МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ
НОВОСИБИРСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ФАКУЛЬТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Ф. И. Соловьева, А. В. Лось, И. Ю. Могильных

СБОРНИК ЗАДАЧ ПО ТЕОРИИ КОДИРОВАНИЯ, КРИПТОЛОГИИ И СЖАТИЮ ДАННЫХ

Учебное пособие

Новосибирск
2013

УДК 519.725(075)
ББК з-811.4 я 73-1
С 603

Соловьева Ф. И., Лось А. В., Могильных И. Ю. Сборник задач по теории кодирования, криптологии и сжатию данных: Учебное пособие / Новосиб. гос. ун-т. Новосибирск, 2013. 100 с.

ISBN 978-5-4437-0184-4

В издании систематически изложены задачи и упражнения по всем разделам теории информации: по теории кодирования, криптологии и сжатию данных. Настоящая разработка отражает и дополняет содержание серий курсов лекций, читаемых авторами в качестве основных и специальных курсов на факультете информационных технологий и механико-математическом факультете Новосибирского государственного университета. В учебном пособии методически продуманы все разделы, информация по изучению предмета подается от простого к сложному: приведены как задачи и упражнения, предназначенные для первоначального ознакомления с предметами теория кодирования, криптология и сжатие данных, так и задачи для углубленного изучения теории информации. Во многих разделах также приведены нерешенные проблемы, исследование которых позволит студентам начать специализацию и изучение соответствующих направлений передовой современной науки теория информации. Предназначено для студентов названных выше факультетов Новосибирского государственного университета, а также может быть полезно студентам других высших учебных заведений России.

Данное издание подготовлено в рамках реализации Мероприятия 1 Программы развития НИУ-НГУ на 2009–2018 годы, нацеленного на совершенствование образовательных технологий, связанных с такими тематиками, как «Технологии обработки, хранения, передачи и защиты информации; Дискретная и вычислительная математика; Технологии распределенных и высокопроизводительных вычислений и систем» направления «Математика, фундаментальные основы информатики и информационные технологии».

ISBN 978-5-4437-0184-4

Оглавление

Введение

«Сборник задач по теории кодирования, криптологии и сжатию данных» является новым задачником. Задачи, включенные в него, сколлекционированы в течение многих лет преподавания этих предметов в Новосибирском государственном университете. Следует заметить, что на сегодняшний день нет подобных современных источников по теории информации, у него отсутствуют аналоги как для студентов НГУ, так и для студентов других вузов страны. Основная цель этого учебника — способствовать усвоению как лекционного материала, так и упражнений и задач, рассматриваемых на семинарских занятиях по предметам «Введение в теорию кодирования» (ФИТ НГУ), «Теория помехоустойчивого кодирования», «Математические методы защиты информации», «Коды и схемы» (ММФ НГУ). Настоящий задачник послужит хорошим подспорьем и дополнением студентам к учебному пособию Ф. И. Соловьевой «Введение в теорию кодирования», переизданному в НГУ в 2011 г. Данный учебник будет способствовать выполнению поставленной в Программе развития НГУ задачи на совершенствование образовательных технологий, связанных с такими тематиками, как «технологии обработки, хранения, передачи и защиты информации» и «дискретная и вычислительная математика».

Сборник задач состоит из трех глав — теории кодирования, криптологии и сжатия данных, которые расположены именно в такой последовательности. В первой главе, посвященной теории кодирования, представлены задачи по многим разделам классической теории кодов, корректирующих ошибки в каналах связи с шумами. Основным теоретическим руководством по первой главе является учебное пособие Ф. И. Соловьевой «Введение в теорию кодирования». Во второй главе рассмотрены задачи, связанные с основными методами шифрования сообщений за исключением задач из популярного раздела о криптосистемах с секретными ключами, который широко доступен в открытой литературе. И, наконец, в третьей главе предложены задачи, связанные со свойствами энтропийной функции, задачи по алфавитному кодированию, оптимальным кодам и адаптивным методам кодирования.

Для упражнений, помеченных значком «^{0}», достаточно начального уровня знаний, необходимо знать только определения. Задачи, помеченные значком «*», требуют достаточно глубоких размышлений и знания университетских курсов алгебры, теории чисел, дискретной математики (раздел комбинаторика), теории вероятностей. В каждом разделе кратко изложены основные определения, свойства и теоремы, необходимые для решения задач и упражнений. Для удобства пользования задачником список литературы разделен на три части согласно имеющимся трем главам. Все решения, ответы и указания к задачам расположены в конце сборника задач в порядке следования соответствующих глав и разделов.

Глава I

Теория кодирования

1. Булев куб. Расстояние Хэмминга

• Векторное пространство всех векторов $x = (x_1, \ldots, x_n)$ длины n над конечным полем $GF(q)$ обозначается E_q^n. В двоичном случае q будем опускать.
• *Расстояние Хэмминга* $d(x, y)$ определяется как число координат, в которых различаются векторы x и y. В двоичном случае $d(x, y) = \sum\limits_{i=1}^{n} x_i \oplus y_i$, для любых $x, y \in E^n$ (далее знак $\oplus$ опускаем, так как из контекста всегда будет ясно, о каком сложении идет речь).
• *Вес Хэмминга* $w(x)$, $x \in E_q^n$, по определению равен числу ненулевых координат вектора x. В двоичном случае $w(x) = \sum\limits_{i=1}^{n} x_i$, для любого $x \in E^n$.

1.1. Доказать, что:

a) $x + E^n = E^n$ для любого $x \in E^n$;

b) $\pi(E^n) = E^n$ для любого $\pi \in S_n$.

• Говорят, что вектор y *предшествует* вектору x (обозначается $y \preceq x$), если множество номеров единичных координат вектора y содержится в множестве номеров единичных координат вектора x.
• *Произведение двух векторов* x и y над любым полем определяется как вектор $x * y = (x_1 y_1, \ldots, x_n y_n)$.

