МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«Национальный исследовательский Нижегородский государственный университет им. Н.И. Лобачевского» (ННГУ)

Институт информационных технологий, математики и механики

Кафедра: Прикладная математика

Профиль подготовки: «Прикладная математика и информатика»

ОТЧЕТ

по учебной технологической (проектно-технологической) практике

на тему:

«Квантовые вычисления: Реализация алгоритма Шора с использованием библиотеки Qiskit от IBM.»

Выполнил: студент группы 3821Б1ПМоп2

_____Богдашкин Сергей Евгеньевич
Подпись

Научный руководитель:
зав. каф. ВВиСП ИИТММ ННГУ

_____Мееров Иосиф Борисович
Подпись

Нижний Новгород
2024

Содержание

1 Введение

Квантовые вычисления представляют собой одно из самых перспективных направлений современной науки и технологий, находящееся на стыке физики, информатики и математики. Квантовые компьютеры, основанные на принципах квантовой механики, обещают значительно превосходить классические компьютеры в решении ряда сложных задач, таких как факторизация больших чисел, моделирование квантовых систем и исследование сложных многомерных пространств.

Рост современных технологий потребовал решения сложных задач, превышающих возможности классического подхода. Наиболее значимой областью является криптография, где квантовые алгоритмы, такие как алгоритм Шора для факторизации чисел, демонстрируют значительные преимущества. Также квантовые вычисления открывают новые горизонты в таких областях, как:

- Химия и материалы: моделирование и оптимизация молекулярных структур, что имеет важное значение в разработке новых лекарств и материалов.

- Машинное обучение: улучшение алгоритмов обучения и оптимизация поиска в больших объемах данных.

- Логистика и оптимизация: решение сложных задач, связанных с оптимизацией маршрутов и распределением ресурсов.

Актуальность исследовательской деятельности в квантовых вычислениях обуславливается быстрым развитием физических технологий, необходимых для создания устойчивых и масштабируемых квантовых систем. Большие технологические компании, такие как IBM, Google, Microsoft, инвестируют значительные ресурсы в развитие квантовых компьютеров и соответствующего программного обеспечения. Универсальные квантовые компьютеры способны решить задачи, которые ранее просто не были выполнимы, что делает квантовые вычисления чрезвычайно актуальным направлением исследований.

Несмотря на обширные перспективы, квантовые вычисления сталкиваются с рядом сложностей:

Физическая реализация кубитов: кубиты крайне чувствительны к шуму и внешним воздействиям, требующим поддержания весьма специфических условий для стабильной работы.

Квантовая декогеренция: квантовые состояния склонны к разрушению под воздействием взаимодействий с окружением, что усложняет длительные вычисления.

Ошибки и коррекция ошибок: необходимость создания и внедрения механизмов коррекции ошибок для поддержания точности вычислений.

Алгоритмическая сложность: разработка и внедрение эффективных алгоритмов для квантовых компьютеров требует кардинально нового подхода по сравнению с классическими вычислениями.

Исследования в области квантовых вычислений охватывают широкий спектр направлений, каждое из которых вносит свой вклад в понимание и развитие технологии. В обобщении можно выделить несколько подходов и классификаций:

- Алгоритмы и теории:

Алгоритм Шора: разработан для эффективной факторизации целых чисел, представляет фундаментальный прорыв в криптографии.

Алгоритм Гровера: используется для поиска элементов в неструктурированных базах данных, повышая скорость поиска.

Квантовые симуляции: алгоритмы для моделирования квантовых систем, что имеет значительное приложение в химии и физике.

- Физическая реализация:

Сверхпроводники: используются для создания кубитов с длительными временами когерентности и высокой надежностью.

Ионные ловушки: кубиты реализованы при помощи удержания ионов в электромагнитных полях, обеспечивая высокую точность манипуляций.

Фотоны: использование квантового света для передачи информации с минимальными потерями.

- Квантовая декогеренция и коррекция ошибок:

Коды коррекции ошибок: разрабатываются для защиты квантовой информации от ошибок, возникающих из-за внешних воздействий.

Схемы коррекции ошибок на уровне аппаратного обеспечения: направлены на улучшение устойчивости кубитов к шумам и другим внешним воздействиям.

- Программное обеспечение и симуляторы:

Qiskit от IBM: предоставляет пользователям инструменты для разработки и выполнения квантовых алгоритмов, позволяя им взаимодействовать с реальными квантовыми процессорами.

Cirq от Google: облегчает разработку квантовых алгоритмов и выполнение их на квантовых процессорах.

MSQDT от Microsoft: направлена на интеграцию квантового программирования в привычные пользователям среды разработки.

Актуальные события и инициативы.

Квантовые вычисления активно развиваются и на уровне государства. В частности, Россия утвердила Дорожную карту по квантовым вычислениям, которая направлена на развитие квантовых технологий и создание квантовых компьютеров. Это включает инвестиции в исследования, развитие инфраструктуры и подготовку специалистов в этой области.

Всероссийский квантовый хакатон, прошедший в Нижегородской области с 21 по 24 ноября, организованный Нижегородским научно-образовательным центром, ИНТЦ "Квантовая долина" и ННГУ им. Н.И. Лобачевского при поддержке Российского квантового центра, продемонстрировал высокую востребованность квантовых технологий. В нём приняли участие команды из студентов, аспирантов и молодых учёных, которые решали задачи в области оптимизации и машинного обучения с использованием квантовых вычислений. Мероприятие способствовало повышению уровня знаний участников, популяризации квантовых технологий и предоставило победителям возможность стажировки в ведущих российских компаниях. Программа включала лекции, мастер-классы и панельные дискуссии, что позволило участникам обсудить новейшие достижения и применение квантовых технологий в реальном секторе экономики.

Развитие квантовых вычислений открывает новые перспективы в различных областях науки и промышленности. Дорожная карта России по квантовым вычислениям и мероприятия, такие как квантовый хакатон, подтверждают высокую востребованность и перспективность данной области. В рамках данной практической работы будет изучен и реализован алгоритм Шора с использованием библиотеки Qiskit от IBM, что позволит получить ценные знания и опыт в области квантовых вычислений.

2 Постановка задачи

2.1 Задача факторизации. Алгоритм Шора.

Факторизация натурального числа заключается в его разложении на простые множители, что гарантируется основной теоремой арифметики. Эта задача предположительно является вычислительно сложной, и на данный момент неизвестно существование эффективного классического алгоритма для ее решения. Однако также не доказано, что такой алгоритм невозможен.

Сложность факторизации больших чисел лежит в основе многих криптографических алгоритмов, таких как RSA. Применение различных математических подходов, включая эллиптические кривые, алгебраическую теорию чисел и квантовые вычисления, показывает широкий интерес к этой задаче.

