Криптография и квантовые вычисления[1]

Мурашко И. В.

[1]Санкт Петербургский Государственный Политехнический Университет

Оглавление

Введение

Целью данного курса является введение в современную криптографию и то каким образом квантовая механика может быть использована для решения сложных криптографических задач.

Курс состоит из 10 лекций, продолжительностью 1 час каждая.

Охватываются следующие вопросы

- Введение в квантовую механику (1, 2 лекции)
- Описание базовых принципов квантовых вычислений (3 лекция)
- Симметричные алгоритмы шифрования и алгоритм Гровера. (4 лекция)
- Классический алгоритм RSA и его связь с задачей поиска периода функции. (5 лекция)
- Дискретное (классическое) преобразование Фурье и его применения для поиска периода период функций. Предлагается реализация дискретного преобразования Фурье на квантовых элементах (6,7 лекция)
- Алгоритм Шора для взлома RSA (8 лекция)
- Классические алгоритмы шифрования, основанные на сложности дискретного логарифмирования. Модификация алгоритма Шора для решения задачи дискретного логарифмирования (9 лекция)
- Последняя лекция 10 лекция посвящена алгоритмам шифрования построенным на базе эллиптических кривых. Рассматривается алгоритм ECDH. Описывается модификация алгоритма Шора для решения задачи дискретного логарифмирования на эллиптических кривых.

По ходу лекций будут даваться необходимые математические пояснения, как то

- Дискретная математика: малая теорема Ферма, алгоритм Евклида и т.п.

- Общая алгебра: понятие группы, теорема Лагранжа, циклическая группа, понятие поля. Поля Галуа.
- Линейная алгебра и операции с матрицами: перемножение матриц, линейные операторы, собственные числа и собственные функции линейных операторов
- Классическая теория вероятности: события, случайные величины, среднее случайной величины

Глава 1

Классическая криптография

С того момента, как была осознана важность информации, стали появляться средства ее защиты.

Изобретались новые методы шифрования, такие например, как шифр Цезаря, в котором каждая буква алфавита заменялась на другую (например, следующую через три позиции в алфавите после нее). Наряду с новыми методами шифрования появлялись способы вскрытия этих шифров, например для шифра Цезаря можно воспользоваться статистическими свойствами языка, на котором писалось исходное сообщение.

Очень часто безопасность шифра обеспечивалась тем, что алгоритм, по которому обеспечивалось шифрование, держался в секрете, как например в рассмотренном выше шифре Цезаря. В современной классической криптографии чаще всего алгоритмы публикуются и доступны для изучения каждому. Секретность обеспечивается тем, что само сообщение смешивается с секретным ключом по некоторому открытому алгоритму.

Допустим нам надо передать некоторое сообщение от Алисы к Бобу по некоторому защищенному каналу связи. Сообщение должно быть представлено в некоторой цифровой форме. Протокол, описывающий такую передачу, состоит из нескольких этапов. На первом Алиса и Боб должны получить некоторую общую случайную последовательность чисел, которая будет называться ключом. Эта процедура называется распределением ключа.

На следующем этапе Алиса должна с помощью некоторого алгоритма E получить из исходного сообщения P и ключа K зашифрованное сообщение C. Данная процедура может быть описана следующим соотношением:

$$E_K(P) = C. \tag{1.1}$$

На третьем этапе полученное зашифрованное сообщение должно быть передано Бобу.

На последнем этапе Боб с помощью известного алгоритма D и полученного на первом этапе ключа K должен восстановить исходное сообщение P

из полученного зашифрованного C. Данная процедура может быть описана следующим соотношением

$$D_K(C) = P. \tag{1.2}$$

При анализе данного протокола возникают следующие вопросы. Как реализовать безопасное распределение ключа. Второй - существует ли абсолютно стойкий алгоритм. И наконец последний - возможна ли безопасная передача зашифрованного сообщения, когда оно не может быть прослушано или подменено.

Классическая криптография дает однозначный ответ только на второй вопрос. Абсолютно криптостойкий алгоритм существует - он носит название одноразового блокнота. Ниже представлено детальное описание этого алгоритма.

1.1 Одноразовый блокнот

Схема одноразового блокнота была предложена в 1917 году Мэйджором Дж. Моборном и Г. Вернамом. Классический одноразовый блокнот представляет собой некоторый набор случайных ключей, каждый из которых равен по размеру отправляемому сообщению и используется только один раз.

Предположим что мы хотим зашифровать сообщение на некотором языке (например на английском). Число символов (букв) которое используется в алфавите обозначим через X. Для английского языка (без знаков препинания и различия регистра) $X = 26$. Далее каждому из символов языка мы назначим некоторое число c, такое что $0 \leq c \leq X$. Например для английского языка можно записать

$$\begin{gathered} A \to 0 \\ B \to 1 \\ \dots \\ Z \to 25 \end{gathered}$$

Процедура шифрования (1.1) описывается следующим выражением

$$E_{K_i}(P_i) = P_i + K_i \mod X = C_i, \tag{1.3}$$

где i номер шифруемого символа.

Процедура дешифрования (1.2) описывается следующим выражением

$$D_{K_i}(C_i) = C_i - K_i \mod X = P_i, \tag{1.4}$$

где i номер шифруемого символа.

a	b	$a \oplus b$
0	0	0
0	1	1
1	0	1
1	1	0

Таблица 1.1: XOR $a \oplus b$

Эта процедура легко обобщается на случай двоичных данных, при этом вместо сложения по модулю используется операция XOR $(a \oplus b)$ как для шифрования, так и для дешифрования :

Клод Шенон показал [8], что если ключ действительно случайный, имеет такую же длину, как исходное сообщение, и не используется повторно, то предложенная схема одноразового блокнота абсолютно защищена.

Согласно Шенону абсолютная защищенность (perfect security) может быть определена следующим образом.

Определение 1.1.1. Шифр (E, D) абсолютно защищен если для любых двух сообщений одинаковой длины m_0 и m_1, некоторого шифротекста c и ключа $k \leftarrow_R K$ вероятности того что исходный текст m_0 или m_1 равны:

$$P\left(E\left(m_0, k\right) = c\right) = P\left(E\left(m_1, k\right) = c\right)$$

Перефразируя это определение можно сказать, что по исходной статистике шифротекста невозможно получить никакой информации об исходном сообщении.

Теорема 1.1.1 (Криптостойкость одноразового блокнота)**.** *Схема одноразового блокнота имеет абсолютную защищенность.*

Доказательство. Обозначим через $|K|$ - число всех возможных ключей длины l. Где l также длина исходных сообщений: $|m_{0,1}| = l$. В силу того, что ключ которым зашифровано сообщение определяется единственным образом:

$$k_{0,1} = c \oplus m_{0,1},$$

получаем для вероятностей

$$P\left(E\left(m_0, k\right) = c\right) = P\left(E\left(m_1, k\right) = c\right) = \frac{1}{|K|}.$$

□

1.2 Проблемы классической криптографии

Если существует абсолютно защищенная криптографическая система (одноразовый блокнот) то что же не так в классической криптографии? Проблема заключается в получении ключей, удовлетворяющих требованиям одноразового блокнота (длина ключа равна длине сообщения, ключ состоит из случайных данных и ни разу не используется повторно) и передачи этих ключей Бобу и Алисе.

Проблемы возникают как на этапе генерации ключей, [1] так и на этапе передачи этих ключей.

Для передачи ключей в классической криптографии используются так называемые алгоритмы с открытым ключом. Существует несколько протоколов обмена ключей, основанных на криптографических системах с открытым ключом. Все они основаны на том, что существует два ключа, первый из которых, называемый открытым (public key), используется только для зашифрования, а второй - закрытый (private key) для дешифрования. Для того чтобы получить закрытый ключ из открытого, необходимо произвести какую-то сложную математическую операцию. Например безопасность одной из наиболее популярных систем с открытым ключом - RSA(см. 5.1), основана на трудности факторизации[2] больших чисел.

Схема протокола распределения ключа, основанная на криптографии с открытым ключом, может быть описана следующим образом. На первом этапе Алиса создает открытый и закрытый ключи и первый из них отсылает Бобу. Боб со своей стороны создает тот ключ, который хотелось бы иметь и Алисе и Бобу (который требуется распределить). Этот ключ шифруется (например по RSA) с помощью открытого ключа Алисы и пересылается ей. Алиса, получая этот зашифрованный ключ, может расшифровать его с помощью своего закрытого ключа.

Если злоумышленник (Ева) хочет узнать передаваемый ключ, она должна решить сложную математическую задачу по факторизации больших чисел. Считается, но не доказано, что сложность факторизации растет экспоненциально с ростом числа цифр в числе [17].[3] Таким образом при увеличении числа цифр задача быстро становится не решаемой.

В этой схеме имеется несколько проблем. Первая связана с тем что сложность факторизации не доказана. Мало того, существуют алгоритмы для квантовых компьютеров - алгоритм Шора(см. 5.2), которые решают зада-

[1] получение больших последовательностей случайных чисел является не тривиальной математической задачей

[2] разложении на простые множители

[3] Наиболее быстрый из известных алгоритмов решает задачу о факторизации числа N за время порядка $O\left(exp\left(log^{\frac{1}{3}}N\,(log\,logN)^{\frac{2}{3}}\right)\right)$.

чу о факторизации числа N за время $O\left(logN\right)$, т. е. за время порядка числа цифр в N. Таким образом в тот момент, когда будет построен квантовый компьютер, все системы, основанные на RSA, утратят свою актуальность.

Глава 2

Основные положения квантовой механики

2.1 Дираковская формулировка квантовой механики

В курсе лекций по квантовой оптике мы будем всюду использовать формализм Дирака [16]. В обычной формулировке квантовой механики мы имеем дело с волновыми функциями, например $\psi(q,t)$ - волновая функция в координатном представлении. Одно и то же состояние системы можно описать волновыми функциями в различных представлениях, связанных друг с другом линейными преобразованиями. Например, волновая функция в импульсном представлении связана с волновой функцией в координатном представлении равенством

$$\phi(p,t) = \frac{1}{2\pi\hbar}\int_{-\infty}^{+\infty}\psi(q,t)\,e^{-i\frac{pq}{\hbar}}dq \tag{2.1}$$

Главное здесь, что одно и то же состояние можно описывать волновыми функциями, выраженными через различные переменные. Отсюда следует, что можно ввести более общее образование, характеризующее состояние системы независимо от представления. Для такого образования Дирак ввел понятие волнового вектора, или вектора состояния, обозначаемого:

$$|\ldots\rangle \tag{2.2}$$

и называемого кет-вектором.

2.1.1 Кет-вектор

$|\dots\rangle$ общее обозначение кет-вектора; $|a\rangle$, $|x\rangle$, $|\psi\rangle$ и т.д. означают кет-векторы, описывающие некоторые частные состояния, символы которых записываются внутри скобок.

2.1.2 Бра-векторы

Каждому кет-вектору соответствует сопряженный ему бра-вектор. Бра-вектор обозначается:

$$\langle\dots|\,,\quad \langle a|\,,\quad \langle\psi|\,. \tag{2.3}$$

Названия бра- и кет-векторы образованы от первой и второй половины английского слова *bra-cket* (скобка).

Таким образом, бра-векторам $\langle a|$, $\langle x|$, $\langle\psi|$ соответствуют сопряженные им кет-векторы $|a\rangle$, $|x\rangle$, $|\psi\rangle$ и наоборот. Для векторов состояний справедливы те же основные соотношения, которые справедливы для волновых функций:

$$|u\rangle = |a\rangle + |b\rangle\,,\quad \langle u| = \langle a| + \langle b|\,,\quad |v\rangle = l\,|a\rangle\,,\quad \langle v| = l\,\langle a|\,. \tag{2.4}$$

Бра- и кет-векторы связаны между собой операцией эрмитового сопряжения:

$$|u\rangle = (\langle u|)^{\dagger}\,,\quad \langle u| = (|u\rangle)^{\dagger}\,. \tag{2.5}$$

В известных случаях это сводится к следующим соотношениям:

$$(\psi\,(q))^{\dagger} = \psi^{*}\,(q)$$

для волновой функции в координатном представлении;

$$\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}^{\dagger} = (a_1^{*}, a_2^{*}, \cdots, a_n^{*})$$

в матричном представлении.

При помощи бра- и кет-векторов можно определить скалярное произведение

$$\langle v|u\rangle = \langle u|v\rangle^{*}\,. \tag{2.6}$$

В конкретных случаях это означает:

$$\langle\psi|\,\phi\rangle = \int \psi^{*}\phi dq$$

в координатном представлении;

$$\langle a|b\rangle = (a_1^*, a_2^*, \cdots, a_n^*) \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} = a_1^* b_1 + a_2^* b_2 + \cdots + a_n^* b_n$$

в матричном представлении.

Из соотношения (2.6) следует, что норма вектора вещественна. Дополнительно полагаем, что норма вектора положительна или равна нулю: $\langle a|a\rangle \geq 0$.

2.1.3 Операторы

В квантовой механике используют линейные операторы. Операторы связывают один вектор состояния с другим:

$$|q\rangle = \hat{L}\,|p\rangle \tag{2.7}$$

Сопряженное равенство имеет вид

$$\langle q| = \langle p|\,\hat{L}^\dagger \tag{2.8}$$

где $\hat{L}^\dagger$ - оператор, сопряженный оператору $\hat{L}$.

Приведем некоторые соотношения, справедливые для линейных операторов:

$$\begin{gathered} \hat{L}^{++} = \hat{L}, \quad \left(l\hat{L}\,|a\rangle\right)^\dagger = l^*\,\langle a|\,\hat{L}^\dagger, \\ \left(\left(\hat{L}_1 + \hat{L}_2\right)|a\rangle\right)^\dagger = \langle a|\left(\hat{L_1}^\dagger + \hat{L_2}^\dagger\right), \\ \left(\left(\hat{L}_1\hat{L}_2\right)|a\rangle\right)^\dagger = \langle a|\left(\hat{L_2}^\dagger\hat{L_1}^\dagger\right), \\ \left(\left(\hat{L}_1\hat{L}_2\hat{L}_3\right)|a\rangle\right)^\dagger = \langle a|\left(\hat{L_3}^\dagger\hat{L_2}^\dagger\hat{L_1}^\dagger\right), \text{ и т.д.} \end{gathered} \tag{2.9}$$

Заметим, что алгебра операторов совпадает с алгеброй квадратных матриц. Матричные элементы операторов обозначаются следующим образом:

$$\langle a|\,\hat{L}\,|b\rangle = L_{ab} \tag{2.10}$$

Для матричных элементов справедливы равенства

$$\langle a|\,\hat{L}\,|b\rangle^* = \langle b|\,\hat{L}^\dagger\,|a\rangle\,, \quad \langle a|\,\hat{L_1}\hat{L_2}\,|b\rangle^* = \langle b|\,\hat{L_2}^\dagger\hat{L_1}^\dagger\,|a\rangle \tag{2.11}$$

2.1.4 Собственные значения и собственные векторы операторов

Собственные значения и собственные векторы операторов определяются равенством

$$\hat{L}\,|l_n\rangle = l_n\,|l_n\rangle\,, \tag{2.12}$$

где l_n собственное значение; $|l_n\rangle$ собственный вектор.

Для бра-векторов имеем аналогичные равенства:

$$\langle d_n|\,\hat{D} = d_n\,\langle d_n|\,. \tag{2.13}$$

Если операторы соответствуют наблюдаемым величинам, они должны быть самосопряженными:

$$\hat{L} = \hat{L}^\dagger. \tag{2.14}$$

Собственные значения самосопряженного (эрмитова) оператора вещественны. Действительно из

$$\hat{L}\,|l\rangle = l\,|l\rangle$$

следует что

$$\langle l|\,\hat{L}\,|l\rangle = l\,\langle l|\,|l\rangle\,.$$

С другой стороны, вспоминая про (2.9): $\langle l|\,\hat{L}^\dagger = l^*\,\langle l|$, из (2.14) имеем

$$\langle l|\,\hat{L}\,|l\rangle = l^*\,\langle l|\,|l\rangle\,.$$

Таким образом $l\,\langle l|\,|l\rangle = l^*\,\langle l|\,|l\rangle$, т. е. $l = l^*$

Собственные векторы самосопряженного оператора ортогональны. Действительно рассмотрим два собственных вектора $|l_1\rangle$ и $|l_2\rangle$:

$$\hat{L}\,|l_1\rangle = l_1\,|l_1\rangle\,, \quad \hat{L}\,|l_2\rangle = l_2\,|l_2\rangle$$

Из второго соотношения получаем

$$\langle l_1|\,\hat{L}\,|l_2\rangle = l_2\,\langle l_1|\,|l_2\rangle$$

С учетом вещественности собственных чисел и соотношения (2.14) для вектора $|l_1\rangle$ получим:

$$\langle l_1|\,\hat{L} = l_1\,\langle l_1|\,.$$

Откуда

$$\langle l_1|\,\hat{L}\,|l_2\rangle = l_1\,\langle l_1|\,|l_2\rangle\,.$$

Таким образом

$$(l_1 - l_2)\,\langle l_1|\,|l_2\rangle = 0, \quad \text{т. е. } \langle l_1|\,|l_2\rangle = 0, \text{ т. к. } l_1 \neq l_2.$$

2.1.5 Наблюдаемые величины. Разложение по собственным векторам. Полнота системы собственных векторов

Операторы, соответствующие наблюдаемым физическим величинам, являются самосопряженными операторами. Это обеспечивает действительность значений наблюдаемой физической величины. Имеем набор собственных состояний некоторого эрмитового оператора $|l_n\rangle$, $\hat{L}\,|l_n\rangle = l_n\,|l_n\rangle$. Если набор собственных состояний полный, согласно принципам квантовой механики любое состояние можно представить суперпозицией состояний $|l_n\rangle$:

$$|\psi\rangle = \sum_{(n)} c_n\,|l_n\rangle\,. \tag{2.15}$$

Отсюда для коэффициентов разложения имеем: $c_n = \langle l_n|\,\psi\rangle$, и, следовательно, справедливо равенство

$$|\psi\rangle = \sum_{(n)} \langle l_n|\,\psi\rangle\,|l_n\rangle = \sum_{(n)} |l_n\rangle\,\langle l_n|\,\psi\rangle\,. \tag{2.16}$$

Из равенства 2.16 следует важное соотношение:

$$\sum_{(n)} |l_n\rangle\,\langle l_n| = \hat{I}. \tag{2.17}$$

где $\hat{I}$ - единичный оператор. Это равенство является условием полноты системы собственных векторов (условием разложимости).

2.1.6 Оператор проектирования

Рассмотрим оператор $\hat{P}_n = |l_n\rangle\,\langle l_n|$. Результатом действия этого оператора на состояние $|\psi\rangle$ будет

$$\hat{P}_n\,|\psi\rangle = \sum_{(k)} |l_n\rangle\,\langle l_n|\,c_k\,|l_k\rangle = c_n\,|l_n\rangle\,. \tag{2.18}$$

Оператор $\hat{P}_n = |l_n\rangle\,\langle l_n|$ называется оператором проектирования.

Можно написать следующие свойства этого оператора

$$\sum_{(n)} \hat{P}_n = \hat{I}. \tag{2.19}$$

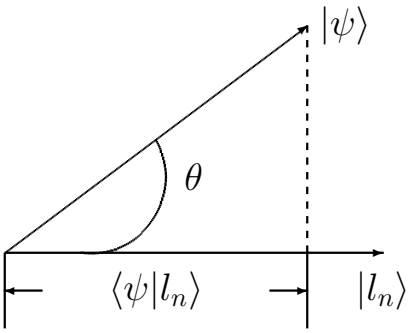


Рис. 2.1: Оператор проектирования. Действие оператора может быть интерпретировано как проекция вектора $|\psi\rangle$ на ось $|l_n\rangle$

$$\hat{P}_n^2 = \hat{P}_n. \tag{2.20}$$

Действие оператора проектирования имеет простую геометрическую интерпретацию (см. рис. 2.1):

$$\hat{P}_n |\psi\rangle = \cos\theta \, |l_n\rangle ,$$

где $\cos\theta = \langle\psi|l_n\rangle = c_n$.

2.1.7 След оператора

В ортонормированном базисе $\{|l_n\rangle\}$ величина

$$Sp\hat{L} = \sum_n \langle l_n| \hat{L} |l_n\rangle \tag{2.21}$$

называется следом оператора $\hat{L}$. При определенных условиях [14] ряд 2.21 абсолютно сходится и не зависит от выбора базиса.

Если использовать матричное представление

$$L_{kn} = \langle l_k| \hat{L} |l_n\rangle ,$$

то след оператора - сумма диагональных элементов матричного представления

$$Sp\hat{L} = \sum_n L_{nn}$$

Можно написать следующие свойства следа оператора:

$$Sp\left(l\hat{L} + m\hat{M}\right) = lSp\hat{L} + mSp\hat{M},$$
$$Sp\left(\hat{L}\hat{M}\right) = Sp\left(\hat{M}\hat{L}\right). \tag{2.22}$$

2.1.8 Средние значения операторов

Среднее значение оператора $\hat{L}$ в состоянии $|\psi\rangle$ дается равенством

$$\left\langle \hat{L} \right\rangle_{\psi} = \langle\psi| \hat{L} |\psi\rangle \tag{2.23}$$

при условии

$$\langle\psi|\psi\rangle = 1.$$

Действительно, если принять, что $|\psi\rangle$ раскладывается в ряд по собственным функциям оператора $\hat{L}$ следующим образом:

$$|\psi\rangle = \sum_n c_n |l_n\rangle ,$$

то $\hat{L}|\psi\rangle$ можно записать как

$$\hat{L}|\psi\rangle = \sum_n l_n c_n |l_n\rangle ,$$

где l_n собственное число соответствующее собственному состоянию $|l_n\rangle$. Если теперь подставить два последних выражения в (2.23) то получим:

$$\langle\psi| \hat{L} |\psi\rangle = \sum_{n,m} l_n c_n c_m^* \langle l_m|l_n\rangle = \sum_n l_n c_n c_n^* = \sum_n l_n |c_n|^2 ,$$

что (при условии $\langle\psi|\psi\rangle = 1$) доказывает, что выражение (2.23) действительно представляет собой выражение для среднего значения оператора $\hat{L}$ в состоянии $|\psi\rangle$. [1]

Если взять некоторый ортонормированный базис $\{|n\rangle\}$, образующий полный набор, т. е. подчиняющийся условию (2.17): $\sum_n |n\rangle\langle n| = \hat{I}$, то выражение (2.23) может быть переписано следующим образом:

$$\left\langle \hat{L} \right\rangle_{\psi} = \langle\psi| \hat{L} |\psi\rangle = \langle\psi| \hat{I}\hat{L} |\psi\rangle =$$
$$= \sum_n \langle\psi|n\rangle \langle n| \hat{L} |\psi\rangle = \sum_n \langle n| \hat{L} |\psi\rangle \langle\psi|n\rangle = Sp\left(\hat{L}\hat{\rho}\right),$$

где $\hat{\rho} = |\psi\rangle\langle\psi| = \hat{P}_\psi$ - оператор проектирования на состояние $|\psi\rangle$. С учетом (2.22) можно записать

$$\left\langle \hat{L} \right\rangle_{\psi} = Sp\left(\hat{\rho}\hat{L}\right). \tag{2.24}$$

[1] Для этого достаточно вспомнить, что $|c_n|^2$ задает вероятность получить систему в состоянии $|l_n\rangle$, то есть получить показание измерительного прибора в l_n

2.1.9 Представление операторов через внешние произведения собственных векторов

Дважды используя условие полноты (2.16), получим

$$\hat{A} = \hat{I}\hat{A}\hat{I} = \sum_{(l)}\sum_{(l')} |l\rangle \langle l| \hat{A} |l'\rangle \langle l'| = \sum_{(l)}\sum_{(l')} |l\rangle \langle l'| A_{ll'}, \tag{2.25}$$

где $A_{ll'} = \langle l| \hat{A} |l'\rangle$ - матричный элемент оператора $\hat{A}$ в представлении $|l\rangle$.

Оператор, выраженный через свои же собственные векторы, может быть представляем разложением [2]

$$\hat{L} = \sum_{(l)} l |l\rangle \langle l| . \tag{2.26}$$

Обобщение этого равенства для операторной функции имеет вид

$$F\left(\hat{L}\right) = \sum_{(l)} F(l) |l\rangle \langle l| . \tag{2.27}$$

2.1.10 Волновые функции в координатном и импульсном представлениях

Переход от вектора состояния к волновой функции осуществляется посредством скалярного умножения этого вектора состояния на вектор состояния соответствующей наблюдаемой величины. Например, для волновой функции в координатном представлении

$$\phi(q) = \langle q| \psi\rangle . \tag{2.28}$$

где $\langle q|$ - собственный вектор оператора координаты. В импульсном представлении получим

$$\phi(p) = \langle p| \psi\rangle . \tag{2.29}$$

где $\langle p|$ - собственный вектор оператора импульса.

2.2 Динамика изменения волновой функции

Волновая функция $|\phi\rangle$ может изменяться посредством двух механизмов:

- Редукция волновой функции во время измерения
- Уравнение Шрёдингера в промежутках между двумя последовательными измерениями

[2] При условии нормировки собственных векторов: $\langle l|l\rangle = 1$

2.2.1 Уравнение Шрёдингера

Изменение состояния чистой квантовой системы между двумя последовательными измерениями описывается следующим уравнением (Шрёдингера)

$$i\hbar\frac{\partial\left|\phi\right\rangle}{\partial t}=\hat{\mathcal{H}}\left|\phi\right\rangle. \tag{2.30}$$

Уравнение (2.30) является обратимым и, соответственно, не применимо к описанию изменения волновой функции в момент измерения.

Стоит отметить связь уравнения Шредингера с теоремой Стоуна (**??**) TBD.

Уравнение Шрёдингера в представлении взаимодействия

Допустим что в гамильтониане можно выделить две части:

$$\hat{\mathcal{H}}=\hat{\mathcal{H}}_0+\hat{\mathcal{V}}.$$

Введем следующее преобразование волновой функции:

$$\left|\phi\right\rangle_I=\exp\left\{\left(\frac{i\hat{\mathcal{H}}_0t}{\hbar}\right)\right\}\left|\phi\right\rangle$$

и посмотрим чему будет равно следующее выражение:

$$\begin{aligned}
i\hbar\frac{\partial\left|\phi\right\rangle_I}{\partial t}&=i\hbar\frac{i\hat{\mathcal{H}}_0}{\hbar}\exp\left\{\left(\frac{i\hat{\mathcal{H}}_0t}{\hbar}\right)\right\}\left|\phi\right\rangle+\exp\left\{\left(\frac{i\hat{\mathcal{H}}_0t}{\hbar}\right)\right\}i\hbar\frac{\partial\left|\phi\right\rangle}{\partial t}=\\
&=-\hat{\mathcal{H}}_0\exp\left\{\left(\frac{i\hat{\mathcal{H}}_0t}{\hbar}\right)\right\}\left|\phi\right\rangle+\exp\left\{\left(\frac{i\hat{\mathcal{H}}_0t}{\hbar}\right)\right\}\left(\hat{\mathcal{H}}_0+\hat{\mathcal{V}}\right)\left|\phi\right\rangle=\\
-\hat{\mathcal{H}}_0\exp\left\{\left(\frac{i\hat{\mathcal{H}}_0t}{\hbar}\right)\right\}\left|\phi\right\rangle&+\hat{\mathcal{H}}_0\exp\left\{\left(\frac{i\hat{\mathcal{H}}_0t}{\hbar}\right)\right\}\left|\phi\right\rangle+\exp\left\{\left(\frac{i\hat{\mathcal{H}}_0t}{\hbar}\right)\right\}\hat{\mathcal{V}}\left|\phi\right\rangle=\\
&=\exp\left\{\left(\frac{i\hat{\mathcal{H}}_0t}{\hbar}\right)\right\}\hat{\mathcal{V}}\left|\phi\right\rangle=\\
&=\exp\left\{\left(\frac{i\hat{\mathcal{H}}_0t}{\hbar}\right)\right\}\hat{\mathcal{V}}\exp\left\{\left(-\frac{i\hat{\mathcal{H}}_0t}{\hbar}\right)\right\}\exp\left\{\left(\frac{i\hat{\mathcal{H}}_0t}{\hbar}\right)\right\}\left|\phi\right\rangle=\\
&=\hat{\mathcal{V}}_I\left|\phi\right\rangle_I,
\end{aligned}$$

где

$$\hat{\mathcal{V}}_I=\exp\left\{\left(\frac{i\hat{\mathcal{H}}_0t}{\hbar}\right)\right\}\hat{\mathcal{V}}\exp\left\{\left(-\frac{i\hat{\mathcal{H}}_0t}{\hbar}\right)\right\} \tag{2.31}$$

гамильтониан взаимодействия в представлении взаимодействия.

Таким образом получаем уравнение Шрёдингера в представлении взаимодействия:

$$i\hbar\frac{\partial\left|\phi\right\rangle_I}{\partial t}=\hat{\mathcal{V}}_I\left|\phi\right\rangle_I. \tag{2.32}$$

Уравнение движения матрицы плотности

Из соотношения (2.30) имеем

$$i\hbar\frac{\partial\left|\phi\right\rangle}{\partial t}=\hat{\mathcal{H}}\left|\phi\right\rangle,$$
$$-i\hbar\frac{\partial\left\langle\phi\right|}{\partial t}=\hat{\mathcal{H}}\left\langle\phi\right|,$$

таким образом для матрицы плотности $\hat{\rho}=\left|\phi\right\rangle\left\langle\phi\right|$ получаем

$$i\hbar\frac{\partial\hat{\rho}}{\partial t}=i\hbar\frac{\partial\left|\phi\right\rangle\left\langle\phi\right|}{\partial t}=i\hbar\left(\frac{\partial\left|\phi\right\rangle}{\partial t}\left\langle\phi\right|+\left|\phi\right\rangle\frac{\partial\left\langle\phi\right|}{\partial t}\right)=$$
$$=\hat{\mathcal{H}}\left|\phi\right\rangle\left\langle\phi\right|-\left|\phi\right\rangle\left\langle\phi\right|\hat{\mathcal{H}}=\left[\hat{\mathcal{H}},\hat{\rho}\right] \tag{2.33}$$

Уравнение (2.33) часто называется квантовым уравнением Лиувилля и уравнением фон Неймана.