1.2. Доказать, что для любых векторов $x, y \in E^n$ справедливо:

a) $d(x, y) = w(x + y)$;

b) $w(x + y) = w(x) + w(y) - 2w(x * y)$;

c) $w(x + y) \geq w(x) - w(y)$, причем равенство достигается тогда и только тогда, когда выполняется $y \preceq x$;

d) Доказать, что $d(x, z) = d(x + y, z + y)$ для любых $x, y, z \in E^n$.

1.3. Доказать, что расстояние Хэмминга является метрикой, а E^n — метрическим пространством:

a) $d(x, y) \geq 0$, причем $d(x, y) = 0 \Leftrightarrow x = y$ (аксиома тождества);

b) $d(x, y) = d(y, x)$ (аксиома симметрии);

c) $d(x, y) + d(y, z) \geq d(x, z)$ (аксиома треугольника) для любых $x, y, z \in E^n$.

1.4. Доказать, что расстояние Хэмминга является метрикой, а E_q^n — метрическим пространством.

1.5. Доказать, что для любых векторов $x, y \in E_3^n$ справедливо $w(x+y) = w(x) + w(y) - f(x*y)$, где $f(x*y) = a + 2b$, если вектор $x*y$ содержит a единиц и b двоек.

1.6. Найти число векторов в пространстве E_q^n для любого $q \geq 2$.

1.7. Найти число неупорядоченных пар соседних векторов:

a) в пространстве E^n (пар векторов на расстоянии 1 по Хэммингу);

b) в пространстве E_q^n.

1.8. Найти число векторов:

a) в сфере радиуса r в пространстве E^n, в пространстве E_q^n;

b) в шаре радиуса r в пространстве E^n, в пространстве E_q^n.

1.9. Найти:

a) число неупорядоченных пар векторов x, y в пространстве E^n таких, что $d(x,y) = k$;

b) аналогично для пространства E_q^n.

1.10. Пусть $x, y \in E^n$, $d(x,y) = m$. Найти число векторов z, удовлетворяющих условию:

a) $d(x,z) + d(z,y) = d(x,y)$;

b) $d(x,z) = k$, $d(y,z) = r$;

c) $d(x,z) \leq k$, $d(y,z) = r$;

d) $d(x,z) \leq k$, $d(y,z) \geq r$.

1.11. Показать, что всякое подмножество пространства E^n, содержащее не менее $n+2$ векторов, содержит пару несравнимых векторов ($n \geq 2$).

1.12.* Показать, что мощность любого подмножества попарно несравнимых векторов пространства E^n не превосходит $C_n^{\lfloor n/2 \rfloor}$.

1.13. Найти число различных баз:

a) в пространстве E^n;

b) в пространстве E_q^n.

• Отображение I из пространства E_q^n в себя называется *изометрией*, если

$$d(x,y) = d(I(x), I(y))$$

для любых $x, y \in E_q^n$.

• Группа *автоморфизмов* пространства E_q^n определяется как группа его изометрий.

Известно, что любой автоморфизм пространства $E_q^n, q \geq 2$, может быть описан преобразованиями вида $(\pi, \tau_1, \tau_2, \ldots, \tau_n)$, где π — подстановка из S_n (симметрической группы подстановок длины n) на множестве координатных позиций, $\tau_1, \ldots, \tau_n$ — n подстановок из S_q на q элементах поля $GF(q)$, действующих на $x \in E_q^n$ следующим образом:

$$(\pi, \tau_1, \tau_2, \ldots, \tau_n)(x) = (\tau_1(x_\pi(1)), \ldots, \tau_n(x_\pi(n)).$$

Таким образом,

$$\mathrm{Aut}(E_q^n) = \{(\pi, \tau_1, \tau_2, \ldots, \tau_n) : \pi \in S_n, \tau_i \in S_q, i = 1, 2, \ldots, n\}.$$

Отметим, что в двоичном случае группу автоморфизмов можно представить с помощью подстановки π на множестве координат и сдвигом на некоторый вектор $v \in E^n$, т. е.

$$\mathrm{Aut}(E^n) = E^n \leftthreetimes S_n = \{(\pi, v) \mid \pi(E^n) + v = E^n, v \in E^n, \pi \in S_n\},$$

где $\leftthreetimes$ — полупрямое произведение.

• *Группой симметрий* $\mathrm{Sym}(E_q^n)$ пространства E_q^n, $q \geq 2$, называется множество

$$\mathrm{Sym}(E_q^n) = \{\pi : \pi \in S_n, \pi(E_q^n) = E_q^n\}.$$

1.14. Доказать, что любая подстановка $\pi \in S_n$ является линейным преобразованием в пространстве E^n.

1.15. Найти порядок группы симметрий и группы автоморфизмов:

a) пространства E^n;

b) пространства E_q^n.

1.16.* Доказать, что преобразование пространства E^n является изометрией тогда и только тогда, когда оно получено некоторой перестановкой координат всех векторов в E^n и прибавлением некоторого вектора $v \in E^n$ ко всем векторам.

2. Линейные коды

• *q-значным кодом* называется произвольное подмножество пространства E_q^n, элементы кода называются *кодовыми словами*.

• *Кодовые параметры* кода C — это тройка $(n, |C|, d)_q$, где:
n — *длина* кода;
$|C|$ — *мощность* кода;
d — *кодовое расстояние* кода, $d = \min\limits_{x,y \in C, x \neq y} d(x, y)$.
В двоичном случае параметры кода будем обозначать $(n, |C|, d)$, опуская q.

• Код называется *линейным*, если он образует подпространство в E_q^n, его параметры обозначаются также $[n, k, d]_q$, где k — *размерность* кода, т. е. $|C| = q^k$. В двоичном случае будем обозначать параметры кода $[n, k, d]$.

