DOI 10.31891/2307-5732-2023-323-4-87-94
УДК 004.89

ГРИНЬКО ІРИНА
Хмельницький національний університет
ORCID ID: 0009-0005-4855-0495
e-mail: grinko.ira2001@gmail.com
СКРИПНИК ТЕТЯНА
Хмельницький національний університет
ORCID ID: 0000-0002-8531-5348
e-mail: tkskripnik1970@gmail.com
БАРМАК ОЛЕКСАНДР
Хмельницький національний університет
ORCID ID: 0000-0003-0739-9678
e-mail: alexander.barmak@gmail.com

КВАНТОВІ ЗГОРТКОВІ НЕЙРОННІ МЕРЕЖІ: ОСОБЛИВОСТІ РЕАЛІЗАЦІЇ У ТЕХНІЧНИХ, ПРИРОДНИЧИХ І СОЦІАЛЬНО-ЕКОНОМІЧНИХ СИСТЕМАХ

У роботі проведені аналіз та дослідження застосування квантових згорткових нейронних мереж для технічних, природничих і соціально-економічних інформаційних систем. Квантові згорткові нейронні мережі є новим підходом до обробки інформації, який базується на принципах квантової механіки та штучного інтелекту. В технічних системах досліджено можливість застосування квантових згорткових нейронних мереж для розв'язання складних задач, таких як спроби злому криптографічних ключів та криптографічного шифрування. Результати показали, що квантові згорткові нейронні мережі можуть забезпечити більш точні та швидкі обчислення в порівнянні з класичними нейронними мережами.

У природничих системах проведено дослідження використання квантових згорткових нейронних мереж для моделювання та прогнозування складних природних процесів. Досліджено їхню ефективність у розумінні та вивченні складних молекулярних структур. Виявлено, що квантові згорткові нейронні мережі можуть забезпечити більш точні та швидкі результати у порівнянні зі звичайними методами обробки даних.

У соціально-економічних системах досліджено можливості використання квантових згорткових нейронних мереж для аналізу соціальних мереж, прогнозування фінансових ринків та криптовалют. Виявлено, що застосування квантових згорткових нейронних мереж може покращити точність прогнозування та забезпечити більш ефективне прийняття рішень у соціально-економічних системах.

Результати дослідження підтвердили, що квантові згорткові нейронні мережі мають потенціал для використання в різних сферах, включаючи технічні, природничі та соціально-економічні системи. Вони здатні досягти більшої точності, швидкості обробки та прогностичної здатності порівняно з традиційними методами.

Ключові слова: квантові обчислення, нейронні мережі, штучний інтелект, кубіти.

HRYNKO IRYNA., SKRYPNYK TETYANA, BARMAK OLEXANDER
Khmelnytskyi National University

QUANTUM CONVOLUTIONAL NEURAL NETWORKS: IMPLEMENTATION SPECIFICS IN TECHNICAL, NATURAL, AND SOCIO-ECONOMIC SYSTEMS

The paper analyses and investigates the usage of quantum convolutional neural networks in technical, natural, and socio-economic systems. Quantum convolutional neural networks are a novel approach to information processing that is based on the principles of quantum mechanics and artificial intelligence. In technical systems, the potential of using quantum convolutional neural networks for solving complex tasks such as image processing, machine learning, and prediction has been explored. The results have shown that quantum convolutional neural networks can provide more accurate and faster computations compared to classical neural networks.

In natural systems, research has been conducted on the use of quantum convolutional neural networks for modeling and predicting complex natural processes. Their effectiveness in understanding genetic data, studying complex molecular structures, and analyzing ecological systems has been investigated. It has been found that quantum convolutional neural networks can deliver more precise and rapid results compared to conventional data processing methods. In socio-economic systems, the possibilities of employing quantum convolutional neural networks for social network analysis, financial market forecasting, and resource management have been studied. The application of quantum convolutional neural networks has the potential to enhance prediction accuracy and facilitate more effective decision-making in socio-economic systems. The research findings confirm that quantum convolutional neural networks have the potential to be utilized in various domains, including technical, natural, and socio-economic systems. They can achieve higher accuracy, processing speed, and predictive capabilities compared to traditional methods.

Keywords: quantum computing, neural networks, artificial intelligence, qubits....

Вступ та постановка проблеми

У своєму найпростішому визначенні штучний інтелект [1] – це набір математичних (статистичних) моделей, які натреновані для аналізу і класифікації даних. Системи ШІ працюють шляхом поєднання в собі інформатики та надійних наборів даних для вирішення поставлених проблем та завдань. Дана комбінація дає змогу штучному інтелекту навчатися на основі шаблонів і особливостей проаналізованих даних. Кожний раз, виконуючи цикл обробки даних, система штучного інтелекту перевіряє та вимірює свою результативність та використовує підсумки для отримання додаткового досвіду.