Оператор эволюции. Представление Гейзенберга и представление Шредингера

Изменение волновой функции по закону (2.30) может быть также описано с помощью некоторого оператора (эволюции) $\hat{U}\left(t,t_0\right)$:

$$\left|\phi\left(t\right)\right\rangle=\hat{U}\left(t,t_0\right)\left|\phi\left(t_0\right)\right\rangle. \tag{2.34}$$

Уравнение (2.30) может быть переписано в виде

$$\left|\phi\left(t\right)\right\rangle=\exp\left(-\frac{i}{\hbar}\hat{\mathcal{H}}\left(t-t_0\right)\right)\left|\phi\left(t_0\right)\right\rangle,$$

откуда для оператора эволюции имеем

$$\hat{U}\left(t,t_0\right)=\exp\left(-\frac{i}{\hbar}\hat{\mathcal{H}}\left(t-t_0\right)\right) \tag{2.35}$$

Оператор эволюции - унитарный. Действительно:

$$\hat{U}(t,t_0)\,\hat{U}^{\dagger}(t,t_0) = \\ = \exp\left(-\frac{i}{\hbar}\hat{\mathcal{H}}(t-t_0)\right)\exp\left(+\frac{i}{\hbar}\hat{\mathcal{H}}(t-t_0)\right) = \hat{I}$$

Наряду с представлением Шредингера где операторы от времени не зависят а меняются волновые функции существует представление Гейзенберга где операторы меняются во времени.

Очевидно средние значения операторов не должны зависеть от представления:

$$\langle\phi_H(t_0)|\,\hat{A}_H(t)\,|\phi_H(t_0)\rangle = \langle\phi_S(t)|\,\hat{A}_S\,|\phi_S(t)\rangle = \\ = \langle\phi_H(t_0)|\,\hat{U}^{\dagger}(t,t_0)\,\hat{A}_S\hat{U}(t,t_0)\,|\phi_H(t_0)\rangle\,,$$

откуда с учетом $\hat{A}_H(t_0) = \hat{A}_S(t_0)$ получаем закон эволюции операторов в представлении Гейзенберга:

$$\hat{A}_H(t) = \hat{U}^{\dagger}(t,t_0)\,\hat{A}_H(t_0)\,\hat{U}(t,t_0) \tag{2.36}$$

При этом уравнение для оператора $\hat{A}_H$ будет выглядеть следующим образом:

$$\frac{\partial\hat{A}_H}{\partial t} = \frac{i}{\hbar}\hat{\mathcal{H}}\hat{U}^{\dagger}(t,t_0)\,\hat{A}_H(t_0)\,\hat{U}(t,t_0) - \\ -\frac{i}{\hbar}\hat{U}^{\dagger}(t,t_0)\,\hat{A}_H(t_0)\,\hat{U}(t,t_0)\,\hat{\mathcal{H}} = \frac{i}{\hbar}\left[\hat{\mathcal{H}},\hat{A}_H\right] \tag{2.37}$$

2.2.2 Различия между чистыми и смешанными состояниями. Декогеренция

Определение 2.2.1 (Чистое состояние)**.** Если состояние системы описывается матрицей плотности $\hat{\rho}$ которая представима в виде

$$\hat{\rho} = |\psi\rangle\langle\psi| \tag{2.38}$$

то данное состояние называется чистым.

Определение 2.2.2 (Смешанное состояние)**.** Если состояние системы описывается матрицей плотности $\hat{\rho}$ которая **не** представима в виде (2.38), т.е.

$$\hat{\rho} \neq |\psi\rangle\langle\psi|$$

то данное состояние называется смешанным.

Рис. 2.2: Модель двухуровневого атома, используемого для описания декогеренции.

Особый интерес представляет собой различие между чистыми и смешанными состояниями, в частности - каким образом происходит переход от чистых состояний к смешанным.

Рассмотрим двухуровневое состояние (см. рис. 2.2). В чистом состоянии оно описывается следующей волновой функцией:

$$|\phi\rangle = c_a |a\rangle + c_b |b\rangle ,$$

соответствующая матрица плотности имеет вид

$$\begin{aligned} \hat{\rho} = |\phi\rangle \langle\phi| = \\ = |c_a|^2 |a\rangle \langle a| + |c_b|^2 |b\rangle \langle b| + \\ + c_a c_b^* |a\rangle \langle b| + c_b c_a^* |b\rangle \langle a| , \end{aligned} \tag{2.39}$$

или в матричном виде

$$\hat{\rho} = \begin{pmatrix} |c_a|^2 & c_a c_b^* \\ c_b c_a^* & |c_b|^2 \end{pmatrix} .$$

Матрица плотности для смешанного состояния имеет только диагональные элементы:

$$\begin{aligned} \hat{\rho} = \begin{pmatrix} |c_a|^2 & 0 \\ 0 & |c_b|^2 \end{pmatrix} = \\ = |c_a|^2 |a\rangle \langle a| + |c_b|^2 |b\rangle \langle b| . \end{aligned} \tag{2.40}$$

Переход от (2.39) к (2.40) называется декогеренцией. В описании процесса декогеренции мы будем следовать [15].

Отличие смешанных состояний от чистых проявляется во влиянии окружения $\mathcal{E}$. В случае чистых состояний рассматриваемая система и ее окружение независимы, т. е.

$$|\phi\rangle_{pure} = |\phi\rangle_{at} \otimes |\mathcal{E}\rangle . \tag{2.41}$$

В случае смешанных состояний атом и его окружение образуют так называемое перепутанное состояние в котором состояниям $|a\rangle$ и $|b\rangle$ соответствуют различимые состояния окружения $|\mathcal{E}_a\rangle$ и $|\mathcal{E}_b\rangle$.

$$|\phi\rangle_{mix} = c_a |a\rangle |\mathcal{E}_a\rangle + c_b |b\rangle |\mathcal{E}_b\rangle . \tag{2.42}$$

Матрица плотности соответствующая (2.42) имеет вид

$$\begin{aligned} \hat{\rho}_{mix} = |\phi\rangle_{mix} \langle\phi|_{mix} = \\ = |c_a|^2 |a\rangle \langle a| \otimes |\mathcal{E}_a\rangle \langle\mathcal{E}_a| + |c_b|^2 |b\rangle \langle b| \otimes |\mathcal{E}_b\rangle \langle\mathcal{E}_b| + \\ + c_a c_b^* |a\rangle \langle b| \otimes |\mathcal{E}_a\rangle \langle\mathcal{E}_b| + c_b c_a^* |b\rangle \langle a| \otimes |\mathcal{E}_b\rangle \langle\mathcal{E}_a| . \end{aligned} \tag{2.43}$$

Если теперь применить к выражению (2.43) усреднение по переменным окружения, то получим

$$\begin{aligned} \langle\hat{\rho}_{mix}\rangle_{\mathcal{E}} = Sp_{\mathcal{E}} (\hat{\rho}) = \\ = \langle\mathcal{E}_a| \hat{\rho}_{mix} |\mathcal{E}_a\rangle + \langle\mathcal{E}_b| \hat{\rho}_{mix} |\mathcal{E}_b\rangle = \\ = |c_a|^2 |a\rangle \langle a| + |c_b|^2 |b\rangle \langle b| . \end{aligned} \tag{2.44}$$

Выражение (2.44) получено в предположении ортонормированного базиса $\{|\mathcal{E}_a\rangle , |\mathcal{E}_b\rangle\}$:

$$\begin{aligned} \langle\mathcal{E}_a |\mathcal{E}_a\rangle = \langle\mathcal{E}_b |\mathcal{E}_b\rangle = 1, \\ \langle\mathcal{E}_a |\mathcal{E}_b\rangle = \langle\mathcal{E}_b |\mathcal{E}_a\rangle = 0. \end{aligned} \tag{2.45}$$

Условия (2.45) являются ключевыми для понимания того почему рассматриваемый базис атомной системы является выделенным и почему например в случае смешанных состояний не рассматривают другие базисы такие как базис полученный преобразованием Адамара по отношению к исходному :

$$\begin{aligned} |\mathcal{A}\rangle = \frac{|a\rangle + |b\rangle}{\sqrt{2}}, \\ |\mathcal{B}\rangle = \frac{|a\rangle - |b\rangle}{\sqrt{2}}. \end{aligned} \tag{2.46}$$

Состояния окружения соответствующие базису (2.46) не являются ортогональными откуда следует невозможность использования (2.46) в качестве базисных векторов для смешанных состояний.

Процесс декогеренции, т. е. перехода от (2.41) к (2.42) может быть описан с помощью уравнения Шредингера, и следовательно теоретически является обратимым. Единственное требование - ортогональность различимых

состояний окружения: $\langle \mathcal{E}_a | \mathcal{E}_b \rangle = 0$. Это требование всегда выполняется для макроскопических систем, где состояние зависит от очень большого числа переменных. При этом в случае макроскопических систем стоит отметить, что существует большое число возможных вариантов конечных состояний $|\mathcal{E}_{a,b}\rangle$ в силу чего обратный процесс становится практически не реализуемым, так как необходимо контролировать большое число возможных переменных которыми описывается состояние окружения. В этом смысле процесс декогеренции имеет такую же природу как и второй закон термодинамики (возрастания энтропии), который описывает необратимые процессы. [3]

Процесс декогеренции является очень быстрым, в частности [13] дает следующую оценку: для систем массой 1 г. при разделении $\Delta x = 1$ см. и температуре $T = 300$ K , времени релаксации равной времени жизни Вселенной $\tau_R = 10^{17}$ с. процесс декогеренции занимает 10^{-23} с.

2.2.3 Редукция волновой функции. Измерение в квантовой механике

Процесс выбора (результата измерения) один из самых сложных в квантовой механике. В отличии от детерминистского изменения волновой функции, описываемого уравнением Шрёдингера (2.30), процесс измерения носит случайный характер и для его описания следует применять другие уравнения.

Рассмотрим вначале чистые состояния и предположим, что производится измерение физической наблюдаемой, описываемой оператором $\hat{L}$. Собственные числа и собственные функции этого оператора $\{l_k\}$ и $\{|l_k\rangle\}$ соответственно. В момент измерения показания прибора могут принимать значения соответствующие собственным числам измеряемого оператора (см. рис. 2.3). Допустим, что показание прибора - l_n в этом случае волновая функция должна быть $|l_n\rangle$, т. о. произошло следующее изменение волновой функции:

$$|\phi\rangle \to |l_n\rangle \,,$$

которое может быть описано действием оператора проецирования $\hat{P}_n = |l_n\rangle \langle l_n|$ (2.18):

$$\hat{P}_n |\phi\rangle = c_n |l_n\rangle \,.$$

Пример 2.2.1 (Измерение энергии двухуровневого атома)**.** *Рассмотрим двухуровневый атом находящийся в чистом состоянии (см. рис. 2.4)* $|\psi\rangle = \frac{1}{\sqrt{2}} |a\rangle + \frac{1}{\sqrt{2}} |b\rangle$.

[3] Здесь надо быть немного аккуратным поскольку второй закон термодинамики применим к закрытым системам, а сами процессы декогеренции происходят в открытых системах

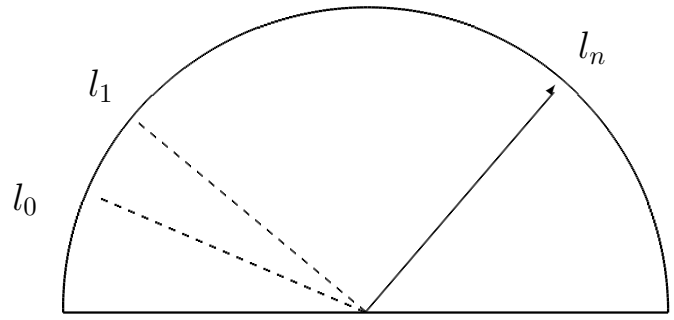
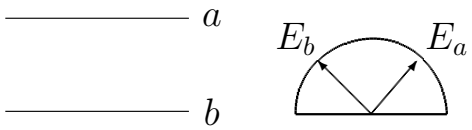
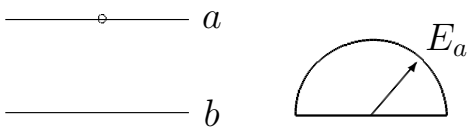


Рис. 2.3: Процесс измерения. Показание прибора соответствует одному из собственных чисел оператора $\hat{L}$: $\{l_k\}$



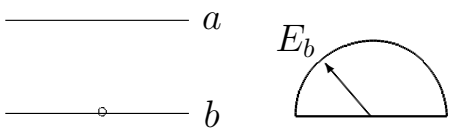
$$|\psi\rangle = \tfrac{1}{\sqrt{2}}\,|a\rangle + \tfrac{1}{\sqrt{2}}\,|b\rangle$$

Рис. 2.4: Процесс измерения энергии двухуровневого атома находящегося в чистом состоянии $|\psi\rangle = \frac{1}{\sqrt{2}}\,|a\rangle + \frac{1}{\sqrt{2}}\,|b\rangle$. Прибором регистрируется значение энергии E_a или E_b.



$$|\psi\rangle \to |a\rangle$$

Рис. 2.5: Процесс измерения энергии двухуровневого атома находящегося в чистом состоянии $|\psi\rangle = \frac{1}{\sqrt{2}}|a\rangle + \frac{1}{\sqrt{2}}|b\rangle$. Прибором регистрируется значение энергии E_a. При измерении происходит следующая редукция $|\psi\rangle \to |a\rangle$



$$|\psi\rangle \to |b\rangle$$

Рис. 2.6: Процесс измерения энергии двухуровневого атома находящегося в чистом состоянии $|\psi\rangle = \frac{1}{\sqrt{2}}|a\rangle + \frac{1}{\sqrt{2}}|b\rangle$. Прибором регистрируется значение энергии E_b. При измерении происходит следующая редукция $|\psi\rangle \to |b\rangle$

Наш прибор измеряет энергию этого атома и оператор Гамильтона имеет 2 собственные функции $|a, b\rangle$, которым соответствуют собственные числа E_a, E_b. Таким образом возможные показания прибора принадлежат множеству $\{E_a, E_b\}$.

В том случае когда стрелка прибора показывает E_a происходит следующая редукция (см. рис. 2.5)

$$|\psi\rangle \to |a\rangle\,.$$

Аналогично в случае E_b происходит следующая редукция (см. рис. 2.6)

$$|\psi\rangle \to |b\rangle\,.$$

Не существует способа предсказать результат который будет получен в результате единичного измерения. Вместе с тем можно сказать с какой вероятностью будет получен тот или иной результат.

Действительно в случае смешанного состояния

$$\hat{\rho} = \sum_n |c_n|^2 \, |l_n\rangle \, \langle l_n|$$

коэффициенты $P_n = |c_n|^2$ задают вероятности обнаружить систему в состоянии $|l_n\rangle$.

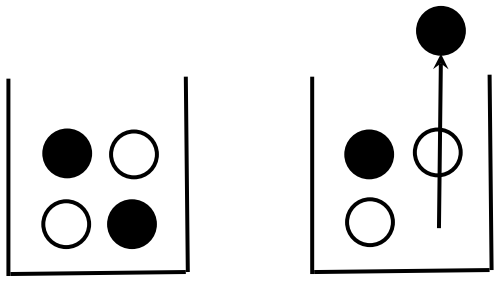


Рис. 2.7: Пример смешанного состояния. Цвет шара не меняется в результате “измерения”

Для чистого состояния

$$|\phi\rangle = \sum_n c_n |l_n\rangle$$

мы также имеем, что вероятность обнаружить систему в состоянии $|l_n\rangle$ задается числом $P_n = |c_n|^2$.

Основное отличие чистых и смешанных состояний с точки зрения измерения заключается в том, что в первом случае (чистое состояние) в процессе измерение меняется волновая функция, т. е. само состояние. При этом если в процессе измерения было получено некоторое конечное состояние $|l_i\rangle$, то нельзя сказать, что оно было таким же и до измерения. Смешанные состояния ведут себя подобно классическим объектам, т. е. если в процессе измерения было получено состояние $|l_i\rangle$, то можно утверждать, что оно было таким же и до измерения, а само измерение представляет собой выбор одного состояния из многих возможных.

Пример 2.2.2. Выбор из урны с шарами двух цветов *Допустим у нас имеется урна с 4 шарами. С вероятностью* $\frac{1}{2}$ *будет извлечен либо белый либо черный шар. Допустим что в результате эксперимента был получен черный шар. Если рассматриваемая система является квантовой и находится в смешанном состоянии (см. рис. 2.7), то состояние извлеченного шара (цвет) не изменилось в результате эксперимента.*

Если рассматриваемая система является чистой(см. рис. 2.8), то состояние каждого шара описывается суперпозицией двух цветов - черного и белого. Таким образом в результате эксперимента эта суперпозиция разрушается и шар приобретает определенный цвет (черный в нашем случае), т. е. можно сказать что цвет шара меняется.

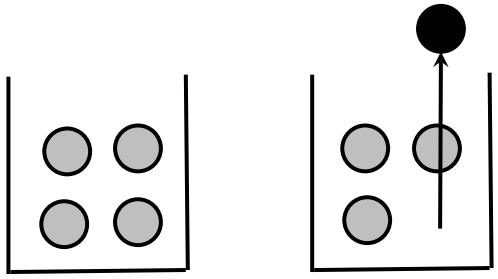


Рис. 2.8: Пример чистого состояния. Цвет шара меняется в результате "измерения"

2.3 Составные системы

Системы состоящие из нескольких частей ведут себе принципиально различным образом для случая классических и квантовых систем.

В качестве примера рассмотрим систему из двух частиц. Положение первой из них описывается 3 координатами, которые представляют собой точку в некотором линейном пространстве L_1: $(x_1, y_1, z_1) \in L_1$. Для второй допустим имеем 2 координаты в пространстве L_2 полностью задающие расположение: $(x_2, y_2) \in L_2$. Очевидно что для полного описания положения двух частиц нам необходимо 5 координат: $(x_1, y_1, z_1, x_2, y_2) \in L_1 \times L_2$. Таким образом составные системы, в классическом случае, описываются точками в пространстве $L^{classical}$, которое является декартовым произведение исходных: $L = L_1 \times L_2$. Отличительной особенностью декартова произведения является то, что размерности соответствующих пространств складываются:

$$\dim L^{classical} = \dim L_1 + \dim L_2.$$

В квантовом случае составная система описывается векторами (точками) в пространстве которое является тензорным произведением исходных:

$$L^{quantum} = L_1 \otimes L_2.$$

В этом пространстве имеется 6 базисных векторов, и соответственно, для описание положения системы необходимо 6 чисел: $(x_1 \cdot x_2, y_1 \cdot x_2, z_1 \cdot x_2, x_1 \cdot y_2, y_1 \cdot y_2, z_1 \cdot y_2) \in L^{quantum}$. Соответствующим образом размерности перемножаются:

$$\dim L^{quantum} = \dim L_1 \cdot \dim L_2.$$

Таким образом если у нас имеется две независимых квантовых системы с волновыми функциями $|\psi_1\rangle$ и $|\psi_2\rangle$ то составная система будет иметь следующую волновую функцию

$$|\psi_{12}\rangle = |\psi_1\rangle \otimes |\psi_2\rangle ,$$

при этом очевидно имеют место следующие равенства

$$|\psi_1\rangle = Sp_2 |\psi_{12}\rangle \,, \qquad |\psi_2\rangle = Sp_1 |\psi_{12}\rangle \tag{2.47}$$

т.е. для того чтобы получить состояние подсистемы 1 надо взять след по состояниям системы 2 от общей волновой функции.

Глава 3

Квантовые вычисления

Алгоритмы играют большую роль в вычислительной технике. Алгоритм представляет собой последовательность шагов необходимых для получения ответа на некоторую задачу. Каждая задача характеризуется некоторым числом, который определяет ее размер. Сложность алгоритма оценивается как число простейших операций необходимых для решения поставленной задачи. Очевидно, что в большинстве случаев (но не всегда) это число растет с размером задачи.

Пример 3.0.1. Поиск элемента массива *Задача - найти элемент массива, удовлетворяющий некоторым условиям. Размером задачи является число элементов массива* N.

В общем случае (не структурированный массив данных) поиск ведется простым перебором. Этот поиск требует число операций (сравнений) которое растет линейно с размером массива $O(N)$.

В случае структурированных данных число операций требуемое для поиска может быть уменьшено. Например в случае отсортированного массива сложность задачи растет как $O(logN)$.

Вместе с тем существование алгоритма еще не гарантирует его практической реализуемости. В частности алгоритмы требующие экспоненциального числа шагов от размера исходной задачи считаются практически не реализуемыми не смотря на то, что с теоретической точки зрения решение существует.

Одним из примеров является задача о факторизации натурального числа, т. е. задача о разложении его на простые множители (см. пример 3.0.2).

Пример 3.0.2. Факторизация натуральных чисел *Задача - найти разложение числа на простые множители. Размером задачи является разрядность исходного числа. Например для случая разрядности* $r = 4$*:* $1 \leq N = 15 \leq 2^r = 2^4 = 16$*). Результат может быть найден легко и быстро:* $15 = 3 \cdot 5$.

С ростом числа разрядов r число операций необходимых для факторизации в классических алгоритмах растет как $O\left(2^r\right)$, что для случая $r = 1000 - 2000$ означает практическую невозможность факторизации таких чисел.

Квантовые объекты обладают свойствами отличающимися от классических объектов, соотвественно алгоритмы, построенные на базе квантовых объектов могут в ряде случаев обладать характеристиками недоступными для классических алгоритмов. Например квантовый алгоритм Гровера [2] решает задачу о поиске в неструктурированном массиве данных (см. пример 3.0.1) с помощью $O\left(\sqrt{N}\right)$ операций. Алгоритм Шора [9] позволяет решить задачу о факторизации числа (см. пример 3.0.2) используя линейное число операций $O\left(r\right)$.

3.1 Основные принципы квантовых вычислений

3.1.1 Представление информации. Классические и квантовые состояния

Основное отличие квантовых и классических компьютеров заключается в том как они хранят информацию.

В классическом случае информация хранится в некоторых ячейках памяти. Состояние каждой ячейки памяти описывается одним числом которое может принимать значение 0 или 1. Если объединяются m ячеек памяти то общее состояние классической системы (которое она может принимать в конкретный момент времени) описывается m числами.

В квантовом случае ячейка памяти представлена кубитом для описания которого необходимо два комплексных числа α_0 и α_1 [1]:

$$|\psi\rangle_1 = \alpha_0 |0\rangle + \alpha_1 |1\rangle .$$

Для описания составной системы состоящей из m кубитов необходимо 2^m комплексных чисел. Иначе можно сказать что квантовое состояние содержит в качестве суперпозиции все возможные классические состояния. В качестве примера можно рассмотреть систему состоящию из 3 кубитов:

$$\begin{aligned} |\psi\rangle_3 = \alpha_0 |000\rangle + \alpha_1 |001\rangle + \alpha_2 |010\rangle + \alpha_3 |011\rangle + \\ + \alpha_4 |100\rangle + \alpha_5 |101\rangle + \alpha_6 |110\rangle + \alpha_7 |111\rangle . \end{aligned} \tag{3.1}$$

[1] Более правильно говорить тремя вещественными числами, потому что на $\alpha_{0,1}$ действует следующее ограничение $|\alpha_0|^2 + |\alpha_1|^2 = 1$ откуда с учетом $\alpha_{0,1} = r_{0,1} e^{i\theta_{0,1}}$ получим что $r_0^2 = 1 - r_1^2$

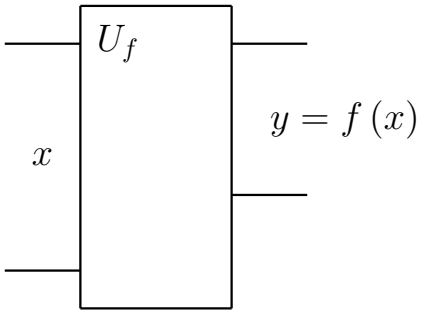


Рис. 3.1: Классические вычисления. На вход подается число x состоящее из n бит, а на выходе имеем результат $y = f(x)$ описываемый m битами

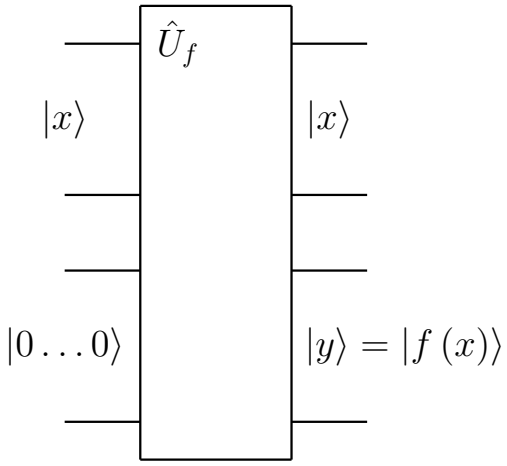


Рис. 3.2: Квантовые обратимые вычисления. На вход подается число $|x\rangle$ состоящее из n кубит и затравка из нулевых состояний (m кубит), а на выходе имеем результат $|y\rangle = |f(x)\rangle$ описываемый m кубитами и исходное состояние $|x\rangle$

Как видно любое классическое состояние системы из 3 бит представлено в качестве одного из членов суперпозиции (3.1). Например число $5_{10} = 101_2$ входит в (3.1) с коэфициентом α_5.

3.1.2 Обратимые вычисления

В классическом случае вычисление состоит в преобразовании исходных n битов в результат, описываемый m битами (см. рис. 3.1). Преобразование при этом задается некоторой функцией $f(x)$. Типичный пример - сложение по модулю 2 (см. табл. 1.1) в котором на входе имеем 2 бита ($n = 2$), а на выходе - 1 бит ($m = 1$).

Такая схема не будет работать в квантовом случае прежде всего потому что изменение чистых квантовых состояний во времени должно осуществятся посредством унитарного оператора эволюции (2.35), т. е. должно быть обра-

тимым что для нашего классического примера невозможно [2]. В силу этого в квантовых вычислениях используют другую схему (см. рис. 3.2) при которой возможны обратимые вычисления.

На вход вместе с исходными данными x описываемыми n кубитами подаются m кубитов в состоянии $|0\rangle$, таким образом чтобы общее число входов и выходов соответствовало друг другу. Следовательно связь между входом и выходом может быть описана в ввиде [3]

$$\underbrace{|x\rangle}_{n}\underbrace{|f(x)\rangle}_{m} = \hat{U}_f \underbrace{|x\rangle}_{n}\underbrace{|0\ldots0\rangle}_{m}. \tag{3.2}$$

3.2 Квантовые логические элементы

Каким образом может быть сконструирован элемент осуществляющий преобразование $\hat{U}_f$ (3.2). Существует набор элементов из которых можно построить, с заданной точностью, элемент осуществляющий необходимое преобразование $\hat{U}_f$. Такие наборы называются универсальными.

3.2.1 Универсальный набор квантовых вентилей

Тождественное преобразование

$$\hat{\sigma}_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Отрицание

$$\hat{\sigma}_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Фазовый сдвиг

$$\hat{\sigma}_2 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

[2] невозможно получить из одного бита (результат) два бита исходной информации

[3] Более правильно записывать в общем виде как $\underbrace{|x\rangle}_{n}\underbrace{|f(x)\rangle}_{m}\underbrace{|r\rangle}_{k} = \hat{U}_f \underbrace{|x\rangle}_{n}\underbrace{|0\ldots0\rangle}_{m+k}$, где $|r\rangle$ остаток размером k кубит который не используется в вычислениях и служит цели обеспечения унитарности оператора $\hat{U}_f$

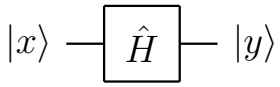


Рис. 3.3: Преобразование Адамара на одном кубите

Преобразование Адамара

Одним из базовых квантовых логических элементов является преобразование Адамара (см. рис. 3.3), которое определяется следующими соотношениями

$$\hat{H}\,|0\rangle = |+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}},$$
$$\hat{H}\,|1\rangle = |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}},$$

В матричной форме это преобразование может быть записано в виде

$$\hat{H} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \tag{3.3}$$

где в качестве базиса выбраны вектора

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

и

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

Из (3.3) можно получить следующее свойство оператора $\hat{H}$:

$$\hat{H}\hat{H} = \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \tag{3.4}$$

Это преобразование используется для получения суперпозиции состояний содержащие все возможные значения аргумента вычисляемой функции (см. рис. 3.4).

CNOT

Матрица преобразования имеет вид

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

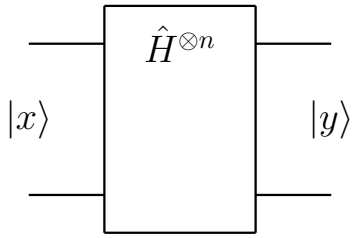


Рис. 3.4: Преобразование Адамара $\hat{H}^{\otimes n}$ на нескольких кубитах

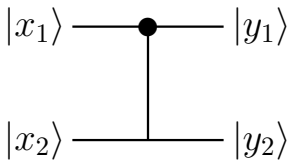


Рис. 3.5: Управляющий элемент CNOT

Данный вентиль (см. рис. 3.5) применяется для двух кубит и инвертирует состояние второго кубита только если первый кубит равен единице.

Таким образом если наше исходное состояние двух кубит было

$$|\psi_i\rangle = a\,|00\rangle + b\,|01\rangle + c\,|10\rangle + d\,|11\rangle$$

то оно преобразуется в

$$CNOT\,|\psi_i\rangle = |\psi_f\rangle = a\,|00\rangle + b\,|01\rangle + c\,|11\rangle + d\,|10\rangle$$

Универсальный набор

Определение 3.2.1 (Универсальный набор квантовых вентилей)**.** Набор квантовых вентилей называют универсальным, если любое унитарное преобразование можно аппроксимировать с заданной точностью конечной последовательностью вентилей из этого набора.

Теорема 3.2.1 (Китаев)**.** *Набор* $\hat{\sigma}_0, \hat{\sigma}_1, \hat{\sigma}_2, \hat{H}, CNOT$ *является универсальным.*

Доказательство. TBD □

3.2.2 Управляющие элементы

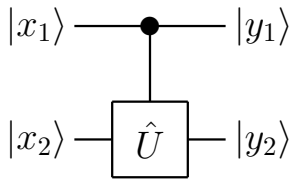


Рис. 3.6: Управляющий элемент

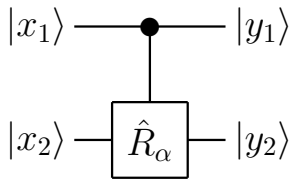


Рис. 3.7: Управляемый фазовый сдвиг $\hat{R}_\alpha$

Глава 4

Алгоритм Гровера

4.1 Алгоритм Гровера

Рассмотрим следующую задачу. Допустим имеется большой набор данных состоящий из N элементов в котором необходимо найти элемент удовлетворяющий некоторым условиям (см. рис. 4.1). Если данные отсортированны, то с помощью алгоритмов типа “разделяй и властвуй” искомый элемент может быть найдет за время порядка $O\left(logN\right)$ (см. разд. 8.9). В ряде случаев исходный набор данных не может быть подготовлен для быстрого поиска, в этом случае классический поиск осуществляется за время порядка $O\left(N\right)$.