• Два кода $C, C' \subset E_q^n$ называются *изоморфными*, если существует подстановка π такая, что $C' = \pi(C) = \{\pi(x) : x \in C\}$.

• Коды $C, C' \subset E_q^n$ называются *эквивалентными*, если существует автоморфизм E_q^n, переводящий C в C', т. е. найдутся n подстановок $\tau_1, \ldots, \tau_n$ на q элементах $\{1, 2, \ldots, q\}$ и подстановка π на n координатных позициях такие, что

$$C' = \{\pi(\tau_1(x_1), \tau_2(x_2), \ldots, \tau_n(x_n)) : x = (x_1, x_2, \ldots, x_n) \in C\}.$$

• Два вектора $x, y \in E^n$ называются *ортогональными*, если их скалярное произведение над $GF(2)$ равно нулю, т. е. $x \cdot y = x_1 y_1 \oplus \ldots \oplus x_n y_n = 0$.

2.1. Пусть проверочная матрица линейного кода задана в каноническом виде $H = [A_{n-k,k} | E_{n-k}]$. Найти вид порождающей матрицы этого кода в каноническом виде.

2.2. Показать, что кодовое расстояние линейного кода равно минимальному из весов его ненулевых кодовых слов.

2.3. Доказать, что если H — проверочная матрица кода длины n, то код имеет кодовое расстояние d тогда и только тогда, когда любые $d - 1$ столбцов матрицы H линейно независимы и найдутся d линейно зависимых столбцов.

2.4. Показать, что в двоичном линейном коде либо каждое кодовое слово имеет четный вес, либо половина кодовых слов имеют четные веса и половина — нечетные.

2.5. Найти число различных линейных:

a) двоичных кодов длины n размерности k;

b) q-значных кодов длины n размерности k.

2.6. Найти число различных линейных:

a) двоичных кодов длины n, размерности k с информационными символами в первых k координатах;

b) аналогично для q-значного случая.

2.7. Найти число различных линейных:

a) двоичных кодов длины n, размерности k, содержащих фиксированный вектор x, с информационными символами в первых k координатах;

b) аналогично для q-значного случая.

2.8. Пусть код задан своей проверочной матрицей

$$\begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Найти кодовое слово, информационный блок которого равен вектору $(1,1,0)$, при условии, что первые три координаты кода являются информационными.

2.9. Построить коды с помощью проверочных матриц:

$$a)\ \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}; \quad b)\ \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

Найти порождающие матрицы этих кодов.

2.10. Эквивалентны ли коды, заданные порождающими матрицами

$$G = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}; \quad G' = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 \end{pmatrix}.$$

2.11. Построить коды с помощью проверочных матриц:

$$a)\ \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}; \quad b)\ \begin{pmatrix} 0 & 2 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 2 & 2 \\ 2 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}; \quad c)\ \begin{pmatrix} 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

Найти порождающие матрицы этих кодов.

2.12. Построить код с помощью порождающей матрицы:

$$a)\ \begin{pmatrix} 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 \end{pmatrix}; \quad b)\ \begin{pmatrix} 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

Пусть информационный блок u кодируется по правилу $x = uG$. Найти кодовое слово x, если а) $u = (101)$, b) $u = (111)$. Найти информационный блок кодового слова: а) $x = (01101)$, b) $x = (011101)$.

2.13. Найти параметры кодов из задач 2.11 и 2.12.

2.14. Доказать, что коды $C_1 = \{0000, 1100, 1010, 0110\}$ и $C_2 = \{0000, 1100, 1010, 1001\}$ изометричны. Эквивалентны ли эти коды?

2.15. Найти группы симметрий кодов из задачи 2.12.

2.16. Найти кодовое слово кода Хэмминга длины 7, если информационный блок равен $(0,1,1,1)$ и код определен проверочной матрицей, заданной в лексикографическом виде.

2.17. Используя теорему о столбцах проверочной матрицы, найти кодовое расстояние кодов со следующими проверочными матрицами:

$$a)\ \begin{pmatrix}0&0&0&1&1&1&1\\0&1&1&0&0&1&1\\1&0&1&0&1&0&1\end{pmatrix};\quad b)\ \begin{pmatrix}1&1&0&0&1\\1&0&1&0&1\\0&1&1&1&0\end{pmatrix};\quad c)\ \begin{pmatrix}1&1&0&1&0\\0&1&1&0&1\\1&0&1&1&1\end{pmatrix}.$$

2.18. Найти параметры кода длины n, заданного проверочной матрицей

$$\begin{pmatrix}1&1&\dots&1\end{pmatrix}.$$

Описать свойства этого кода.

2.19. Доказать, что ненулевой столбец кодовой матрицы двоичного линейного кода размерности k содержит ровно 2^{k-1} единиц.

2.20. Доказать, что ненулевой столбец кодовой матрицы q-значного линейного кода размерности k содержит ровно q^{k-1} единиц.

2.21. Показать, что кодовое расстояние двоичного линейного кода длины n, размерности k не превосходит $\lfloor \frac{n\cdot 2^{k-1}}{2^k-1} \rfloor$.

2.22. Каковы параметры кода, полученного из линейного кода с кодовым расстоянием d, заданного проверочной матрицей $H_{r\times n}$ добавлением одной или более строк. Какой из этих кодов является подкодом другого кода?

2.23. Найти проверочную и порождающую матрицы произвольного двоичного линейного кода длины n, размерности 1 с повторением (код, у которого передаваемый символ повторяется n раз).

2.24.* Доказать *теорему Симониса*: для любого линейного $[n,k,d]_q$-кода существует линейный код с теми же параметрами такой, что его база состоит из кодовых слов минимального веса d.

• Код $C^\perp = \{y \in E_q^n \mid x\cdot y = x_1y_1+\ldots+x_ny_n = 0 \text{ для всех } x \in C\}$ называется *ортогональным кодом* к линейному коду C длины n.
• Линейный код C называется *самоортогональным*, если $C = C^\perp$.