Алгоритм Шора представляет собой квантовый алгоритм факторизации с полиномиальной сложностью. Его значимость заключается в том, что он позволяет, при наличии квантового компьютера с тысячами логических кубитов, взламывать криптографические системы с открытым ключом.

Примером такой системы является RSA, где открытый ключ M представляет собой произведение двух больших простых чисел. Взлом шифра RSA требует нахождения этих множителей, что практически невозможно с помощью существующих классических алгоритмов. Алгоритм Шора может значительно ускорить этот процесс, выполняя факторизацию за полиномиальное время. Это ставит под угрозу текущую криптографическую защиту, основанную на сложности факторизации, включая не только RSA, но и аналогичные схемы.

Таким образом, достижения в области квантовых вычислений предвещают значительные изменения в криптографии и информационной безопасности.

2.2 Постановка задачи учебной практики.

Целью работ на третьем курсе являлось изучение принципов квантовых вычислений и реализация достаточно сложного квантового алгоритма алгоритма с использованием симулятора идеального квантового компьютера.

В ходе выполнения работ по по учебной технологической (проектно-технологической) практике осеннего семестра были решены следующие задачи:

- Изучен алгоритм Шора, вспомогательные алгоритмы его классической и квантовой частей.
- Вспомогательный алгоритм квантовой части – квантовое преобразование Фурье — реализован с использованием симулятора IBM qiskit.

Для достижения целей в весеннем семестре было необходимо решить следующие задачи:

1. Реализовать все вспомогательные алгоритмы квантовой части алгоритма Шора.
2. Реализовать алгоритм, выполняющий построение квантовой схемы квантовой части алгоритма Шора для заданных входных параметров с использованием библиотеки симуляции квантовых вычислений IBM qiskit.
3. Провести эксперименты для проверки работоспособности, производительности и сложности алгоритма.

3 Квантовые вычисления.

3.1 Состояние Квантовой системы. Идеальный квантовый компьютер.

Идеальный квантовый компьютер – это теоретическое устройство, которое с максимальной точностью выполняет вычисления, опираясь на квантовую механику. Такой компьютер использует кубиты – квантовые аналоги классических битов, способные находиться одновременно в состоянии 0 и 1. Основные свойства идеального квантового компьютера включают: отсутствие декогеренции, идеальные унитарные гейты и полная изоляция от внешних помех.

Состояние идеального квантового компьютера может быть описано вектором состояния в гильбертовом пространстве. Для системы из 2 кубитов, это состояние будет суперпозицией всех возможных базисных состояний:

$$|\psi\rangle = u\,|0\rangle \;+\; v\,|1\rangle$$

Где комплексные коэффициенты u и v удовлетворяют следующему условию: $|u|^2 + |v|^2 = 1.$

Математическое описание базисных состояний сводится к их представлению в матричном виде:

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

На основе этого представления записывается произвольное состояние кубита: $|\psi\rangle = \begin{bmatrix} u \\ v \end{bmatrix}.$

Система из двух кубитов задается линейной комбинацией состояний:

$$|00\rangle = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \quad |01\rangle = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \quad |10\rangle = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}, \quad |11\rangle = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}.$$

Аналогичным образом вводятся состояния

$$|00\ldots00\rangle,\ |00\ldots01\rangle,\ \ldots,\ |11\ldots11\rangle$$

для системы из нескольких взаимодействующих между собой кубитов. Такие квантовые состояния называются состояниями вычислительного базиса.

В общем случае состояние квантовой системы из N кубитов описывается вектором $|\psi\rangle \in \mathbb{C}^{2^N}$ гильбертова пространства.

3.2 Операции над кубитами (гейты).

Квантовые гейты – это унитарные операции, которые изменяют состояние кубитов. Они смещают и вращают вектор состояния в гильбертовом пространстве. Основные квантовые гейты включают:

Гейт Адамара:

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

Гейт Паули-X: аналог логической операции NOT, меняющий местами состояния 0 и 1.

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

Поворот, фазовый сдвиг:

$$P(\varphi) = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{bmatrix}$$

Контролируемое отрицание: Гейт Swap:

$$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} SWAP = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Широко применяется графическое представление квантовых операций в виде схем или диаграмм. Квантовая схема — это упорядоченная последовательность элементов и соединяющих их линий связи, т.е. «проводов». Обычно рассматривают только ациклические схемы, в которых данные проходят в одном направлении — слева направо, и провода не возвращают биты в предыдущее положение в схеме. Входные состояния приписываются проводам, входящим слева. За один шаг по времени каждый провод может вводить данные не более чем в один гейт. Выходные состояния считываются с линий связи, выходящих из схемы справа.

Далее, для удобства и простоты реализация алгоритма будет рассматриваться путем последовательного объединения и созданий гейтов и представления их на общей схеме.

Измерение – это процесс, при котором квантовое состояние переходит в одно из классических состояний с определенной вероятностью. Если кубит находится в суперпозиции:

$|\psi\rangle = \alpha | 0 \rangle + \beta | 1 \rangle$

то при измерении он перейдет в состояние 0 с вероятностью |α|^2 и в состояние 1 с вероятностью |β|^2. Измерение нарушает исходное квантовое состояние, фиксируя его в одно из возможных базисных состояний.

Квантовые вычисления являются революционным подходом к решению задач, которые намного превышают возможности классических компьютеров. В прошлом семестре были подробно рассмотрены вспомогательные операции для квантовых алгоритмов, в частности квантовое преобразование Фурье. Все это составляет основу для разработки эффективных квантовых алгоритмов и позволяет квантовым компьютерам выполнять вычисления с невероятной скоростью и точностью. Развитие квантовых вычислений продолжает находить новые возможности в различных областях науки, техники и промышленности.

4 Квантовые вычисления.

4.1 Введение. Математическая основа и структура алгоритма Шора.

В основе алгоритма Шора лежит идея сведения задачи факторизации числа к задаче нахождения периода последовательности [1]. Как нетрудно показать, если последовательность $|\alpha\_1, \alpha\_2, \ldots, \alpha\_\{M-1\}$ имеет период k, где k - делитель M , т.е. $a_i = a_j$ при любых $i \equiv j\,(mod)\,k$, для соответствующего состояния квантовой системы:

$$|\alpha\rangle = \sum_{j=0}^{M-1} \alpha_j \,|j\rangle$$

выборка из преобразования Фурье (повторенная достаточное количество раз) позволяет с большой вероятностью найти его период [3].