Одним из примеров являются алгоритмы симметричного шифрования в которых стоит задача определения ключа по известному шифрованному тексту и соотвествующему ему оригинальному тексту. В этом случае предварительная обработка данных представляется невозможной и решением задачи “в лоб” является простой перебор всех возможных значений.

Алгоритм Гровера [2] решает задачу неструктурированного поиска за вре-

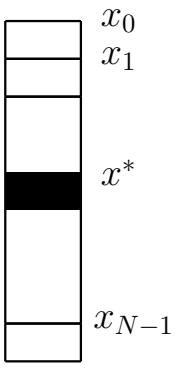


Рис. 4.1: Поиск в неструктурированном объеме данных (поиск "иголки в стоге сена")

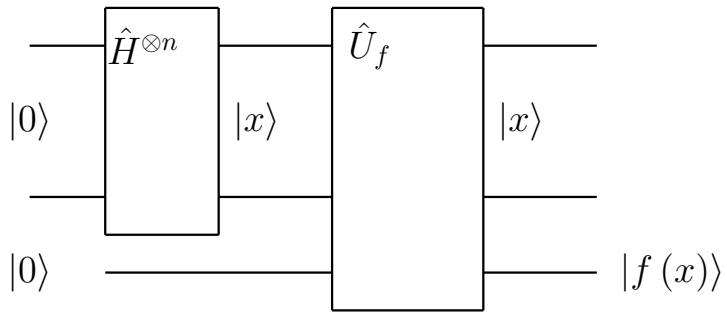


Рис. 4.2: Вычисление функции $f(x)$. На выходе схемы имеем суперпозицию состояний вида $\frac{1}{\sqrt{N}}\left(\sum_{x\neq x^*}|x\rangle\otimes|0\rangle+|x^*\rangle\otimes|1\rangle\right)$

мя порядка $O\left(\sqrt{N}\right)$.

4.1.1 Описание алгоритма

Допустим у нас имеется квантовый контур который вычисляет значение функции $f(x)$ которая может принимать только два значения: 0 и 1. При этом значение 1 справедливо только для искомого элемента:

$$\begin{aligned} f(x)|_{x=x^*} &= 1, \\ f(x)|_{x\neq x^*} &= 0. \end{aligned} \tag{4.1}$$

На рис. 4.2 изображена схема для вычесления искомой функции. На выходе мы имеем сотояние вида

$$|out\rangle = \frac{1}{\sqrt{N}}\left(\sum_{x\neq x^*}|x\rangle\otimes|0\rangle+|x^*\rangle\otimes|1\rangle\right), \tag{4.2}$$

где N - общее число элементов в последовательности в которой производится поиск.

Если посмотреть на выражение (4.2), то можно заметить, что предложенная схема, несмотря на то что она производит вычисление функции в искомой точке, не позволяет выбрать искомый элемент, потому что все элементы результирующей последовательности равновероятны, т. е. каждый элемент может быть выбран (в результате измерения) с одинаковой вероятностью: $\frac{1}{N}$.

Гровером был предложен алгоритм, который позволил бы повысить вероятность обнаружения искомого элемента в результирующей суперпозиции (4.2).

Схема, реализующая алгоритм Гровера представляет собой некоторый блок, описываемый оператором $\hat{U}_G$, который повторяется некоторое число

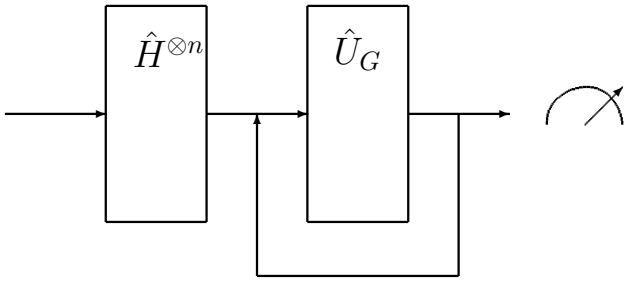


Рис. 4.3: Алгоритм Гровера

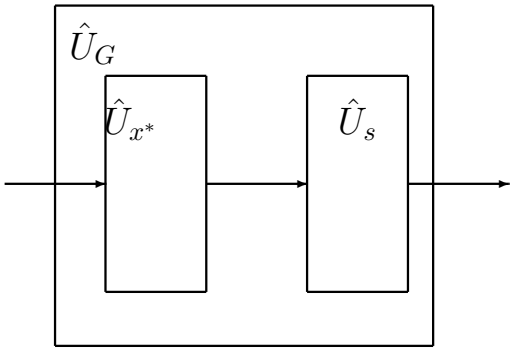


Рис. 4.4: Алгоритм Гровера. Базовый элемент

раз (см. рис. 4.3). При этом на каждом шаге итерации вероятность обнаружения искомого элемента повышается.

Базовый элемент $\hat{U}_G$ представляет собой последовательное действие двух операторов (см. рис. 4.4):

$$\hat{U}_G = \hat{U}_s \hat{U}_{x^*},$$

где $\hat{U}_{x^*}$ - оператор инверсии фазы, $\hat{U}_s$ - оператор обращения относительно среднего.

Действие оператора $\hat{U}_{x^*}$ описывается следующим соотношением (см. рис. 4.5):

$$\hat{U}_{x^*} \left(\sum_x \alpha_x |x\rangle \right) = \sum_x \alpha_x (-1)^{f(x)} |x\rangle . \tag{4.3}$$

Оператор $\hat{U}_{x^*}$ может быть переписан в виде

$$\hat{U}_{x^*} = \hat{I} - 2 |x^*\rangle \langle x^*| .$$

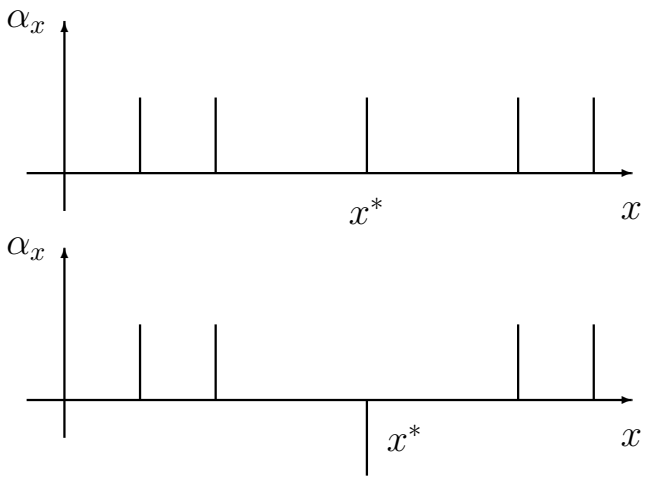


Рис. 4.5: Алгоритм Гровера. Инверсия фазы. Описывается следующим соотношением $\hat{U}_{x^*}\left(\sum_x \alpha_x |x\rangle\right) = \sum_x \alpha_x (-1)^{f(x)} |x\rangle$

Действительно

$$\left(\hat{I} - 2|x^*\rangle\langle x^*|\right)\left(\sum_x \alpha_x |x\rangle\right) =$$
$$= \sum_x \alpha_x |x\rangle - 2\alpha_{x^*}|x^*\rangle = \sum_{x\neq x^*} \alpha_x |x\rangle - \alpha_{x^*}|x^*\rangle =$$
$$= \sum_x \alpha_x (-1)^{f(x)} |x\rangle ,$$

что совпадает с (4.3).

Действие оператора $\hat{U}_s$ описывается следующим соотношением (см. рис. 4.6):

$$\hat{U}_s\left(\sum_x \alpha_x |x\rangle\right) = \sum_x (2\mathcal{M} - \alpha_x)|x\rangle , \qquad (4.4)$$

где $\mathcal{M} = \sum_x \frac{\alpha_x}{N}$.

Оператор $\hat{U}_s$ может быть переписан в следующем виде

$$\hat{U}_s = 2|s\rangle\langle s| - \hat{I},$$

где $|s\rangle = \frac{1}{\sqrt{N}}\sum_x |x\rangle$ - начальное состояние в алгоритме Гровера. Действи-

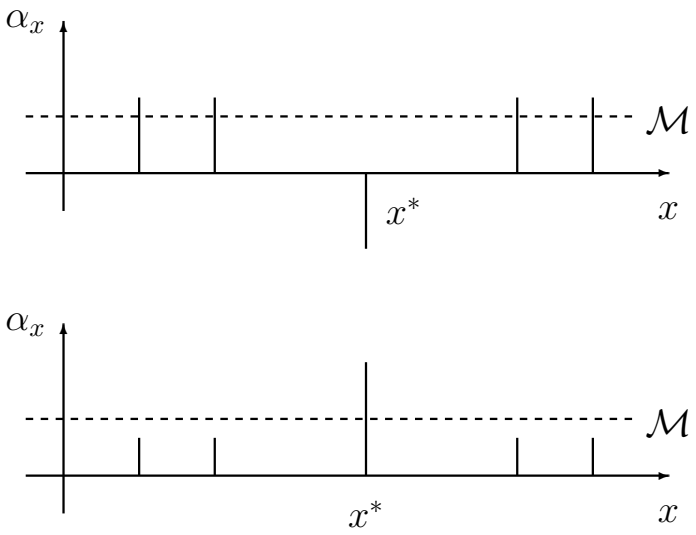


Рис. 4.6: Алгоритм Гровера. Обращение относительно среднего. Описывается следующим соотношением $\hat{U}_s \left(\sum_x \alpha_x |x\rangle\right) = \sum_x (2\mathcal{M} - \alpha_x) |x\rangle$

тельно

$$\begin{aligned}
&\left(2 |s\rangle \langle s| - \hat{I}\right) \left(\sum_x \alpha_x |x\rangle\right) = \\
&= 2 \sum_x \alpha_x \langle s|x\rangle |s\rangle - \sum_x \alpha_x |x\rangle = \\
&= \frac{2}{N} \sum_x \alpha_x \sum_x |x\rangle - \sum_x \alpha_x |x\rangle = \\
&= \sum_x (2\mathcal{M} - \alpha_x) |x\rangle ,
\end{aligned}$$

что совпадает с (4.4).

4.1.2 Анализ алгоритма Гровера

Схематическая форма записи алгоритма Гровера приведена в алг. 1.

Нас будет интересовать два вопроса: какова алгоритмическая сложность алгоритма Гровера и существуют ли алгоритмы которые могут выполнять задачу поиска в неструктурированном объеме данных более эффективно чем алгоритм Гровера.

Критерием эффективности алгоритма служит следующий факт: хороший алгоритм должен находить искомое значение с минимальным числом вызовов функции (4.1).

Алгоритм 1 Алгоритм Гровера

$|\psi\rangle_0 \Leftarrow \frac{1}{\sqrt{N}} \sum_x |x\rangle$
$t \Leftarrow 1$
repeat
  $|\psi\rangle_t \Leftarrow \hat{U}_s \hat{U}_{x^*} |\psi\rangle_{t-1}$
  $t \Leftarrow t + 1$
until $(t < \frac{\pi}{4}\sqrt{N})$
return результат измерения состояния $|\psi\rangle_t$

Рассмотрим самую первую итерацию. Начальное состояние $|\psi\rangle_0$ имеет следующий вид

$$|\psi\rangle_0 = \sum_x \alpha_x |x\rangle = |s\rangle = \frac{1}{\sqrt{N}} \sum_x |x\rangle = \frac{1}{\sqrt{N}} \sum_{x \neq x^*} |x\rangle + \frac{1}{\sqrt{N}} |x^*\rangle .$$

Таким образом коэффициент перед искомым элементом имеет вид $\alpha_x^* = \frac{1}{\sqrt{N}}$.

После применения оператора инверсии фазы U_{x^*} из (4.3) получим

$$\hat{U}_{x^*} |\psi\rangle_0 = \frac{1}{\sqrt{N}} \sum_{x \neq x^*} |x\rangle - \frac{1}{\sqrt{N}} |x^*\rangle = \sum_x \beta_x |x\rangle ,$$

где $\beta_{x^*} = -\frac{1}{\sqrt{N}}$ и $\beta_{x \neq x^*} = \frac{1}{\sqrt{N}}$.

После применения оператора обращения относительно среднего $\hat{U}_s$ из (4.4) получим

$$\hat{U}_G |\psi\rangle_0 = \hat{U}_s \hat{U}_{x^*} |\psi\rangle_0 = \hat{U}_s \sum_x \beta_x |x\rangle =$$

$$= \sum_x (2M - \beta_x) |x\rangle \approx \sum_{x \neq x^*} \left(2\frac{1}{\sqrt{N}} - \frac{1}{\sqrt{N}} \right) |x\rangle +$$

$$+ \left(2\frac{1}{\sqrt{N}} + \frac{1}{\sqrt{N}} \right) |x^*\rangle = \frac{1}{\sqrt{N}} \sum_{x \neq x^*} |x\rangle + \frac{3}{\sqrt{N}} |x^*\rangle . \qquad (4.5)$$

При выводе (4.5) было принятно

$$\mathcal{M} = \frac{\sum_x \alpha_x}{N} \approx \frac{N}{N\sqrt{N}} = \frac{1}{\sqrt{N}}.$$

Таким образом после первой итерации алгоритма Гровера амплитуда α_{x^*} возросла на $\frac{2}{\sqrt{N}}$. Если апроксимировать этот результат на произвольную ите-

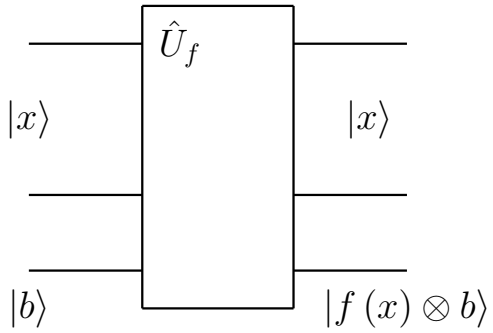


Рис. 4.7: Алгоритм Гровера. Реализация инверсии фазы (оператор $\hat{U}_{x^*}$). Приняв $b = |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$ получим для изображенной схемы $\hat{U}_f \left(\sum_x \alpha_x |x\rangle\right) \otimes |-\rangle = \sum_x \alpha_x (-1)^{f(x)} |x\rangle \otimes |-\rangle$

рацию, то можно получить, что 50% вероятность обнаружить $|x^*\rangle$ будет достижима за следующее число итераций:

$$\frac{1}{\sqrt{2}} / \frac{2}{\sqrt{N}} = \frac{\sqrt{N}}{2\sqrt{2}} = O\left(\sqrt{N}\right).$$

Более точные расчеты [4] дают для числа итераций $\frac{\pi}{4}\sqrt{N}$.

Можно задать вопрос об оптимальности алгоритма Гровера: существует ли квантовый алгоритм, который выполняет поиск в неструктурированном объеме данных быстрее чем за $O\left(\sqrt{N}\right)$ обращений к функции (4.1). В статье [10] показано, что такого алгоритма не существует.

4.1.3 Реализация базовых элементов алгоритма Гровера

Инверсия фазы

Каким образом может быть реализована инверсия фазы: как выглядит квантовый логический элемент который осуществляет преобразование (4.3), т. е. каким образом $f(x)$ может быть "послано" в фазу?

Рассмотрим схему изображенную на рис. 4.7. Предложенная схема осуществляет следующее преобразование:

$$|x\rangle \otimes |b\rangle \to |x\rangle \otimes |b \oplus f(x)\rangle,$$

где введено следующее обозначение: $a \oplus b = a + b \mod 2$.

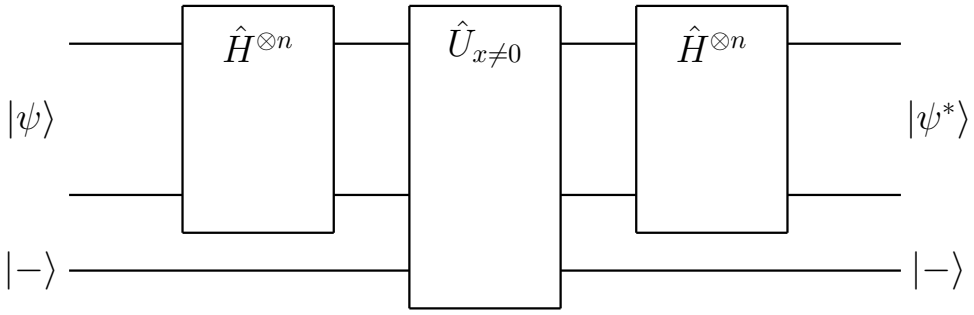


Рис. 4.8: Алгоритм Гровера. Реализация обращения относительно среднего (оператор $\hat{U}_s$): $|\psi\rangle \otimes |-\rangle \rightarrow |\psi^*\rangle \otimes |-\rangle$, где $|\psi\rangle = \sum_x \alpha_x |x\rangle$, $|\psi^*\rangle = \sum_x (2\mathcal{M} - \alpha_x) |x\rangle$. Предложенная схема осуществляет следующее преобразование: $\hat{H}^{\otimes n}\hat{U}_{x\neq 0}\hat{H}^{\otimes n} \sum_x \alpha_x |x\rangle \otimes |-\rangle = \sum_x (2\mathcal{M} - \alpha_x) |x\rangle \otimes |-\rangle$

Для случая $|b\rangle = |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$ имеем

$$
\begin{aligned}
|x\rangle \otimes |-\rangle \rightarrow |x\rangle \otimes \left(\frac{|0 \oplus 0\rangle - |1 \otimes 0\rangle}{\sqrt{2}}\right) = \\
= |x\rangle \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) = |x\rangle \otimes |-\rangle, x \neq x^*, \\
|x\rangle \otimes |-\rangle \rightarrow |x\rangle \otimes \left(\frac{|0 \oplus 1\rangle - |1 \oplus 1\rangle}{\sqrt{2}}\right) = \\
= |x\rangle \otimes \left(\frac{|1\rangle - |0\rangle}{\sqrt{2}}\right) = - |x\rangle \otimes |-\rangle, x = x^*,
\end{aligned}
$$

т. о. мы имеем следующее преобразование

$$
|x\rangle \otimes |-\rangle \rightarrow (-1)^{f(x)} |x\rangle \otimes |-\rangle . \tag{4.6}
$$

Обращение относительно среднего

Рассмотрим схему изображенную на рис. 4.8. Элемент $\hat{U}_{x\neq 0}$ осуществляет преобразование аналогичное (4.6) при этом функция $f(x = 0) = 0$, и $f(x \neq 0) = 1$, т. о.

$$
\begin{aligned}
\hat{U}_{x\neq 0} |x\rangle \otimes |-\rangle = |x\rangle \otimes |-\rangle, x = 0, \\
\hat{U}_{x\neq 0} |x\rangle \otimes |-\rangle = - |x\rangle \otimes |-\rangle, x \neq 0,
\end{aligned}
$$

т. е. матрица преобразования выглядит следующим образом

$$\hat{U}_{x\neq 0} = \begin{pmatrix} 1\otimes|-\rangle & 0 & 0 & \cdots & 0 \\ 0 & -1\otimes|-\rangle & 0 & \cdots & 0 \\ 0 & 0 & -1\otimes|-\rangle & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & -1\otimes|-\rangle \end{pmatrix} =$$

$$= \left\{ \begin{pmatrix} 2 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix} - \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix} \right\} \otimes |-\rangle \,.$$

Объединяя этот результат с двумя преобразованиями Адамара , и воспользовавшись (3.4), получаем:

$$\hat{H}^{\otimes n} \left\{ \begin{pmatrix} 2 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix} - \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix} \right\} \otimes |-\rangle \, \hat{H}^{\otimes n} =$$

$$= \left\{ \hat{H}^{\otimes n} \begin{pmatrix} 2 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix} \hat{H}^{\otimes n} - \hat{H}^{\otimes n} \hat{I} \hat{H}^{\otimes n} \right\} \otimes |-\rangle =$$

$$= \left\{ \begin{pmatrix} \frac{2}{N} & \frac{2}{N} & \frac{2}{N} & \cdots & \frac{2}{N} \\ \frac{2}{N} & \frac{2}{N} & \frac{2}{N} & \cdots & \frac{2}{N} \\ \frac{2}{N} & \frac{2}{N} & \frac{2}{N} & \cdots & \frac{2}{N} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \frac{2}{N} & \frac{2}{N} & \frac{2}{N} & \cdots & \frac{2}{N} \end{pmatrix} - \hat{I} \right\} \otimes |-\rangle =$$

$$= \left\{ \begin{pmatrix} \frac{2}{N}-1 & \frac{2}{N} & \frac{2}{N} & \cdots & \frac{2}{N} \\ \frac{2}{N} & \frac{2}{N}-1 & \frac{2}{N} & \cdots & \frac{2}{N} \\ \frac{2}{N} & \frac{2}{N} & \frac{2}{N}-1 & \cdots & \frac{2}{N} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \frac{2}{N} & \frac{2}{N} & \frac{2}{N} & \cdots & \frac{2}{N}-1 \end{pmatrix} \right\} \otimes |-\rangle \,. \qquad (4.7)$$

Если воздействовать оператором $\hat{H}^{\otimes n}\hat{U}_{x\neq 0}\hat{H}^{\otimes n}$, то используя результат

(4.7) получим:

$$\hat{H}^{\otimes n}\hat{U}_{x\neq 0}\hat{H}^{\otimes n}\sum_x \alpha_x |x\rangle =$$

$$= \begin{pmatrix} \frac{2}{N}-1 & \frac{2}{N} & \frac{2}{N} & \cdots & \frac{2}{N} \\ \frac{2}{N} & \frac{2}{N}-1 & \frac{2}{N} & \cdots & \frac{2}{N} \\ \frac{2}{N} & \frac{2}{N} & \frac{2}{N}-1 & \cdots & \frac{2}{N} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \frac{2}{N} & \frac{2}{N} & \frac{2}{N} & \cdots & \frac{2}{N}-1 \end{pmatrix} \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_{N-1} \end{pmatrix} =$$

$$= \begin{pmatrix} \frac{2}{N}\sum_x \alpha_x - \alpha_0 \\ \frac{2}{N}\sum_x \alpha_x - \alpha_1 \\ \frac{2}{N}\sum_x \alpha_x - \alpha_2 \\ \vdots \\ \frac{2}{N}\sum_x \alpha_x - \alpha_{N-1} \end{pmatrix} = \sum_x (2\mathcal{M} - \alpha_x)|x\rangle .$$

Т. о. схема предложенная на рис. 4.8 действительно осуществляет обращение относительно среднего.

Глава 5

Криптосистемы с открытым ключом. Алгоритм RSA

Криптосистемы с открытым ключом являются основными используемыми в настоящий момент. Кроме того квантовые компьютеры могут эффективно их взламывать. В дальнейшем мы рассмотрим поподробнее эти алгоритмы.

5.1 Алгоритм RSA

Алгоритм RSA (аббревиатура от фамилий Rivest, Shamir и Adleman) - несимметричный алгоритм шифрования [1], основанный на сложности разложения числа на простые множители.

5.1.1 Генерация ключей

Состоит из нескольких шагов

- Выбираются два простых числа p и q
- Вычисляется произведение выбранных простых чисел $n = p \cdot q$
- Вычисляется функция Эйлера (8.3.1) (см. свойства 8.3.1 и 8.3.2) $\phi(n) = (p-1)(q-1)$
- Выбирается целое число e такое что $1 < e < \phi(n)$ и e и $\phi(n)$ взаимно просты, т. е. НОД $(e, \phi(n)) = 1$.

[1] Несимметричным (с открытым ключом) называется такой алгоритм шифрования, в котором используются два различных ключа: один для шифрования, а второй для де-шифрования

- вычисляем $d \equiv e^{-1} \mod \phi(n)$, т. е. $d \cdot e \equiv 1 \mod \phi(n)$.

Открытый ключ состоит из двух чисел: модуля n и открытой экспоненты e. Именно эти два числа используются для шифрования исходного сообщения.

Закрытый ключ состоит тоже из двух чисел: модуля n и закрытой экспоненты d.

Исходные числа p и q держатся в секрете, так как с их помощью вычисление $\phi(n)$ становится тривиальным .

При этом стоит отметить, что для получения закрытого ключа по открытому необходимо вычислить $\phi(n)$ при известном n. Эта задача является сложной (если не известны p и q), как это отмечено в комментарии 8.3.1.

Пример 5.1.1. (RSA. Генерация ключей) *Выбираем два простых числа* $p = 3$ *и* $q = 7$. *Произведение этих чисел* $n = 21$. *Функция Эйлера (8.3.1)* $\phi(n) = (p-1)(q-1) = 2 \cdot 6 = 12$.

Выбираем число e *(открытая экспонента), таким образом, что* $1 < e < 12$ *и НОД* $(e, 12) = 1$. *Очевидно* $e = 5$ *удовлетворяет заявленным условиям.*

Вычисляем закрытую экспоненту $d \equiv 5^{-1} \mod 12$, *т. е.* $d = 5$. *Действительно* $5 \cdot 5 = 25 = 2 \cdot 12 + 1$, *т. е.* $5 \cdot 5 \equiv 1 \mod 12$.

Т. о. получаем

- *Открытый ключ* $(n = 21, e = 5)$
- *Закрытый ключ* $(n = 21, d = 5)$

5.1.2 Шифрование

Допустим надо зашифровать некоторое сообщение M. Вначале оно переводится в целое число(числа) m такое, что $0 < m < \phi(n)$. Далее вычисляется за зашифрованный текст c:

$$c \equiv m^e \mod n \tag{5.1}$$

Пример 5.1.2. (RSA. Шифрование) *Допустим у нас есть открытый ключ* $(n = 21, e = 5)$ *(см. прим. 5.1.1) и мы хотим зашифровать следующее сообщение* $m = 1101_2 = 11_{10}$. *Шифротекст вычисляется по формуле* (5.1) $c \equiv 11^5 \mod 21 = 2$.

5.1.3 Де-шифрование

m может быть восстановлено из c по следующей формуле:

$$m \equiv c^d \mod n. \tag{5.2}$$

Имея m можно восстановить исходное сообщение M.

Пример 5.1.3. (RSA. Де-шифрование) *Допустим у нас есть закрытый ключ* $(n = 21, d = 5)$ *(см. прим. 5.1.1) и шифротекст* $c = 2$ *из примера 5.1.2.*

Исходный текст вычисляется по формуле (5.2) $m \equiv 2^5 \mod 21 = 11 = 1101_2$.

5.1.4 Доказательство

Хотим доказать что

$$(m^e)^d \equiv m \mod p \cdot q$$

для любых положительных числ m когда p и q простые числа, а e и d удовлетворяют выражению

$$d \cdot e \equiv 1 \mod \phi(p \cdot q),$$

которое мы можем переписать в виде

$$d \cdot e - 1 = h(p-1)(q-1).$$

Таким образом

$$m^{e \cdot d} = m m^{h(p-1)(q-1)}.$$

Далее возможны два случая: когда m делится на p и когда m и p взаимно просты.

В первом случае

$$m^{e \cdot d} \equiv m \equiv 0 \mod p$$

Во втором случае используем малую теорему Ферма (Теорема 8.4.1) :

$$m m^{h(p-1)(q-1)} = m \left(m^{p-1}\right)^{h(q-1)} \equiv m \cdot 1^{h(q-1)} \equiv m \mod p.$$

Аналогично имеем либо

$$m^{e \cdot d} \equiv m \equiv 0 \mod q$$

либо в силу малой теоремы Ферма

$$mm^{h(p-1)(q-1)} = m\left(m^{q-1}\right)^{h(p-1)} \equiv m \cdot 1^{h(p-1)} \equiv m \mod q.$$

Таким образом мы имеем следующие два типа соотношений: тривиальное равенство

$$\begin{aligned} x_1 = m \equiv m \mod p, \\ x_1 = m \equiv m \mod q, \end{aligned}$$

и только, что полученные соотношения

$$\begin{aligned} x_2 = m^{ed} \equiv m \mod p, \\ x_2 = m^{ed} \equiv m \mod q, \end{aligned}$$

откуда в силу китайской теоремы об остатках (Теорема 8.5.1)

$$x_1 \equiv x_2 \mod p \cdot q$$

т.е.

$$m^{e \cdot d} \equiv m \mod n$$

5.2 Алгоритм Шора

Один из наиболее популярных алгоритмов шифрования RSA (см. разд. 5.1) построен на предположении о сложности факторизации (разложимости на простые множители) больших чисел. Соответственно алгоритмы позволяющие осуществлять разложение на простые множители представляют особый интерес. Ниже представлено описание такого алгоритма предложенное Шором [9].

5.2.1 Факторизация чисел и нахождение периода функций

Задача факторизации некоторого числа N тесно связана с нахождением периода функций. Рассмотрим следующую, которая называется функцией возведения в степень по модулю

$$f(x, a) = a^x \mod N. \tag{5.3}$$

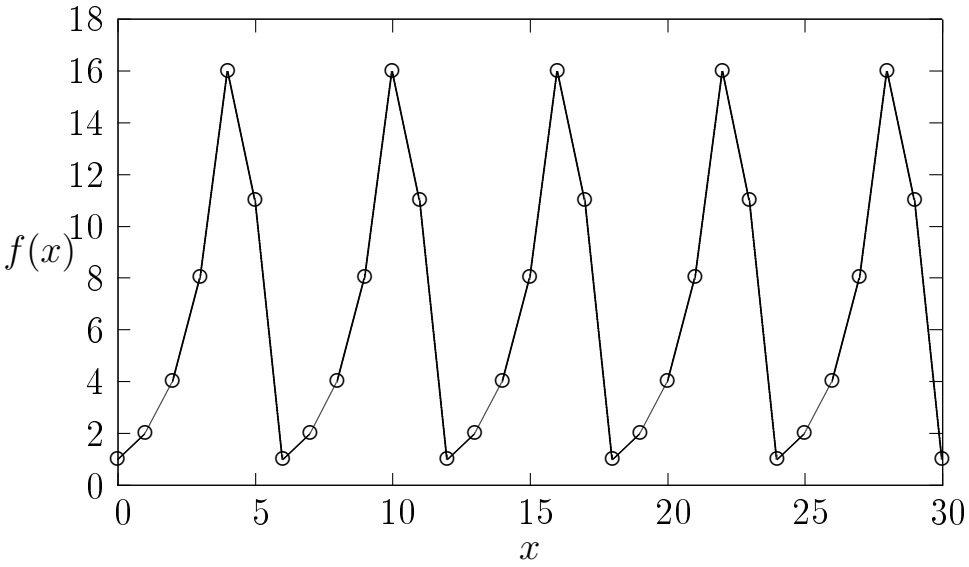


Рис. 5.1: График функции $f(x,a) = a^x \mod N$ при $a = 2$, $N = 21$. Период функции $r = 6$.