Потужним інструментом в машинному навчанні є глибоке навчання та одними з найпопулярніших глибоких нейронних мереж є згорткові нейронні мережі. Одна з ключових операцій в згортковій нейронній

мережі – це операція згортки (convolution), яка виконується на вхідних даних. Згортка використовує фільтри або ядра, які є матрицями чисел. Ці ядра переміщуються по вхідному зображенню з певним кроком і виконують операцію множення між відповідними пікселями зображення та відповідними елементами ядра, а потім додають результати множення. Ця операція може бути подана у вигляді матричного множення між вектором, який є вихідним значенням зображення та ядром.

Під час використання великого об’єму даних для навчання, наприклад, для обробки великого об’єму інформації потрібна більша кількість часу. Крім цього може виникнути проблема спроможності фізичних ресурсів обчислювальної техніки [2]. Для вирішення та уникнення даних проблем використовуються квантові комп’ютери. Квантові комп'ютери можуть потенційно виконувати певні обчислення швидше, ніж класичні комп'ютери, зокрема у випадку обчислень, пов'язаних з обробкою великих об'ємів даних. Це відкриває нові можливості для використання згорткових нейронних мереж на квантових комп'ютерах. На жаль, в даний час квантові комп'ютери ще не є настільки розвиненими, щоб можна було ефективно використовувати їх для обробки зображень за допомогою згорткових нейронних мереж. Проте, дослідження у цій області продовжуються, і можливо, що у майбутньому квантові комп'ютери будуть використовуватися для збільшення швидкості та точності згорткових нейронних мереж.

Отже, головною метою цієї статті є дослідження квантових обчислень та нейронних мереж у контексті задач для різних галузей.

Теоретичний матеріал

Процес переходу від біта до кубіта та назад є одним з ключових аспектів квантових обчислень. У більшості випадків, біт можна розглядати як два можливих стани: 0 або 1. Кубіт, з іншого боку, може перебувати в будь-якому стані, що є суперпозицією 0 та 1. Для перетворення біта в кубіт можна використовувати таке поняття як гейт Адамара [3].

Гейт Адамара використовується для перетворення одного біта у кубіт за допомогою умовної операції. Процес переходу від біта до кубіта за допомогою схеми Адамара відбувається наступним чином. Спочатку маємо біт зі значенням 0 або 1, який можна подати у вигляді вектора-стовпця з двох елементів:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \tag{1}$$

Далі застосовуємо до цього вектора схему Адамара, що визначається наступною формулою:

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \tag{2}$$

Тоді, якщо ми застосуємо цю матрицю до векторів $|0 ma|1$, ми отримаємо наступні кубіти:

$$\begin{aligned} H|0\rangle &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |\varphi\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = |+\rangle, \\ H|1\rangle &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |\beta\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = |-\rangle \end{aligned} \tag{3}$$

Таким чином, ми отримали кубіти $|+\rangle$ та $|-\rangle$, які є двома базисними стани кубіту. Вони представлені наступним чином:

$$\begin{aligned} |+\rangle &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \\ |-\rangle &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}, \end{aligned} \tag{4}$$

Перехід від кубіта до біта також здійснюється за допомогою гейта Адамара. Якщо ми застосуємо гейт Адамара до кубіта в стані $|+\rangle$ та $|-\rangle$, отримаємо біт в стані $|0\rangle$ та $|1\rangle$ відповідно:

$$\begin{aligned} H|+\rangle &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle, \\ H|-\rangle &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle, \end{aligned} \tag{2.8}$$

Щоб повернутися від кубіта до біта, необхідно виконати процес вимірювання. Коли вимірюється кубіт, він переходить в один з базисних станів $|0\rangle$ або $|1\rangle$. Зазвичай вимірюванням кубіта звужується квантовий стан системи до класичного бітового значення 0 або 1. При вимірюванні, ймовірність отримати

результат $|0\rangle$ або $|1\rangle$ визначається квадратом амплітуди кожного стану.

Квантові алгоритми, такі як оцінка квантової фази (QPE) і варіаційний квантовий розв'язувач власних сигналів (VQE), широко вивчаються в квантовій хімії як потенційні шляхи для вирішення проблем, які нерозв'язні для звичайних комп'ютерів. Алгоритм VQE (Variational Quantum Eigensolver) – це квантовий алгоритм для розрахунку енергії основного стану молекули з використанням квантових комп'ютерів. Давайте розглянемо детальніше алгоритм VQE на прикладі молекули водню H_2.

Для розв'язання квантової задачі на квантовому комп'ютері необхідно використовувати кубіти, які можна використовувати як рівні 0 та 1. В алгоритмі VQE, ми використовуємо додатковий параметр θ, який буде використовуватися для визначення кутів на квантовому гейті.