Действительно, рассмотрим вектор $|\alpha>$, который имеет период k и сдвиг 0 (с ненулевыми членами $\alpha_0, \alpha_k, \alpha_{2k}, \ldots,$ всего k/M штук). Чтобы сумма квадратов всех модулей ненулевых членов равнялась 1, сделаем их равными $\sqrt{k/M}$

$$|\alpha\rangle = \sum_{j=0}^{M/k-1} \sqrt{\frac{k}{M}}\,|jk\rangle\,.$$

В этом случае преобразование Фурье также будет периодическим с периодом M /k и сдвигом 0:

$$|\beta\rangle = \frac{1}{\sqrt{k}} \sum_{j=0}^{k-1} |\frac{jM}{k}\rangle\,.$$

Иными словами, преобразование Фурье β сосредоточено в слагаемых с номерами, кратными M /k. При многократном измерении подобной квантовой системы мы получим гистограмму, на которой видны пики в индексах, кратных M /k. Таким образом, задача о нахождении периода последовательности решена.

Чтобы свести задачу факторизации числа к задаче нахождения периода последовательности, воспользуемся известным из алгебры суждением[2]:

Лемма. *Пусть N — нечётное составное число, имеющее как минимум два разных простых множителя. Выберем случайное число x от 0 до $N-1$, взаимно простое с N, считая все такие числа равновероятными. Тогда с вероятностью $1/2$ или больше порядок r числа x по модулю N окажется чётным, а число $x^{r/2}$ будет нетривиальным квадратным корнем из N.*

Порядком числа x по модулю N называется наименьшее положительное целое число r, при котором $x^r \equiv 1 \pmod N$.

Если для натурального числа a взять последовательность его степенейa^1, a^2, …, a^M,

то последовательностm $(a^1 \, mod \, N)$, $(a^2 \, mod \, N)$, …, $(a^M \, mod \, N)$ остатков этих чисел по модулю N будет периодической с периодом r, где r - порядок числа a по модулю N.

Для такой последовательности с помощью выборки из квантового преобразования Фурье можно получить ее период. Следовательно, можно применить Лемму для нахождения делителя числа N. Таким образом, мы подошли к общей схеме алгоритма Шора.

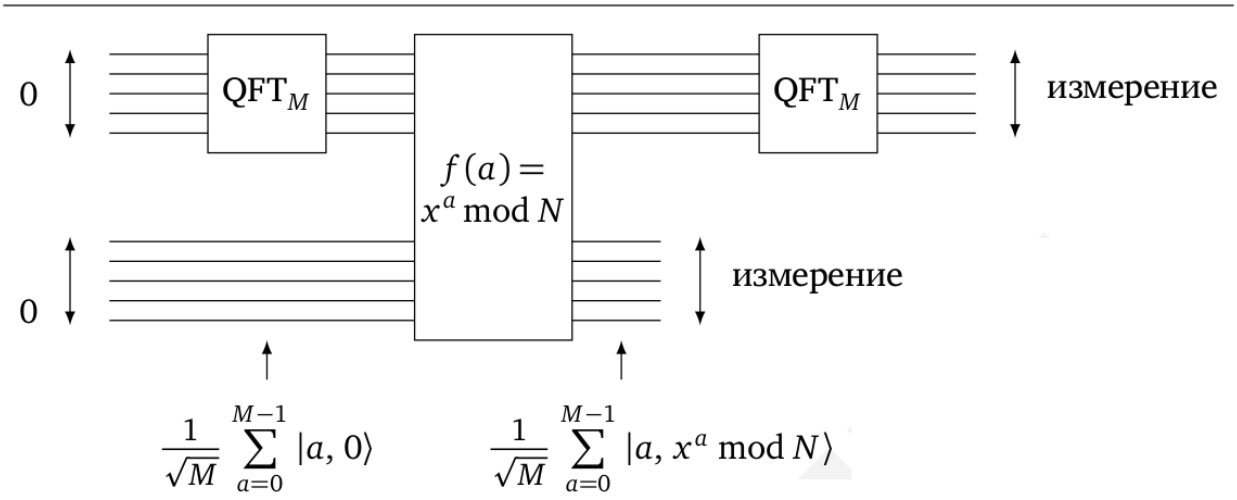


Рис. 1 Квантовый алгоритм разложения на множители.

4.2 Общая схема алгоритма Шора.

Вход: составное нечетное N

Выход: один из множителей N

1. Проверим, не представляется ли исходное число в виде степени натурального числа $N = p^q$, $p \geq 1$ и $q \geq 2$. Если представляется, то множитель найден.
2. Выбираем случайное (равномерно распределенное) число x между 1 и $N - 1$. Если НОД$(x, N) = 1$, то множитель найден, иначе продолжаем.
3. В качестве M выберем степень двойки, близкую к N.
4. Повторяем $s = 2 \log N$ следующие действия:
    a. Слова из нулевых битов помещаем в два квантовых регистра, первый из которых вмещает в себя остаток по модулю M, а второй - по модулю N.
    b. Используем периодическую функцию $f(a) = x^a \, mod \, N$ для создания периодической суперпозиции длины M:
        i. Применяем квантовое преобразование Фурье к первому регистру и получаем в нём суперпозицию
        $$\sum_{x=0}^{M-1} \frac{1}{\sqrt{M}} |a, 0\rangle$$
        ii. Вычисляем $f(a) = x^a \, mod \, N$ с использованием квантовой схемы, получаем суперпозицию:

$$\sum_{x=0}^{M-1} \frac{1}{\sqrt{M}} |a, x^a \mod N\rangle$$

iii. Измеряем содержимое второго регистра. После этого первый регистр содержит периодическую суперпозицию:

$$|\alpha\rangle = \sum_{j=0}^{M/r-1} \sqrt{\frac{r}{M}} |jr + k\rangle ,$$

Где k - некоторый сдвиг между 0 и r − 1, а r - период x по модулю N.

c. Производим квантовую выборку из преобразования Фурье первого регистра, получая в результате некоторый индекс между 0 и M − 1. Пусть g - наибольший общий делитель полученных индексов $j_1, \ldots, j_s$

5. Если M /g чётно, то вычисляем $\text{НОД}\left(N, x^{\frac{M}{2g}} + 1\right)$. Если мы получили нетривиальный делитель N, выдаём его в качестве результата, иначе повторяем выполнение алгоритма с шага 2.

* Более подробно схема описана в работе [4].

4.3 Описание вспомогательных гейтов в алгоритме Шора.

Квантовое преобразование Фурье.

Квантовое преобразование Фурье — линейное преобразование квантовых битов (кубитов), являющееся квантовым аналогом дискретного преобразования Фурье. Реализация квантового преобразования Фурье подробно описана в работе [5].