2.25. Найти число векторов, ортогональных данному ненулевому вектору из E^n.

2.26. Пусть H, G — проверочная и порождающая матрицы линейного кода соответственно. Доказать, что $H\cdot G^T = \mathbf{0}$ и $G\cdot H^T = \mathbf{0}$. Исследуя связь между H и G, найти число проверочных и порождающих матриц данного $[n,k]$-кода.

2.27. Показать, что $(C^\perp)^\perp = C$ для любого линейного кода из E^n.

2.28. Пусть $C+D = \{x+y \mid x\in C, y\in D\}$, где C, D – линейные коды. Показать, что $(C+D)^\perp = C^\perp \cap D^\perp$.

2.29. Найти код, ортогональный двоичному коду с повторением длины n.

2.30. Доказать, что $Sym(C^\perp) = Sym(C)$ для любого двоичного линейного кода C.

2.31. Построить все самоортогональные двоичные коды длины 4 и 8, указать их параметры.

2.32. Доказать, что код с проверочной матрицей $H = [A \mid I]$ над полем $GF(q)$ является самоортогональным тогда и только тогда, когда A – квадратная матрица, такая что $AA^\top = -I$.

• Множество всех обратимых $(k \times k)$-матриц над полем Галуа $GF(q)$, $q \geq 2$, образует полную линейную группу относительно операции умножения матриц. Эта группа обозначается через $GL(k, q)$.

2.33. Найти порядок полной линейной группы $GL(k, q)$.

2.34. Доказать, что подстановка координат, задаваемая некоторой перестановочной матрицей P, принадлежит группе симметрий некоторого двоичного линейного кода с порождающей матрицей G тогда и только тогда, когда $MG = GP$ для некоторой обратимой матрицы M.

2.35. Будет ли группа симметрий произвольного двоичного линейного кода размерности k изоморфна подгруппе полной линейной группы $GL(k, 2)$?

2.36.* Найти число различных матриц размера $k \times n$ ранга r над $GF(q)$.

3. Границы объемов кодов

• Граница *Хэмминга*: $|C| \le \frac{2^n}{\sum\limits_{i=0}^{t} C_n^i}$, где $t = \lfloor \frac{d-1}{2} \rfloor$.
Код, достигающий границы Хэмминга, называется *совершенным*.

• Граница *Синглтона*: $|C| \le 2^{n-d+1}$.
Код, достигающий границы Синглтона, называется *MDS-кодом* (maximal distance separable), или максимально дистанционно разделимым кодом, иногда в русскоязычной литературе его обозначают как МДР-код.

• Граница *Варшамова – Гилберта для линейных кодов*:
если $\sum\limits_{i=0}^{d-2} C_{n-1}^i < 2^r$, то существует линейный $[n, k, d']$-код такой, что $k \ge n - r$ и $d' \ge d$.

• Граница *Плоткина*: $|C| \le 2\lfloor \frac{d}{2d-n} \rfloor$, если $n < 2d$.

Двоичные коды C и C' *эквивалентны*, если существуют такие $\pi \in S_n$ и $x \in E^n$, что $x + \pi(C) = C'$.
Код *максимален*, если его мощность максимальна при данных n и d.

3.1. Доказать, что код с минимальным расстоянием d может исправлять $\lfloor (d-1)/2 \rfloor$ ошибок. Если d четно, то код может одновременно исправлять $(d-2)/2$ ошибки и обнаруживать $d/2$ ошибок.

3.2. Верно ли, что код, исправляющий t ошибок, обнаруживает:

a) не менее $2t+1$ ошибок;

b) не менее $2t$ ошибок;

c) не более $2t$ ошибок?

3.3. Существует ли двоичный код с параметрами:

a) $(16, 10, 9)$;

b) $(10, 17, 7)$;

c) $(14, 1024, 3)$?

3.4. Доказать, что существует троичный $[11, 6, 4]$-код.

3.5. Показать, что не существует максимальных кодов мощности 3.

3.6. Найти параметры кода, заданного проверочной матрицей H. Убедиться, что найденные параметры удовлетворяют упомянутым выше границам объемов кодов.

$$a)\, H = \begin{pmatrix} 1 & 0 & 1 & 2 & 0 \\ 2 & 2 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}; \qquad b)\, H = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 \end{pmatrix}.$$

3.7. Обобщить для q-значных кодов границы:

a) Хэмминга;

b) Синглтона;

c) Варшамова – Гилберта.

• *Характеристической функцией* кода C называется булева функция $f : E^n \to \{0,1\}$ такая, что $f(x_1,\ldots,x_n) = 1$ тогда и только тогда, когда вектор $(x_1,\ldots,x_n)$ принадлежит коду C.
• Пусть $A(n,d)$ обозначает мощность максимального двоичного кода длины n с расстоянием d.

3.8. Сколько ошибок исправляет и обнаруживает код длины n с характеристической функцией f:

a) $f(x_1,\ldots,x_n) = x_1 \oplus \ldots \oplus x_n$;

b) $f(x_1,\ldots,x_n) = x_1 \cdot \ldots \cdot x_n \vee \overline{x}_1 \cdot \ldots \cdot \overline{x}_n$?

3.9. Привести пример максимального кода мощности 2. Сколько существует максимальных кодов длины n с кодовым расстоянием 2?

3.10. Показать, что $A(3k,2k)$ равно 4.

3.11. Показать, что:

a) $A(n,2r-1) = A(n+1,2r)$;

b) $A(n,d) \le 2A(n-1,d)$.

• Обозначим через $N(k,d)$ минимально возможную длину двоичного линейного кода размерности k с минимальным расстоянием d.

3.12. Доказать, что для линейного $[N(k,d),k,d]$-кода справедлива следующая граница:

$$N(k,d) \ge d + N(k-1,\lceil d/2\rceil),$$

именуемая границей *Грайсмера*.