Алгоритм VQE складається з наступних етапів:

1. Підготовка вихідного стану: Створення початкового стану з використанням квантових гейтів на кубітах. Зазвичай, як початковий стан використовують одиничний вектор $|0\rangle$ на кожному кубіті. Далі до цих станів можна застосовувати квантові гейти для отримання більш складного стану. Початковий вихідний стан на кубітах може бути вибраний відповідно до властивостей системи. Наприклад, у випадку молекули водню, яка має два атоми водню, можна використовувати два кубіти, кожен з яких відповідає одному атому водню. Для цього можна використовувати схему Адамара. Наприклад, якщо ми маємо два кубіти, то схема Адамара буде виглядати наступним чином:

$$\mathrm{H} = H_1 \otimes H_2 \,, \tag{5}$$

де H_1 та H_2 – гейти Адамара, що застосовуються до першого та другого кубітів відповідно. Отже, застосувавши схему Адамара до початкового стану $|0\rangle$, отримаємо стан рівномірної суперпозиції, який можна використовувати як початковий стан для методу VQE.

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |01\rangle + |10\rangle + |11\rangle), \tag{6}$$

2. Побудова гамільтоніана: Визначення гамільтоніана системи. Гамільтоніан – це оператор, що описує енергетичний стан молекули. У випадку молекули водню, гамільтоніан може бути записаний в такій формі:

$$\mathrm{H} = \alpha Z_0 + \beta X_0 \, X_1 + \gamma Z_1 \,, \tag{7}$$

де X та Z – оператори Паулі, а коефіцієнти α, β та γ – константи, які залежать від геометрії молекули та властивостей її складових атомів.

3. Третім кроком буде використовуючи згорткову мережу на класичному комп'ютері, обчислити енергію молекули, що відповідає квантовому стану $|\Psi(\theta)\rangle$. Енергію можна обчислити шляхом вимірювання очікуваної величини гамільтоніана H у квантовому стані $|\Psi(\theta)\rangle$:

$$\mathrm{E}(\theta) = \langle\Psi(\theta)|\mathrm{H}|\Psi(\theta)\rangle, \tag{8}$$

де E(θ) – енергія, залежна від параметрів θ вихідного стану ψ(θ), H – гамільтоніан системи.

4. Варіаційна оптимізація: Використання класичного оптимізатора для знаходження оптимальних значень параметрів θ, які мінімізують енергію системи. Це може бути здійснено шляхом використання різних методів оптимізації, таких як градієнтний спуск або метод Нелдера-Міда.

5. Повторення кроків 3 та 4 до тих пір, поки не буде досягнуто достатньої точності вимірювання енергії. Це може бути досягнуто шляхом встановлення критерію зупинки, такого як максимальна кількість ітерацій або задана точність енергії.

6. Отримання результату: Після знаходження оптимальних значень параметрів θ, можна використовувати ці значення для побудови фінального вихідного стану ψ(θ) та обчислення остаточної енергії системи E(θ), яка буде наближеною енергією основного стану молекули водню.

Прикладом реалізації та цікавою сферою дослідження в економічному та фінансовому секотрі є поняття арбітражу [4]. Арбітраж описує той факт, що один і той самий актив може мати різні ціни на різних ринках і може бути торгований між кількома ринками для отримання позитивного доходу. Тобто, за наявності набору активів та транзакційних витрат, можливо створити цикл між різними ринками, який може забезпечити позитивний дохід.

Для того, щоб перетворити задачу оптимізації арбітражної можливості на проблему, яку можна застосувати для параметризованих квантових ланцюгів, потрібно закодувати проблему оптимізації арбітражу в гамільтоніан. Ми реалізуємо кодування, спочатку складаючи задачу цілочисельного програмування. Припустимо, що в графі G є $|V| = n$ вершин, то для кожної вершини $i \in V$, визначаються n бінарні змінні $x_{i,k}$ де $k \in [0, K-1]$ такі, що:

$$x_{i,k} = \begin{cases} 1 \\ 0, \end{cases} \tag{9}$$

Потрібно зауважити, що коефіцієнти у гамільтоніані є великими числами, що можуть вплинути на точність підрахунку в квантовому комп'ютері.

