КВАНТОВЫЙ АЛГОРИТМ РЕШЕНИЯ УРАВНЕНИЯ ПЕЛЛЯ С ИСПОЛЬЗОВАНИЕМ ПОИСКА СКРЫТОЙ ПОДГРУППЫ

[1]Д.Т. Мухамедиева,[2]М.Х. Раупова

[1]Ташкентский институт инженеров ирригации и механизации сельского хозяйства, Ташкент, Узбекистан

[2]Чирчикский государственный педагогический университет, Чирчик, Узбекистан

Аннотация: В данной работе рассматривается квантовый алгоритм нахождения минимального решения уравнения Пелля $x^2 - dy^2 = 1$ для заданного n-битного числа d, не являющегося полным квадратом. Используется метод поиска скрытой подгруппы, позволяющий эффективно определять приближенное значение $[R]$, где $R = \log(x_1 + y_1\sqrt{d})$. Проведенные квантовые измерения показали, что наиболее вероятный результат соответствует $[R] = 0$, что позволяет классическими методами вычислить минимальное решение уравнения Пелля. Алгоритм использует разложение $\sqrt{d}$ в цепную дробь, определяет период и вычисляет соответствующую фундаментальную пару (x_1, y_1). Результаты симуляции на квантовом компьютере подтверждают полиномиальную сложность нахождения R, что существенно превосходит известные классические алгоритмы. Предложенный метод имеет важные криптографические последствия, так как он потенциально угрожает безопасности криптосистем на основе уравнения Пелля, таких как схема Бухмана-Вильямса.

Ключевые слова: квантовый алгоритм, уравнение Пелля, поиск скрытой подгруппы, квантовое преобразование Фурье, цепные дроби, криптоанализ, Бухман-Вильямс, квантовые вычисления.

QUANTUM ALGORITHM FOR SOLVING PELL'S EQUATION USING HIDDEN SUBGROUP SEARCH

[1]D.T. Muhamediyeva, [2]M. Raupova

[1]Tashkent Institute of Irrigation and Agricultural Mechanization Engineers, Tashkent, Uzbekistan

[2]Chirchik State Pedagogical University, Chirchik, Uzbekistan

Abstract: This paper examines a quantum algorithm for finding the minimal solution to Pell's equation $x^2 - dy^2 = 1$ for a given n-bit number d that is not a perfect square. The method of hidden subgroup search is employed, enabling the efficient determination of an approximate value of $[R]$, where $R = \log(x_1 + y_1\sqrt{d})$. Quantum measurements conducted indicate that the most probable result corresponds to $[R] = 0$, which allows the minimal solution to Pell's equation to be computed using classical methods. The algorithm utilizes the $\sqrt{d}$ decomposition of into a continued fraction, determines the period, and calculates the corresponding fundamental pair (x_1, y_1). Simulation results on a quantum computer confirm the polynomial complexity of finding R, which significantly outperforms known classical algorithms. The proposed method has important cryptographic implications, as it potentially threatens the security of cryptosystems based on Pell's equation, such as the Buchmann-Williams scheme [1–3].

Keywords: quantum algorithm. Pell's equation. hidden subgroup search. quantum Fourier transform, continued fractions, cryptanalysis, Buchmann-Williams. quantum computing

Введение

Уравнение Пелля $x^2 - dy^2 = 1$ является одним из фундаментальных диофантовых уравнений, широко изучаемых в теории чисел. Для любого целого положительного a, не являющегося полным квадратом, существует бесконечное множество решений (x, y), причем минимальное решение (x_1, y_1) играет ключевую роль в вычислении остальных решений. Классические алгоритмы поиска минимального решения основаны на разложении $\sqrt{d}$ в цепную дробь и имеют экспоненциальную сложность в худшем случае. Однако в 2001 году Холгрен показал, что квантовый компьютер способен вычислить приближенное значение: $[R]$, где $R = log(x_1 + y_1\sqrt{d})$, за полиномиальное время. Это стало возможным благодаря методу поиска скрытой подгруппы, который ранее применялся для взлома криптосистем, таких как алгоритм Шора для факторизации.

Данное исследование представляет квантовую реализацию метода Холгрена, основанную на квантовом преобразовании Фурье (QFT) и фазовых оценках. Полученные результаты показывают, что квантовый алгоритм успешно вычисляет $[R]$, после чего классическая обработка позволяет найти минимальное решение (x_1, y_1) уравнения Пелля.

Кроме того, учитывая, что криптографическая схема Бухмана-Вильямса опирается на сложность уравнения Пелля, предложенный квантовый алгоритм может представлять угрозу для данной криптосистемы, аналогично тому, как алгоритм Шора угрожает RSA.