3.13. Доказать, что $N(k,d) \ge \sum_{i=0}^{k-1}\lceil d/2^i\rceil$.

3.14. Найти $N(5,7)$. Существует ли код, удовлетворяющий границе Грайсмера?

3.15. Найти $N(k,2^{k-1})$. Существует ли код, удовлетворяющий границе Грайсмера?

3.16.* Пусть C — код четной длины n, исправляющий две ошибки. Доказать, что $|C| \le \frac{2^n}{n+2}$.

4. Совершенные коды

• Код с расстоянием $d = 2t + 1$ называется *совершенным*, если шары радиуса t с центрами в кодовых словах, не пересекаясь, покрывают все пространство E_q^n.
Линейный двоичный код, проверочная матрица которого состоит из всевозможных различных ненулевых столбцов длины r, называется двоичным *кодом Хэмминга* с r проверками на четность.

• Пусть $C^{\frac{n-1}{2}}$ — любой совершенный двоичный код длины $\frac{n-1}{2}$ с расстоянием 3, $\lambda : C^{\frac{n-1}{2}} \to \{0,1\}$ — произвольная функция. Множество

$$C^n = \{(u, u+v, |u| + \lambda(v)) \,|\, u \in E^{\frac{n-1}{2}}, v \in C^{\frac{n-1}{2}}\},$$

где $|u| = u_1 \oplus \ldots \oplus u_{\frac{n-1}{2}}$ является совершенным двоичным кодом длины n с расстоянием 3 и называется *кодом Васильева*.

Теорема о существовании совершенных кодов (Зиновьев В. А. и Леонтьев В. К., независимо Тиетвайнен А., 1972)
Нетривиальный совершенный код над любым полем Галуа $GF(q)$ должен иметь те же самые параметры, что и один из кодов Хэмминга или Голея, т. е.:

1) q-значный $(n = (q^m - 1)/(q - 1), q^{n-m}, 3)$-код Хэмминга;

2) двоичный $[23, 12, 7]$-код Голея;

3) троичный $[11, 6, 5]_3$-код Голея.

4.1. Существует ли совершенный двоичный код длины 149?

4.2. Доказать, что не существует совершенного двоичного кода длины 21 с кодовым расстоянием 7.

4.3. Найти проверочные матрицы двоичного кода Хэмминга длины 7 в лексикографическом и каноническом видах.

4.4. Показать, что совершенные двоичные коды с расстоянием 7 существуют только для длин $n = 7$ и $n = 23$.

4.5. Определить параметры двоичного кода Хэмминга. Доказать, что двоичный код Хэмминга единствен с точностью до эквивалентности.

4.6. Построить проверочную матрицу с r строками q-значного кода Хэмминга, вычислить параметры кода. Доказать единственность кода с точностью до эквивалентности.

4.7. Доказать, что q-значный код Хэмминга является совершенным.

4.8. Найти проверочную матрицу:

a) с двумя строками для троичного кода Хэмминга, построить код;

b) с тремя строками для троичного кода Хэмминга.

4.9. Построить код Хэмминга длины 4 над $GF(3)$.

4.10. Найти порождающую и проверочную матрицы кода Хэмминга длины 6 над $GF(5)$. Определить параметры этого кода.

4.11. Найти код, ортогональный:

a) двоичному коду Хэмминга длины 7;

b) троичному коду Хэмминга длины 4;

c) двоичному коду Хэмминга длины 15.

• Двоичный код C^n обладает свойством *антиподальности*, если для любого кодового слова $x \in C^n$ выполняется $x + \mathbf{1}^n \in C^n$, где $\mathbf{1}^n$ — единичный вектор длины n, т. е. вектор, все координаты которого равны 1.

4.12. Доказать, что код Хэмминга обладает свойством *антиподальности*.

4.13. Используя порождающую матрицу кода Хэмминга, доказать, что кодовое расстояние не менее 3.

4.14. Вычислить нижние оценки числа различных и числа неэквивалентных кодов Васильева длины n.

4.15. Показать, что имеет место разбиение $E^n = \bigcup_{i=0}^{n} (C + e_i)$ для любого совершенного кода C длины n с расстоянием 3.

4.16. Доказать, что в коде, ортогональном двоичному коду Хэмминга длины n, все ненулевые векторы имеют вес $(n+1)/2$.

4.17. Доказать, что расширенный код Хэмминга длины 8 самоортогонален.

4.18. Доказать, что двоичный расширенный код Хэмминга единствен с точностью до изоморфизма.

4.19. Найти конструктивно базу двоичного кода Хэмминга длины n среди кодовых слов веса 3.

4.20. Найти группу автоморфизмов (найти порядок и перечислить все автоморфизмы):

a) двоичного кода Хэмминга длины 7;

b) двоичного расширенного кода Хэмминга длины 8.

4.21. Найти группу автоморфизмов троичного кода $\{000, 111, 222\}$, перечислить все автоморфизмы.

4.22. Найти группу автоморфизмов (найти порядок и перечислить все автоморфизмы) троичного кода Хэмминга длины 4.

4.23. Найти группу симметрий и группу автоморфизмов:

a) двоичного кода Хэмминга длины n;

b) двоичного расширенного кода Хэмминга длины N.

4.24. Найти группу перестановочных автоморфизмов q-значного кода Хэмминга длины n.

• *Свитчингом* по i-й координате подмножества R совершенного двоичного кода C называется замена значения этой координаты всех векторов множества R. Полученное множество обозначим $R+e_i$, где e_i — вектор веса 1 с ненулевой i-й координатной позицией. Множество $R \subseteq C$ называется *i-компонентой* совершенного кода C, если $O(R) = O(R+e_i)$, где $O(R)$ — множество всех векторов из E^n, находящихся на расстоянии не больше 1 от R. В результате получается новый совершенный код $C' = (C \setminus R) \cup (R + e_i)$ с теми же параметрами, что и C. В этом случае говорят, что код C' получен из кода C *свитчингом* i-компоненты R.