Оскільки граф G має n вершин, ми маємо n^2 змінних в загальному, значення яких позначаються рядом бітів $x = x_0 \ldots x_{n-1,K-1}$. Поки що припустимо, що рядок бітів x представляє арбітражний цикл. Тоді для кожного ребра $(i, j, w_{ij}) \in E$, ми матимемо $x_{i,k} = x_{j,k+1} = 1$, тобто $x_{i,k} \cdot x_{j,k+1} = 1$, якщо тільки арбітражний цикл відвідує вершину i в час k і вершину j в час $k+1$. В іншому випадку буде $x_{i,k} \cdot x_{j,k+1} = 0$. Отже, логарифм прибутку циклу є:

$$P(x) = -\sum_{i,j \in V} \log(c_{ij}) \sum_{k=0}^{K-1} x_{i,k} x_{j,k+1}, \tag{10}$$

Для того, щоб x представляв дійсний арбітражний цикл, потрібно виконувати наступне обмеження:

$$\sum_{i=0}^{n-1} x_{i,k} \; ma \sum_{k=0}^{K-1} \sum_{(i,j \notin E)} x_{i,k} x_{j,k+1} \tag{11}$$

де перше рівняння гарантує відвідування лише однієї вершини в кожен час. Друге – обмежує виявлення неіснуючого ребра в знайденому арбітражному циклі. Ці два рівняння забезпечують те, що параметризовані квантові схеми знаходять x як простий цикл. Тоді функцію вартості при зазначеному обмеженні можна сформулювати нижче:

$$C_x = -P(x) + A \sum_{k=0}^{K-1} (1 - \sum_{i=0}^{n-1} x_{i.k})^2 + A \sum_{k=0}^{K-1} \sum_{(i,j) \notin E} x_{i,k} x_{j,k+1}, \tag{12}$$

де V – кількість вершин графа, E – множина ребер графа та K – кількість вершин найбільш корисного циклу. Зверніть увагу, що оскільки ми хочемо максимізувати $P(x)$, забезпечуючи x, що представляє дійсний арбітражний цикл, ми краще встановимо A великою, щонайменше більшою за найбільшу вагу ребер.

Ми тепер потрібно перетворити функцію вартості C_x в гамільтоніан, щоб реалізувати кодування задачі оптимізації можливостей арбітражу. Кожна змінна $x_{i,k}$ має два можливі значення, 0 та 1, що відповідають квантовим станам $|0\rangle$ та $|1\rangle$. Зверніть увагу, що кожна змінна відповідає кубіту, тому для вирішення задачі оптимізації можливостей арбітражу потрібно n^2 кубитів. Оператор Паулі Z має два власні стани, $|0\rangle$ та $|1\rangle$. Власні значення дорівнюють 1 та -1 відповідно. Тому ми розглядаємо кодування функції вартості в гамільтоніан, використовуючи матрицю Паулі Z.

Тепер розглянемо відображення:

$$x_{i,k} \to \frac{I - Z_{i,k}}{2}, \tag{13}$$

де $Z_{i,k} = I \otimes I \otimes \ldots \otimes Z \otimes \ldots \otimes I$ Z виконується на кубіті на позиції (i,k). Під час цього відображення значення $x_{i,k}$ можна проілюструвати по-іншому. Якщо кубіт (i,k) перебуває в стані $|0\rangle$, тоді $x_{i,k} |1\rangle = \frac{I - Z_{i,k}}{2} |1 = 1|1\rangle$, що означає, що вершина i відвідується в момент часу k. Крім того, для кубіту (i,k), який перебуває в стані $|0\rangle$, $x_{i,k} |0\rangle = \frac{I - Z_{i,k}}{2} |0 = 0|0\rangle$.

Таким чином, використовуючи вищезазначене відображення, ми можемо перетворити функцію вартості C_x в гамільтоніан H_c для системи n^2 кубітів і реалізувати квантову оптимізацію можливостей арбітражу. Тоді ґрунтовий стан H_c є оптимальним рішенням задачі оптимізації можливостей арбітражу.

Загрозою для сучасної криптографії є алгоритм Шора. Це квантовий алгоритм, який дозволяє розкладати складні числа на прості множники. Для застосування алгоритму Шора до криптографічних ключів RSA, які базуються на складних числах, можна використовувати його для розкладання публічного ключа на прості множники. Ідея цього алгоритму досить проста. На вхід подаються два регістри кубітів:

перший відповідає вхідним значенням функції, другий – вихідним. У першому регістрі створюється суперпозиція всіх можливих вхідних значень, другий регістр ініціалізується фіксованим станом, після чого на виході ми отримуємо квантову суперпозицію всіх можливих входів та відповідних їм виходів. Потім робимо вимірювання вихідного регістру, в результаті чого отримуємо деяке випадкове значення функції, а в іншому регістрі – суперпозицію всіх аргументів функції, що відповідають отриманому значенню. Далі застосовуємо квантове перетворення Фур'є над першим регістром і в вимірювальному вимірюванні отримуємо величину, пропорційну оберненому періоду функції. Повторюючи цю операцію кілька разів і використовуючи класичний алгоритм Євкліда для пошуку найбільшого спільного дільника (НСД), ми отримуємо сам період.

Даний алгорим можна розділити умовно на дві частин: класичне розкладання на множники функції та квантове обчислення періоду даної функції.

