрицями та уміння програмувати мовою Python. Підтримку самих популярних квантових мов і пакетів SDK, як Q#, Qiskit та Cirq, представляє Azure Quantum. Корисними є сервіси: https://www.zhinst.com/europe/en/quantum-computing-systems/labone-q?gclid=Cj0KCQiAmaibB; https://qiskit.org; https://pennylane.readthedocs.io. Організувані курси «Quantum School for Young Students» для студентів[Quantum Information Science: Making the Leap. – September 25, 2018. https://www.nist.gov/blogs/taking-measure/quantuminformation-science-making-leap; .Quantum program for high school students gets a new name, gears up for hybrid learning. https://uwaterloo.ca/institute-forquantum-computing/news/quantum-program-high-school-students-getsnew-name-gears] та «Quantum Computing as a High School Module» [https://arxiv.org/pdf/1905.00282.pdf] для шкіл. Більш практичний курс з квантових обчислень пропонує IBM (зареєструватися на платформі IBM Quantum можна за наявним обліковим записом Google) в межах проєкту Qiskit Foundation [https://qiskit.org/textbook/preface.html]. Настільною книгою для навчання може бути: *Кайзер С., Гранад К. К15 Изучаем квантовые вычисления на Python и Q# / пер. с анг. А. В. Логунова. – М.: ДМК Пресс, 2021. – 430 с.* [https://dmkpress.com/files/PDF/978-5-97060-935-4.pdf]

Література

1. Шевченко С. Квантовий комп'ютер: стан проблеми у світі та в Україні. Стенограма доповіді на засіданні Президії НАН України 8 грудня 2021 року. http://dspace.nbuv.gov.ua /bitstream/handle/123456789/ 185014/07-Shevchenko.pdf?sequence=1

2. Shannon C. Collected Papers / Edited by N.J.A Sloane and Aaron D. Wyner. — IEEE press, 1993. — 923 с. — ISBN 0-7803-0434-9.

3. Weisner S. Association for Computing Machinery, Special Interest Group in Algorithms and Computation Theory. 1983. Vol. 15, 78—83; Conjugate coding. Sigact News 15, 78-88 (1983)**.**

4. Feynman R. Simulating physics with computers. Int. J.Theor.Phys.21,467 (1982). 5.Deitsh D. Quantum theory, the church-turing principle and the universal quantum computer.Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences, vol.400, no1818, 97117, Jul.1985. https://doi.org/10.1098/rspa.1985.0070;

5. D. Deutsch. Uncertainty in quantum measurements. Phys. Rev. Lett., 50(9):631–633, 1983; D. Deutsch, A. Barenco, and A. Ekert. Universality in quantum computation. Proc. R. Soc. London A, 449(1937):669– 677, 1995.;D. Deutsch. Quantum theory, the Church-Turing Principle and the universal quantum computer.Proc. R. Soc. Lond.A,400:97, 1985.;

6. D.Deutsch.Quantum computational networks.Proc.R.Soc.London A, 425:73, 1989. 6.Simon D. On the power of quantum computation. In Proceedings, 35th Annual Symposium on Foundations of Computer Science, pages 116–123, IEEE Press, Los Alamitos, CA, 1994;

7. On the power of quantum computation. SIAM J. Comput., 26(5):1474–1483, 1997. 7. Shor P. Algorithms for quantum computation: discrete logarithms and factoring / Foundation of Computer Science, 1994 Proceedings, 35th Annual symposiumon. – 1994. – pp.124-134**.**

8. Elani Z. Qubit, Quantum Entanglement and all that:Quantum Computing Made Simple. https://www.academia.edu/41804659/Qubit_ Quantum _Entanglement_and_all_that_ Quantum_ Computing_Made_Simple.

9. Ye Z., Lu Y. Quantum science: a review and current research trends . Journal of Management Analytics . Volume 9, 2022 - Issue 3.383-402.

10. Kitaev A., Shen A., Vyalyi M.. Classical and Quantum Computation. Graduate Studies in Mathematics Vol.47. American Mathematical Society Providence, Rhode Island. https://www.ams.org/books/gsm/047/gsm047-endmatter.pdf.

11. Benenti G., Casati G., D., Chapter 3 of: *Principles of Quantum Computation and Information*, World Scientific 2018 (doi:10.1142/10909, 2004 pdf).

12.All Nobel Prizes 2022 - NobelPrize.org.

13. Berkeley Physics Course: Wichmann E. Quantum Physics.v.4 McGraw-Hill Boo k Company ; Reif F. Statistical Physics.v.5 McGraw-Hill Book Company .

14. Wooters K., Zurek H. A single quantum cannot be cloned. Nature. 1982. – Vol. 299, 802.

15. Einstein A., Podolsky B., Rosen N. Can Quantum-Mechanical Description of Physical Reality Be Considered Complete? . Phys. Rev. / G. D. Sprouse. American Physical Society, 1935. Vol. 47, Iss. 10,777–780. ISSN 0031-899X; 1536-6065 — doi:10.1103/PHYSREV.47.777.