4.25. Найти i-компоненты кода Хэмминга длины 7.

4.26. Доказать, что конструкция Васильева является свитчинговой. Выписать (аналитически) i-компоненту кода Васильева, содержащую нулевой вектор.

4.27. Найти разложение кода Хэмминга длины n на i-компоненты.

4.28. Доказать, что при $n = 2^k, k \geq 2$, существует разбиение пространства E^n на непересекающиеся сферы радиуса 1.

4.29. Доказать, что в совершенном двоичном коде число кодовых слов четного и нечетного весов совпадают.

4.30. Доказать, что произвольный совершенный двоичный код длины n, содержащий нулевой вектор, однозначно определяется множеством своих кодовых слов веса $(n+1)/2$.

• Код называется *дистанционно инвариантным*, если число всех кодовых слов на расстоянии k от фиксированного кодового слова не зависит от выбора этого кодового слова.

4.31.* Доказать, что совершенный и расширенный совершенный двоичные коды с расстоянием 3 дистанционно инвариантны. Вывести точные формулы числа кодовых слов веса k при условии, что код содержит нулевой вектор.

4.32. Доказать, что совершенный и расширенный совершенный двоичные коды с расстоянием 3 антиподальны.

4.33.* Доказать, что q-значный совершенный код с расстоянием 3 дистанционно инвариантен. Вывести точные формулы числа кодовых слов веса k при условии, что код содержит нулевой вектор.

• Формула Стирлинга $n^n e^{-n}\sqrt{2\pi n} \leq n! \leq e^{\frac{1}{12n}} n^n e^{1-n}\sqrt{2\pi n}$.

4.34. Доказать неравенство

$$\begin{pmatrix} n \\ (n-1)/2 \end{pmatrix} \leq \frac{2^n}{\sqrt{n}}.$$

4.35. Доказать, что число $A_{\frac{n-1}{2}}$ всех кодовых слов веса $\frac{n-1}{2}$ произвольного совершенного кода, содержащего нулевое слово, удовлетворяет неравенству

$$A_{\frac{n-1}{2}} \leq c\frac{2^n}{n\sqrt{n}},$$

где c — некоторая константа.

4.36.* Доказать, что число N_n различных совершенных двоичных кодов длины n удовлетворяет неравенству

$$N_n \leq 2^{2^{n-\frac{3}{2}\log n+\log\log(en)}}.$$

• *Ядро кода* C, содержащего нулевой вектор, определяется следующим образом:

$$Ker(C) = \{x \,|\, x \in C,\, x + C = C\}.$$

4.37. Доказать, что не существует совершенного двоичного кода длины n с размерностью ядра $dim(Ker(C))$, равной $n - \log(n+1) - 1$.

4.38. Доказать, что $Sym(C) \leq Sym(Ker(C))$.

• *Ранг кода* определяется как размерность его линейной оболочки.

4.39.* Доказать, что для любого совершенного двоичного кода C длины n справедливо $dim(Ker(C)) + r(C) \geq n + 1$, где $dim(Ker(C))$ и $r(C)$ — размерность ядра и ранг кода C соответственно.

4.40.* Доказать, что базу q-значного, $q \geq 2$, кода Хэмминга длины n можно выбрать среди кодовых слов веса 3.

4.41.* Доказать, что число различных расширенных совершенных двоичных кодов длины $n+1$ ровно вдвое больше числа различных совершенных двоичных кодов длины n.

4.42.* Доказать, что для любого кодового слова x кода $< C >^{\perp}$, где C — произвольный совершенный код, выполняется $w(x) = (n+1)/2$.

4.43.* Доказать, что для любого совершенного кода C длины $n = 2^m - 1$ ранга $r = n - m - p$, где $n - m + 1 \leq r \leq n - 1$, найдется разбиение

$$I_0 \cup I_1 \cup \ldots \cup I_t = \{1, 2, \ldots, n\}, I_i \cap I_j = \emptyset$$

при $i \neq j$, где $t = 2^{m-p} - 1$, $|I_0| + 1 = |I_1| = \ldots = |I_t| = 2^p$. Кроме того, для каждого $x \in < C >^{\perp}$ выполняется $I_0 \cap x = \emptyset$ и для каждого I_j, $j = 1, 2, \ldots, t$ либо $I_j \cap supp(x) = \emptyset$, либо $I_j \subseteq supp(x)$.

4.44. (**Нерешенная проблема**). Найти нижнюю оценку числа различных двоичных совершенных кодов полного ранга длины $n > 15$.

4.45. (**Нерешенная проблема**). Найти новую верхнюю оценку числа различных двоичных совершенных кодов длины $n > 15$.

5. Способы построения кодов

• Пусть C и D — коды с параметрами $(\frac{n}{2}, M_1, d_1)$ и $(\frac{n}{2}, M_2, d_2)$ соответственно. Тогда говорят, что код $C^n = \{(u, u+v) \,|\, u \in C, v \in D\}$ получен из кодов C и D применением *конструкции Плоткина*. Он имеет параметры $(n, M_1 \cdot M_2, \min\{2d_1, d_2\})$.

5.1. Определить параметры кода, полученного из $(n, |C|, d)$-кода C:

a) *выкалыванием* кодовой координаты;

b) *выбрасыванием* (выбором всех кодовых слов четного веса);

c) *укорочением* (выбором всех кодовых слов с фиксированным значением в некоторой координате и последующим ее удалением).

5.2. Пусть $(n, |C|, d)$-код C не содержит вектор u. Найти параметры кода C', полученного из C *пополнением* с помощью вектора u, т. е. $C' = C \cup (u + C)$. В случае линейного кода C показать, что C' также линеен.