Для початку потрібно визначити три константи:

- M – число, що використовується для розкладання на множники;
- N – розмір регістра пам'яті. Бітовий розмір даної пам'яті $n = \log_2 N$, що в два рази більше M;
- t – рандомий параметр, такий що: $1 < t < M \; i \; НСД\left(t, M\right) = 1.$

Класична частина алгоритму має наступні кроки:

1) розрахувати $K = НСД(t, N)$;

2) якщо, $K \neq 1$ то K нетривіальний фактор N і алгоритм на цьому закінчується;

3) в іншому випадку потрібно скористатися підпрограмою пошуку квантового періоду, щоб знайти r , що позначає період наступної функції;

4) якщо r виявилося парне число, то перейти до пункту 1;

5) якщо виконується умова $a^{\frac{r}{2}} = -1 mod N$, то перейти до пункту 1;

6) в іншому випадку обидва $НСД\left(a^{\frac{r}{2}} + 1, N\right) та НСД\left(a^{\frac{r}{2}} - 1, N\right)$ є нетривіальними факторами.

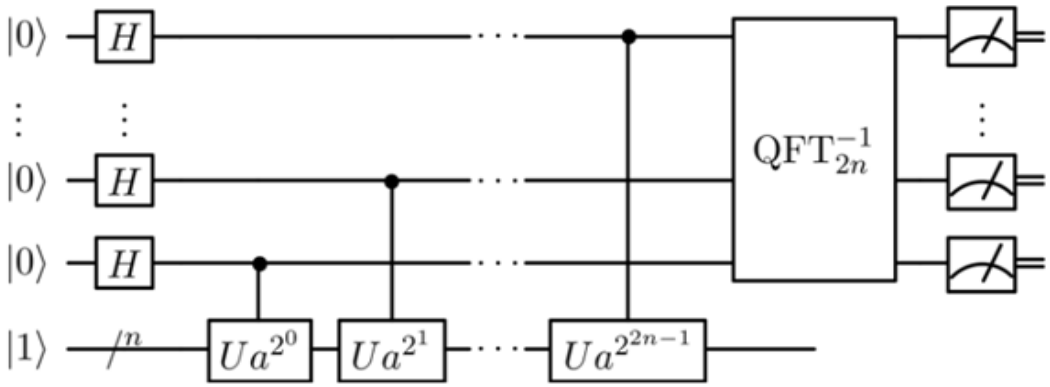

Рис. 1. Квантова підпрограма в алгоритмі Шора

Квантова підготовка включає створення суперпозиції квантових станів, а квантова фазова оцінка дозволяє знайти періодичність функції, що визначає факторизацію числа.

Основна формула, яка використовується в квантовій підготовці, це формула Гадамарда. Вона використовується для перетворення базисних квантових станів ($|0\rangle$ та $|1\rangle$) у рівновагу суперпозицій:

$$H|0 = \frac{1}{\sqrt{2}}(|0 + |1), \tag{14}$$

$$H|1 = \frac{1}{\sqrt{2}}(|0 - |1), \tag{15}$$

Ці формули дозволяють створити рівновагу суперпозицію з n кубітів, використовуючи послідовність Гадамарда на кожному кубіті.

У квантовій фазовій оцінці використовується квантовий алгоритм зворотного дискретного перетворення Фур'є (QFT). Формула QFT виглядає наступним чином:

$$QFTH|\psi = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} e^{\frac{2\pi i x y}{N}} |\psi_y, \tag{16}$$

де $|\psi\rangle$ – квантовий стан, $N = 2^m$ – кількість можливих станів, x та y – цілі числа в діапазоні від 0 до $N-1$, а $e^{\frac{2\pi ixy}{N}}$ – комплексне число, яке дозволяє зв'язати квантові стани $|\psi_x\rangle$ та $|\psi_y\rangle$.

Результати та дискусія

Для обчислення енергії зв'язку для гамільтоніанів H1, H2 та H3 з використанням Estimator для кожного гамільтоніана із вказаним анзацом. Зіткнувши один генератор випадкових чисел, за допомогою VQE і SLSQP optimizer, використовуються вказані анзаци і гамільтоніани для обчислення мінімальної власної енергії і біндуючої енергії для H1, H2 та H3.

```
Results using Estimator for H_1, H_2 and H_3 with the ansatz

Binding energy for H_1: -0.4365811096105766 MeV
Binding energy for H_2: -1.7491595316575461 MeV
Binding energy for H_3: -2.045670898257444 MeV
```

Рис. 2. Обчислення енергії звязку

Графіки результатів, отриманих під час виконання алгоритму VQE зображені на рисунку 3.