Функция (5.3) зависит от анализируемого числа N и двух аргументов x и a. Аргумент a выбирается из следующих условий

$$\begin{aligned} 0 < a < N, \\ \text{НОД}(N,a) = 1. \end{aligned} \tag{5.4}$$

Типичный график функции (5.3) представлен на рис. 5.1.

Условия выбора коэффициента a (5.4) такие что a и N не имеют общих делителей. Если же такие делители существуют, то они являются искомым решением задачи факторизации и легко находятся с помощью алгоритма Евклида (см. разд. 8.1).

Функция (5.3) периодическая, т. е. существует такое число r, что $f(x+r,a) = f(x,a)$. Минимальное из возможных чисел r называется периодом функции (5.3).

Для доказательства периодичности отметим, что $f(x,a)$ не может быть равной нулю. Действительно если выполнено условие $f(x,a) = 0$, то

$$\exists x \in \{0,1,\dots\} : a^x = k \cdot N,$$

где k - целое число, что не возможно в силу взаимной простоты a и N (5.4) [2].

Таким образом область значений функции (5.3) ограничена множеством

$$f(x,a) \in \{1,\dots,N-1\},$$

[2] При это предполагается очевидно, что $N > 1$

откуда

$$\exists k, j : k > j, k, j \in \{0, 1, \ldots, N\}, f(k, a) = f(j, a),$$

что и доказывает периодичность функции (5.3).

Пусть $k = j + r$, тогда

$$a^k \mod N = a^{j+r} \mod N = a^j a^r \mod N = a^j \mod N,$$

т. к. a и N взаимно просты то мы можем записать

$$a^r \equiv 1 \mod N. \tag{5.5}$$

Период функции (5.3) может быть как четным так и нечетным. В алгоритме Шора нам интересен первый вариант: период - четное число. В противном случае выбирают новое число a и повторяют нахождение периода. Таким образом с учетом $r = 2 \cdot l$ мы можем переписать (5.5) в виде

$$a^{2 \cdot l} \equiv 1 \mod N,$$

при этом в силу того r - минимальное число удовлетворяющее условию периодичности, то

$$a^l \not\equiv 1 \mod N.$$

Если при этом подобрать число a таким образом, что

$$a^l \not\equiv -1 \mod N,$$

то имеем

$$\left(a^l - 1\right)\left(a^l + 1\right) = k \cdot N, \tag{5.6}$$

где k - некоторое целое число. Из (5.6) получаем что $a^l \pm 1$ имеют общие нетривиальные (отличные от 1) делители с N.

Пример 5.2.1. Нахождение делителей числа $N = 21$ *В качестве примера рассмотрим задачу о нахождении делителей числа* $N = 21$. *Выбрав* $a = 2$ *мы получим период функции* (5.3) $r = 6$ *(см. рис. 5.1). Очевидно что*

$$2^3 \equiv 8 \mod 21 \not\equiv -1 \mod 21.$$

Таким образом находя соответствующие наибольшие общие делители решаем задачу

$$\begin{aligned} НОД\left(2^3 - 1, 21\right) &= НОД(7, 21) = 7, \\ НОД\left(2^3 + 1, 21\right) &= НОД(9, 21) = 3, \\ 21 &= 7 \cdot 3. \end{aligned}$$

Таким образом задача факторизации числа N может быть сведена к задаче о нахождении периода некоторой функции посредством следующего алгоритма:

Алгоритм 2 Алгоритм Шора

$a \Leftarrow 0$
repeat
  Выбрать новое число a такое, что $0 < a < N$
  if НОД $(a, N) \neq 1$ **then**
    return a
  end if
  Найти период r функции $f(x, a) = a^x \mod N$
until $(r \not\equiv 0 \mod 2)$ **or** $(a^{\frac{r}{2}} \equiv -1 \mod N)$
return НОД $\left(a^{\frac{r}{2}} \pm 1, N\right)$

5.3 Дискретное преобразование Фурье

Преобразование Фурье играет важную роль в обработке цифровых сигналов, в частности для анализа периодических последовательностей.

5.3.1 Определение

Определение 5.3.1. Допустим имеется M отсчетов $x_0, x_1, \ldots, x_{M-1}$ тогда дискретное преобразование Фурье задается следующим соотношением

$$\tilde{X}_k = \frac{1}{\sqrt{M}} \sum_{m=0}^{M-1} x_m e^{-\frac{2\pi i}{M} k \cdot m}, \tag{5.7}$$

которое так же записывается в виде

$$\{x_m\} \longleftrightarrow \left\{\tilde{X}_k\right\}.$$

Обратное преобразование Фурье может быть получено с помощью аналогичного соотношения

$$x_k = \frac{1}{\sqrt{M}} \sum_{m=0}^{M-1} \tilde{X}_m e^{\frac{2\pi i}{M} k \cdot m},$$

На рис. 5.2 приведен график некоторой периодической функции и ее преобразования Фурье.

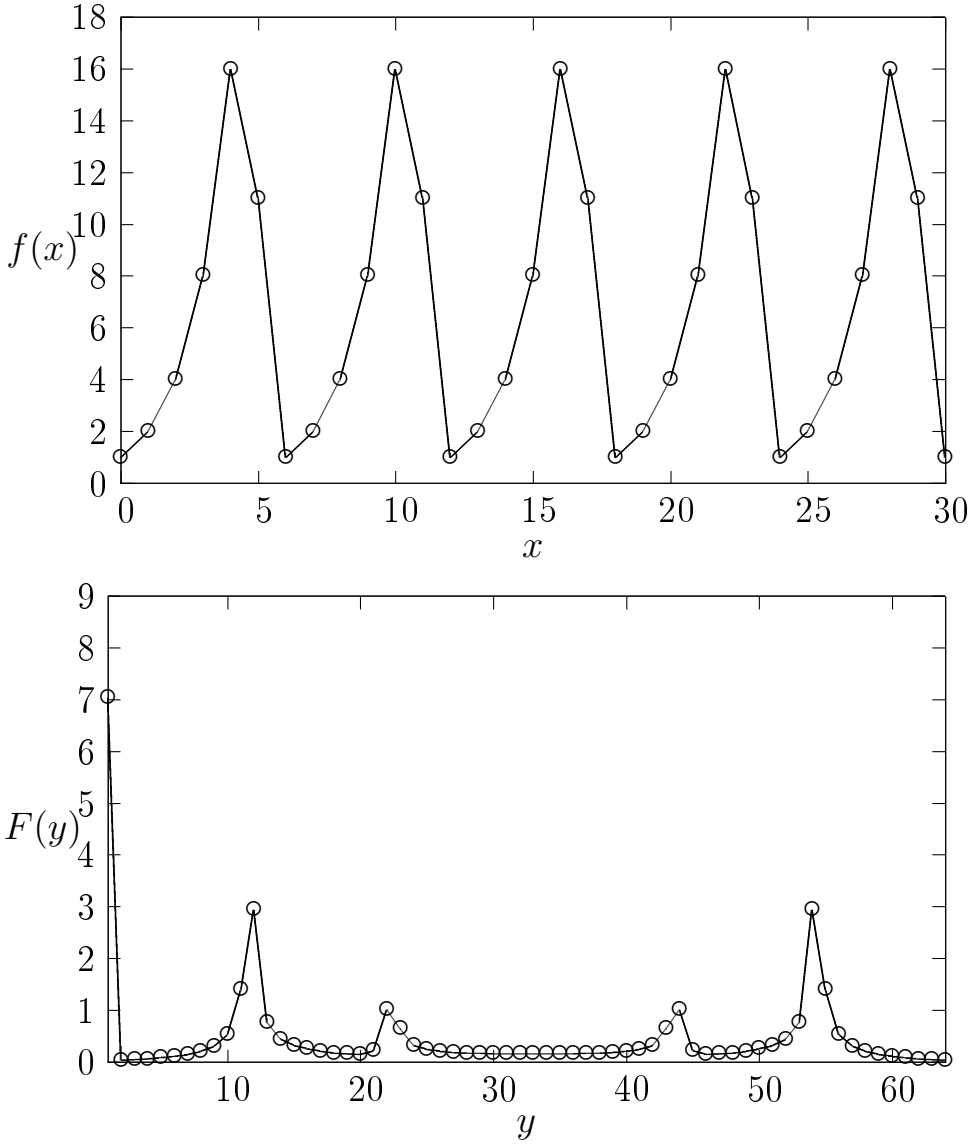


Рис. 5.2: Периодическая функция $f(x,a) = a^x \mod N$ при $a = 2$, $N = 21$ (верхний график) и ее дискретное преобразование Фурье (нижний график)ю Период исходной функции $r = 6$. Число отсчетов $M = 64$, видны локальные максимумы с периодом $T \approx \frac{M}{r} \approx 10.67$

Выражение (5.7) может быть также переписано в матричной форме

$$\vec{\tilde{X}} = \hat{F}\vec{x},$$

где

$$\vec{x} = \begin{pmatrix} x_0 \\ x_1 \\ \vdots \\ x_{M-1} \end{pmatrix}, \vec{\tilde{X}} = \begin{pmatrix} \tilde{X}_0 \\ \tilde{X}_1 \\ \vdots \\ \tilde{X}_{M-1} \end{pmatrix},$$

а матрица $\hat{F}$ имеет вид

$$\hat{F} = \frac{1}{\sqrt{M}} \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & e^{-i\omega} & e^{-2i\omega} & \cdots & e^{-(M-1)i\omega} \\ 1 & e^{-2i\omega} & e^{-4i\omega} & \cdots & e^{-2(M-1)i\omega} \\ 1 & e^{-3i\omega} & e^{-6i\omega} & \cdots & e^{-3(M-1)i\omega} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & e^{-(M-1)i\omega} & e^{-2(M-1)i\omega} & \cdots & e^{-(M-1)(M-1)i\omega} \end{pmatrix}, \tag{5.8}$$

где

$$\omega = \frac{2\pi}{M}.$$

Для матричного элемента матрицы (5.8) можно записать

$$F_{nm} = \frac{1}{\sqrt{M}} e^{-i\omega nm}, \tag{5.9}$$

где $n, m \in \{0, 1, \ldots, M-1\}$.

5.3.2 Свойства дискретного преобразования Фурье

Следует отметить следующие свойства преобразования Фурье, которые играют основную роль в алгоритме Шора:

Лемма 5.3.1. (Сдвиг) *Если* $\{x_n\} \longleftrightarrow \left\{\tilde{X}_k\right\}$ *то* $\left\{x_{(n-m) \mod M}\right\} \longleftrightarrow \left\{e^{-i\omega mk}\tilde{X}_k\right\}$

Доказательство. Для последовательности $\left\{x_{(n-m) \mod M}\right\}$ можно записать

$$\left\{x_{(n-m) \mod M}\right\} = \begin{pmatrix} x_{-m \mod M} \\ x_{-m+1 \mod M} \\ \vdots \\ x_{-1 \mod M} \\ x_0 \\ x_1 \\ \vdots \\ x_{M-m-1} \end{pmatrix} = \begin{pmatrix} x_{M-m} \\ x_{M-m+1} \\ \vdots \\ x_{M-1} \\ x_0 \\ x_1 \\ \vdots \\ x_{M-m-1} \end{pmatrix},$$

при этом

$$\hat{F}\left\{x_{(n-m) \mod M}\right\} = \\ = \frac{1}{\sqrt{M}} \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & e^{-i\omega} & e^{-2i\omega} & \cdots & e^{-(M-1)i\omega} \\ 1 & e^{-2i\omega} & e^{-4i\omega} & \cdots & e^{-2(M-1)i\omega} \\ 1 & e^{-3i\omega} & e^{-6i\omega} & \cdots & e^{-3(M-1)i\omega} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & e^{-(M-1)i\omega} & e^{-2(M-1)i\omega} & \cdots & e^{-(M-1)(M-1)i\omega} \end{pmatrix} \begin{pmatrix} x_{M-m} \\ x_{M-m+1} \\ \vdots \\ x_0 \\ \vdots \\ x_{M-m-1} \end{pmatrix} = \\ = \begin{pmatrix} \frac{x_{M-m}}{\sqrt{M}} + \frac{x_{M-m+1}}{\sqrt{M}} + \cdots + \frac{x_0}{\sqrt{M}} + \cdots + \frac{x_{M-m-1}}{\sqrt{M}} \\ \frac{x_{M-m}}{\sqrt{M}} + \frac{e^{-i\omega}x_{M-m+1}}{\sqrt{M}} + \cdots + \frac{e^{-i\omega m}x_0}{\sqrt{M}} + \cdots + \frac{e^{-i\omega(M-1)}x_{M-m-1}}{\sqrt{M}} \\ \frac{x_{M-m}}{\sqrt{M}} + \frac{e^{-2i\omega}x_{M-m+1}}{\sqrt{M}} + \cdots + \frac{e^{-2i\omega m}x_0}{\sqrt{M}} + \cdots + \frac{e^{-2i\omega(M-1)}x_{M-m-1}}{\sqrt{M}} \\ \vdots \\ \frac{x_{M-m}}{\sqrt{M}} + \frac{e^{-mi\omega}x_{M-m+1}}{\sqrt{M}} + \cdots + \frac{e^{-mi\omega m}x_0}{\sqrt{M}} + \cdots + \frac{e^{-mi\omega(M-1)}x_{M-m-1}}{\sqrt{M}} \\ \vdots \end{pmatrix}. \quad (5.10)$$

С учетом соотоношения

$$e^{-i\omega kM} = 1, k \in \{0, 1, \dots\},$$

выражение (5.10) может быть переписано в следующем виде

$$\hat{F}\left\{x_{(n-m) \mod M}\right\} = \\ = \frac{1}{\sqrt{M}} \begin{pmatrix} x_{M-m} + \cdots + x_{M-m-1} \\ e^{-i\omega m} e^{-i\omega(M-m)} x_{M-m} + \cdots + e^{-i\omega 2m} e^{-i2\omega(M-m-1)} \\ e^{-i\omega 2m} e^{-i2\omega(M-m)} x_{M-m} + \cdots + e^{-i\omega 2m} e^{-i2\omega(M-m-1)} \\ \vdots \end{pmatrix} = \\ = \begin{pmatrix} \tilde{X}_0 \\ e^{-i\omega m}\tilde{X}_1 \\ e^{-i\omega 2m}\tilde{X}_2 \\ \vdots \end{pmatrix}.$$

□

Лемма 5.3.2. (Периодичность) *Если последовательность* $\{x_n\}$ *имеет период* r*:* $x_n = x_{n+r}$*, а число отсчетов* M *кратно* r*, то не нулевые члены преобразования Фурье следуют с периодом* $\frac{M}{r}$*.*

Доказательство. Действительно если $M \mod r = 0$ и $kr \mod M \neq 0$, то

$$1 - e^{-i\omega kr} \neq 0,$$

откуда

$$\tilde{X}_k = \frac{1}{\sqrt{M}} \sum_{n=0}^{M-1} e^{-i\omega kn} x_n = \\ = \frac{1}{\sqrt{M}} \left(\sum_{n=0}^{r-1} e^{-i\omega kn} x_n + \sum_{n=0}^{r-1} e^{-i\omega k(n+r)} x_{n+r} + \right. \\ \left. + \sum_{n=0}^{r-1} e^{-i\omega k(n+2r)} x_{n+2r} + \ldots \right) = \\ = \frac{1}{\sqrt{M}} \left(\sum_{n=0}^{r-1} e^{-i\omega kn} x_n + \sum_{n=0}^{r-1} e^{-i\omega k(n+r)} x_n + \sum_{n=0}^{r-1} e^{-i\omega k(n+2r)} x_n + \ldots \right) = \\ = \frac{1}{\sqrt{M}} \left(\sum_{n=0}^{r-1} x_n e^{-i\omega kn} \sum_{l=0}^{\frac{M}{r}-1} e^{-i\omega klr} = \sum_{n=0}^{r-1} x_n e^{-i\omega kn} \frac{1 - e^{-i\omega k \frac{M}{r} r}}{1 - e^{-i\omega kr}} \right) = \\ = \frac{1}{\sqrt{M}} \frac{1 - e^{-i\omega kM}}{1 - e^{-i\omega kr}} \sum_{n=0}^{r-1} x_n e^{-i\omega kn} = 0. \quad (5.11)$$

Если $M \mod r = 0$ и $kr \mod M = 0$, то

$$e^{-i\omega kr} = e^{-i\frac{2\pi}{M}kr} = 1,$$

откуда

$$\tilde{X}_k = \frac{1}{\sqrt{M}} \sum_{n=0}^{M-1} e^{-i\omega kn} x_n =$$

$$= \frac{1}{\sqrt{M}} \left(\sum_{n=0}^{r-1} e^{-i\omega kn} x_n + \sum_{n=0}^{r-1} e^{-i\omega kn} x_{n+r} + \sum_{n=0}^{r-1} e^{-i\omega kn} x_{n+2r} + \dots \right) =$$

$$= \frac{1}{\sqrt{M}} \left(\sum_{n=0}^{r-1} e^{-i\omega kn} x_n + \sum_{n=0}^{r-1} e^{-i\omega kn} x_n + \sum_{n=0}^{r-1} e^{-i\omega kn} x_n + \dots \right) =$$

$$= \frac{1}{\sqrt{M}} \frac{M}{r} \sum_{n=0}^{r-1} e^{-i\omega kn} x_n \neq 0. \quad (5.12)$$

Таким образом из выражений (5.11) и (5.12) следует что ненулевые члены следуют с периодом $T = \frac{M}{r}$. □

Комментарий 5.3.1. (Периодичность максимумов) *Стоит отметить, что выражение (5.11) (в случае когда период не кратен числу отсчетов: $M \mod r \neq 0$) будет приближенно равно 0 для тех значений k которые сильно отличаются от значений кратных $\frac{M}{r}$, т. е. локальные максимумы перобразования Фурье будут повторяться с периодом $\frac{M}{r}$.*

5.3.3 Быстрое преобразование Фурье

Вычисления по формуле (5.7) имеют сложность порядка $O\left(M^2\right)$, где M - число элементов (отсчетов) [3].

Существует алгоритм быстрого расчета по формуле (5.7) который имеет сложность $O\left(M \log M\right)$.

Воспользовавшись парадигмой “разделяй и властвуй” (см. разд. 8.9) можно обратить внимание на форму записи (5.9) и заметить, что выражение (5.7) может быть переписано в в виде

$$\tilde{X}_k = \sum_{m=0}^{M-1} F_{km}^M x_m,$$

[3] Действительно необходимо получить M элементов, для подсчета каждого из которых требуется M операций умножения

где запись F_{km}^{M} обозначает, что используется матрица (5.9) размера $M \times M$. Если M четно, то

$$\tilde{X}_k = \sum_{m=0}^{M-1} F_{k,m}^{M} x_m = \sum_{m=0}^{\frac{M}{2}-1} F_{k,2m}^{M} x_{2m} + \sum_{m=0}^{\frac{M}{2}-1} F_{k,2m+1}^{M} x_{2m+1},$$

где

$$F_{k,2m}^{M} = e^{-i\omega k 2m} = e^{-ikm\frac{2\pi}{\frac{M}{2}}} = F_{k,m}^{\frac{M}{2}},$$
$$F_{k,2m+1}^{M} = e^{-i\omega k(2m+1)} = e^{-i\omega k} e^{-ikm\frac{2\pi}{\frac{M}{2}}} = e^{-2\pi i\frac{k}{M}} F_{k,m}^{\frac{M}{2}},$$

т. е.

$$\tilde{X}_k = \sum_{m=0}^{\frac{M}{2}-1} F_{k,m}^{\frac{M}{2}} x_{2m} + \exp\left\{\left(-2\pi i\frac{k}{M}\right)\right\} \sum_{m=0}^{\frac{M}{2}-1} F_{k,m}^{\frac{M}{2}} x_{2m+1}. \tag{5.13}$$

Сложность вычислений по формуле (5.13) определяется следующим соотношением

$$T(M) = 2T\left(\frac{M}{2}\right) + O(M). \tag{5.14}$$

В справедливости (5.14) можно убедится если заметить что вычисления сложности $T(M)$ в (5.13) распадаются на две подзадачи по вычислениям сложности $T\left(\frac{M}{2}\right)$.

Используя основную теорему о рекуррентных соотношениях (случай 2) (Теорема 8.8.1) получаем

$$T(M) = O(M \log M).$$

5.4 Квантовое преобразование Фурье

Для анализа периодических последовательностей (функций) может быть использовано дискретное преобразование Фурье (см. разд. 5.3), которое определяется следующим соотношением (5.7):

$$\tilde{X}_k = \sum_{m=0}^{M-1} x_m e^{-\frac{2\pi}{M}k\cdot m}, \tag{5.15}$$

где исходная последовательность чисел $\{x_m\}$ имеет M членов.

5.4.1 Схема квантового преобразования Фурье

Квантовое преобразование Фурье [4] имеет дело с состояниями вида

$$|x\rangle = \sum_{k=0}^{M-1} x_k |k\rangle , \tag{5.16}$$

где имеется последовательнеость амплитуд $\{x_k\}$, которая задает исходную последовательность для преобразования Фурье (5.15). В базисном векторе $|k\rangle$ записан номер члена этой последовательности.

Очевидно, что члены последовательности (5.16) должны удовлетворять условию нормировки

$$\sum_k |x_k|^2 = 1.$$

Допустим что некоторый оператор $\hat{F}^M$ (оператор квантового преобразования Фурье) преобразует базисный вектор $|k\rangle$ по правилу задаваемому соотношением (5.7):

$$\hat{F}^M |k\rangle = \frac{1}{\sqrt{M}} \sum_{j=0}^{M-1} e^{-i\omega kj} |j\rangle_{inv} \tag{5.17}$$

Системы базисных векторов $\{|k\rangle\}$ и $\{|k\rangle_{inv}\}$ представляют собой один и тот же набор векторов которые пронумерованны различным способом.

Из (5.16) и (5.17) получим

$$\begin{aligned}
\hat{F}^M |x\rangle = \sum_{j=0}^{M-1} x_k \hat{F}^M |k\rangle = \\
= \frac{1}{\sqrt{M}} \sum_{k=0}^{M-1} \sum_{j=0}^{M-1} e^{-i\omega kj} x_k |j\rangle_{inv} = \\
= \sum_{j=0}^{M-1} \left\{ \frac{1}{\sqrt{M}} \left(\sum_{k=0}^{M-1} e^{-i\omega kj} x_k \right) \right\} |j\rangle_{inv} = \\
= \sum_{j=0}^{M-1} \tilde{X}_j |j\rangle_{inv} = \left| \tilde{X} \right\rangle_{inv},
\end{aligned}$$

где

$$\tilde{X}_j = \tilde{X}_j^M = \frac{1}{\sqrt{M}} \sum_{k=0}^{M-1} e^{-i\omega kj} x_k. \tag{5.18}$$

[4] Для анализа работы схемы квантового преобразования Фурье была использована работа [3]

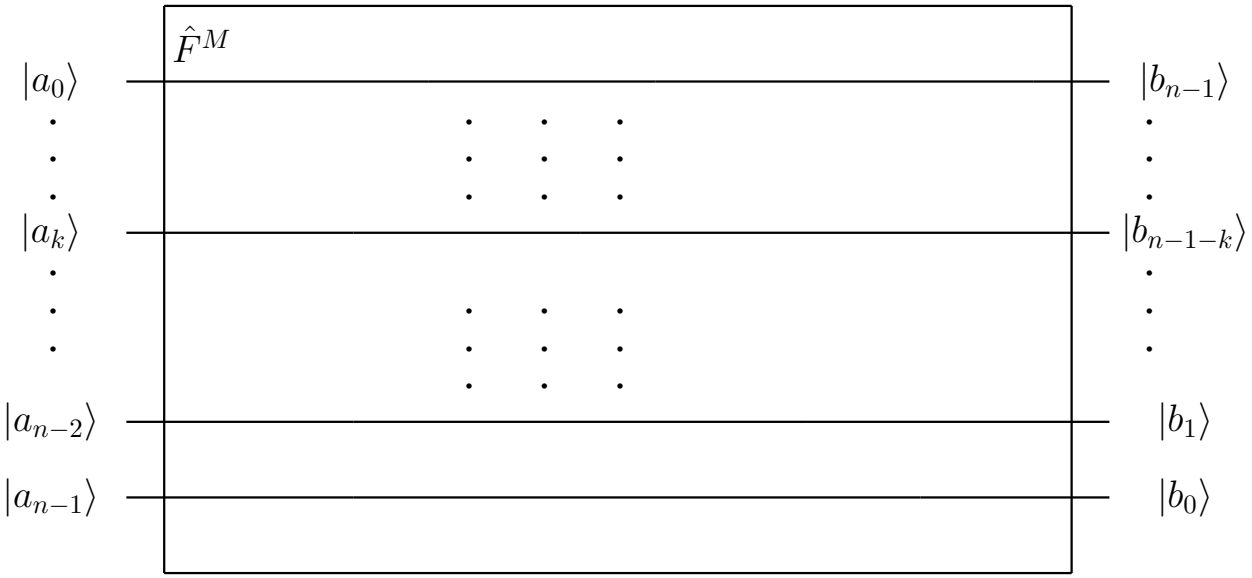


Рис. 5.3: Схема квантового преобразования Фурье основанная на алгоритме быстрого преобразования Фурье. Исходные данные и данные на выходе

Выражение (5.18) повторяет классический аналог (5.7), т. е. можно записать

$$|x\rangle \longleftrightarrow \left|\tilde{X}\right\rangle_{inv}.$$

Допустим теперь, что на вход нашей системы подается состояние вида (5.16) которое представляет собой суперпозицию M базисных состояний $\{|k\rangle\}$ (см. рис. 5.3). Предположим что число базисных состояний является степенью двойки, т. е. базисное состояние представимо в виде тензорного произведения $n = \log_2 M$ кубитов:

$$|k\rangle = \left|a_0^{(k)}\right\rangle \otimes \left|a_1^{(k)}\right\rangle \otimes \cdots \otimes \left|a_{n-1}^{(k)}\right\rangle,$$

где

$$k = a_0^{(k)} + 2^1 a_1^{(k)} + \cdots + 2^{n-1} a_{n-1}^{(k)},$$
$$a_i^{(k)} \in \{0, 1\}.$$

На выходе (см. рис. 5.3) мы имеем суперпозицию M базисных состояний $\{|j\rangle_{inv}\}$, где для состояния $|j\rangle_{inv}$ получим

$$|j\rangle_{inv} = \left|b_{n-1}^{(j)}\right\rangle \otimes \left|b_{n-2}^{(j)}\right\rangle \otimes \cdots \otimes \left|b_0^{(j)}\right\rangle,$$

где

$$j = b_0^{(j)} + 2^1 b_1^{(j)} + \cdots + 2^{n-1} b_{n-1}^{(j)},$$
$$b_i^{(j)} \in \{0, 1\}.$$

Из формулы (5.13) можно заметить, что если у нас имеется входной сигнал x состоящий из $n = \log_2 M$ битов, то бит $a_0^{(k)}$ может быть использован для выбора четных (первого члена суммы (5.13)) или нечетных (второго члена суммы (5.13)).