ъ

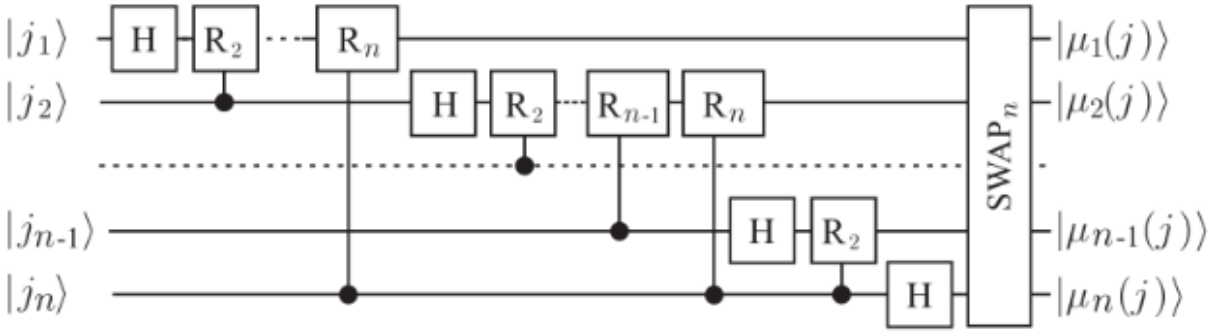


Рис. 2 Квантовая схема Фурье-преобразования n-кубитов.

Квантовое сложение .

Квантовое сложение - схема, применяемая для сложения двух чисел и оптимальная для запуска на квантовом компьютере. С ее помощью можно складывать число, хранящееся в классическом представлении с числом из пространства Фурье [2]. Схема выполняет преобразование:

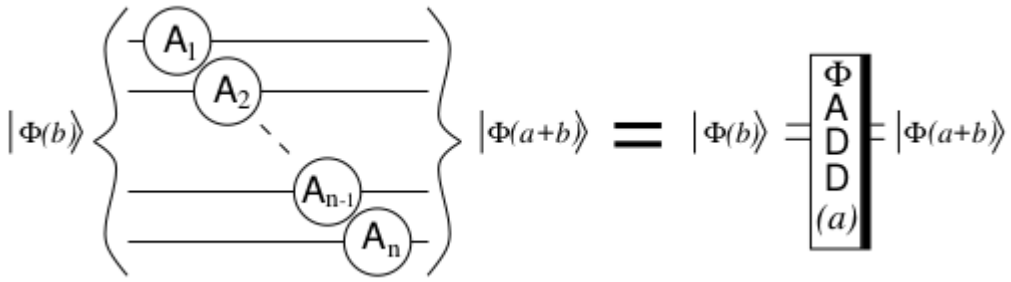


Рис. 3 Схема для сложения классического значения a и квантового значения b в пространстве Фурье. Гейты A_i вычисляются классическими комбинациями фазовых сдвигов..

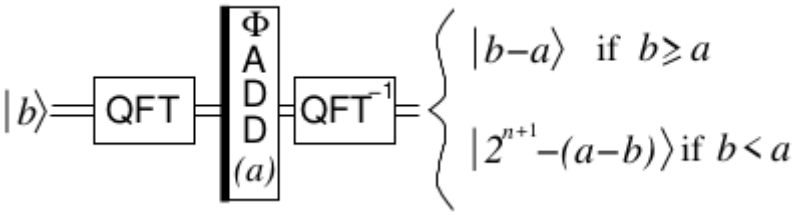
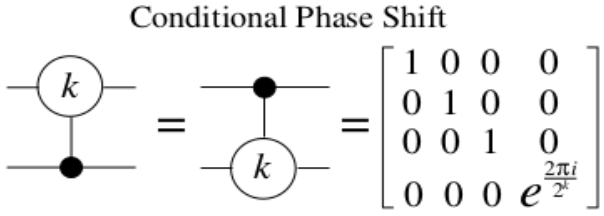


Рис. 4 Эффект обратного гейта ϕADD(a) на |ϕ(b)|

Реализация гейта сложения и поворота.



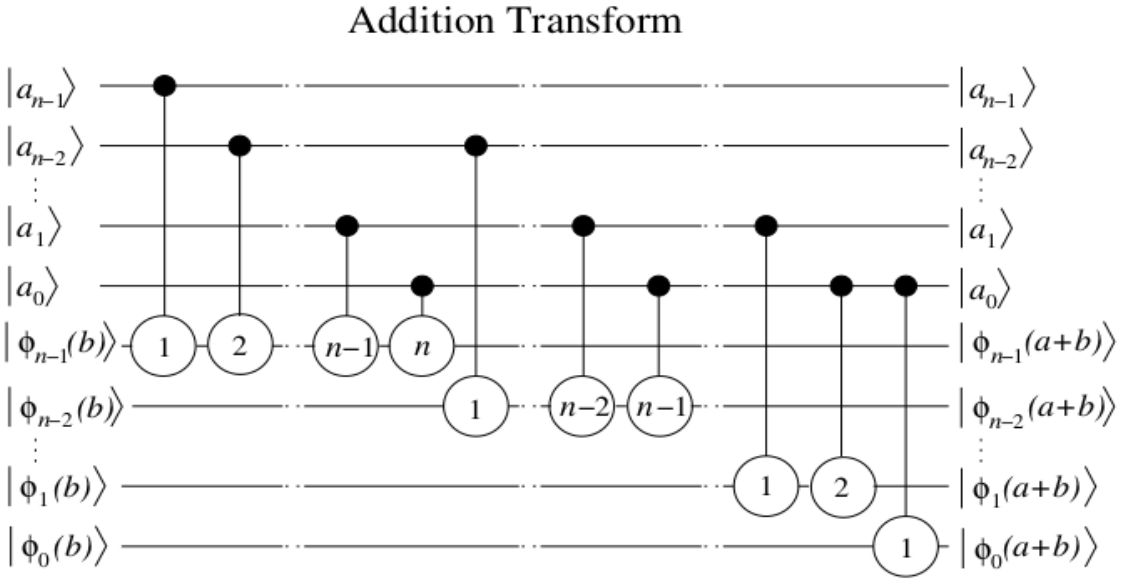


Рис. 5 Квантовое сложение, описанное Дрейпером [6]

Реализация гейта сложение по модулю .