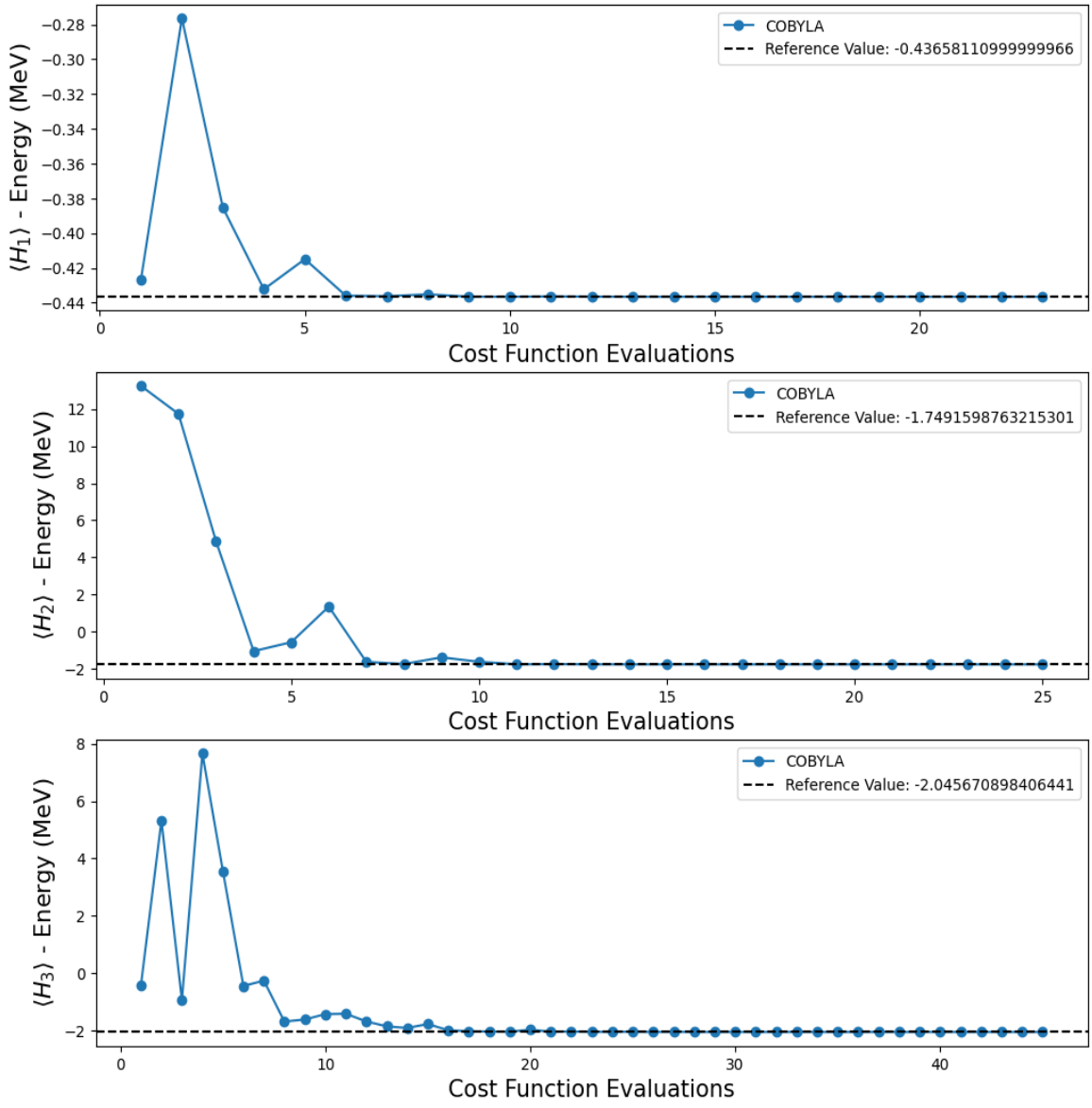

Рис. 3. Графіки енергії

Криптовалюти, як відомо, нестабільні, і їх складно передбачити, однак передбачення їхньої вартості є великим фінансовим стимулом. Метою реалізації даної програми є порівняння квантових і класичних методів машинного навчання для прогнозування часових рядів криптовалюти. Це може бути корисним для трейдерів і інвесторів, які хочуть приймати обґрунтовані рішення щодо купівлі, продажу або утримання криптовалют.

Використані дані – це ціна криптовалюти Ethereum за 2019–2023 роки, включаючи відкриття, максимум, мінімум, закриття, скориговане закриття та обсяг за кожен день. Результати зображені на рисунку 4.