Действительно, исключая $a_0^{(k)}$, состояние (5.16) можно представить в виде суммы четных и нечетных компонент:

$$\begin{aligned}
|x\rangle = \sum_{k=0}^{M-1} x_k |k\rangle = \sum_{k=0}^{M-1} x_k \left|a_0^{(k)}\right\rangle \otimes \left|a_1^{(k)}\right\rangle \otimes \cdots \otimes \left|a_{n-1}^{(k)}\right\rangle = \\
= \sum_{m=0}^{\frac{M}{2}-1} x_{k=2m} |0\rangle \otimes \left|a_1^{(k)}\right\rangle \otimes \cdots \otimes \left|a_{n-1}^{(k)}\right\rangle + \\
+ \sum_{m=0}^{\frac{M}{2}-1} x_{k=2m+1} |1\rangle \otimes \left|a_1^{(k)}\right\rangle \otimes \cdots \otimes \left|a_{n-1}^{(k)}\right\rangle = \\
= \sum_{m=0}^{\frac{M}{2}-1} x_{k=2m} |0\rangle \otimes |m\rangle + \sum_{m=0}^{\frac{M}{2}-1} x_{k=2m+1} |1\rangle \otimes |m\rangle = \\
= \sum_{m=0}^{\frac{M}{2}-1} x_{2m} |2m\rangle + \sum_{m=0}^{\frac{M}{2}-1} x_{2m+1} |2m+1\rangle ,
\end{aligned}$$

где

$$m = a_1^{(k)} + 2^1 a_2^{(k)} + \cdots + 2^{n-2} a_{n-1}^{(k)}.$$

Применяя преобразование Фурье только для старших бит $\hat{F}^{\frac{M}{2}}$, т. е. исключая $a_0^{(k)}$, получим (см. рис. 5.4):

$$\begin{aligned}
|x\rangle \to \hat{F}^{\frac{M}{2}} \sum_{m=0}^{\frac{M}{2}-1} x_{2m} |2m\rangle + \hat{F}^{\frac{M}{2}} \sum_{m=0}^{\frac{M}{2}-1} x_{2m+1} |2m+1\rangle = \\
= \hat{F}^{\frac{M}{2}} \sum_{m=0}^{\frac{M}{2}-1} x_{2m} |0\rangle \otimes |m\rangle + \hat{F}^{\frac{M}{2}} \sum_{m=0}^{\frac{M}{2}-1} x_{2m+1} |1\rangle \otimes |m\rangle = \\
= \sum_{m=0}^{\frac{M}{2}-1} x_{2m} |0\rangle \otimes \hat{F}^{\frac{M}{2}} |m\rangle + \sum_{m=0}^{\frac{M}{2}-1} x_{2m+1} |1\rangle \otimes \hat{F}^{\frac{M}{2}} |m\rangle . \qquad (5.19)
\end{aligned}$$

С учетом выражения (5.17) получим

$$\hat{F}^{\frac{M}{2}} |m\rangle = \sqrt{\frac{2}{M}} \sum_{j=0}^{\frac{M}{2}-1} e^{-i\frac{4\pi}{M}mj} |j\rangle_{inv} .$$

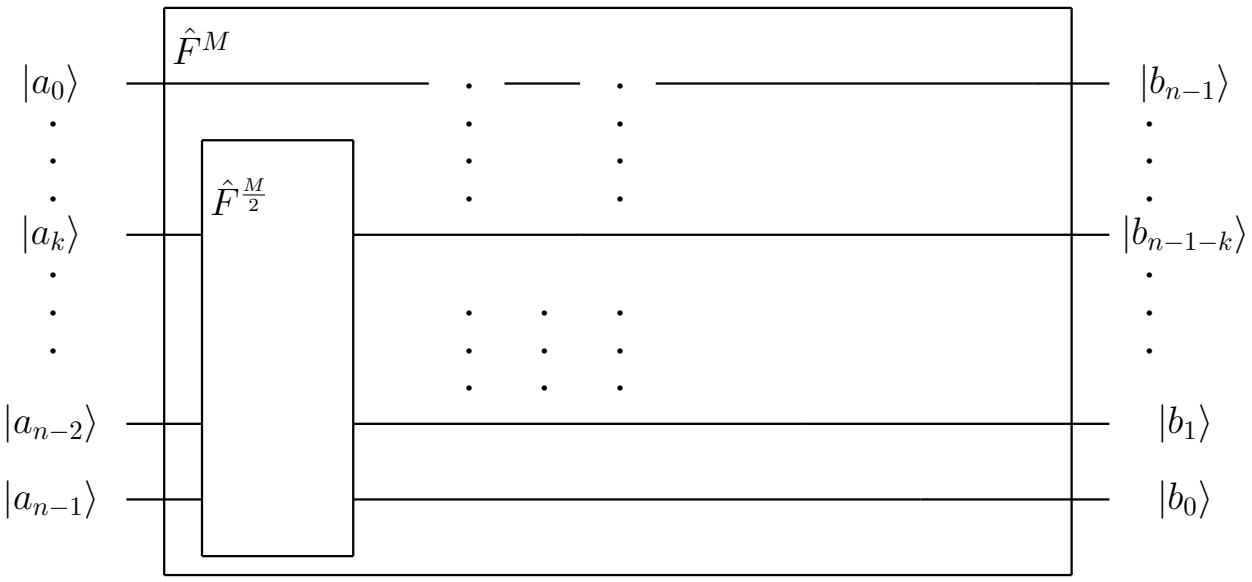


Рис. 5.4: Схема квантового преобразования Фурье основанная на алгоритме быстрого преобразования Фурье. Шаг 1: $|x\rangle \rightarrow \hat{F}^{\frac{M}{2}} \sum_{m=0}^{\frac{M}{2}-1} x_{2m} |2m\rangle + \hat{F}^{\frac{M}{2}} \sum_{m=0}^{\frac{M}{2}-1} x_{2m+1} |2m+1\rangle$

Таким образом для (5.19) имеем

$$
\begin{aligned}
|x\rangle \rightarrow \sum_{m=0}^{\frac{M}{2}-1} x_{2m} |0\rangle \otimes \hat{F}^{\frac{M}{2}} |m\rangle + \sum_{m=0}^{\frac{M}{2}-1} x_{2m+1} |1\rangle \otimes \hat{F}^{\frac{M}{2}} |m\rangle = \\
= \sqrt{\frac{2}{M}} \sum_{j=0}^{\frac{M}{2}-1} e^{-i\frac{4\pi}{M}mj} \sum_{m=0}^{\frac{M}{2}-1} x_{2m} |0\rangle \otimes |j\rangle_{inv} + \\
+ \sqrt{\frac{2}{M}} \sum_{j=0}^{\frac{M}{2}-1} e^{-i\frac{4\pi}{M}mj} \sum_{m=0}^{\frac{M}{2}-1} x_{2m+1} |1\rangle \otimes |j\rangle_{inv} = \\
= \sum_{j=0}^{\frac{M}{2}-1} \left(\sqrt{\frac{2}{M}} \sum_{m=0}^{\frac{M}{2}-1} e^{-i\frac{4\pi}{M}mj} x_{2m} \right) |j\rangle_{inv} + \\
+ \sum_{j=0}^{\frac{M}{2}-1} \left(\sqrt{\frac{2}{M}} \sum_{m=0}^{\frac{M}{2}-1} e^{-i\frac{4\pi}{M}mj} x_{2m+1} \right) \left| \frac{M}{2} + j \right\rangle_{inv} = \\
= \sum_{j=0}^{\frac{M}{2}-1} \tilde{A}_j |j\rangle_{inv} + \sum_{j=0}^{\frac{M}{2}-1} \tilde{B}_j \left| \frac{M}{2} + j \right\rangle_{inv},
\end{aligned}
$$

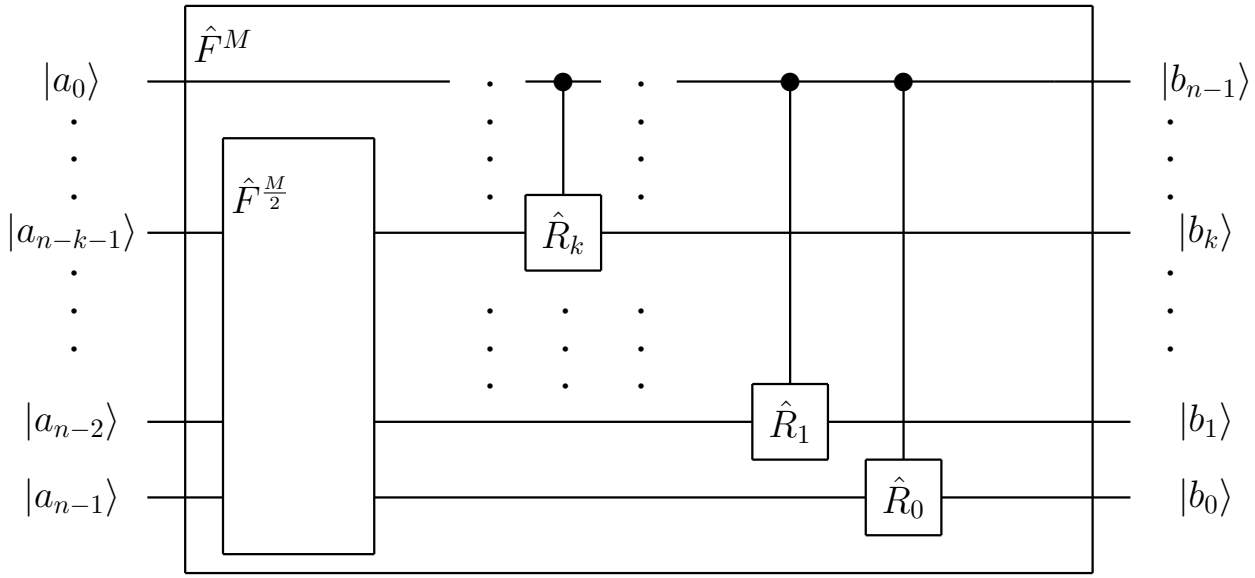


Рис. 5.5: Схема квантового преобразования Фурье основанная на алгоритме быстрого преобразования Фурье. Шаг 2: $|x\rangle \rightarrow \hat{F}^{\frac{M}{2}} \sum_{m=0}^{\frac{M}{2}-1} x_{2m} |2m\rangle + \hat{R}\hat{F}^{\frac{M}{2}} \sum_{m=0}^{\frac{M}{2}-1} x_{2m+1}$

где

$$\tilde{A}_j = \sqrt{\frac{2}{M}} \sum_{m=0}^{\frac{M}{2}-1} e^{-i\frac{4\pi}{M}mj} x_{2m}$$
$$\tilde{B}_j = \sqrt{\frac{2}{M}} \sum_{m=0}^{\frac{M}{2}-1} e^{-i\frac{4\pi}{M}mj} x_{2m+1} \tag{5.20}$$

Если добавить теперь фазовый сдвиг для нечетных элементов, т. е. для тех у которых $a_0^k = 1$ то получим схему изображенную на рис. 5.5:

$$\begin{aligned} |x\rangle \rightarrow \hat{F}^{\frac{M}{2}} \sum_{m=0}^{\frac{M}{2}-1} x_{2m} |2m\rangle + \hat{R}\hat{F}^{\frac{M}{2}} \sum_{m=0}^{\frac{M}{2}-1} x_{2m+1} |2m+1\rangle = \\ = \sum_{j=0}^{\frac{M}{2}-1} \tilde{A}_j |j\rangle_{inv} + \sum_{j=0}^{\frac{M}{2}-1} \tilde{B}_j \hat{R} \left|\frac{M}{2}+j\right\rangle_{inv}, \\ = \sum_{j=0}^{\frac{M}{2}-1} \tilde{A}_j |j\rangle_{inv} + \sum_{j=0}^{\frac{M}{2}-1} \tilde{C}_j \left|\frac{M}{2}+j\right\rangle_{inv}. \end{aligned} \tag{5.21}$$

Воспользовавшись выражением

$$\hat{R}_l \left| b_l^{(j)} \right\rangle = exp\left(-2\pi i \frac{b_l^{(j)}}{2^{n-l}} \right) \left| b_l^{(j)} \right\rangle$$

получим, что оператор $\hat{R}$ действует на состояние $\left| \frac{M}{2} + j \right\rangle_{inv}$ следующим образом:

$$\begin{aligned} \hat{R} \left| \frac{M}{2} + j \right\rangle_{inv} &= \hat{R} \left| 1 \right\rangle \otimes \left| j \right\rangle_{inv} = \\ = \left| 1 \right\rangle \otimes \hat{R}_0 \left| b_0^{(j)} \right\rangle \otimes \cdots \otimes \hat{R}_{n-2} \left| b_{n-2}^{(j)} \right\rangle &= \\ = \prod_{l=0}^{n-2} exp\left(-2\pi i \frac{2^l b_l^{(j)}}{2^n} \right) \left| 1 \right\rangle \otimes \left| j \right\rangle_{inv} &= \\ = exp\left(-2\pi i \frac{j}{M} \right) \left| \frac{M}{2} + j \right\rangle_{inv} & \end{aligned} \tag{5.22}$$

При выводе (5.22) было учтено, что $j = b_0^{(j)} + 2^1 b_1^{(j)} + \cdots + 2^{n-2} b_{n-2}^{(j)}$.

Таким образом для $\tilde{C}_j$ в (5.21) имеем

$$\begin{aligned} \tilde{C}_j = \sqrt{\frac{2}{M}} \sum_{m=0}^{\frac{M}{2}-1} e^{-2\pi i \frac{j}{M}} e^{-i\frac{4\pi}{M} m j} x_{2m+1} = \\ = \sqrt{\frac{2}{M}} \sum_{m=0}^{\frac{M}{2}-1} e^{-i\frac{2\pi}{M}(2m+1)j} x_{2m+1} \end{aligned} \tag{5.23}$$

Если теперь применить преобразование Адамара для кубита $|a_0\rangle$, то получим схему изображенную на рис. 5.6. При этом исходное состояние преоб-

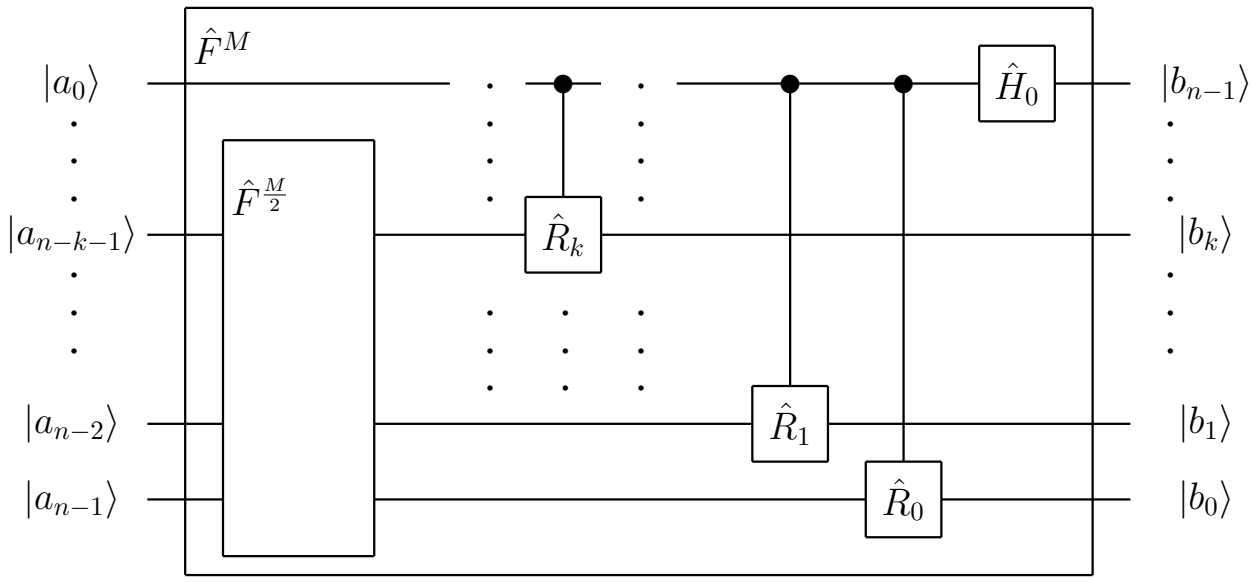


Рис. 5.6: Схема квантового преобразования Фурье основанная на алгоритме быстрого преобразования Фурье

разуется по следующему закону:

$$|x\rangle \to \hat{H}_0\hat{F}^{\frac{M}{2}}\sum_{m=0}^{\frac{M}{2}-1} x_{2m}\,|2m\rangle + \hat{H}_0\hat{R}\hat{F}^{\frac{M}{2}}\sum_{m=0}^{\frac{M}{2}-1} x_{2m+1} =$$

$$= \sum_{j=0}^{\frac{M}{2}-1} \tilde{A}_j\hat{H}\,|0\rangle\otimes|j\rangle_{inv} + \sum_{j=0}^{\frac{M}{2}-1} \tilde{C}_j\hat{H}\,|1\rangle\otimes|j\rangle_{inv} =$$

$$= \frac{1}{\sqrt{2}}\sum_{j=0}^{\frac{M}{2}-1} \tilde{A}_j\,(|0\rangle+|1\rangle)\otimes|j\rangle_{inv} + \frac{1}{\sqrt{2}}\sum_{j=0}^{\frac{M}{2}-1} \tilde{C}_j\,(|0\rangle-|1\rangle)\otimes|j\rangle_{inv} =$$

$$= \sum_{j=0}^{\frac{M}{2}-1} \frac{\tilde{A}_j+\tilde{C}_j}{\sqrt{2}}\,|0\rangle\otimes|j\rangle_{inv} + \sum_{j=0}^{\frac{M}{2}-1} \frac{\tilde{A}_j-\tilde{C}_j}{\sqrt{2}}\,|1\rangle\otimes|j\rangle_{inv} =$$

$$= \sum_{j=0}^{\frac{M}{2}-1} \frac{\tilde{A}_j+\tilde{C}_j}{\sqrt{2}}\,|j\rangle_{inv} + \sum_{j=0}^{\frac{M}{2}-1} \frac{\tilde{A}_j-\tilde{C}_j}{\sqrt{2}}\left|\frac{M}{2}+j\right\rangle_{inv}. \quad (5.24)$$

Для членов (5.24) с учетом равенств (5.20) и (5.23) имеем:

$$\frac{\tilde{A}_j + \tilde{C}_j}{\sqrt{2}} = \sqrt{\frac{1}{M}} \sum_{m=0}^{\frac{M}{2}-1} e^{-i\frac{4\pi}{M}mj} x_{2m} + \sqrt{\frac{1}{M}} \sum_{m=0}^{\frac{M}{2}-1} e^{-i\frac{2\pi}{M}(2m+1)j} x_{2m+1} = \\ = \sqrt{\frac{1}{M}} \sum_{m=0}^{M-1} e^{-i\frac{2\pi}{M}mj} x_m \qquad (5.25)$$

и

$$\frac{\tilde{A}_j - \tilde{C}_j}{\sqrt{2}} = \sqrt{\frac{1}{M}} \sum_{m=0}^{\frac{M}{2}-1} e^{-i\frac{4\pi}{M}mj} x_{2m} - \sqrt{\frac{1}{M}} \sum_{m=0}^{\frac{M}{2}-1} e^{-i\frac{2\pi}{M}(2m+1)j} x_{2m+1} = \\ = \sqrt{\frac{1}{M}} \sum_{m=0}^{M-1} e^{-i\frac{2\pi}{M}mj} x_m \frac{1+e^{-i\pi m}}{2} - \sqrt{\frac{1}{M}} \sum_{m=0}^{M-1} e^{-i\frac{2\pi}{M}mj} x_m \frac{1-e^{-i\pi m}}{2} = \\ = \sqrt{\frac{1}{M}} \sum_{m=0}^{M-1} e^{-i\frac{2\pi}{M}mj} e^{-i\pi m} x_m = \sqrt{\frac{1}{M}} \sum_{m=0}^{M-1} e^{-i\frac{2\pi}{M}mj} e^{-i\frac{2\pi}{M}m\frac{M}{2}} x_m = \\ = \sqrt{\frac{1}{M}} \sum_{m=0}^{M-1} e^{-i\frac{2\pi}{M}m\left(\frac{M}{2}+j\right)} x_m \qquad (5.26)$$

Объединяя (5.24), (5.25) и (5.26) окончательно получим

$$|x\rangle \to \sum_{j=0}^{\frac{M}{2}-1} \sqrt{\frac{1}{M}} \sum_{m=0}^{M-1} e^{-i\frac{2\pi}{M}mj} x_m |j\rangle_{inv} + \\ + \sum_{j=0}^{\frac{M}{2}-1} \sqrt{\frac{1}{M}} \sum_{m=0}^{M-1} e^{-i\frac{2\pi}{M}m\left(\frac{M}{2}+j\right)} x_m \left|\frac{M}{2}+j\right\rangle_{inv} = \\ = \sum_{j=0}^{M-1} \tilde{X}_j^M |j\rangle_{inv}$$

5.4.2 Нахождение периода функций с помощью квантового преобразования Фурье

Для определения периода функции (5.3) используется схема представленная на рис. 5.7.

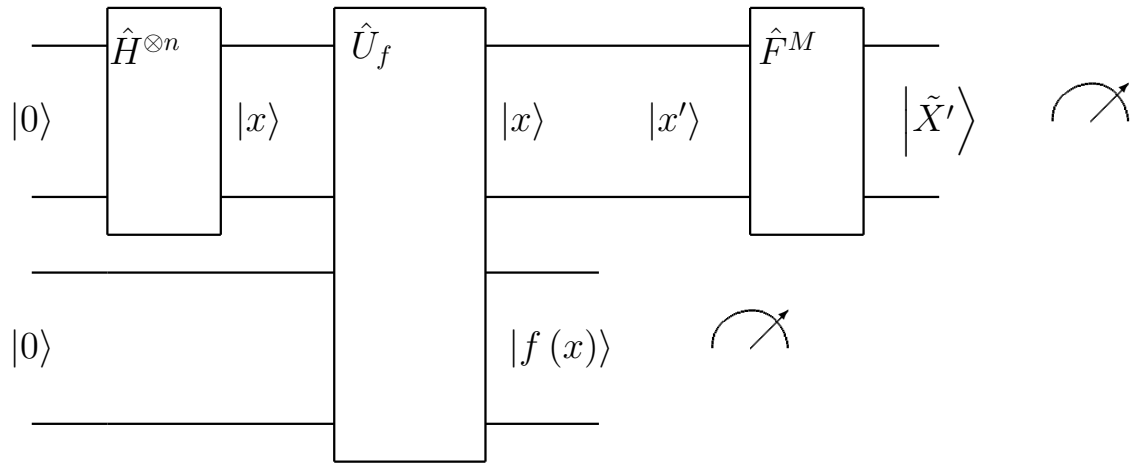


Рис. 5.7: Определение периода функций с помощью квантового преобразования Фурье

Первым элементом стоит преобразование Адамара n кубит, которое подготавливает исходное состояние в виде:

$$|in\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \otimes |0\rangle .$$

После элемента вычисляющего функцию $\hat{U}_f$ имеем для состояния

$$\hat{U}_f |in\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \otimes |f(x)\rangle .$$

После измерения значения функции в списке координат останутся только те элементы для которых значение функции будет равно измеренному значению. В результате на вход элемента, измеряющего преобразование Фурье подается состояние вида

$$|in'\rangle = \sum_{x'} |x'\rangle ,$$

где все ненулевые элементы имеют одинаковую амплитуду и следуют с периодом равным периоду исследуемой функции. При этом начальное значение будет со сдвигом который зависит от эксперимента (в разных экспериментах будет разный сдвиг). В силу леммы 5.3.1 фурье образ будет одинаковым для различных измерений функций.

Далее в силу леммы 5.3.2 (о периодичности)(см. также комментарий 5.3.1) следует что наиболее вероятные отсчеты (максимумы вероятности) следуют с периодом связанным с исходным периодом функции. Таким образом в результате нескольких экспериментов период искомой функции может быть найден с требуемым уровнем вероятности (см. рис. 5.8).

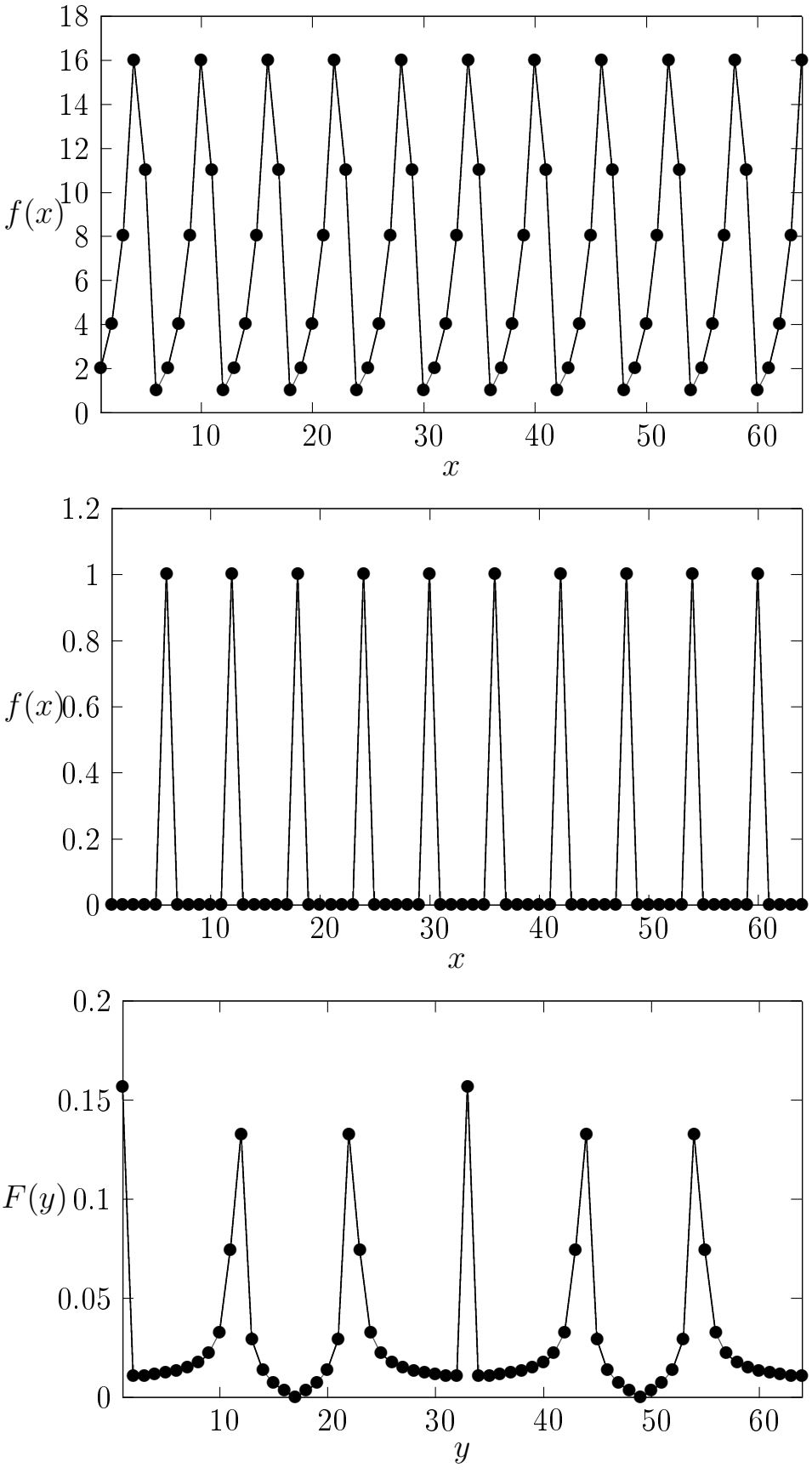


Рис. 5.8: Алгоритм Шора. Нахождение периода функции $f(x, a) = a^x \bmod N$ при $a = 2$, $N = 21$ (верхний график). Значение функции 1 повторяется с периодом $r = 6$ (средний график). Локальные максимумы преобразования Фурье от среднего графика идут с периодом $\frac{M}{r} \approx 10.67$ (нижний график). См прим. 5.4.1

Пример 5.4.1. Нахождение периода функции $f(x) = 2^x \mod 21$ *В качестве примера рассмотрим задачу о нахождении периода функции* $f(x, a) = a^x \mod N$ *при* $a = 2$, $N = 21$ *см. рис. 5.8*

Число отсчетов M *должно быть степенью двойки. В нашем примере мы выбираем* $M = 2^6 = 64$ *в качестве числа отсчетов. Таким образом необходимо 6 кубит для нашего примера.*

Исходное состояние после преобразования Адамара имеет вид:

$$|in\rangle = \frac{1}{8}\sum_{x=0}^{63} |x\rangle \otimes |0\rangle ,$$

где $|x\rangle$ *представляет собой тензорное произведение 6 кубит которые кодируют бинарное представление аргумента исследуемой функции. Например при* $x = 5_{10} = 000101_2$ *имеем*

$$|x\rangle = |0\rangle \otimes |0\rangle \otimes |0\rangle \otimes |1\rangle \otimes |0\rangle \otimes |1\rangle$$

После вычисления функции мы имеем состояние вида (см. верхний график на рис. 5.8)

$$\hat{U}_f |in\rangle = \frac{1}{8}\sum_{x=0}^{63} |x\rangle \otimes |f(x)\rangle =$$

$$= \frac{1}{8}\left(|0\rangle \otimes |2\rangle + |1\rangle \otimes |4\rangle + |2\rangle \otimes |8\rangle + \cdots + \right.$$

$$\left. + |62\rangle \otimes |8\rangle + |63\rangle \otimes |16\rangle\right). \qquad (5.27)$$

Если результат измерения функции был равен 1, *то из всей суммы* (5.27) *останутся члены для которых значение функции равно* 1 *(см. средний график на рис. 5.8):*

$$|in'\rangle = \frac{1}{\sqrt{10}}\left(|5\rangle \otimes |1\rangle + |11\rangle \otimes |1\rangle + |17\rangle \otimes |1\rangle + \cdots + |60\rangle \otimes |1\rangle\right). \qquad (5.28)$$

Выражение (5.28) *содержит 10 членов одинаковой амплитуды, поэтому нормирующий множитель имеет вид* $\frac{1}{\sqrt{10}}$.

Преобразование фурье для последовательности (5.28) *изображено на нижнем графике рис. 5.8. Наиболее вероятными значениями результата измерения фурье образа будут значения соответствующие локальным максимумам которые повторяются с периодом* $\frac{M}{r} \approx 10.67$ *откуда можно найти период искомой функции* $r = 6$.

Глава 6

Криптосистемы с открытым ключом. Алгоритмы использующие дискретный логарифм.

Криптосистемы с открытым ключом являются основными используемыми в настоящий момент. Кроме того квантовые компьютеры могут эффективно их взламывать. В дальнейшем мы рассмотрим поподробнее эти алгоритмы.

6.1 Дискретный логарифм

Определение 6.1.1 (Дискретный логарифм)**.** Рассмотрим некоторую абелеву мультипликативную группу G и уравнение

$$g^x = a \tag{6.1}$$

Решение этого уравнения, т.е. целое неотрицательное число x удовлетворяющее равенству (6.1) называется дискретным логарифмом.

Уравнение (6.1) в общем случае имеет решение не для любых значений a. Но в том случае, если g - порождающий элемент G, т.е. $G =< g >$, то решение всегда существует и оно единственно. В дальнейшем говоря о дискретном логарифме мы будем предполагать, что g выбрано таким образом, что $G =< g >$.

В прикладной криптографии часто имеют дело с особой разновидностью дискретного логарифма в кольце вычетов по модулю p:

Определение 6.1.2 (Дискретный логарифм в кольце вычетов по модулю p)**.** Дискретным логарифмом $ind_g(a) \mod p$ [1] называется минимальное число x, которое удовлетворяет следующему уравнению (если такое число существует):

$$g^x \equiv a \mod p \tag{6.2}$$

Пример 6.1.1. ($ind_3 14 \mod 17$) *Решим задачу методом перебора [12]:*

$$\begin{array}{lllll} 3^1 \equiv 3 \mod 17, & 3^2 \equiv 9 \mod 17, & 3^3 \equiv 10 \mod 17, & 3^4 \equiv 13 \mod 17, \\ 3^5 \equiv 5 \mod 17, & 3^6 \equiv 15 \mod 17, & 3^7 \equiv 11 \mod 17, & 3^8 \equiv 16 \mod 17, \\ 3^9 \equiv 14 \mod 17, & 3^{10} \equiv 8 \mod 17, & 3^{11} \equiv 7 \mod 17, & 3^{12} \equiv 4 \mod 17, \\ 3^{13} \equiv 12 \mod 17, & 3^{14} \equiv 2 \mod 17, & 3^{15} \equiv 6 \mod 17, & 3^{16} \equiv 1 \mod 17, \end{array}$$

т. о. можно видеть, что $ind_3 14 \mod 17 = 9$, *т. к.* $3^9 \equiv 14 \mod 17$.