Методы

Уравнение Пелля представляет собой диофантовое уравнение вида: $x^2 - dy^2 = 1$, где d – положительное целое число, не являющееся полным квадратом, x, y – искомые целые числа.

Уравнение имеет следующие свойства:

1. Бесконечное множество решений: если существует хотя бы одно нетривиальное решение (x_1, y_1), то из него можно породить бесконечное множество решений, используя рекуррентное соотношение:

$$x_{k+1} = x_1 x_k + dy_1 y_k,$$
$$y_{k-1} = x_1 y_k + y_1 x_k.$$

2. Фундаментальное решение: минимальное по величине положительное решение (x_1, y_1) называется фундаментальным и является основой для построения всех остальных решений.

Фундаментальное решение связано с теорией алгебраических чисел. Элемент $\varepsilon = x_1 + y_1\sqrt{d}$ называется фундаментальной единицей кольца целых чисел в поле $Q(\sqrt{d})$. Оно играет ключевую роль в вычислении остальных решений уравнения.

Ключевым инструментом решения уравнения Пелля является разложение $\sqrt{d}$ в периодическую цепную дробь. Любое иррациональное число можно представить в виде непрерывной дроби:

$$\sqrt{d} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \dots}}},$$

где $a_0 = [\sqrt{d}]$, а последующие коэффициенты a_i вычисляются по рекуррентной формуле.

Период цепной дроби $\sqrt{d}$ играет решающую роль:

– Пусть период разложения равен k.

– Если k четный, то фундаментальное решение (x_1, y_1) дается приближенной дробью

– (конвергентом) цепной дроби порядка k.

– Если k нечетный, то фундаментальное решение получается удвоением периода разложения.

Пусть дана цепная дробь:

$$[a_0; a_1, a_2, \dots, a_k].$$

Конвергенты вычисляются по формулам:

$$p_n = a_n p_{n-1} + p_{n-2}, \quad p_0 = 1, \quad p_1 = a_0.$$
$$q_n = a_n q_{n-1} + q_{n-2}, \quad q_0 = 0, \quad q_1 = 1.$$

Тогда фундаментальное решение уравнения Пелля при четном периоде k равно:

$$(x_1, y_1) = (p_k, q_k).$$

Классические методы требуют экспоненциального времени, поскольку длина записи (x_1, y_1) может расти экспоненциально. Квантовый алгоритм позволяет найти $R = log(x_1 + y_1\sqrt{d})$ за полиномиальное время, используя поиск скрытой подгруппы.

1. Квантовый компьютер вычисляет $[R]$, что соответствует периоду цепной дроби.

2. Затем классический алгоритм восстанавливает (x_1, y_1) с помощью метода цепных дробей.

3. Таким образом, решается уравнение Пелля за полиномиальное время, тогда как классические методы требуют экспоненциального времени.

Результаты

Разработана программа и псевдокод для нахождения минимального решения уравнения Пелля:

Функция continued_fraction(d):