5.3. Пусть $[n, k, d]$-код C не содержит вектор u. Пусть код C' получен из C *удлинением* путем добавления информационного символа, т. е. пополнением с помощью вектора u, а затем расширением с помощью общей проверки на четность. Найти параметры кода C' и доказать его линейность.

5.4. Найти все коды, полученные из кода Хэмминга длины 7 методами, описанными в задаче 5.1.

5.5. Пусть G_1 и G_2 — порождающие матрицы линейных кодов с параметрами $[n_1, k_1, d_1]$ и $[n_2, k_2, d_2]$ соответственно. Найти параметры кода с порождающей матрицей

$$a) \begin{pmatrix} G_1 & \mathbf{0} \\ \mathbf{0} & G_2 \end{pmatrix}; \quad b) \begin{pmatrix} G_1 & G_2 \end{pmatrix} \text{ при } k_1 = k_2.$$

5.6. Построить максимальный двоичный код длины 7 такой, чтобы расстояние между произвольной парой кодовых слов было равно 4.

5.7. Построить расширенный код Хэмминга длины 8 добавлением общей проверки на четность. Доказать, что код имеет расстояние 4, обнаруживает 2 ошибки и исправляет одну ошибку.

5.8. Построить максимальный код длины 8 с попарным расстоянием между кодовыми словами, равным 4.

5.9. Найти проверочную матрицу кода Хэмминга длины 15, используя проверочную матрицу кода Хэмминга длины 7. Аналогично для расширенного кода Хэмминга длины 16, используя проверочную матрицу расширенного кода Хэмминга длины 8. Обобщить конструкцию для произвольной длины кода $n = 2^r - 1$.

5.10. Найти порождающую матрицу расширенного кода Хэмминга длины 16, построенного с помощью конструкции Плоткина. Какие коды для этого нужно использовать?

• Иногда полезно строить коды, рассматривая сужение известных кодов над некоторым алфавитом, затем возможно применение к полученным кодам каскадной конструкции с целью получения кодов с хорошими параметрами.

5.11.* Доказать, что сужение кода Хэмминга длины 6 над полем Галуа $GF(5)$ над алфавитом $\{0, 1, \ldots, 4\} \setminus \{i\}$, $i \neq 0$, имеет мощность 164, а сужение над алфавитом $\{1, \ldots, 4\}$ — мощность 160.

6. Декодирование

I. Пусть p — вероятность ошибки (искажения одного символа) в канале связи. Появление неправильного кодового слова на выходе декодера называется *ошибкой декодирования*, ее вероятность равна

$P_{\text{ош}} \stackrel{df}{=} \frac{1}{|C|} \sum\limits_{i=1}^{|C|} prob\{$ выход декодера $\neq x^i \,|\, x^i$ было передано$\}$.

• При декодировании по принципу максимума правдоподобия

$P_{\text{ош}} = 1 - \sum\limits_{i=0}^{n} \alpha_i p^i (1-p)^{n-i}$, где α_i — число лидеров веса i смежных классов кода.

• Код с расстоянием $d = 2t+2$ называется *квазисовершенным*, если шары радиуса $t+1$ с центрами в кодовых вершинах покрывают всё пространство E^n (при этом шары будут пересекаться).

6.1. Можно ли декодировать сообщение, переданное по двоичному симметричному каналу связи, если вероятность искажения символа равна $p = 1/2$?

6.2. Доказать, что синдром S_y вектора y равен нулевому вектору тогда и только тогда, когда y является кодовым вектором.

6.3. Доказать, что синдром полученного вектора равен сумме тех столбцов проверочной матрицы кода, в которых произошли ошибки.

6.4. Доказать, что два вектора u и v принадлежат одному и тому же смежному классу по линейному коду тогда и только тогда, когда их синдромы равны.

6.5. Доказать, что имеется взаимно однозначное соответствие между синдромами и смежными классами.

6.6. Найти вероятность того, что полученный вектор отличается от переданного вектора в k координатных позициях при условии передачи информации по двоичному симметричному каналу связи с вероятностью искажения символа $0 < p < 1/2$.

6.7. Доказать, что для любого совершенного двоичного кода длины n справедливо

$$P_{\text{ош}} = 1 - \sum_{i=0}^{t} C_n^i p^i (1-p)^{n-i}.$$

6.8. Доказать, что для любого квазисовершенного кода длины n выполняется

$$P_{\text{ош}} = 1 - \sum_{i=0}^{t} C_n^i p^i (1-p)^{n-i} - \alpha_{t+1} p^{t+1} (1-p)^{n-t-1}.$$

6.9. Для линейного кода, заданного порождающей матрицей

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix},$$

построить таблицу стандартного расположения. Декодировать слово (110111) по таблице стандартного расположения и слово (101011) с помощью синдрома.

6.10. Пусть код задан порождающей матрицей

$$G = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 \end{pmatrix}.$$

Декодировать сообщение:

a) (1110000);

b) (1010101).

6.11. Пусть код задан проверочной матрицей

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

Какой вид имеет синдром, если в канале связи произошла 1 ошибка? А если 2 ошибки? Можно ли с помощью этого кода обнаруживать 2 ошибки? Если да, то как это сделать? Описать декодирование.

6.12. Вычислить вероятность ошибки декодирования для кода из задачи 6.11, если вероятность ошибки в канале связи $p = 0,001$.

6.13. Найти распределение лидеров смежных классов двоичного кода Хэмминга длины n и вероятность его ошибки декодирования.

6.14. Построить таблицу синдромов для расширенного двоичного кода Хэмминга длины 8. Найти вероятности правильного декодирования и ошибки декодирования для $p = 0,02$.

II. *Функция энтропии* $\mathcal{H}(x)$ для двоичного симметричного канала связи определяется равенством

$$\mathcal{H}(x) = -x\log x - (1-x)\log(1-x)$$

при $0 < x < 1$, при $x = 0$ и $x = 1$ полагают $\mathcal{H}(0) = \mathcal{H}(1) = 0$. Отметим, что $\log x$ здесь и далее рассматривается по основанию 2.