Задача о нахождении дискретного логарифма является сложной задачей. Самый быстрый из известных алгоритмов [1] решает ее за время порядка $O\left(c \cdot exp\left(\log p^{\frac{1}{3}} \log\log p^{\frac{2}{3}}\right)\right)$, где c - некоторая константа, что обуславливает широкое применение алгоритмов использующих дискретный логарифм в криптографии.

6.2 Протокол Диффи-Хеллмана (Diffie-Hellman, DH)

Предположим существуют два абонента Алиса и Боб. Им известны два числа g и p, которые не являются секретными.

Алиса выбирает случайное число a и пересылает Бобу следущее значение

$$A \equiv g^a \mod p. \tag{6.3}$$

Боб вычисляет следующее число (с помощью секретной случайной величины b)

$$B \equiv g^b \mod p. \tag{6.4}$$

Алиса, с помощью только ей известного числа a вычисляет ключ

$$K \equiv B^a \mod p \equiv g^{ab} \mod p. \tag{6.5}$$

Боб может получить то же самое значение ключа с помощью своего секретного числа b:

$$K \equiv A^b \mod p \equiv g^{ab} \mod p. \tag{6.6}$$

[1] От слова **ind**ex - альтернативного названия для дискретного логорифма

Таким образом Алиса и Боб получают один и тот же ключ, который в дальнейшем может быть использован для переди сообщения с помощью симметричных алгоритмов шифрования (например AES).

Пример 6.2.1. (Диффи-Хеллман) *Исходные данные (открытая информация):* $g = 2$, $p = 23$. *Алиса выбирает случайное число* $a = 6$ *и вычисляет по формуле* (6.3) *число* $A = 18$ *и отсылает его Бобу. Боб выбирает случайное число* $b = 9$ *и, с помощью формулы* (6.4), *получает* $B = 6$ *и отсылает и отсылает это число Алисе.*

Алиса вычисляет ключ $K = 12$ *по формуле* (6.5). *Боб может получить тоже значение ключа* $K = 12$ *используя* (6.6)

Злоумышленнику Еве известны числа g, p, A и B. Для получения ключа K Еве необходимо получить одно из секретных чисел a или b:

$$a \equiv ind_g(A) \mod p,$$

откуда с помощью (6.5) получается искомое значение K.

6.3 Схема Эль-Гамаля (Elgamal)

Одной из вариаций протокола Диффи-Хелмана является схема Эль Гамаля. Следует различать алгоритм шифрования и алгоритм цифровой подписи Эль-Гамаля. Цифровая подпись Эль-Гамаля лежит в основе стандартов цифровой подписи США (DSA) и России (ГОСТ Р 34.10-94).

Ниже мы рассмотрим алгоритм в режиме шифрования.

6.3.1 Генерация ключей

- Генерируется простое число p.
- Выбирается целое число g
- Выбирается случайное целое число $x : 1 < x < p$.
- Вычисляется $y = g^x \mod p$

Открытым ключом является тройка p, g, y. Закрытым ключом является число x.

Пример 6.3.1 (Генерация ключей (Elgamal))**.** *Выбираем* $p = 21, g = 10, x = 3$. $y = 10^3 \mod 21 = 13$.

6.3.2 Шифрование

Шифруемое сообщение M должно удовлетворять критерию $0 < M < p$.

- Выбирается сессионный ключ - случайное число $k : 1 < k < p - 1$.
- Вычисляется $a = g^k \mod p$
- Вычисляется $b = y^k M \mod p$

Пара чисел (a, b) считается шифротекстом.

Пример 6.3.2 (Шифрование (Elgamal)). *Допустим мы хотим зашифровать* $M = 6$. *Выбираем* $k = 7$. $a = 10^7 \mod 21 = 10$, $b = 13^7 \cdot 6 \mod 21 = 15$.

6.3.3 Дешифрование

Зная закрытый ключ x мы можем восстановить исходное сообщение с помощью

$$M = b \cdot (a^x)^{-1} \mod p, \tag{6.7}$$

действительно в силу того что

$$(a^x)^{-1} = g^{-kx} \mod p$$

имеем

$$b \cdot (a^x)^{-1} = y^k M g^{-kx} = g^{kx} M g^{-kx} = M \mod p.$$

Пример 6.3.3 (Дешифрование (Elgamal)). *Зашифрованное сообщение из прим.* 6.3.3 $C = (a = 10, b = 15)$. *Используя* (6.7) *имеем*

$$M = 15 \cdot 13 \mod 21 = 6$$

где было использовано

$$\left(10^3\right)^{-1} \equiv 13 \mod 21,$$

т.к. $13 \cdot 10^3 = 1 \mod 21$. *Таким образом мы восстановили зашифрованное в прим.* 6.3.3 *сообщение* $M = 6$.

6.4 Двумерное преобразование Фурье

6.4.1 Определение

Определение 6.4.1 (Двумерное преобразование Фурье)**.** Допустим у нас имеется двумерный сигнал $x\left(k_1, k_2\right)$, где $k_1, k_2 \in \{0, \ldots, M-1\}$. Двумерным преобразованием Фурье называется двумерная функция

$$\tilde{X}\left(j_1, j_2\right), j_1, j_2 \in \{0, \ldots, M-1\}$$

такая, что

$$\tilde{X}\left(j_1, j_2\right) = \frac{1}{M} \sum_{k_1=0}^{M-1} \sum_{k_2=0}^{M-1} x\left(k_1, k_2\right) e^{-i\omega\left(k_1 j_1 + k_2 j_2\right)},$$

где

$$\omega = \frac{2\pi}{M}.$$

6.5 Квантовое преобразование Фурье и дискретное логарифмирование

Дискретный логарифм (см. разд. 6.1) является основой для большого числа современных криптографических алгоритмов (см. разд. 6.3, разд. 6.2). Вместе с тем метод предложеный Шором для факторизации целых чисел может быть также применен для вычисления дискретных логарифмов, что делает возможным взлом соотвествующих криптографических алгоритмов.

Поставим задачу следующим образом: имеется выражение

$$b = a^x \mod p,$$

в котором числа a, b и p заданны, а число x является неизвестным, которое необходимо определить. По аналогии с применением квантового преобразования Фурье для факторизации чисел (см. разд. 5.2.1), мы должны построить некоторую периодическую функцию, период которой даст нам возможность определить искомое число x. Выберем в качестве анализируемой функции

$$f\left(x_1, x_2\right) = b^{x_1} a^{x_2} = a^{x \cdot x_1} a^{x_2} \mod p \tag{6.8}$$

В качестве примера мы будем рассматривать квантовый аналог решения задачи из прим. 6.1.1:

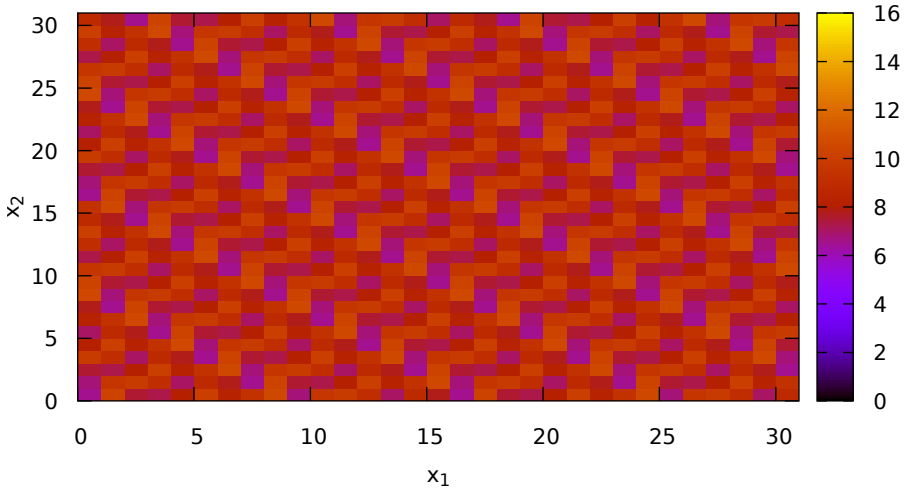


Рис. 6.1: Исследуемая функция $f(x_1, x_2) = 14^{x_1}3^{x_2}$

Пример 6.5.1. ($ind_3 14 \mod 17$) *В нашем примере* $p = 17$, $b = 14$ *и* $a = 3$. *Функция* (6.8) *имеет вид*

$$f(x_1, x_2) = b^{x_1}a^{x_2} = 14^{x_1}3^{x_2}.$$

и изображена на рис. 6.1.

$b = 14$, *так же как и* $a = 3$ *является генератором* $(\mathbb{Z}/17\mathbb{Z})^\times$. *При этом* $3 \equiv 14^9 \mod 17$. *При этом периодами изображенной функции, как это видно из рис. 6.1, будут следующие числа*

$$\begin{aligned} t_1 &\equiv 1 \mod 16, \\ t_2 &\equiv 9 \mod 16 \end{aligned} \tag{6.9}$$

В по аналогии с решением задачи факторизации производится измерение этой функции. Допустим в результате измерения мы получили число $c \in (\mathbb{Z}/p\mathbb{Z})^\times$. В силу того, что a является порождающим элементом (см. опред. 8.6.4) мультипликативной группы $(\mathbb{Z}/p\mathbb{Z})^\times$ (см. опред. 8.6.5) $\exists x_0 : c = a^{x_0}$. Т. о. с учетом малой теоремы Ферма (Теорема 8.4.1) $a^{p-1} \equiv 1 \mod p$ и следовательно

$$x_0 \equiv xx_1 + x_2 \mod q,$$

где $q = p - 1$. Из этого выражения следует, что

$$x_2 \equiv x_0 - xx_1 \mod q.$$

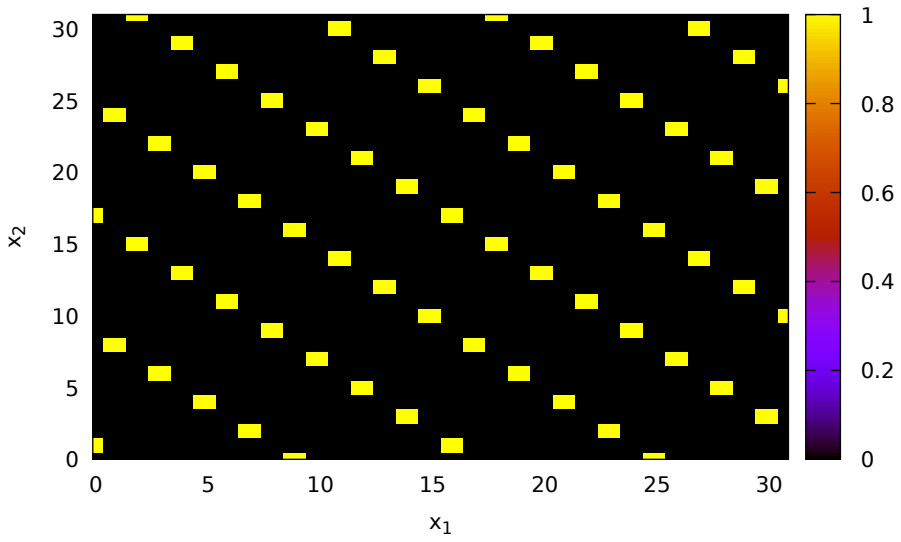


Рис. 6.2: Исследуемая функция $f(x_1, x_2) = 14^{x_1} 3^{x_2}$. Отмечены только те пары x_1, x_2 при которых $f(x_1, x_2) = 3, x_0 = 1$.

Т. е. если функция является периодической по первому аргументу:

$$f(x_1 + t_1, x_2) = f(x_1, x_2),$$

то она будет периодической по второму аргументу

$$f(x_1, x_2 + t_2) = f(x_1, x_2),$$

при этом

$$t_2 \equiv x t_1 \mod q. \tag{6.10}$$

6.5.1 Двумерное преобразование Фурье и период функции $f(x_1, x_2)$

Нашей исследуемой функцией будет являться следующая:

$$f'(x_1, x_2) = \begin{cases} 1, x x_1 + x_2 \equiv x_0 \mod q \\ 0, x x_1 + x_2 \not\equiv x_0 \mod q \end{cases} \tag{6.11}$$

Пример 6.5.2. ($ind_3 14 \mod 17$)

Продолжая пример 6.5.1 допустим, что в результате измерения функции f мы получили значение $f = 3$. Т. е. $f = a^{x_0} = 3^{x_0} \equiv 3 \mod 17$. В результате для x_1, x_2 останутся только те значения, которые соответствуют наблюдаемому значению функции (см. рис. 6.2), т.е. $x x_1 + x_2 = x_0 \equiv 1 \mod 16$. При этом при фиксированных значениях x, x_1 и числе отсчетов $M = q = 16$.

Для Фурье образа $\tilde{f}'$ имеем

$$\tilde{f}'(j_1, j_2) = \frac{1}{M} \sum_{x_1=0}^{M-1} \sum_{x_2=0}^{M-1} f'(x_1, x_2)\, e^{-i\omega(x_1 j_1 + x_2 j_2)}, \tag{6.12}$$

где $\omega = \frac{2\pi}{M}$, M - число отсчетов.

Прежде всего рассмотрим случай когда $M = q$. В этом случае имеется два варианта для x_2:

1. $x_2 = x_0 - x x_1$, если $x_0 \geq x x_1$
2. $x_2 = x_0 + q - x x_1$, если $x_0 < x x_1$

Т. о.

$$e^{-i\omega x_2 j_2} = e^{-i\omega(x_0 - x x_1 + q) j_2} =$$
$$= e^{-i\omega(x_0 - x x_1) j_2 - i\omega q j_2} = e^{-i\omega(x_0 - x x_1) j_2},$$

т. е. оба варианта совпадают и могут быть сведены к первому: $x_2 = x_0 - x x_1$.

Т. о. продолжая (6.12) получим

$$\tilde{f}'(j_1, j_2) = \frac{1}{M} \sum_{x_1=0}^{M-1} \sum_{x_2=0}^{M-1} f'(x_1, x_2)\, e^{-i\omega(x_1 j_1 + x_2 j_2)} =$$
$$= \frac{1}{M} \sum_{x_1=0}^{M-1} e^{-i\omega(x_1 j_1 + (x_0 - x x_1) j_2)} =$$
$$= e^{-i\omega x_0 j_2} \frac{1}{M} \sum_{x_1=0}^{M-1} e^{-i\omega x_1 (j_1 - x j_2)} = \frac{1}{M} e^{-i\omega x_0 j_2} \sum_{x_1=0}^{M-1} e^{-i\omega x_1 (j_1 - x j_2)}. \tag{6.13}$$

В выражении (6.13) $\tilde{f}'(j_1, j_2) = e^{-i\omega x_0 j_2} \neq 0$, если выполнено

$$j_1 \equiv x j_2 \mod M. \tag{6.14}$$

В противном случае по формуле геометрической прогрессии

$$\tilde{f}'(j_1 \neq x j_2, j_2) = e^{-i\omega x_0 j_2} \frac{1}{M} \sum_{x_1=0}^{M-1} e^{-i\omega x_1 (j_1 - x j_2)} =$$
$$= \frac{e^{-i\omega x_0 j_2}}{M} \frac{e^{-i\omega M (j_1 - x j_2)} - 1}{e^{-i\omega (j_1 - x j_2)} - 1} =$$
$$= \frac{e^{-i\omega x_0 j_2}}{M} \frac{e^{-i\frac{2\pi}{M} M (j_1 - x j_2)} - 1}{e^{-i\omega (j_1 - x j_2)} - 1} = 0.$$

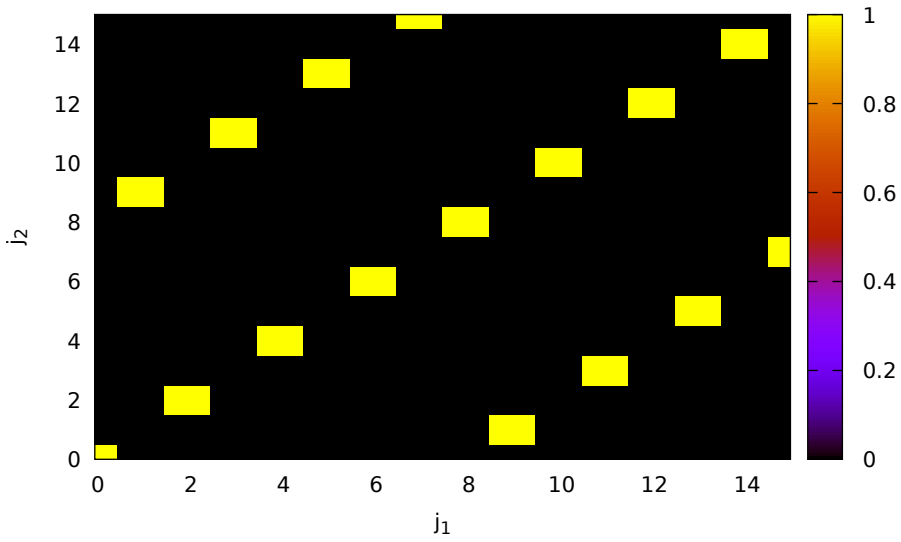


Рис. 6.3: Фурье образ функции с рис. 6.2. Число отсчетов $M = 16$. Координаты максимума $j_1 = 9$, $j_2 = 1$. Решением уравнения $3^x \equiv 14 \mod 17$ является $x \equiv 9 \cdot 1^{-1} \equiv 9 \mod 16$. С учетом того, что период меньше числа отсчетов, можно заключить, что $x = 9$

Т. о. для определения периода нам необходимо найти координаты (j_1, j_2) некоторого максимума преобразования Фурье и воспользоваться выражением

$$x \equiv j_1 j_2^{-1} \mod M, \tag{6.15}$$

которое следует из (6.14).

Комментарий 6.5.1 (О делителях нуля $\mathbb{Z}/M\mathbb{Z}$)**.** *Если существует такое число y, что*

$$j_2 y \equiv 0 \mod M,$$

то j_2 называется делителем нуля. При этом очевидно также, что

$$НОД(j_2, M) \neq 1,$$

таким образом из разд. 8.2.2 следует что j_2^{-1} не существует. Следовательно для таких j_2 выражение (6.15) не определено. В этом случае необходимо использовать другие координаты (j_1, j_2).

Пример 6.5.3. ($ind_3 14 \mod 17$)

Фурье образ функции с рис. 6.2 изображен на рис. 6.3 из которого видно, что с наибольшей вероятностью будут регистрироваться отсчеты которые следуют с интервалом $T_{j_1} = 9$ по координате j_1 и с интервалом $T_{j_2} = 1$ по координате j_2. С учетом того, что число отсчетов $M = 16$ можно

получить координаты максимума преобразования Фурье $j_1 = 9$ *и* $j_2 = 1$. *Решением уравнения* $3^x \equiv 14 \mod 17$ *является, в соответствии с* (6.15), $x = 9 \cdot 1^{-1} = 9$, *что соответствует результату прим. 6.1.1.*

Аналогичный результат можно получить, если взять точку с координатами $j_1 = 11, j_2 = 3$. *С учетом* $3 \cdot 11 = 33 \equiv 1 \mod 16$ *имеем* $j_2^{-1} \equiv 11 \mod 16$, *т. е.* $x \equiv 11 \cdot 11 \equiv 121 \equiv 9 \mod 16$, *что опять же соответствует результату прим. 6.1.1.*

Стоит отметить, что точки лежащие на диагонали, например $j_1 = 6, j_2 = 6$ *не дадут корректного результата потому как* $НОД(6, 16) = 2 \neq 1$

Стоит отметить, что полученный результат (6.15) находится в прямом соответствии с леммой 5.3.2 для одномерного преобразования Фурье. При этом также имеет место и аналог комментария 5.3.1, который гласит, что в случае когда число отсчетов преобразования Фурье не равно q: $M \neq q$, но при этом $M \approx q$, мы можем все равно приближенно считать верным выражение (6.15) [6].

Пример 6.5.4. ($ind_2 14 \mod 59$)

В качестве примера рассмотрим $p = 59$ *при этом число отсчетов* $M = 64 \approx q = p - 1 = 58$. *Генератором группы* $\mathbb{F}_{59}$ *(см. разд. 8.2.3) является* $g = 2$, *т. е.* $\mathbb{F}_{59} = \langle 2 \rangle$. *Это значит, что уравнение* $2^x \equiv b \mod 59$ *будет иметь решение для любых* b, *в частности* $x = 19$ *является решением уравнения*

$$2^x \equiv 14 \mod 59.$$

Исследуемая функция имеет вид

$$f(x_1, x_2) = 14^{x_1} 2^{x_2} \mod 59,$$

Допустим, что $x_0 = 50$, *т.е. зарегистрировано значение функции* $f(x_1, x_2) = 2^{x_0} = 2^{50} \equiv 3 \mod 59$.

Как было указано выше, для числа отсчетов преобразования Фурье имеем $M = 64$. *Стоит отметить, что* $q = p - 1 = 58 \not\equiv 0 \mod 64$.

Фурье образ отсчетов функции

$$f'(x_1, x_2) = \begin{cases} 1, & \text{если } 14^{x_1} 2^{x_2} \equiv 3 \mod 59 \\ 0, & \text{если } 14^{x_1} 2^{x_2} \not\equiv 3 \mod 59 \end{cases}$$

изображен на рис. 6.4. Три нижних максимума имеют координаты

$$(j_1, j_2) \approx (20, 1), (41, 2.2), (62, 3),$$

что дает следующие оценки для x: $x \approx 20, 18.6, 20.6$, *что находится близко к реальному значению* $x = 19$.

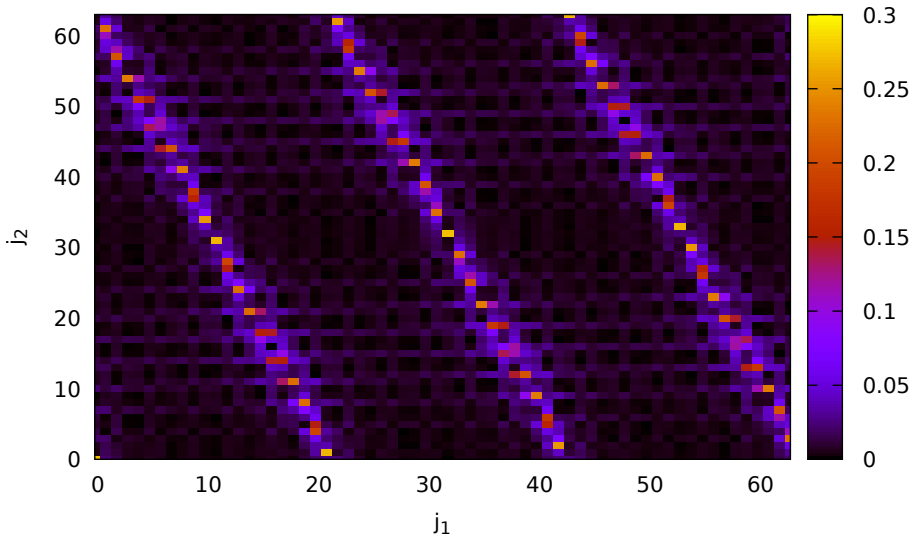


Рис. 6.4: Фурье образ отсчетов функции $f'(x_1, x_2)$ Число отсчетов $M = 64$. Три нижних максимума имеют координаты $\approx (20, 1), (41, 2.2), (62, 3)$, что дает следующие оценки для x: $x \approx 20, 18.6, 20.6$, что находится близко к реальному значению $x = 19$

Пример 6.5.5. ($ind_3 14 \mod 19$)

В качестве примера рассмотрим задачу определения x такого, что

$$3^x \equiv 14 \mod 19.$$

Исследуемая функция имеет вид

$$f(x_1, x_2) = 14^{x_1} 3^{x_2} \mod 19,$$

Допустим, что $x_0 = 1$, т.е. зарегистрировано значение функции $f(x_1, x_2) = 3$.

Число отсчетов преобразования Фурье возьмем $M = 64$. Стоит отметить, что $18 \not\equiv 0 \mod 64$.

Фурье образ отсчетов функции

$$f'(x_1, x_2) = \begin{cases} 1, & \text{если } 14^{x_1} 3^{x_2} \equiv 3 \mod 19 \\ 0, & \text{если } 14^{x_1} 3^{x_2} \not\equiv 3 \mod 19 \end{cases}$$

изображен на рис. 6.5. Самый нижний максимум имеет координаты $j_1 = 46, j_2 = 3.5$ откуда имеем для оценки

$$x \approx \frac{46}{3.5} \approx 13.14.$$

Стоит отметить что решение искомого уравнения $x = 13$ соответствует найденному приближенному решению.

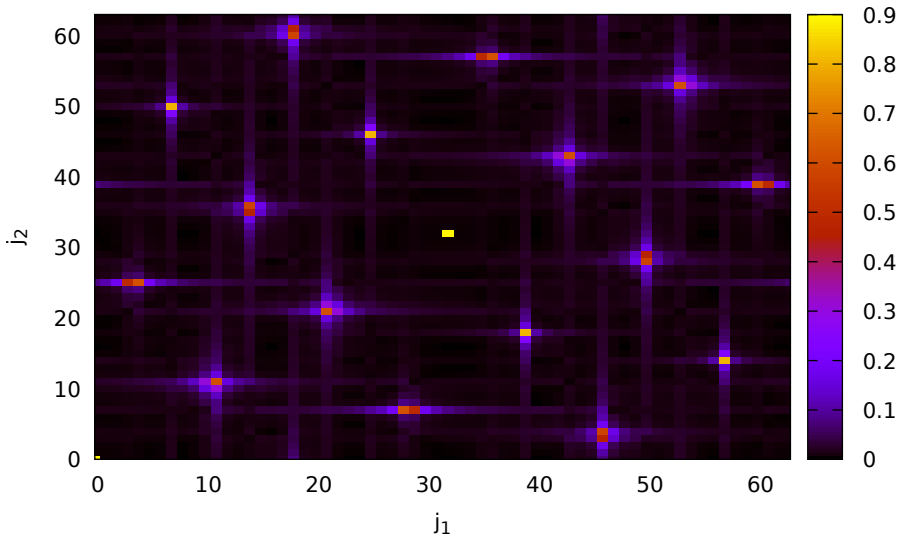


Рис. 6.5: Фурье образ отсчетов функции $f'(x_1, x_2)$ Число отсчетов $M = 64$. Координаты максимума $j_1 \approx 46$, $j_2 \approx 3.5$. Решением уравнения $3^x \equiv 14 \mod 19$ является $x = 13 \approx \frac{46}{3.5} \approx 13.14$

6.5.2 Двумерное квантовое преобразование Фурье

Для определения периодов функции двух аргументов можно воспользоваться двумерным преобразованием Фурье, которое может быть построено из блоков осуществляющих одномерное преобразование Фурье, как это изображено на рис. 6.6. Для анализа этой схемы рассмотрим тривиальный случай когда на входе имеем (см. также (5.16))

$$|x\rangle = |x\rangle_1 \otimes |x\rangle_2 ,$$
$$|x\rangle_{1,2} = \sum_{k_{1,2}=0}^{M-1} x_{k_{1,2}}^{(1,2)} |k_{1,2}\rangle .$$

С учетом того, что на выходе получается

$$\left|\tilde{X}\right\rangle = \left|\tilde{X}_1\right\rangle \otimes \left|\tilde{X}_2\right\rangle ,$$

где

$$\left|\tilde{X}_{1,2}\right\rangle = \sum_{j_{1,2}=0}^{M-1} \tilde{X}_{j_{1,2}}^{(1,2)} |j_{1,2}\rangle$$

и в соответствии с (5.18)

$$\tilde{X}_{j_{1,2}}^{(1,2)} = \frac{1}{\sqrt{M}} \sum_{k_{1,2}=0}^{M-1} e^{-i\omega_{1,2} k_{1,2} j_{1,2}} x_{k_{1,2}}^{(1,2)} .$$

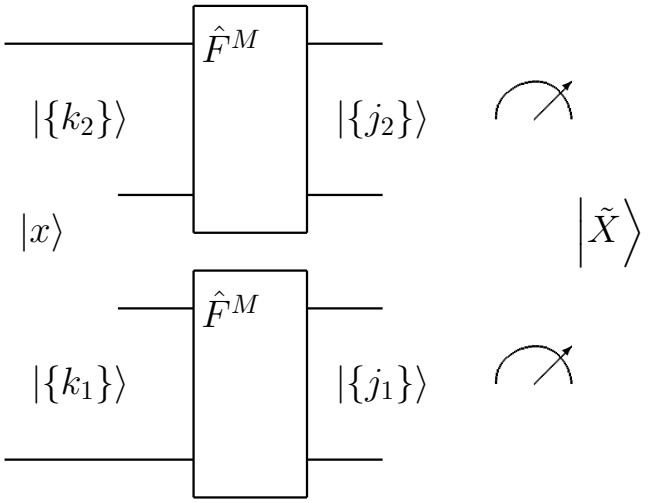


Рис. 6.6: Схема двумерного квантового преобразования Фурье. На входе имеем сигнал $|x\rangle = \sum_{k_1,k_2=0}^{M-1} x\left(k_1,k_2\right)|k\rangle_1 \otimes |k\rangle_2$. Сигнал на выходе $\left|\tilde{X}\right\rangle = \sum_{k_1,k_2=0}^{M-1} \tilde{X}\left(j_1,j_2\right)|j_1\rangle \otimes |j_2\rangle$ является двумерным преобразование Фурье от исходного $|x\rangle$

получим

$$\left|\tilde{X}\right\rangle = \left|\tilde{X}_1\right\rangle \otimes \left|\tilde{X}_2\right\rangle =$$
$$= \sum_{j_1=0}^{M-1}\sum_{j_2=0}^{M-1} \tilde{X}_{j_1}^{(1)}\tilde{X}_{j_2}^{(2)}|j_1\rangle \otimes |j_2\rangle =$$
$$= \sum_{j_1=0}^{M-1}\sum_{j_2=0}^{M-1} \tilde{X}_{j_1,j_2}|j_1\rangle \otimes |j_2\rangle ,$$

где

$$\tilde{X}_{j_1,j_2} = \frac{1}{\left(\sqrt{M}\right)^2}\sum_{k_1=0}^{M-1}\sum_{k_2=0}^{M-1} e^{-i\omega(k_1j_1+k_2j_2)}x_{k_1}^{(1)}x_{k_2}^{(2)} =$$
$$= \frac{1}{\left(\sqrt{M}\right)^2}\sum_{k_1=0}^{M-1}\sum_{k_2=0}^{M-1} e^{-i\omega(k_1j_1+k_2j_2)}x_{k_1,k_2}$$

что, в соответствии с определением 6.4.1, является двумерным преобразованием Фурье от исходного двумерного сигнала

$$|x\rangle = \sum_{k_1=0}^{M-1}\sum_{k_2=0}^{M-1} x_{k_1}^{(1)}x_{k_2}^{(2)}|k_1\rangle \otimes |k_2\rangle = \sum_{k_1=0}^{M-1}\sum_{k_2=0}^{M-1} x_{k_1,k_2}|k_1\rangle \otimes |k_2\rangle .$$

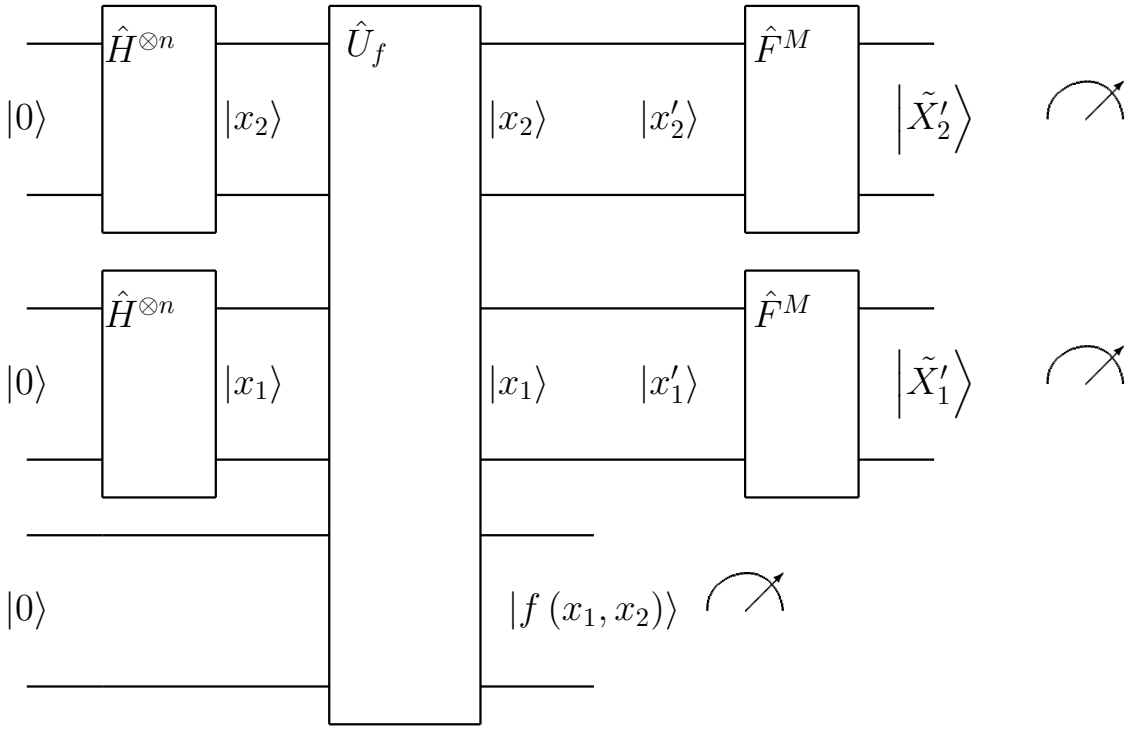


Рис. 6.7: Определение периода функций двух аргументов с помощью квантового преобразования Фурье

Следовательно используя схему, изображенную на рис. 6.7 можно определить координаты максимумов двумерного преобразования Фурье j_1, j_2 и в дальнейшем используя (6.15) определить искомое x.