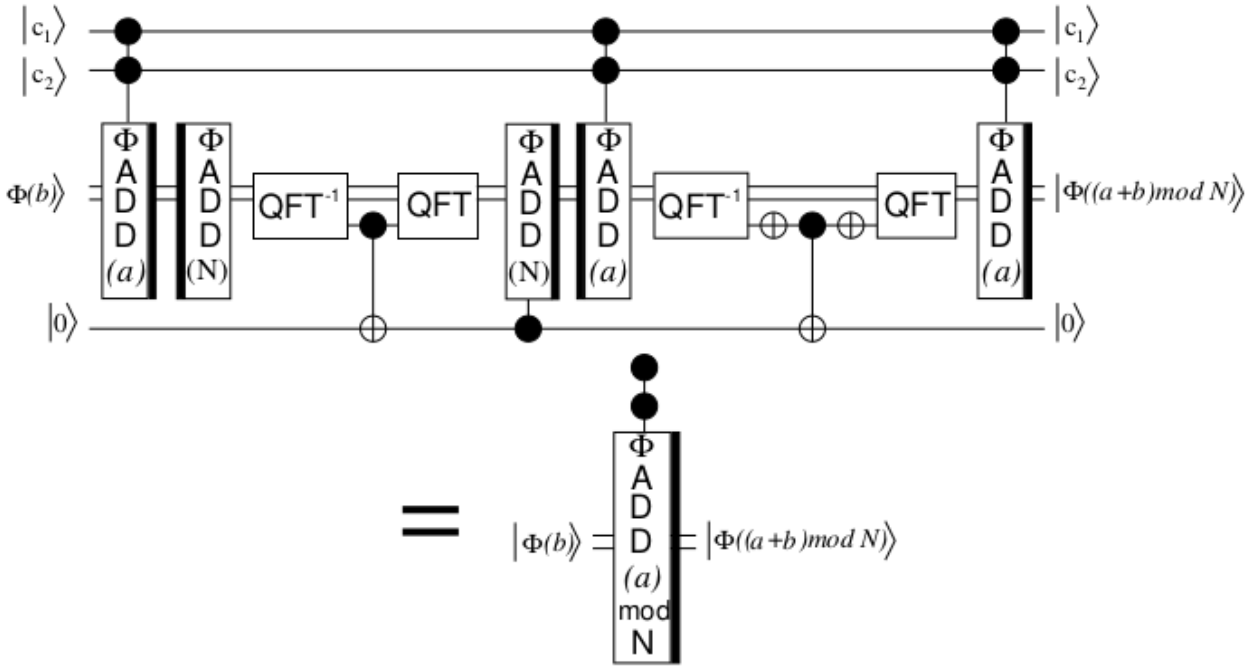


Рис. 6 Дважды контролируемый ФADD(a)MOD(N) гейт с c1 = c2 = 1. Если один из контролирующих кубитов в состоянии |0i, результат выполнения операции |Φ(b)i при b < N.

Реализация гейта умножения по модулю .

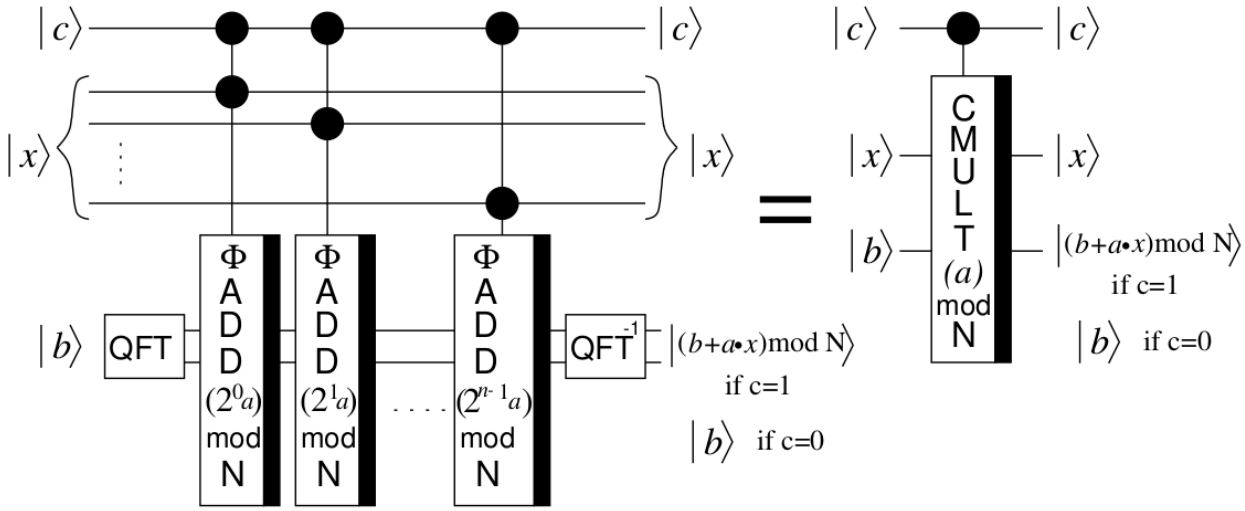


Figure 6: The $CMULT(a)MOD(N)$ gate.

Рис. 7 Схема CMULT(a)MOD(N) гейта (умножение по модулю).

Вышеописанная последовательность гейтов на схеме, позволяет нам реализовать главный в алгоритме Шора **гейт Возведения в степень.**

*Именно эта операция нам и нужна для вычисления периодической функции $f(a) = a^x \ mod \ N$.

\

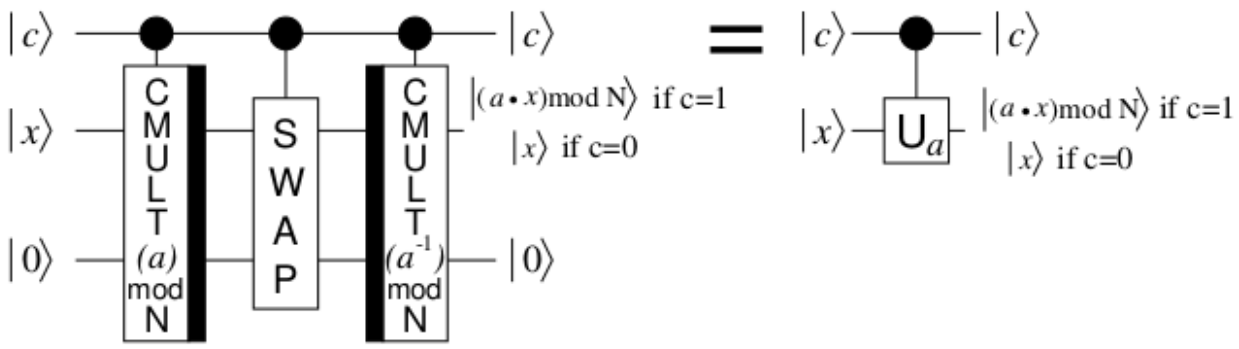


Рис. 8 схема контролируемого U_a гейта.

Далее, последовательно применяя гейты $U_{a^{2^0}}, U_{a^{2^1}}, U_{a^{2^2}}, \ldots, U_{a^{2^{2n-1}}}$ мы можем потроить итоговую схему для периодической функции $f(a) = a^x \, mod \, N$.