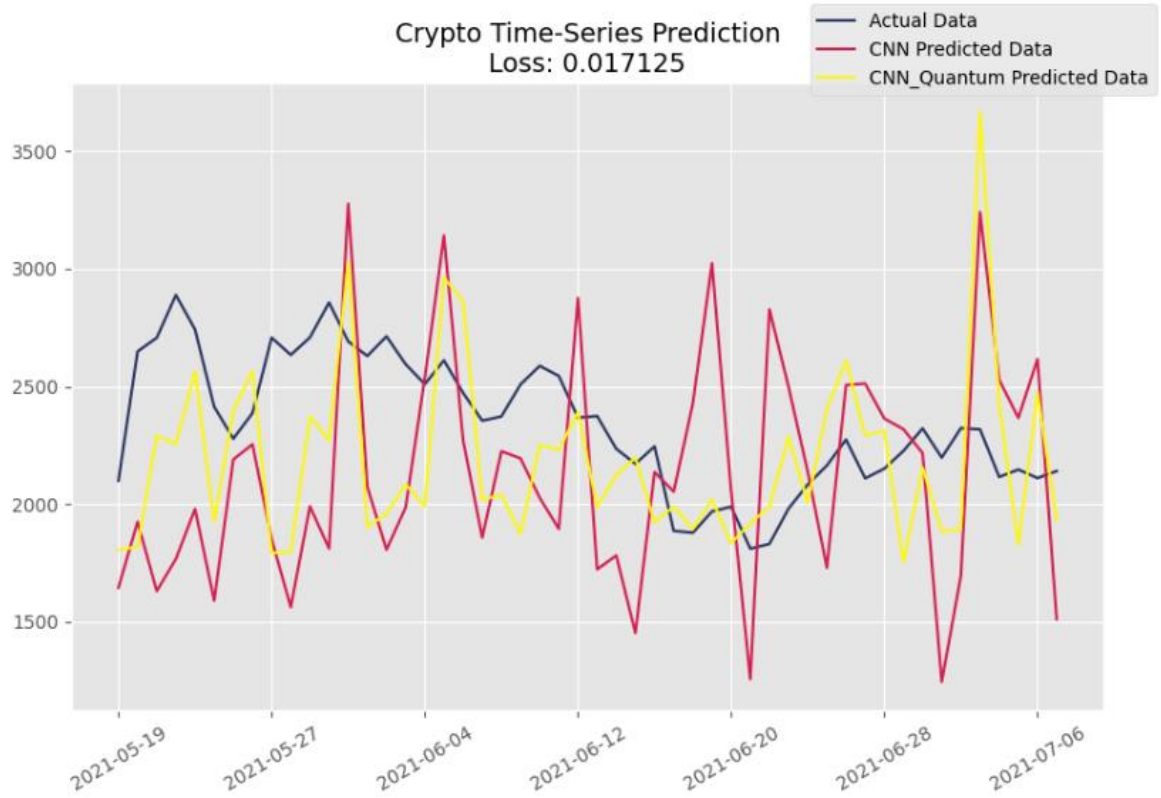

Рис. 4. Порівняння всіх результатів

Також була створена програмна реалізація, яка використовує квантові згорткові нейронні мережі для криптоаналізу та шифрування. Вони є потужним інструментом, який комбінує переваги квантових обчислень та здатності згорткових нейронних мереж до розпізнавання зразків. Реалізація програмного продукту відбувалася за допомогою мови програмування Python. Був використаний модуль Qiskit від IBM Quantum Experience для розробки квантової схеми, яка працює на кубітах замість традиційних бітів.

Розроблена програмна реалізація може бути використана для криптоаналізу різних криптографічних систем та для передбачення їх руйнування шляхом зламу.

Для шифрування введеного тексту використовується RSA алгоритм. Суть алгоритму полягає в генерації двох ключів: публічного та приватного. Публічний ключ використовується для шифрування даних, тоді як приватний ключ використовується для розшифрування.

Процес RSA розшифровки реалізовується функцією decrypt, яка використовує алгоритм RSA для розшифрування зашифрованого повідомлення з використанням пакета ключів. Ці значення визначають приватний ключ для розшифрування. Результати даного процесу зображені на рисунку 5.

