КВАНТОВІ ОБЧИСЛЕННЯ ТА КВАНТОВА КРИПТОГРАФІЯ

КОМП'ЮТЕРНИЙ ПРАКТИКУМ №1

"Дослідження реалізації алгоритму Шора"

1. Мета роботи

Дослідження особливостей реалізації квантового алгоритму Шора.

2. Основні теоретичні відомості

Необхідні теоретичні відомості містяться в роботі:

1) P.W. Shor, Algorithms For Quantum Computation: Discrete Logs and Factoring, Proceedings of the 35th Symposium on the Foundations of Computer Science (1994), 124-134.

2) P.W. Shor, Polynomial-Time Algorithms for Prime Factorisation and Discrete Logarithms on a Quantum Computer, SIAM Journal on Computing 26 5 (1997), 1484-1509.

3) Zalka C. Shor's algorithm with fewer (pure) qubits [електронний ресурс] / C. Zalka // arXiv, Quantum Physics Archive, preprint arXiv:quant-ph/0601097. – 2006. Режим доступу: https://arxiv.org/abs/quant-ph/0601097

4) Mosca M. The hidden subgroup problem and eigenvalue estimation on a quantum computer / M. Mosca, A. Ekert // Quantum Computing and Quantum Communications, LNCS, Springer, Berlin Heidelberg. – 1999. – Vol. 1509. – pp. 174-188.

5) Parker S. Efficient factorization with a single pure qubit and logN mixed qubits / S. Parker, M. Plenio // Physical Review Letters. – 2000. – Vol. 85. – pp. 3049-3052.

6) Griffiths R. Semiclassical fourier transform for quantum computation / R. Griffiths, C.-S. Niu // Physical Review Letters. – 1996. – Vol. 76. – pp. 3228-3231.

7) S. Beauregard Circuit for Shor's algorithm using $2n + 3$ qubits, arXiv preprint quant-ph/0205095 - 2002.

8) A.G. Fowler, M. Mariantoni, J.M. Martinis, A.N. Cleland Surface codes: Towards practical large-scale quantum computation // Physical Review A86, 032324 - 2012, arXiv:1208.0928.

9) T. Haner, M. Roetteler, K.M. Svore Factoring using $2n + 2$ qubits with Toffoli based modular multiplication // arXiv preprint arXiv:1611.07995 - 2016.

3. Порядок і рекомендації щодо виконання роботи

Комп'ютерний практикум виконується бригадами, які містять від однієї особи до 3 людей.

4. Завдання на комп'ютерний практикум

Дослідити реалізацію алгоритму Шора та його модифікацій на одній із високорівневих мов програмування для квантової моделі обчислень.

Для власного варіанту завдань необхідно запрограмувати стандартний алгоритм Шора: обчислити розміри вхідних регістрів, реалізувати основні операції квантових вентилів та запрограмувати постобробку отриманих результатів вимірювань. Знайти розклад кожного числа N на прості множники згідно з власним варіантом завдань. Використати значення a_1, a_2 та a_3 для пошуку їх порядків за модулем N. Для кожного з цих елементів виконати алгоритм Шора не менше 10 разів. Всі результати вимірювань, а також їх аналіз повинні міститися в звіті. Для одного з виконань алгоритму Шора для елемента, який допоміг розкласти число N на прості множники навести всі проміжні значення обох регістрів з поясненнями (за один крок взяти проходження одного вентиля квантової схеми алгоритму Шора).

Реалізувати різні варіанти модифікації алгоритму Шора, які дозволяють зменшити зменшити кількість необхідних кубітів з використанням напівкласичного перетворення Фур'є та повторного використання кубітів, та виконати розклад числа N з використанням цих модифікацій. Оцінити кількості необхідних квантових вентилів таких реалізацій.

Знайти максимальний розмір квантових регістрів, для якого реалізація квантового алгоритму пошуку періоду періодичної функції працює за прийнятний час.

5. Оформлення результатів роботи та звіту

Результатом роботи є всі тексти програм, скомпільовані виконувані файли (які мають запускатися на чистій ОС; якщо є потреба, можна використовувати контейнери), необхідна документація щодо використання бібліотеки з прикладами застосування та звіт.

Звіт до комп'ютерного практикуму оформлюється згідно зі стандартними правилами оформлення наукових робіт, за такими винятками:

- дозволяється використовувати шрифт Times New Roman 12pt та одинарний інтервал між рядками;
- дозволяється не починати нові розділи з окремої сторінки;
- дозволяється не включати анотацію, перелік термінів та позначень і перелік використаних джерел;
- не обов'язково оформлювати зміст.

Звіт має містити:

- мету проведення комп'ютерного практикуму;
- постановку задачі;
- хід виконання роботи, опис труднощів, що виникали, та шляхів їх подолання;
- детальний опис алгоритму Шора;
- детальні описи модифікацій алгоритму Шора, які дозволяють зменшити зменшити кількість необхідних кубітів з використанням напівкласичного перетворення Фур'є та повторного використання кубітів (з оцінками складності);

– порівняльний аналіз всіх версій алгоритму Шора;
– результати виконання версій алгоритму Шора з їх аналізом;
– висновки до роботи.

Тексти програм не включати у звіт.

Комп'ютерний практикум вважається виконаним після надіслання всіх текстів програм, скомпільованих виконуваних файлів, необхідної документації щодо використання програм з прикладами застосування, звіту та після теоретичного захисту роботи. Дата теоретичного захисту роботи назначається виключно після надсилання всіх необхідних матеріалів та їх перевірки за допомогою тестування коректності та швидкодії (включаючи перевірку на плагіат).

6. Варіанти завдань

1) $N = 437$, $a_1 = 3$, $a_2 = 6$, $a_3 = 10$;
$N = 493$, $a_1 = 7$, $a_2 = 21$, $a_3 = 33$;

2) $N = 481$, $a_1 = 2$, $a_2 = 7$, $a_3 = 9$;
$N = 451$, $a_1 = 6$, $a_2 = 16$, $a_3 = 37$.