16. Bell J. On the Einstein Podolsky Rosen paradox Physics. G.D. Sprouse – American Physical Society, 1964. – Vol.1 – Is.3, 195-200.

17. Aspect A. et.al.Experimental test of Bell`s inequalities using time-varying analyzers. Phys.Rev. Lett. 1982,v.49,1804-1807.

18. А.Н. Омельянчук, Е.В. Ильичев, С.Н. Шевченко. Квантовые когерентные явления в джозефсоновских кубитах. Киев: Наукова думка.. 2013.

19. Bennett C., Brassard G. et al. Teleporting of unknown quantum state via classical and Einstein-Podolsky-Rosen channels. Phys. Rev. Lett.Vol.70. –13 – 1993.

20. Bennett C.Quantum cryptography using any two nonorthogonal states", Phys. Rev. Lett. 68, 3121-3124 (1992)].

21. Grover L.Quantum Mechanics helps in searching for a needle in a haystack. arXiv:quant-ph/9706033 (quant-ph). 22. Kaiser S. , Granade C. . Learn Quantum Computing with Python and Q#: A hands-on approach.

23. B. Omer. Simualtion of Quantum Computers. – Vienna:TU. - 1996. – 23.

24. ECOQC White Paper on Quantum Key Distribution and Cryptography / Romain Alleaume, Jan Bouda, Cyril Branciard [et al.|. - Preprint : http://www. arxiv.org/abs/quant-ph/0701168vl.

25.QPN-8505. Security Gateway: Data Sheet / MagiQ Technologies, Inc.. - Somerville, Massachusetts, USA : MagiQ Technologies, Inc., 2007, 110.12.2011]. - Mode of access: http://www.magiqtech.com/MagiQ/ Products_files/ 8505_Data_Sheet.pdf.

26. Clavis [Electronic resource] : Quantum key distribution for r&d applications / ID Quantique SA. - Electronic data. - Geneva, Switzerland : http ://www. idquantique.com /scientific-instrumentation/clavis2-qkd-platforrn.html.

27. Elliot C. Quantum Cryptography in Practice / Elliot C., Pearson D, Troxel G. - Preprint : arXiv:quant-ph/0307049.

28. Килин С. Квантовая информация/ УФН, 1999, т.169, №5, 507–527

29. Miszczak, J. Sec. 3 of: *Models of quantum computation and quantum programming languages*, Bull. Pol. Acad. Sci.-Tech. Sci., Vol. 59, No. 3 (2011), pp. 305-324 (arXiv:1012.6035).

30. Войтович І.Д. Перспективи квантових обчислень з використанням надпровідності/ І.Д. Войтович, В.М. Корсунський // Математичні машини і системи. – 2008. – № 4. – С. 23-56.

31. Крохмальський Т. Квантові комп'ютери: основи й алгоритми (короткий огляд) / Т. Крохмальський // Журнал фізичних досліджень. Ін-ут фізики конденсованих систем НАН України. – 2004. – Т.8, № 1. – С. 1-15.

Kosobutsky P.S.
Lviv Polytechnic National University

PHYSICAL FOUNDATIONS OF QUANTUM INFORMATICS: FROM QUANTUM MECHANICS THROUGH QUANTUM COMPUTING TO QUANTUM CRYPTOGRAPHY

A methodical analysis of the basic problem related to quantum calculations of parameters of physical systems was made. Emphasis is placed on the physical principles of the operation of a quantum computer, with an emphasis on the fact that simultaneous access to all quantum states is important in quantum computing, which allows the simultaneous change of the quantum state from all superpositions in the qubit system. Emphasis is placed on the fact that in quantum algorithms the Fourier transform and the Hadamard transform are the basic operations - as a simple discrete Fourier transform. The reader's attention is drawn to the fact that quantum computing is primarily implemented in quantum objects with the properties of elementary NOT gates and controlled CNOT, which can be implemented on a Mach-Zehnder interferometer using the phenomena of photon interference and rotation of its polarization vector.

Despite the progress of conventional computers, the need for the development of quantum computing is due to the technological limitation due to the dimensional quantization of the electronic spectrum and the exponential increase in the time of calculations by classical algorithms when the volume of data increases. However, the widespread use of quantum computers is limited by a number of problems. This is, first of all, insufficient accuracy and high sensitivity to external influences that can destroy the quantum state. Therefore, to increase the accuracy of calculations on a quantum computer, the calculation algorithm must be repeated a certain number of times, and to avoid the destruction of the quantum states of the qubit, low temperatures are used.

Key words: **quantum information, quantum computing, quantum superposition, entanglement of quantum objects, quantum computer**