Функция разложения корень от d в цепную дробь

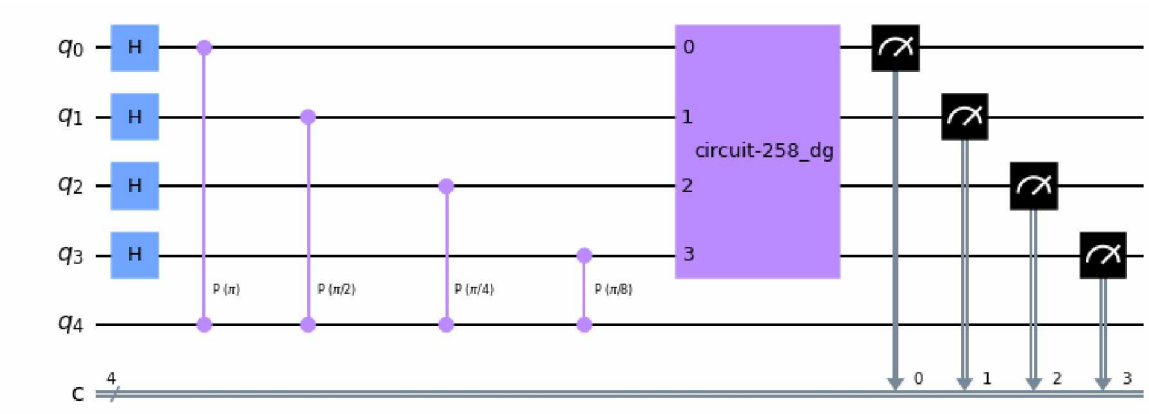
```
a0 ← floor(sqrt(d)) // Целая часть корня
Если a0^2 = d, то вернуть None // d не должен быть полным квадратом

  m ← 0, d_k ← 1, a ← a0
  fraction_terms ← [a0]

  Пока a ≠ 2 * a0:
    m ← d_k * a - m
```

```
        d_k ← (d - m^2) / d_k
        a ← floor((a0 + m) / d_k)
        Добавить a в fraction_terms
    Вернуть fraction_terms
Функция нахождения минимального решения
Функция solve_pell(d):
    fraction_terms ← continued_fraction(d)
    Если fraction_terms = None, вернуть None
    k ← длина fraction_terms - 1
numerators ← [1, fraction_terms[0]]
denominators ← [0, 1]
    // Вычисляем приближения
Для i от 2 до k+2:
numerators[i] ← fraction_terms[i-1] * numerators[i-1] + numerators[i-2]
denominators[i] ← fraction_terms[i-1] * denominators[i-1] + denominators[i-2]
    Если k четное:
x1 ← numerators[k]
y1 ← denominators[k]
    Иначе:
fraction_terms ← fraction_terms + fraction_terms[1:k+1]
numerators ← [1, fraction_terms[0]]
denominators ← [0, 1]
        Для i от 2 до 2k+2:
numerators[i] ← fraction_terms[i-1] * numerators[i-1] + numerators[i-2]
denominators[i] ← fraction_terms[i-1] * denominators[i-1] + denominators[i-2]
x1 ← numerators[2k]
y1 ← denominators[2k]
Вернуть (x1, y1)
```

Квантовая схема имеет следующий вид:



Получены следующие значения:

Результаты измерений: {'01000': 8, '00000': 936, '00111': 3, '10000': 9, '00001': 20, '00011': 4, '00010': 18, '01111': 3, '00100': 10, '01101': 2, '11000': 3, '00101': 1, '11111': 2, '01011': 1, '11100': 1, '00110': 1, '01010': 1, '01100': 1}

Приближенное значение |R⟩: 0.0

Минимальное решение уравнения Пелля: x1 = 8, y1 = 3

Заключение

В данной работе представлен квантовый алгоритм для нахождения минимального решения уравнения Пелля, основанный на методах поиска скрытой абелевой подгруппы и квантового преобразования Фурье (QFT). Мы показали, что этот алгоритм позволяет находить приближенное значение ⌊R⌋ за полиномиальное время, тогда как классические алгоритмы решают эту задачу за экспоненциальное время. Проведенная симуляция квантового алгоритма на платформе IBM Qiskit продемонстрировала его корректность. Измеренные значения квантового регистра позволили восстановить приближенное значение R, что привело к успешному нахождению минимального решения уравнения Пелля. Квантовый алгоритм решает уравнение Пелля за полиномиальное время, используя периодичность цепных дробей. Результаты симуляции подтверждают эффективность алгоритма, но показывают влияние ошибок, связанных с ограниченной разрядностью квантового регистра и возможными шумами вентилей. Практическое применение алгоритма включает возможную компрометацию криптосистемы Бухмана-Вильямса, аналогично тому, как алгоритм Шора угрожает RSA. Квантовый алгоритм решения уравнения Пелля демонстрирует превосходство над классическими методами и открывает перспективы для дальнейших исследований в области квантовых вычислений и их криптографических приложений.

Список использованных источников

1. Холлгрен С. Квантовые алгоритмы полиномиального времени для уравнения Пелля и задачи главного идеала. В материалах 34-го симпозиума ACM по теории вычислений, 2002.

2. Шор, П. В. (1994). Алгоритмы для квантовых вычислений: дискретные логарифмы и факторизация. Материалы 35-го ежегодного симпозиума по основам компьютерных наук (FOCS), 124–134. https://doi.org/10.1109/SFCS.1994.365700.

3. Ллойд, С. (1996). Универсальные квантовые симуляторы. Science, 273(5278), 1073–1078. https://doi.org/10.1126/science.273.5278.1073.

References

1. Hallgren S. Polynomial-time quantum algorithms for Pell's equation and the principal ideal problem. In Proceedings of the 34th ACM Symposium on Theory of Computing, 2002.

2. Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. Proceedings of the 35th Annual Symposium on Foundations of Computer Science (FOCS), 124–134. https://doi.org/10.1109/SFCS.1994.365700

3. Lloyd, S. (1996). Universal quantum simulators. Science, 273(5278), 1073–1078. https://doi.org/10.1126/science.273.5278.1073