На этом этапе мы получаем всё необходимое, чтобы собрать итоговую схему для квантвой части алгоритма Шора:

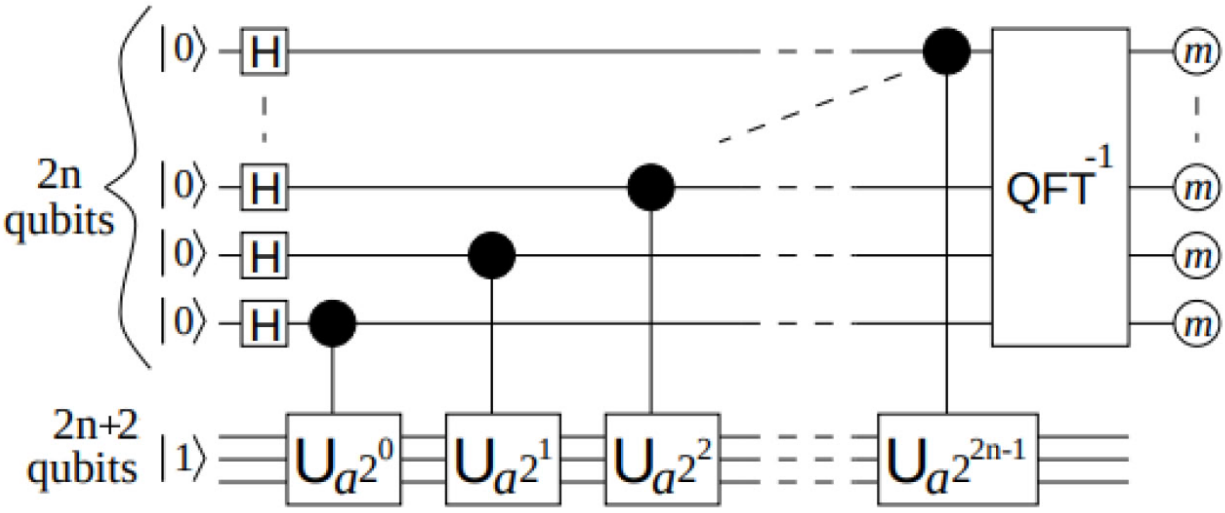


Рис. 9 Квантовая часть алгоритма Шора. U_a реализует $|x \succ \rightarrow |(ax) \, mod \, N \succ$.

После измерения и классической постобработки получаем порядок r числа a по модулю N.

Такой алгоритм требует 4n + 2 кубит для разложения n-битного числа N < 2n. Именно он и был реализован в рамках научной работы с помощью библиотеки qiskit от IBM. Последовательная реализация всех гейтов представлена в приложении А.

В статье Стефана Борегара [2] также представлена реализация общей схемы 2n+3 кубит. Для достижения этой оптимизации нужно изменить измерение результатов с параллельного процесса на последовательное измерение. Это сокращает верхний регистр/control, который в начале алгоритма Shor будет снабжен 2n множеством адамаров, до одного кубита.

5 Вычислительные эксперименты.

5.1 Выполнение алгоритма Шора.

Представим общую схему квантовой части алгоритма Шора: на регистр, содержащий суперпозицию всех базисных состояний, накладывается периодическая функция, после чего проводится квантовое преобразование Фурье. В результате, состояние регистра будет сосредоточено в компонентах, кратных числу r — искомому периоду. Это значит, что при измерении системы вероятность получить одно из базисных состояний, кратных r, крайне высока. Повторяя данный эксперимент достаточное количество раз, можно построить гистограмму распределения результатов, в которой пики указывают на значения, кратные r. Таким образом, по гистограмме мы можем определить период r и, соответственно, с высокой вероятностью решить задачу факторизации числа. Рассмотрим данный процесс на примере.

Как отмечалось ранее, для разложения n-битного числа потребуется 4n+2 кубита. В симуляторе это выражается в необходимом размере вектора, содержащего 2^{4n+2} значений. Тестирование алгоритма имеет смысл проводить на составных нечетных числах, которые не являются степенью натурального числа. Ввиду ограничений по физической памяти вычислительных устройств, эксперименты будем проводить только для чисел 15 и 21. Оценки затрат памяти для применения алгоритма Шора к составным нечетным числам приведены в таблице:

N	n	Длина вектора состояния
15	4	2^{18}
21	5	2^{22}
35	6	2^{26}

Рассмотрим подробно работу алгоритма Шора для разложения числа $N = 15$ и покажем корректность выполнения. Выбираем случайное число $x = 2$, $\text{НОД}(x, N) = 1$.Выбираем $M = 2^{2 \cdot 4} = 256$.

Выполняем квантовую часть алгоритма, сначала построим необходимую схему (рис. 10), следом, измерениями на идеальном квантовом симуляторе получим гистограмму (Рис. 11). с пиками в значениях: 0, 64, 128, 192(гистограмма представлена в двоичной системе счисления). Так как наш квантовый симулятор моделирует идеальный квантовый компьютер, указанные пики хорошо заметны на диаграмме. Здесь происходит идеальная симуляция, поэтому наши значения представлены чётко.