Глава 7

Эллиптическая криптография

В настоящее время особенной популярностью пользуется особая разновидность дискретного логарифмирования которая называется криптографией на эллиптических кривых. Причиной этой популярности служит тот факт, что в данный момент не существует эффективных алгоритмов взлома криптографии на эллиптических кривых. Наиболее эффективный классических алгоритм ρ-метод Полларда имеет эффективность $O\left(\sqrt{N}\right)$ [5]. Это выгодно отличает данные криптографические алгоритмы от RSA и обычного дискретного логарифмирования, для которых существую достаточно эффективные классические алгоритмы взлома, что вынуждает использовать более длинные числовые последовательности для данных алгоритмов, например 4096 бит для RSA.

7.1 Эллиптическая криптография

7.1.1 Эллиптические кривые над полем $\mathbb{R}$

В эллиптической криптографии рассматривают определенные наборы объектов которые образуют группу (см. разд. 8.6). В качестве такого набора мы будем рассматривать точки принадлежащие некоторой кривой (см. рис. 7.1):

$$E : y^2 = x^3 + ax + b,$$

где коэффициенты a, b должны удовлетворять следующему соотношению

$$4a^3 + 27b^2 \neq 0,$$

в этом случае кубическое уравнение $x^3 + ax + b = 0$ будет иметь 3 различных действительных корня [11].

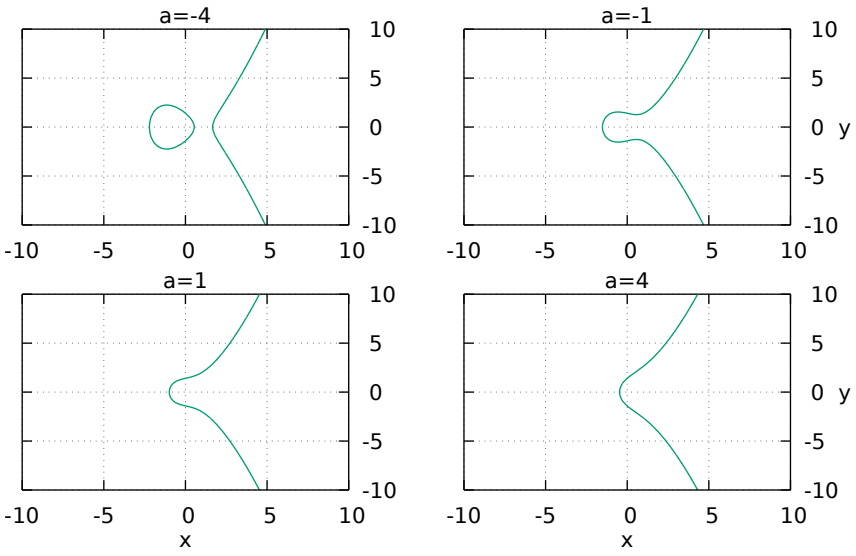


Рис. 7.1: Эллиптическая кривая $y^2 = x^3 + ax + 2$ над полем вещественных чисел $\mathbb{R}$ при различных значениях параметра a

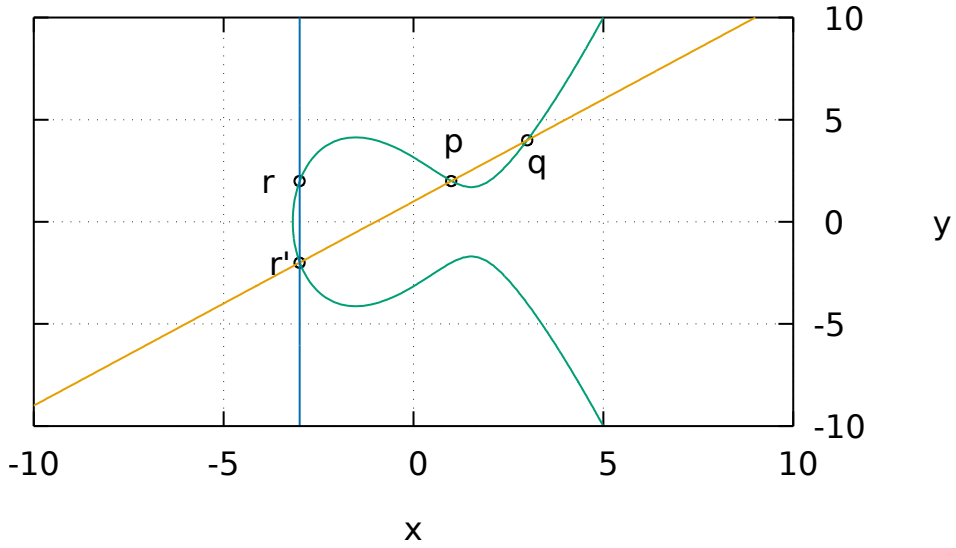


Рис. 7.2: Эллиптическая кривая $y^2 = x^3 - 7x + 10$ над полем вещественных чисел $\mathbb{R}$. Сложение двух точек $p(1, 2)$ и $q(3, 4)$. Прямая проходящая через эти точки пересекает кривую еще в третьей точке $r'(-3, -2)$. Симметричная r' относительно кривой точка $r(-3, 2)$ является суммой исходных двух: $p+q = r$

В соответствии с определением 8.6.1 для точек на кривой задана некоторая бинарная операция которая двум точкам p, q с координатами (p_x, p_y) и (q_x, q_y), соответственно, сопоставляет третью точку r с координатами (r_x, r_y), данную операцию мы будем называть сложением:

$$p + q = r.$$

Существует простая геометрическая интерпретация операции сложения (см. рис. 7.2). Допустим имеется 2 точки на кривой которые мы хотим сложить: p и q с координатами $(x_p, y_p), (x_q, y_q)$ соответственно. Если $x_p \neq x_q$, то через эти точки можно провести прямую, которая имеет наклон

$$m = \frac{y_p - y_q}{x_p - x_q}.$$

и пересекает кривую в точке r'. Если эта точка имеет координаты $(x_{r'}, y_{r'})$, то в силу того, что на лежит на прямой с наклоном m:

$$m = \frac{y_{r'} - y_p}{x_{r'} - x_p},$$

следовательно

$$y_{r'} = y_p + m\left(x_{r'} - x_p\right).$$

Эта точка должна принадлежать кривой, т.е.

$$y_{r'}^2 = \left(y_p + m\left(x_{r'} - x_p\right)\right)^2 = x_{r'}^3 + ax_{r'} + b$$

которое можно переписать

$$x_{r'}^3 - m^2 x_{r'}^2 + \cdots = 0.$$

Уравнение $x^3 - m^2x^2 + \cdots = 0$ имеет 3 корня: $x_p, x_q, x_{r'}$, т.е. его можно также переписать в виде

$$(x - x_{r'})(x - x_p)(x - x_q) = x^3 - (x_{r'} + x_p + x_q)x^2 + \cdots = 0.$$

Т.о.

$$x_{r'} + x_p + x_q = m^2.$$

Следовательно

$$\begin{aligned} x_{r'} &= m^2 - x_p - x_q, \\ y_{r'} &= y_p + m\left(x_{r'} - x_p\right), \end{aligned}$$

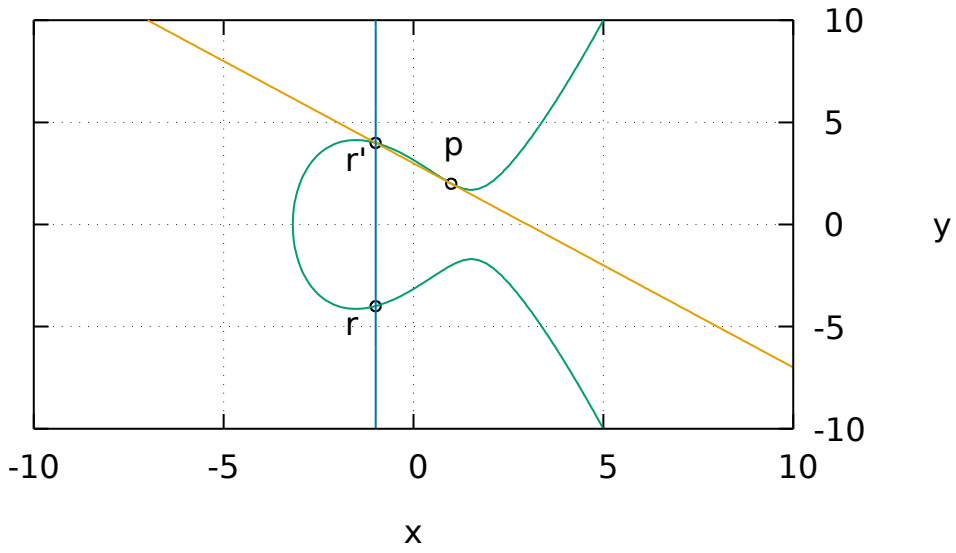


Рис. 7.3: Эллиптическая кривая $y^2 = x^3 - 7x + 10$ над полем вещественных чисел $\mathbb{R}$. Сложение двух точек с одинаковыми координатами $p(1, 2)$: $2p = r(-1, -4)$

Отразив эту точку относительно оси X мы получим финальную точку r которую будем называть суммой исходных точек (см. рис. 7.2). Координаты этой точки x_r, y_r могут быть получены по следующим формулам

$$\begin{aligned} x_r &= m^2 - x_p - x_q, \\ y_r &= -y_p + m\left(x_p - x_r\right). \end{aligned} \tag{7.1}$$

В случае $x_p = x_q$ возможны два варианта:

1. $y_p = y_q$ (см. рис. 7.3). В случае когда точки на кривой приближаются друг к другу, прямая линия, проведенная через них, стремиться к касательной. Коэффициент m может быть найден по следующей формуле: $m = \frac{dy}{dx}$. С учетом $2ydy = 3x^2dx + adx$ имеем $m = \frac{dy}{dx} = \frac{3x^2+a}{2y}$. дальнейший расчет ведется по формулам (7.1).

2. $y_p \neq y_q$ (см. рис. 7.4). В этом случае, в силу симметрии кривой относительно оси X возможен только один вариант: $y_p = y_q$ и кривая

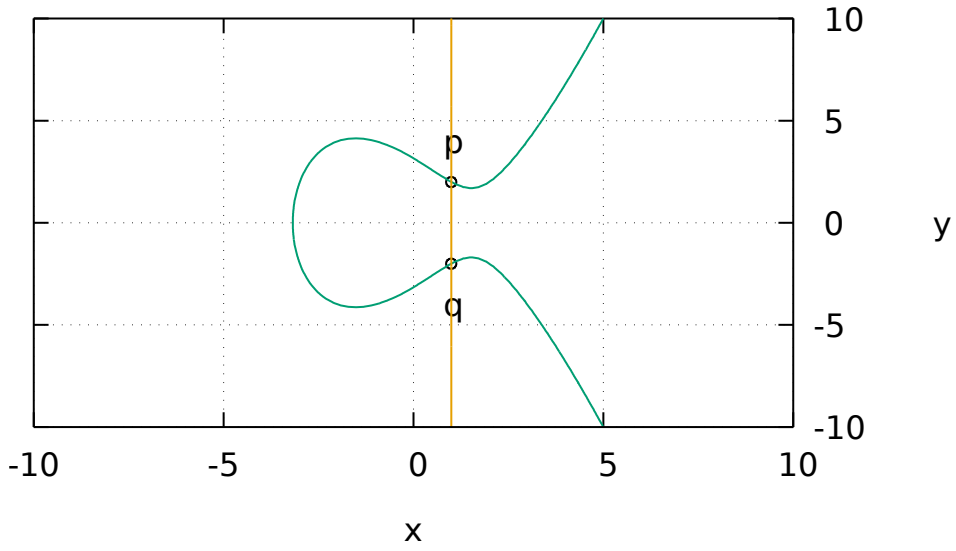


Рис. 7.4: Эллиптическая кривая $y^2 = x^3 - 7x + 10$ над полем вещественных чисел $\mathbb{R}$. Сложение двух точек $p(1, 2)$ и $q(1, -2)$. Прямая проходящая через эти точки не пересекает кривую. Результат сложения - нулевой элемент: $p + q = 0$, т.е. $q = -p$

проходящая через эти две точки не пересекает кривую в третьей точке. Для этого случая вводят еще одну точку 0 в которую уходит прямая линия проведенная через две точки. Таким образом, в этом случае мы имеем $p + q = 0, q = -p$.

Таким образом мы можем определить эллиптическую кривую над полем вещественных чисел $\mathbb{R}$ как следующее множество точек

$$E(\mathbb{R}) = \left\{(x, y) \in \mathbb{R} \times \mathbb{R} : y^2 = x^3 + ax + b, \right\} \cup \{0\}. \tag{7.2}$$

где $a, b \in \mathbb{R}$.

Для данных точек определена бинарная операция, которую мы назвали сложением. На множестве есть нулевой элемент, так же для каждого элемента можно определить обратный элемент. Можно доказать, что введенная операция является ассоциативной: $(a + b) + c = a + (b + c)$ [11]. Таким образом множество $E(\mathbb{R})$ образует группу относительно операции сложения. С учетом очевидного равенства $p + q = q + p$, данная группа будет являться коммутативной, т.е. Абелевой (см. определение 8.6.3).

Комментарий 7.1.1 (Об операции сложения)**.** *Введенная операция сложения для точек на эллиптической кривой выглядит на первый взгляд неестественно, почему бы не использовать более очевидные операции сложения точек на плоскости, например правила сложения векторов. В этом случае, если $p, q \in E(\mathbb{R})$, то вполне может быть что $p+q \notin E(\mathbb{R})$ и, следовательно, будет нарушено основное свойство группы - связанность (closure). Вместе с тем для определенной нами бинарной операции (7.1) справедливы все свойства групп, и соответственно, все вытекающие из этого свойства, такие например как теорема Лагранжа (см. теор. 8.6.2), которые могут быть применены к введенным нам объектам.*

7.1.2 Эллиптические кривые над полем $\mathbb{F}_p$

Множество (7.2) вместе с операцией сложения (7.1) может определено над произвольным полем (см. определение 8.7.1), т.е. не только над $\mathbb{R}$. С точки зрения криптографии особый интерес представляет поле $\mathbb{F}_p$ (см. разд. 8.2.3). Можно определить множество элементов эллиптической кривой над полем $\mathbb{F}_p$ аналогично выражению (8.2.3):

$$E(\mathbb{F}_p) = \left\{(x, y) \in \mathbb{F}_p \times \mathbb{F}_p : y^2 \equiv x^3 + ax + b, \right\} \cup \{0\}. \tag{7.3}$$

где $a, b \in \mathbb{F}_p$.

На рис. 7.5 изображено такое множество для поля $\mathbb{F}_{19}$, т.е. $p = 19$. Уравнение кривой $y^2 \equiv x^3 - 7x + 10 \mod 19$.

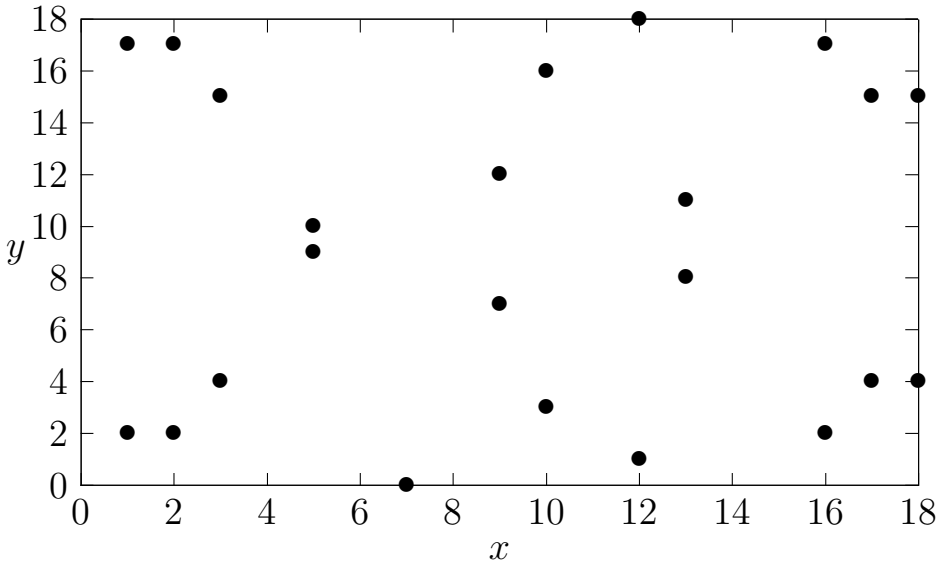


Рис. 7.5: Эллиптическая кривая $y^2 = x^3 - 7x + 10$ над полем $\mathbb{F}_{19}$

Для каждой точки a с координатами x_a, y_a определен обратный элемент $-a$ с координатами $x_{-a} = x_a, y_{-a} \equiv -y_a \mod p$.

Для точек на данной кривой задан следующий закон сложения $a + b = c, b \neq -a$

$$\begin{aligned} x_c &\equiv m^2 - x_a - x_b \mod p, \\ y_c &\equiv -y_a + m\left(x_a - x_c\right) \mod p, \end{aligned} \tag{7.4}$$

где $(x_{a,b,c}, y_{a,b,c})$ - координаты точек a, b и c соответственно. Для коэффициента m используются следующие соотношения:

$$\begin{aligned} m &= \left(y_a - y_b\right)\left(x_a - x_b\right)^{-1} \mod p, \text{ если } x_a \neq x_b \\ m &= \left(3x^2 + a\right)\left(2y\right)^{-1} \mod p, \text{ если } x_a = x_b. \end{aligned}$$

Очевидно что если $b = -a$, то $a + b = a + (-a) = 0$.

7.1.3 Скалярное умножение и дискретный логарифм

Допустим n некоторое натуральное число $n \in \mathbb{N}$ и $a \in E\left(\mathbb{F}_p\right)$. Определим скалярное произведение следующим образом

$$n \cdot a = a + a + \ldots a = \sum_{k=1}^{n} a$$

Наивная реализация требует $O\left(n\right)$ операций сложения, но с помощью парадигмы “разделяй и властвуй” (см. разд. 8.9) может быть сведено к $O\left(\log n\right)$ операций сложения.

Пример 7.1.1 (Скалярное произведение). *Рассмотрим эллиптическую кривую*

$$E\left(\mathbb{F}_{19}\right)=\{(x,y)\in\mathbb{F}_{19}\times\mathbb{F}_{19}:y^2\equiv x^3-7x+10\}\cup\{0\},$$

изображенную на рис. 7.5. Выберем в качестве точки $p=(13,8)$, *тогда*

$$\begin{aligned}
0\cdot p&=0,\\
1\cdot p=p&=(13,8),\\
2\cdot p=p+p&=(16,7),\\
3\cdot p=2\cdot p+p&=(18,5),\\
4\cdot p=3\cdot p+p&=(12,1),\\
5\cdot p=4\cdot p+p&=(5,10),\\
6\cdot p=5\cdot p+p&=(7,0),\\
7\cdot p=6\cdot p+p&=(5,9),\\
8\cdot p=7\cdot p+p&=(12,18),\\
9\cdot p=8\cdot p+p&=(18,4),\\
10\cdot p=9\cdot p+p&=(16,2),\\
11\cdot p=10\cdot p+p&=(13,11),\\
12\cdot p=11\cdot p+p&=0
\end{aligned}$$

Как видно из прим. 7.1.1 каждый элемент эллиптической кривой является генератором некоторой циклической подгруппы. Вместе с тем вся группа точек на эллиптической кривой не обязательно является циклической (TBD). С другой стороны для формирования задачи дискретного логарифма нам требуется именно циклическая группа. Таким образом для заданной эллиптической кривой вначале вычисляют ее порядок, для этого существует эффективный алгоритм Шуфа [7]. После этого находится простой делитель найденного порядка и ищется точка которая является генератором подгруппы выбранного порядка. Для того чтобы это сделать используется следующий факт. Для любой точки $g\in E$ имеет место соотношение

$$Ng=0,$$

где $N=|E|$ -порядок (число точек) эллиптической кривой. Допустим p - некоторый простой делитель числа N:

$$N=hp$$

тогда

$$Ng=p\left(hg\right)=0.$$

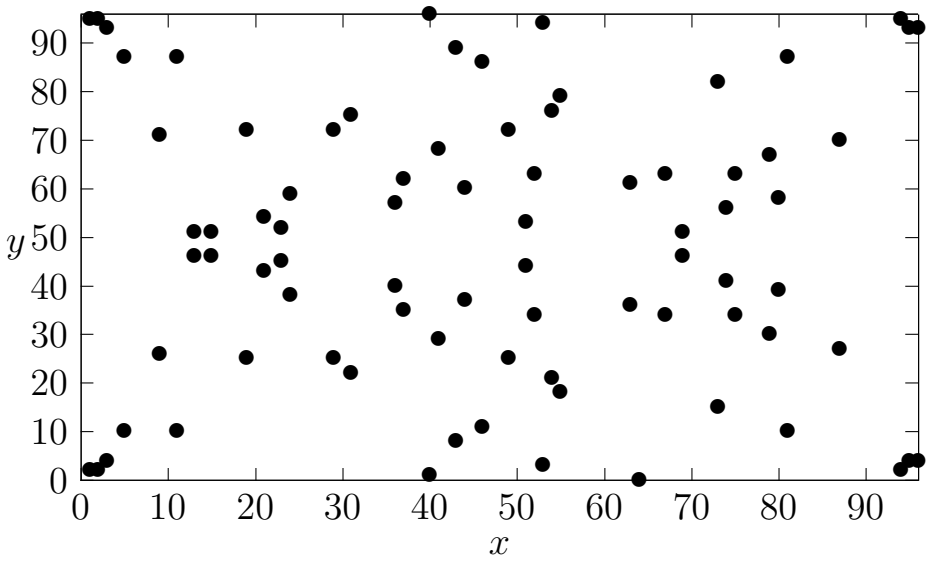


Рис. 7.6: Эллиптическая кривая $y^2 = x^3 - 7x + 10$ над полем $\mathbb{F}_{97}$

Т. о. если $hg \neq 0$, то точка $g' = hg$ будет генератором циклической подгруппы порядка p.

Комментарий 7.1.2. *Имеет смысл в качестве порядка подгруппы выбирать именно простое число, поскольку если порядок группы простой то по теореме Лагранжа (см. теор. 8.6.2) у нее есть только тривиальные подгруппы - сама группа и группа состоящая из единичного элемента. Т. о. в силу $hg \neq 0$ остается только сама группа, которая является циклической с порядком p.*

Пример 7.1.2 (Выбор базовой точки)**.** *Рассмотрим эллиптическую кривую*

$$E = E(\mathbb{F}_{97}) = \{(x, y) \in \mathbb{F}_{97} \times \mathbb{F}_{97} : y^2 \equiv x^3 - 7x + 10\} \cup \{0\},$$

изображенную на рис. 7.6. Порядок этой кривой:

$$N = |E| = 82.$$

Число 82 имеет 2 делителя: 41 и 2. Т. о. существует циклическая подгруппа порядка 41, т.е. $h = 2$.

Возьмем точку $g = (1, 2) \in E$ ее порядок: $|\langle g \rangle| = 82$, т.е. эта точка не подходит. Рассчитываем

$$g' = hg = 2g = (96, 93) \neq 0.$$

При этом $|\langle g' \rangle| = 41$, т.е. мы нашли требуемую базовую точку.

Если имеется две точки на кривой $a, b \in E(\mathbb{F}_p)$ то имеет смысл вопрос о существовании такого $x \in \mathbb{N}$:

$$x \cdot a = b$$

данная задача называется дискретным логарифмом на эллиптических кривых.

7.2 Алгоритм ECDH

Алгоритм ECDH является модификацией алгоритма Диффи-Хеллмана (см. разд. 6.2) для эллиптических кривых. Протокол Диффи-Хеллмана является протоколом обмена ключей. В нашем случае публикуются следующие параметры эллиптической кривой: (p, a, b, g, n, h), где p, a, b задают кривую

$$E(\mathbb{F}_p) = \{(x, y) : y^2 \equiv x^3 + ax + b \mod p\} \cup \{0\},$$

g - базовая точка порядка n: $|\langle g \rangle| = n$, h - кофактор группы $\langle g \rangle$, т.е. $|| = nh$.

Алиса выбирает закрытый ключ $d_a \in \{1, \ldots, n-1\}$ и формирует открытый ключ $A = d_a g$. Боб также формирует закрытый $d_b \in \{1, \ldots, n-1\}$ и открытый $B = d_b g$ ключи. Алиса и Боб обмениваются этими ключами. Далее каждый из них вычисляет реальный ключ по правилу $K = d_a B = d_b A$.

Пример 7.2.1 (Алгоритм ECDH). *Возьмем кривую и базовую точку из прим. 7.1.2. Т.о.*

$$(p, a, b, g, n, h) = (97, -7, 10, (96, 93), 41, 2)$$

Алиса выбирает $d_a = 5$, *т.е.* $A = (37, 35)$. *Боб выбирает* $d_b = 15$, *т.о.* $B = (15, 51)$. *Ключ у Алисы* $K = d_a B = (46, 11)$ *и ключ у Боба* $K = d_b A = (46, 11)$ *совпадают.*

7.3 Алгоритм Шора и дискретный логарифм на эллиптических кривых

Рассмотрим эллиптическую кривую

$$E(\mathbb{F}) = \{(x, y) \in \mathbb{F}_p \times \mathbb{F}_p, y^2 = x^3 + ax + b, \}$$

с заданной базовой точкой $g \in E(\mathbb{F}_p)$ такой что:

$$ng = 0.$$

Требуется решить следующую задачу: при заданном $q \in E(\mathbb{F}_p)$ найти такое x, что

$$xg = q \mod n \tag{7.5}$$

Рассмотрим следующую вспомогательную функцию

$$f(x_1, x_2) = x_1 q + x_2 g = (x x_1 + x_2) g, \tag{7.6}$$

где $q, g \in E(\mathbb{F}_p)$ и взяты из условий нашей задачи (7.5). Данная функция аналогична (6.8) использованной в решении задачи дискретного логарифма. Далее производится измерение этой функции. Результатом этого измерения является некоторая точка $c \in E(\mathbb{F}_p)$. Вместе с тем из (7.6) следует что $c \in \langle g \rangle$, т.е. $\exists x_0$ такая что $c = x_0 g$.