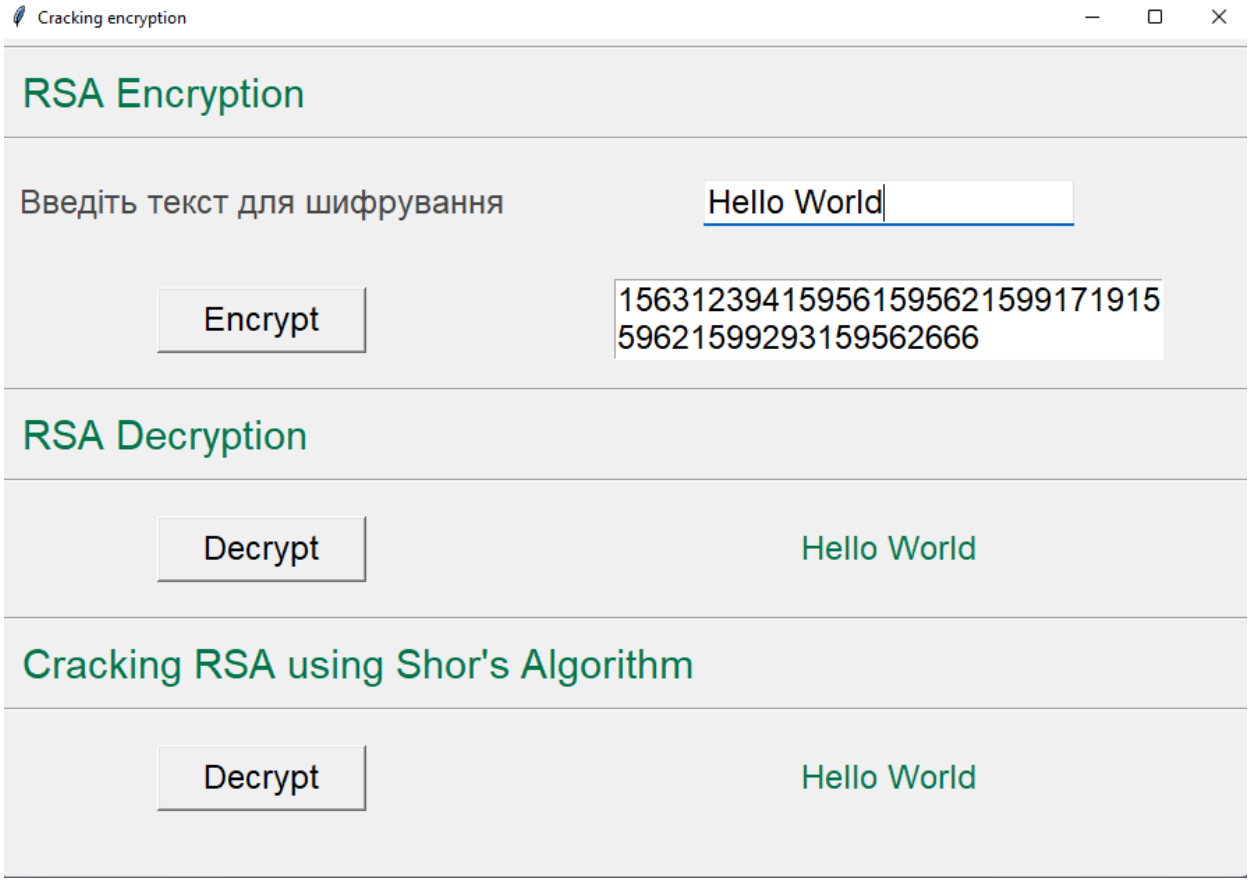

Рис. 5. Результат роботи програми

Висновки

Застосування квантових згорткових нейронних мереж дозволяє отримати більш точні прогнози в порівнянні з класичними моделями, зокрема, в областях, де присутні складні залежності між даними. Програмна реалізація показала свою ефективність в прогнозуванні цін криптовалют, а також може бути застосована в інших сферах, де важливо точне прогнозування на основі великої кількості даних.

Застосування квантових згорткових нейронних мереж у криптографії відкриває нові можливості для розробки стійких криптосистем, які забезпечують високий рівень захисту від атак з використанням квантових обчислювальних алгоритмів. Програмна реалізація показала ефективність в дешифруванні інформації, де квантові згорткові нейронні мережі використовуються для розшифрування даних.

У подальших дослідженнях можна розширити обсяг використання квантових згорткових нейронних мереж у криптографії та інших галузях, де вимоги до безпеки та точності є критичними. Також можна продовжувати дослідження в напрямку покращення алгоритмів квантової обчислювальної мережі та їхнього застосування в практичних задачах.

В загальному результати дослідження показали, що квантові нейронні мережі мають потенціал для поліпшення ефективності і точності аналізу даних у різних інформаційних системах. Вони можуть забезпечити швидку обробку великого обсягу даних, а також здатні до виявлення складних залежностей та патернів у вхідних даних.

References

1. Auria, Laura & Moro, Rouslan. (2008). Support Vector Machines (SVM) as a Technique for Solvency Analysis. SSRN Electronic Journal. 1. 10.2139/ssrn.1424949.

2. Guijo, D., Onofre, V., Bimbo, G.D., Mugel, S., Estepa, D., … Orús, R. (2022). Quantum artificial vision for defect detection in manufacturing. ArXiv, 2208.04988.

3. Flöther, Frederik. (2023). The state of quantum computing applications in health and medicine. 10.48550/arXiv.2301.09106.

4. Pistoia, M., Ahmad, S.F., Ajagekar, A., Buts, A., Chakrabarti, S., … Yalovetzky, R. (2021). Quantum Machine Learning for Finance. 10.48550/arXiv.2109.04298.