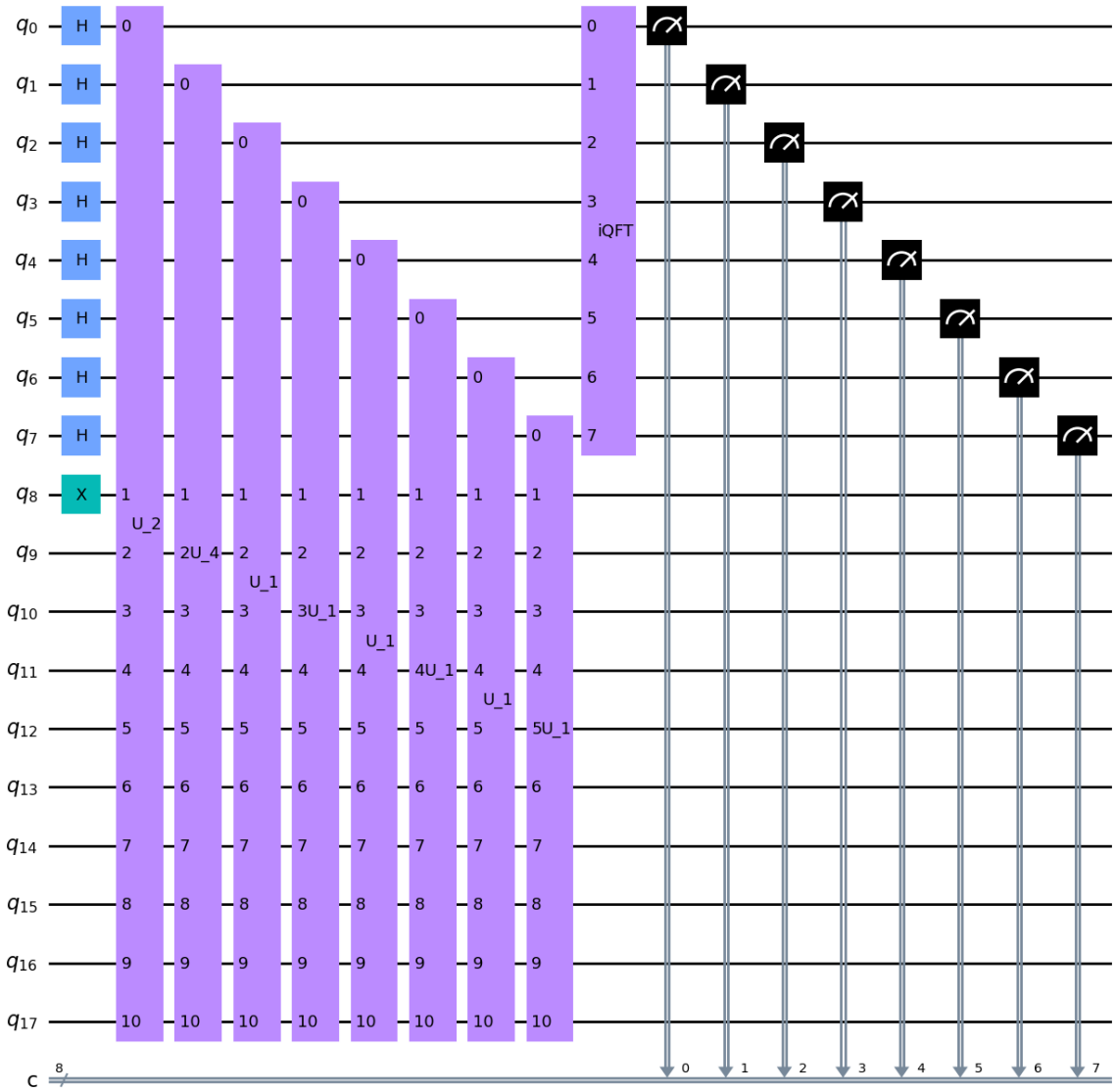


рис. 10 Квантовая схема полученная для N=15, a=2, n=4

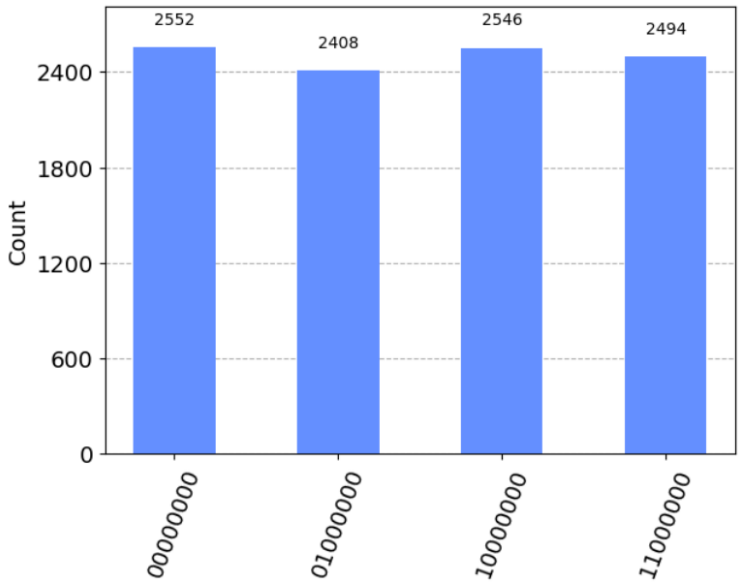


Рис. 11 гистограмма, полученная в результате 10 000 запусков на симуляторе схемы(рис. 10)

Наибольшим общим делителем полученных чисел будет $\text{НОД}\,(0,\ 64,\ 128,\ 192) = 64$. Число $M/g = 4$ чётно. $\text{НОД}\left(N,\ x^{\frac{M}{2g}} + 1\right) = 5$ - искомый делитель числа $N = 15$.

Также, представим гистограммы, полученные для N= 21 и N=35 (для a=13):

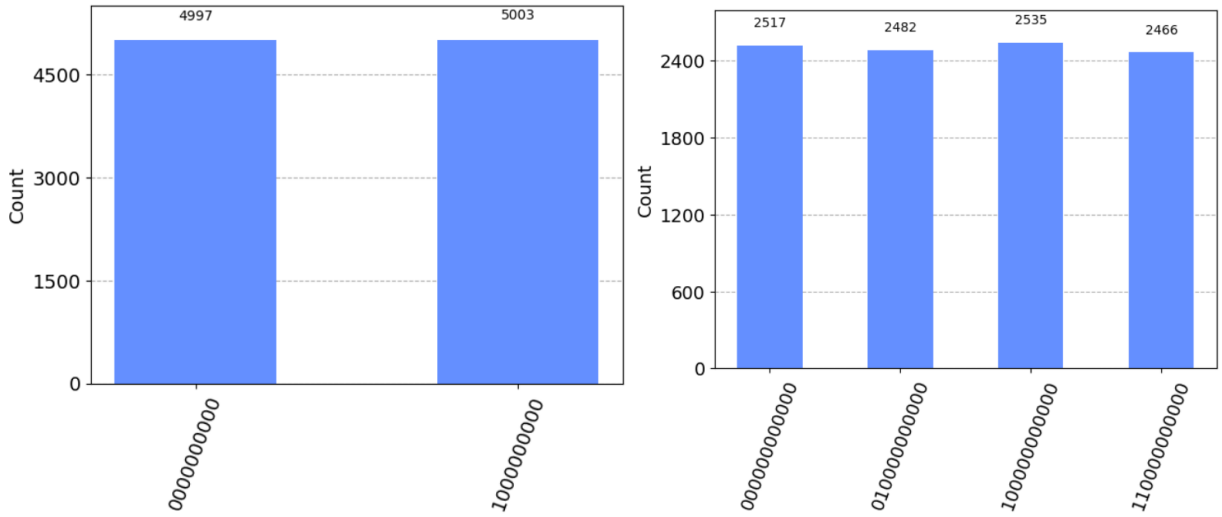


Рис. 12 гистограммы для факторизации N=21 и N=35 (при a=13)

5.2 Вычислительные эксперименты

Проверка корректности/работоспособности алгоритма

Целью данного эксперимента было убедиться в способности квантовой части алгоритма Шора выделять порядок числа и находить множители заданных чисел. Алгоритм проверялся на парах значений (N, a), где N — число, подлежащее факторизации, a — основание, выбранное случайным образом так, чтобы НОД(a, N)=1.

Методика проведения эксперимента:

Для каждой пары (N, a) квантовая часть алгоритма запускалась на симуляторе, и результаты измерений сохранялись в виде гистограммы. На основе полученной гистограммы выделялся порядок, необходимый для выполнения классической части алгоритма Шора и нахождения множителей числа N. Примеры полученных гистограммы приведены на рис. 11-12.