Т.о., по аналогии с (6.11), мы составляем следующую функцию

$$f'(x_1, x_2) = \begin{cases} 1, x x_1 + x_2 \equiv x_0 \mod n \\ 0, x x_1 + x_2 \not\equiv x_0 \mod n \end{cases} \tag{7.7}$$

Координаты (j_1, j_2) максимума Фурье образа $\tilde{f}'$ дают в соответствии с формулой (6.15) некоторое значение искомого числа x. В нашем случае практически всегда $n \neq M$ поэтому мы можем использовать только приближенную оценку

$$x \approx \frac{j_1}{j_2}.$$

Пример 7.3.1 (Дискретное логарифмирование на эллиптической кривой)**.** *Рассмотрим задачу из примера 7.2.1 Кривая и базовая точка (см. прим. 7.1.2) имеют вид*

$$(p, a, b, g, n, h) = (97, -7, 10, (96, 93), 41, 2)$$

Допустим, что нам известен публичный ключ Алисы

$$A = (37, 35)$$

и мы хотим найти такое $x \in \{0, 1, \ldots 40\}$ что $xg = A$, как это следует из примера 7.2.1 ответом является $x = d_a = 5$. Нашей исследуемой функцией будет являться

$$f(x_1, x_2) = x_1 A + x_2 g = x_1(37, 35) + x_2(96, 93)$$

В качестве результата измерения выберем $c = g$, т.е. $x_0 = 1$. График функции $f'(x_1, x_2)$, соответствующей этому измерению изображен на

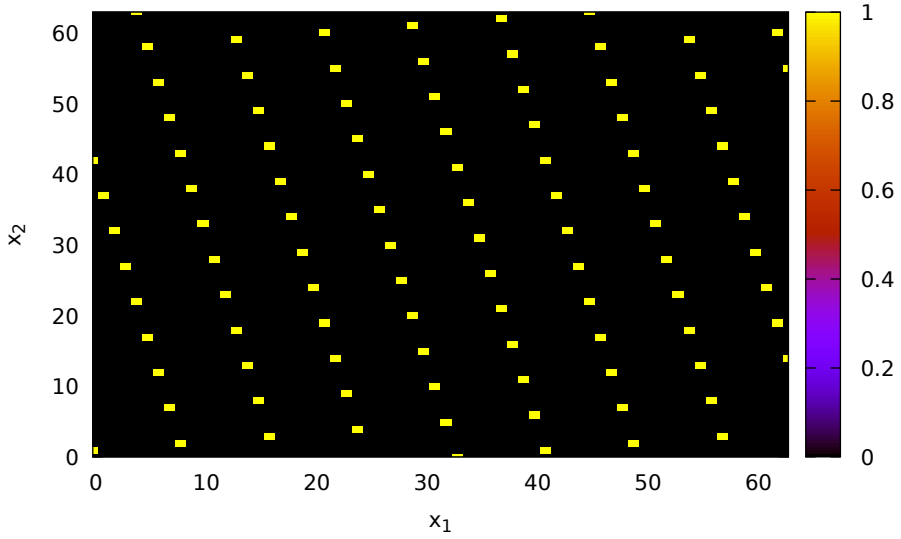


Рис. 7.7: График функции $f'(x_1, x_2)$ при $x_0 = 1$. Т.о. изображены точки x_1, x_2 соответствующие соотношению $x_1 A + x_2 g = g$: $x_1(37, 35) + x_2(96, 93) = (96, 93)$, например $7(37, 35)+7(96, 93) = (96, 93)$, $8(37, 35)+2(96, 93) = (96, 93)$ или $16(37, 35)+3(96, 93) = (96, 93)$. Стоит отметить, что выбранные пары точек соответствуют условию (7.7), действительно имеем $x \cdot 7 + 7 \equiv x \cdot 8 + 2 \mod 41$. То есть если вычесть одно из другого то получим уравнение вида $x\,(8 - 7) = -(2 - 7) = 5 \mod 41$. Или же $x \equiv 5 \mod 41$

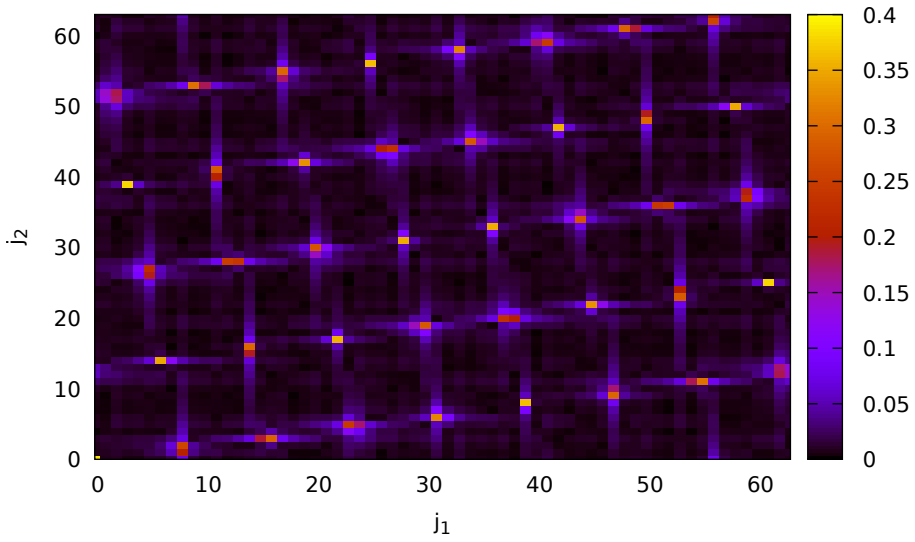


Рис. 7.8: Фурье образ отсчетов функции $f'(x_1, x_2)$ Число отсчетов $M = 64$. Три левых нижних максимума имеют координаты $\approx (8, 2), (15, 3), (24, 5)$, что дает следующие оценки для x: $x \approx 4, 5, 4.8$, что находится близко к реальному значению $x = 5$

рис. 7.7. Стоит отметить, что функция $f'(x_1, x_2)$ периодическая и если взять любые две близко стоявшие точки например $(8, 2)$ и $(16, 3)$ то можно заметить, что период по координате x_1 равен $T_1 = 8$, а по координате x_2 - $T_2 = 1$. Решая уравнение $x = T_2 T_1^{-1} \mod n$ получим $x = 8^{-1} \equiv 5 \mod 41$, что соответствует искомому решению.

Фурье образ функции $f'(x_1, x_2)$, изображен на рис. 7.8. Из него можно найти искомое $x = 5$.

Глава 8

Приложения

8.1 Наибольший общий делитель. Алгоритм Евклида

Определение 8.1.1. Наибольшим общим делителем чисел a и b ($\text{НОД}(a,b)$) называется максимальный из их общих делителей.

Теорема 8.1.1 (Теорема об общих делителях)**.** *Допустим, что выполняются следующие неравенства $a > b > 0$, а число r является остатком от деления a на b. Т. о. можно записать*

$$a = x \cdot b + r, \tag{8.1}$$

где $x \geq 1$, $b > r \geq 0$. Если $r = 0$, то b является максимальным числом на которое делятся без остатка и a и b. В случае, если $r > 0$, то

$$НОД(a,b) = НОД(b,r). \tag{8.2}$$

Доказательство. Для доказательства (8.2) покажем, что любой делитель пары чисел (a,b) является делителем пары чисел (b,r). Пусть d некоторый общий делитель чисел a и b, т. е. $a = d \cdot x_1$, $b = d \cdot x_2$. Т. о. из (8.1) следует

$$r = a - x \cdot b = d \cdot (x_1 - x \cdot x_2),$$

т. е. d является делителем числа r.

Теперь докажем, что любой общий делитель чисел b и r будет является общим делителем чисел a и b, действительно пусть d - общий делитель чисел b и r, т. е. $b = y_1 \cdot d$ и $r = y_2 \cdot d$, т. о. (8.1) переписывается в виде

$$a = x \cdot y_1 \cdot d + y_2 \cdot d = d \cdot (x \cdot y_1 + y_2),$$

т. е. d является делителем числа a.

Таким образом пары чисел (a, b) и (b, r) имеют общие делители, в том числе и максимальный делитель для одной пары будет являться таковым и для второй. □

Соотношение (8.2) приводит к следующему алгоритму вычисления наибольшего общего делителя

Алгоритм 3 Алгоритм Евклида

```
a > b
if b = 0 then
   return a
end if
a ⇐ 0
r ⇐ b
b ⇐ a
repeat
   a ⇐ b
   b ⇐ r
   r ⇐ остаток от деления a на b
until (r ≠ 0)
return b
```

Для оценки сложности алгоритма 3 запишем его в следующем виде

$$f_k = x_k \cdot f_{k+1} + f_{k+2},$$
$$f_0 = a,\ f_1 = b,$$
$$x_k \geq 1,\ f_k > f_{k+1} > f_{k+2},$$

т. о. $f_k > 2 \cdot f_{k+2}$, или же $f_0 > 2 \cdot f_2 > \cdots > 2^n f_{2n}$ т. е. алгоритм остановится при $n = log_2(f_0) = log_2(a)$ [1]. Число шагов алгоритма при этом очевидно равно $2n$ или же $2 \cdot log_2(a)$. Т. о. алгоритмическая сложность алгоритма Евклида может быть записана как $O(\log(a))$.

[1] Дальнейшие выкладки сделаны в предположении, что $log_2(a)$ - целое число

Пример 8.1.1. (НОД $(2345, 1456)$)

$$\begin{aligned} 2345 &= 1456 + 889, \\ 1456 &= 889 + 567, \\ 889 &= 567 + 322, \\ 567 &= 322 + 245, \\ 322 &= 245 + 77, \\ 245 &= 3 \cdot 77 + 14, \\ 77 &= 5 \cdot 14 + 7, \\ 14 &= 2 \cdot 7. \end{aligned}$$

т. о. НОД $(2345, 1456) = 7$. *Число шагов алгоритма* $8 < 2 \cdot log_2 2345 \approx 2 \cdot 11.2 = 22.4$.

8.1.1 Соотношение Безу

Теорема 8.1.2 (Безу)**.** *Если числа* a *и* b *взаимно просты, то уравнение*

$$ax + by = 1$$

имеет целочисленные решения.

Доказательство. Используем алгоритм Евклида 3 для нахождения НОД (a, b). Допустим $a > b$, тогда

$$\begin{aligned} r_1 &= a - bq_0, \\ r_2 = b - r_1 q_1 &= b - (a - bq_0)q_1 = b(1 + q_1 q_0) - aq_1, \\ r_3 = r_1 - r_2 q_2 &= a - bq_0 - (b(1 + q_1 q_0) - aq_1)\, q_2 = \\ &= a(1 + q_1 q_2) - b(q_0 + q_2 + q_0 q_1 q_2), \\ &\dots \\ \text{НОД}\,(a, b) = r_n = r_{n-2} - r_{n-1} q_{n-1} &= \dots = ax + by, \end{aligned} \tag{8.3}$$

что доказывает наше утверждение. □

Комментарий 8.1.1 (О сложности вычисления соотношения Безу)**.** *Вычисления по* (8.3) *эквивалентны шагам в алгоритме 3. Число этих шагов* $O(log_2(a)$*, таким образом алгоритм описанный уравнениями* (8.3) *достаточно эффективный и имеет сложность* $O(log_2(a)$.

Пример 8.1.2 (Соотношение Безу)**.** *Допустим* $a = 25, b = 14$*. Формулы алгоритма Евклида имеют вид*

$$\begin{aligned} 11 &= 25 - 14 \cdot 1, \\ 3 &= 14 - 11 \cdot 1, \\ 2 &= 11 - 3 \cdot 3, \\ 1 &= 3 - 2 \cdot 1. \end{aligned}$$

Из этих формул получаем

$$\begin{aligned} 11 &= 25 - 14 \cdot 1, \\ 3 &= 14 - 25 + 14 = 2 \cdot 14 - 25, \\ 2 = 11 - 3 \cdot 3 &= 25 - 14 - 3 \cdot (2 \cdot 14 - 25) = 4 \cdot 25 - 7 \cdot 14, \\ 1 &= 3 - 2 \cdot 1 = 9 \cdot 14 - 5 \cdot 25. \end{aligned}$$

Т. о.

$$25 \cdot (-5) + 14 \cdot 9 = 1.$$

8.2 Сравнение по модулю

Определение 8.2.1. Запись

$$a \equiv b \mod c \tag{8.4}$$

означает, что a и b имеют одинаковые остатки при делении на c или a и b сравнимы по модулю натурального числа c. При этом число c называется модулем сравнения.

Определение 8.4 может также трактоваться как то, что разность $a - b$ делится на c.

Пример 8.2.1. Сравнение по модулю $30 \equiv 8 \mod 11$*, потому что,* $30 = 2 \cdot 11 + 8$.

Определение 8.2.2 (Отрицательный элемент)**.** Если $a < n$, то $n - a$ будет называться отрицательным по отношению к a элементом и обозначаться $-a \mod n$.

Пример 8.2.2. Отрицательный элемент

$$-5 \equiv 6 \mod 11,$$

поскольку $5 < 11, 6 = 11 - 5$.

8.2.1 Арифметические операции

Лемма 8.2.1 (О сложении по модулю). *Если* $a_1 \equiv a_2 \mod n, b_1 \equiv b_2 \mod n$, *то*

$$a_1 + b_1 \equiv a_2 + b_2 \mod n$$

Доказательство. Можно записать $a_1 = k_1 n + r_a, a_2 = k_2 n + r_a, b_1 = l_1 n + r_b, b_2 = l_2 n + r_b$ откуда

$$a_1 + b_1 = (k_1 + l_1)n + r_a + r_b \equiv r_a + r_b \mod n$$

и

$$a_2 + b_2 = (k_2 + l_2)n + r_a + r_b \equiv r_a + r_b \mod n$$

откуда

$$a_1 + b_1 \equiv a_2 + b_2 \equiv r_a + r_b \mod n$$

□

Лемма 8.2.2 (Об умножении по модулю). *Если* a_1 *equiv*$a_2 \mod n, b_1 \equiv b_2 \mod n$, *то*

$$a_1 \cdot b_1 \equiv a_2 \cdot b_2 \mod n$$

Доказательство. Если $a_1 \equiv a_2 \mod n, b_1 \equiv b_2 \mod n$, то

$$a_1 + b_1 \equiv a_2 + b_2 \mod n$$

Можно записать $a_1 = k_1 n + r_a, a_2 = k_2 n + r_a, b_1 = l_1 n + r_b, b_2 = l_2 n + r_b$ откуда

$$a_1 \cdot b_1 = k_1 l_1 n + l_1 n r_a + k_1 n r_b + r_a r_b \equiv r_a r_b \mod n$$

и

$$a_2 \cdot b_2 = k_2 l_2 n + l_2 n r_a + k_2 n r_b + r_a r_b \equiv r_a r_b \mod n$$

откуда

$$a_1 \cdot b_1 \equiv a_2 \cdot b_2 \equiv r_a r_b \mod n$$

□

8.2.2 Решение уравнений

Очень часто в криптографии имеют дело с уравнениями вида

$$ax \equiv b \mod n, \tag{8.5}$$

где a, b, n известные целые числа, а x неизвестный параметр, подлежащий определению.

Очевидно, что если мы найдем такое целое число a^{-1}, что

$$aa^{-1} \equiv 1 \mod n,$$

то

$$x \equiv ba^{-1} \mod n.$$

Если НОД $(a, n) = 1$, то в соответствии с соотношением Безу (см. теорему Безу (Теорема 8.1.2)) $\exists x, y : ax + ny = 1$, т.е.

$$x \equiv a^{-1} \mod n.$$

При этом, в соответствии с комментарием 8.1.1, a^{-1}, и решение уравнения (8.5), может быть найдено достаточно эффективно.

8.2.3 Поле $\mathbb{F}_p$

Как мы видели в модульной арифметике можно складывать, вычитать, умножать и даже, если сравнение ведется по модулю простого числа, делить. При этом операции сложения и умножения коммутативны и удовлетворяют условию дистрибутивности. Таким образом остатки при делении образуют поле (см. определение 8.7.1) которое называется полем Галуа и обозначается через $\mathbb{F}_p$.

8.3 Функция Эйлера

8.3.1 Определение

Определение 8.3.1 (Функция Эйлера)**.** Функция Эйлера $\phi(n)$ показывает сколько чисел $k \in \{1, ...n-1\}$ взаимно просты с n, т.е. НОД $(k, n) = 1$.

Пример 8.3.1 (Функция Эйлера)**.** *Если взять число* $n = 15$ *то имеется 8 чисел взаимно простых с* 15*:* $1, 2, 4, 7, 8, 11, 13, 14$*. Оставшиеся 7 чисел не являются взаимно простыми с* n *поскольку имеют наибольший общий делитель отличный от 1, например НОД* $(6, 15) = 3$*. Таким образом,* $\phi(15) = 8$*.*

8.3.2 Свойства

Свойство 8.3.1 (Функция Эйлера простого числа)**.** *Если* p *- простое число, то* $\phi(p) = p - 1$

Доказательство. Следует из определения 8.3.1. □

Свойство 8.3.2 (Функция Эйлера произведения (обобщенная мультипликативность)). *Если* $НОД(n, m) = 1$, *то* $\phi(n \cdot m) = \phi(n)\phi(m)$

Доказательство. TBD □

Комментарий 8.3.1 (О сложности вычисления функции Эйлера). *Вычисление функции Эйлера больших чисел является очень сложной задачей. Чаще всего для вычисления используется свойство 8.3.1 в комбинации с 8.3.2. Применений этих свойств для произвольного числа требует его факторизации, поэтому сложность вычисления функции Эйлера сравнима со сложностью задачи факторизации.*

8.4 Малая теорема Ферма

Теорема 8.4.1 (Малая теорема Ферма). *Если* p *простое число, и* a *не делится на* p, *то*

$$a^{p-1} \equiv 1 \mod p \tag{8.6}$$

Доказательство. Рассмотрим следующее соотношение

$$a \cdot k_i \mod p,$$

где $k_i \subset \{1, \ldots, p-1\}$.

Очевидно, что

$$a \cdot k_i \equiv k_j \mod p. \tag{8.7}$$

Действительно

$$a \cdot k_i \mod p \subset \{1, \ldots, p-1\},$$

т. к. любой остаток от деления на p принимает значения $0, 1, \ldots p-1$. Нулевой остаток невозможен т. к. a и p взаимно просты.

Кроме этого каждый из остатков $a \cdot k_i \mod p$ встречается только один раз, действительно допустим что $a \cdot k_i \mod p = a \cdot k_j \mod p$ или же $a \cdot (k_i - k_j) \equiv 0 \mod p$, т. е. a делится на p, что противоречит условию взаимной простоты.

Перемножив все выражения выр. 8.7 получим

$$a \cdot 2a \cdot 3a \cdot \cdots \cdot a(p-1) \equiv 1 \cdot 2 \cdot 3 \cdot \cdots \cdot (p-1) \mod p.$$

или же

$$a^{p-1}(p-1)! \equiv (p-1)! \mod p,$$

откуда получаем требуемое равенство в силу взаимной простоты p и $(p-1)!$:

$$a^{p-1} \equiv 1 \mod p$$

□

8.4.1 Псевдопростые числа

Обобщение малой теоремы Ферма не верно, т. е. если a и p взаимно простые числа которые удовлетворяют соотношению выр. 8.6 то p может быть не простым. Например

$$2^{341-1} \equiv 1 \mod 341,$$

при том, что $341 = 11 \cdot 31$.

Числа p удовлетворяющие соотношению выр. 8.6, но при этом не являющиеся простыми называется псевдопростыми числами по основанию a. Например 341 - первое псевдопростое число по основанию 2.

8.5 Китайская теорема об остатках

Теорема 8.5.1. *Если имеются взаимно простые целые числа $n_1, n_2, \ldots, n_k$, тогда для любого набора целых чисел $a_1, a_2, \ldots a_k$ $\exists x$ такой что*

$$\begin{aligned} x &\equiv a_1 \mod n_1, \\ x &\equiv a_2 \mod n_2, \\ &\vdots \\ x &\equiv a_k \mod n_k, \end{aligned} \tag{8.8}$$

При этом для любых x_1, x_2 удовлетворяющих этому соостношению имеет место равенство

$$x_1 \equiv x_2 \mod N,$$

где $N = n_1 \cdot n_2 \cdot \cdots \cdot n_k$.

8.6 Введение в теорию групп

Определение 8.6.1. Группой $(\mathcal{G}, \circ)$ называется множество элементов $g \in \mathcal{G}$ для которого определена некоторая бинарная операция $\circ$ (часто ее называют умножением, либо сложением):

$$\begin{aligned} &\forall g_1, g_2 \in \mathcal{G}, \\ &g_1 \circ g_2 \in \mathcal{G}. \end{aligned} \tag{8.9}$$

Операция определенная посредством (8.9) обладает свойством ассоциативности:

$$g_1 \circ (g_2 \circ g_3) = (g_1 \circ g_2) \circ g_3.$$

Рассматриваемое множество должно содержать элемент $e_{\mathcal{G}}$ обладающий следующим свойством, справедливым для любого элемента множества g:

$$g \circ e_{\mathcal{G}} = e_{\mathcal{G}} \circ g = g.$$

Для каждого элемента группы g должен существовать обратный элемент $g^{-1} \in \mathcal{G}$, обладающий следующим свойством

$$g \circ g^{-1} = g^{-1} \circ g = e_{\mathcal{G}}$$

Определение 8.6.2 (Моноид)**.** Если для некоторого множества элементов $\mathcal{G}$ у нас не выполнено последнее свойств группы (существование обратного элемента), то данное множество называется моноидом (monoid) или полугруппой.

Определение 8.6.3 (Абелева группа)**.** Группа $(\mathcal{A}, \circ)$ называется абелевой, или коммутирующей если $\forall a_1, a_2 \in \mathcal{A}$: $a_1 \circ a_2 = a_2 \circ a_1$.

Пример 8.6.1. Группа $(\mathbb{Z}, +)$ *Множество целых чисел* $\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}$ *представляет собой группу относительно операции сложения.*

Определение 8.6.4 (Циклическая группа)**.** Циклическая группа G - это группа которая порождена единственным элементом $g : G =< g >$, т.е. все ее элементы являются степенями g. Элемент g называется порождающим элементом, или генератором, группы G.

Определение 8.6.5 (Мультипликативная группа кольца вычетов)**.** Рассмотрим набор целых чисел взаимно простых с n и меньших n, который обозначим через $(\mathbb{Z}/n\mathbb{Z})^{\times}$. В качестве операции умножения двух элементов $a, b \in (\mathbb{Z}/n\mathbb{Z})^{\times}$ примем

$$a \circ b = a \cdot b \mod n.$$

Единичным элементом $e_{(\mathbb{Z}/n\mathbb{Z})^{\times}}$ является 1. Кроме того можно показать, что для каждого $a \in (\mathbb{Z}/n\mathbb{Z})^{\times}$ существует $a^{-1} \in (\mathbb{Z}/n\mathbb{Z})^{\times}$ такой что $a \circ a^{-1} = 1$. Таким образом $(\mathbb{Z}/n\mathbb{Z})^{\times}$ является группой.

Теорема 8.6.1 (О порядке $(\mathbb{Z}/n\mathbb{Z})^{\times}$)**.** *Порядок группы* $(\mathbb{Z}/n\mathbb{Z})^{\times}$ *определяется следующим соотношением*

$$\left|(\mathbb{Z}/n\mathbb{Z})^{\times}\right| = \phi(n),$$

где $\phi(n)$ *- функция Эйлера* (8.3.1) *. При этом если* $n = p$ *- простое число, то*

$$\left|(\mathbb{Z}/p\mathbb{Z})^{\times}\right| = \phi(p),$$

и если $a \in (\mathbb{Z}/p\mathbb{Z})^{\times}, a \neq 1$*, то* a *- генератор рассматриваемой группы, т.е.*

$$a^{p-1} = 1.$$

Доказательство. TBD □

Теорема 8.6.2 (Лагранж)**.** *Для любой конечной группы $\mathcal{G}$ порядок (число элементов) любой подгруппы $\mathcal{H}$ делит порядок $\mathcal{G}$:*

$$|\mathcal{G}| = h\,|\mathcal{H}|\,,$$

где целое число h называется кофактором подгруппы.

8.7 Поля

Определение 8.7.1 (Поле (алгебра))**.** Пусть задана Абелева группа (см. определение 8.6.3) $(\mathcal{F}, +)$. Единичный элемент этой группы $e_{\mathcal{F}}$ - 0. Пусть также $(\mathcal{F} \setminus \{0\}, \cdot)$ - некоторая другая группа (не обязательно Абелева) с единичным элементом 1. Кроме того операции $+, \cdot$ удовлетворяют свойству дистрибутивности, т.е. $\forall a, b, c \in \mathcal{F}$:

$$c \cdot (a + b) = c \cdot a + c \cdot b,$$
$$(a + b) \cdot c = a \cdot c + b \cdot c.$$

В этом случае $(\mathcal{F}, +, \cdot)$ называется полем.

Пример 8.7.1 (Поле $\mathbb{Q}$)**.** *Заметим, что $\mathbb{Z}$ не является полем, поскольку не для любого целого определен обратный элемент относительно операции умножения. Вместе с тем следующее множество будет полем: $\mathbb{Q} = \{a/b \mid a \in \mathbb{Z}, b \in \mathbb{Z} \setminus \{0\}\}$. При этом обратный по отношению к $a/b \in (\mathbb{Q} \setminus \{0\}, \cdot)$ будет b/a.*

Пример 8.7.2 (Поле $\mathbb{R}$)**.** *Вещественные числа образуют поле.*

Пример 8.7.3 (Поле $\mathbb{C}$)**.** *Комплексные числа образуют поле.*

8.8 Основная теорема о рекуррентных соотношениях

Теорема 8.8.1 (Основная теорема о рекуррентных соотношениях)**.** *Если имеется следующее рекурентное соотоношение для сложности некоторого алгоритма*

$$T(n) = aT\left(\frac{n}{b}\right) + f(n)\,,$$

то возможно определить асимптотическое поведение функции $T(n)$ в следующих случаях

1. *Если* $f(n) = O\left(n^{log_b a - \epsilon}\right)$, *при некоторых* $\epsilon > 0$, *то* $T(n) = \Theta\left(n^{log_b a}\right)$
2. *Если* $f(n) = \Theta\left(n^{log_b a} log^k n\right)$, *то* $T(n) = \Theta\left(n^{log_b a} log^{k+1} n\right)$
3. *Если* $f(n) = \Omega\left(n^{log_b a + \epsilon}\right)$, *при некоторых* $\epsilon > 0$ *и* $af\left(\frac{n}{b}\right) \leq cf(n)$ *для некоторой константы* $c < 1$ *и больших* n, *то* $T(n) = \Theta(f(n))$

8.9 Разделяй и властвуй

"Разделяй и властвуй" (divide and conquer) - важная парадигма в решении алгоритмических задач, которая заключается в разделении исходной задачи на более простые.

Предметный указатель

Литература

[1] Gordon, D. M. Discrete logarithms in gf(p) using the number field sieve / Daniel M. Gordon // SIAM J. Discrete Math. — 1993. — Vol. 6. — P. 124–138.

[2] Grover, L. K. A fast quantum mechanical algorithm for database search / Lov K. Grover // ANNUAL ACM SYMPOSIUM ON THEORY OF COMPUTING. — ACM, 1996. — P. 212–219.

[3] Ivan Murashko. Analyze of quantum fourier transform circuit implementation / Ivan Murashko, Constantine Korikov // Internet of Things, Smart Spaces, and Next Generation Networks and Systems - 15th International Conference, NEW2AN 2015, and 8th Conference, ruSMART 2015, St. Petersburg, Russia, August 26-28, 2015, Proceedings / Ed. by Sergey Balandin, Sergey D. Andreev, Yevgeni Koucheryavy. — Springer, 2015. — Vol. 9247 of Lecture Notes in Computer Science. — http://dx.doi.org/10.1007/978-3-319-23126-6.

[4] Nielsen, M. Quantum Computation and Quantum Information / M.A. Nielsen, I.L. Chuang. Cambridge Series on Information and the Natural Sciences. — Cambridge University Press, 2000. — http://books.google.ru/books?id=65FqEKQOfP8C.

[5] Pollard, J. M. Monte carlo method for index computation (mod p) / J. M. Pollard // Mathematics of Computation. — 1978. — Jul. — Vol. 32, no. 143. — P. 918–924. — http://levicivita.uniroma2.it/~eal/montecarlo.pdf.

[6] Proos, J. Shor's discrete logarithm quantum algorithm for elliptic curves / John Proos, Christof Zalka // Quantum Info. Comput. — 2003. — Jul. — Vol. 3, no. 4. — P. 317–344. — https://arxiv.org/abs/quant-ph/0301141.

[7] Schoof, R. J. Elliptic curves over finite fields and the computation of square roots mod p / René J. Schoof // Mathematics of Computation. — 1985. — Vol. 44. — P. 483–494. — URL: http://cr.yp.to/bib/entries.html#1985/schoof.

[8] Shannon, C. E. Communication Theory of Secrecy Systems / Claude E. Shannon // Bell Systems Technical Journal. — 1949. — Vol. 28. — P. 656–715.

[9] Shor, P. W. Algorithms for quantum computation: Discrete logarithms and factoring / Peter W. Shor // FOCS. — IEEE Computer Society, 1994. — P. 124–134.

[10] Strengths and weaknesses of quantum computing / Charles H. Bennett, Ethan Bernstein, Gilles Brassard, Umesh Vazirani // SIAM J. Comput. — 1997. — oct. — Vol. 26, no. 5. — P. 1510–1523. — http://dx.doi.org/10.1137/S0097539796300933.

[11] Washington, L. C. Elliptic Curves: Number Theory and Cryptography, Second Edition / Lawrence C. Washington. — 2 edition. — Chapman & Hall/CRC, 2008.

[12] Wikipedia. Дискретное логарифмирование — Wikipedia, The free encyclopedia. — http://ru.wikipedia.org/wiki/Дискретное_логарифмирование. — 2013. — [Online; accessed 29-October-2013].

[13] Zurek, W. H. Decoherence and the transition from quantum to classical—revisited / W. H. Zurek // Los Alamos Science. — 2002. — no. 27. — P. 2–25. — http://vvkuz.ru/books/zurek.pdf.

[14] В. А. Ильин. Линейная алгебра / В. А. Ильин, Э. Г. Поздняк. — 6 изд. — Москва: Физматлит, 2005. — С. 115.

[15] Михаил Борисович Менский. Квантовые измерения и декогеренция. Модели и феноменология / Михаил Борисович Менский. — Москва: Физматлит, 2001. — С. 228.

[16] Поль Дирак. Принципы квантовой механики / Поль Дирак. — Москва: Наука, 1979.

[17] Физика квантовой информации / Под ред. А. Цайлингера. — Москва: Постмаркет, 2002. — С. 376.