Таблица результатов экспериментов:

(N, a)	Выделенный порядок	Найденное разложение
(15, 2)	4	3 × 5
(21, 13)	2	3 × 7
(35, 13)	4	5 × 7

Таким образом, квантовая часть алгоритма успешно выделяет порядок, что подтверждается полученными разложениями чисел N.

Эксперименты показали, что алгоритм Шора на квантовом симуляторе корректно выделяет порядок и находит множители чисел N, что подтверждает его работоспособность.

Оценка сложности симуляции

Цель данного эксперимента заключалась в экспериментальной оценке сложности алгоритма Шора при использовании квантового симулятора из библиотеки IBM qiskit.

```
simulator = qiskit.Aer.get_backend('aer_simulator')
```

Были произведены замеры времени работы симулятора и глубины квантовой схемы для чисел с различным количеством бит в двоичном представлении (4, 5, 6).

Методика проведения эксперимента:

Алгоритм Шора запускался для чисел N = 15, N = 21 и N = 35 (с n=4, n=5, n=6 соответственно). Для каждого случая измерялось время работы алгоритма и глубина квантовой схемы.

Результаты экспериментов приведены на графике:

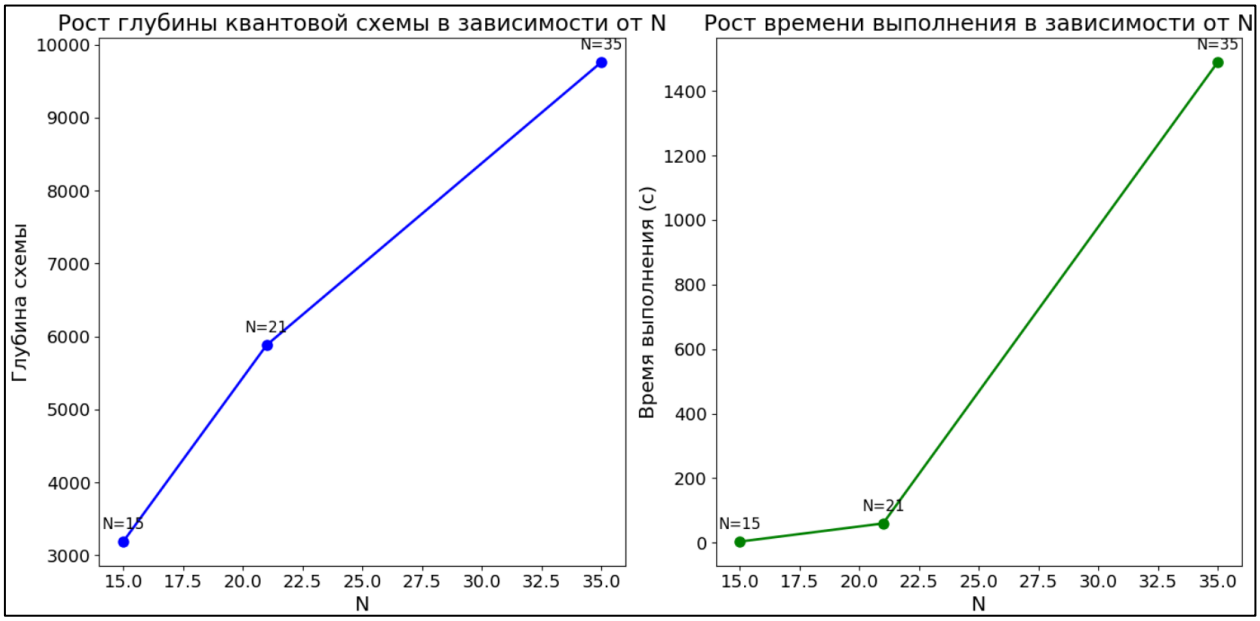


Рис. 13 График изменения глубины квантовой схемы и времени выполнения программы

Из проведенных экспериментов видно, что как глубина квантовой схемы, так и время выполнения значительно растут с увеличением числа бит в двоичном представлении числа N. Графики демонстрируют экспоненциальный рост сложности симуляции, что можно объяснить природой квантового алгоритма и необходимыми ресурсами для его симуляции на классическом компьютере.

Проект проделан с моделированием и оценкой ключевых параметров квантового алгоритма Шора, что является важным шагом к его реализации на квантовых устройствах.

6 Заключение

В ходе учебной практики были достигнуты поставленные цели и решены все задачи, предусмотренные программой. Изучение принципов квантовых вычислений и реализация алгоритма Шора позволили получить глубокие знания и практические навыки в области квантовой информатики.

Основные итоги учебной практики включают:

1. Изучение алгоритма Шора:

Проведено детальное изучение теоретических основ алгоритма Шора, включая его классическую и квантовую части. Понимание принципов работы алгоритма позволило приступить к его реализации на практике.

2. Реализация вспомогательных квантовых алгоритмов:

Успешно реализованы вспомогательные квантовые алгоритмы, такие как квантовое преобразование Фурье, с использованием симулятора идеального квантового компьютера IBM qiskit. Это стало основой для последующей полной реализации алгоритма Шора.

3. Реализация полной квантовой схемы алгоритма Шора:

Разработана и протестирована квантовая схема алгоритма Шора для заданных входных параметров, используя библиотеку для симуляции квантовых вычислений IBM qiskit. Это позволило увидеть алгоритм в действии и понять его применение для факторизации чисел.

4. Экспериментальная проверка:

Проведены эксперименты по проверке работоспособности, производительности и сложности алгоритма. Эти эксперименты показали, что алгоритм может эффективно функционировать при правильно заданных параметрах, а также позволили выявить возможные ограничения и области для улучшения.

Результаты учебной практики продемонстрировали умение работать с квантовыми алгоритмами и использовать современные квантовые технологии. Полученные знания и навыки могут быть применены в дальнейшем обучении и исследовательской деятельности в области квантовых вычислений.

7 Список литературы и источников информации

[1] Shor P. W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer //SIAM review. – 1999. – Т. 41. – №. 2. – С. 303-332.

[2] S. Beauregard (2003), Circuit for Shor's algorithm using 2n+3 qubits, Quantum Information and Computation, Vol. 3, No. 2, pp. 175-185. Also on quant-ph/0205095.

[3] Dasgupta S., Papadimitriou C. H., Vazirani U. V. Algorithms. – New York : McGraw-Hill Higher Education, 2008. – С. 336.

[4] Herman D. et al. A survey of quantum computing for finance //arXiv preprint arXiv:2201.02773. – 2022.

[5] Barenco A. et al. Approximate quantum Fourier transform and decoherence //Physical Review A. – 1996. – Т. 54. – №. 1. – С. 139.

[6] Draper T. G. Addition on a quantum computer //arXiv preprint quant-ph/0008033. – 2000.

[7] Lidar D. A. Lecture notes on the theory of open quantum systems //arXiv preprint arXiv:1902.00967. – 2019.