• *Пропускная способность* $C(p)$ двоичного симметричного канала с вероятностью $0 \le p \le \frac{1}{2}$ равна

$$C(p) = 1 - \mathcal{H}(p) = 1 + p\log p + (1-p)\log(1-p).$$

• *Скоростью* (n, M, d)-кода называется величина $(\log M)/n$.

Теорема Шеннона. *Для любой сколь угодно малой величины $\varepsilon > 0$ и любого $0 < R < C(p)$ существует двоичный код C длины n мощности M и скорости R такой, что вероятность ошибки декодирования P_C удовлетворяет неравенству $P_C < \varepsilon$, где M определяется из соотношения $R = (\log M)/n$.*

6.15. Построить графики функций энтропии $\mathcal{H}(x) = -x\log x - (1-x)\log(1-x)$ и пропускной способности при $0 < x < 1$ для двоичного симметричного канала связи.

6.16.^{0} Доказать $\log n! = n\log n - n + O(\log n)$.

6.17.^{0} Доказать $C_n^m \le \frac{n^n}{m^m(n-m)^{n-m}}$.

6.18. Рассмотрим шар радиуса $[pn]$ с центром в некоторой вершине $x \in E^n$:

$$B_{[pn]}(x) = \{y \in E^n \mid d(x,y) \le [pn]\}.$$

Пусть $0 \le p \le \frac{1}{2}$. Доказать, что его объем

$$|B_{[pn]}(x)| = \sum_{i=0}^{[pn]} C_n^i$$

с помощью функции энтропии $\mathcal{H}(p)$ оценивается следующим образом:

$$\sum_{i=0}^{[pn]} C_n^i \le 2^{n\mathcal{H}(p)}.$$

6.19. Пусть $0 \le p \le \frac{1}{2}$ и $\rho = [\mathcal{E}(\tau) + b]$, где $b = \left(\frac{\mathcal{D}(\tau)}{\varepsilon/2}\right)^{1/2}$, здесь $\mathcal{E}(\tau)$ и $\mathcal{D}(\tau)$ — математическое ожидание и дисперсия случайной величины τ соответственно. Тогда

$$\frac{1}{n}\log|B_\rho(x)| \le \mathcal{H}(p) - O\Big(\frac{1}{\sqrt{n}}\Big) \text{ при } n \to \infty.$$

6.20. Найти вероятность P_i того, что на выходе декодера (для передачи сообщения использовался двоичный код) получено слово, отличное от переданного слова x^i.

6.21. Доказать, что вероятность ошибки P_C для данной схемы декодирования (двоичный случай) удовлетворяет неравенству

$$P_C \le \frac{\varepsilon}{2} + \frac{1}{M}\sum_{i=1}^{M}\sum_{y\in E^n}\sum_{j\ne i} P(y \mid x^i) f(y, x^j),$$

где ε — некоторая бесконечно малая величина.

7. Поля Галуа

• Множество $GF(p) = \{0, 1, \ldots, p-1\}$ с операциями сложения $+$ и умножения $\cdot$ по модулю простого числа p является *простым полем*. *Кольцо многочленов* $F[x]$ состоит из всех многочленов от переменной x с коэффициентами из поля $GF(p)$. Многочлен $g(x) \in F[x]$ *неприводим* над $GF(p)$, если он не может быть представлен в виде произведения двух многочленов из $F[x]$ меньшей степени.

7.1. Найти все неприводимые над $GF(2)$ многочлены степени, не превышающей 3.

7.2. Доказать, что многочлен $M(x) = x^5 + x^2 + 1$ неприводим над $GF(2)$.

7.3. Найти разложения многочленов на неприводимые над $GF(2)$ множители:

a) $x^5 + x^4 + x^2 + x$;

b) $x^{16} - x$.

7.4. Рассмотрим множество K всех корней многочлена $x^{p^m} - x$ над полем $GF(p)$. Доказать, что K является полем.

7.5. Рассмотрим множество K всех корней многочлена $x^{p^m} - x$ над полем $GF(p)$. Доказать, что все корни различны и, следовательно, $|K| = p^m$.

• Построенное в задаче 7.4 поле K называется *расширением Галуа* поля $GF(p)$ и обозначается $GF(p^m)$. Оно содержит $GF(p)$ в качестве наименьшего подполя, число p называется его *характеристикой*.

7.6. Доказать, что для любого простого p в поле характеристики p справедливо равенство $(x - y)^p = x^p - y^p$.

• *Порядком* элемента β конечного поля называется наименьшее целое положительное число k такое, что $\beta^k = 1$.

7.7.^{0} Доказать, что порядок любого элемента поля Галуа $GF(p^m)$ не делится на p.

7.8.^{0} Доказать, что если элемент α некоторой группы имеет порядок k и α^n есть единица этой группы, то k делит n.

7.9. Пусть элементы β и γ коммутативной группы имеют порядки m и n соответственно, причем $(m, n) = 1$. Доказать, что порядок элемента $\beta \cdot \gamma$ равен mn.

7.10. Пусть порядок элемента β коммутативной группы равен n. Доказать, что порядок элемента β^k равен $\frac{n}{(n,k)}$.

• Ненулевые элементы поля $GF(p^m)$ образуют циклическую группу $\{1, \alpha, \alpha^2, \ldots, \alpha^{p^m-2}\}$. Порождающий элемент этой группы (например α) называется *примитивным элементом* поля. Ненулевой многочлен $g(x) \in F[x]$ наименьшей степени, корнем которого является примитивный элемент поля, называется *примитивным*.

Теорема Ферма. *Каждый элемент поля Галуа* $GF(p^m)$ *является корнем уравнения*

$$x^{p^m} - x = 0.$$

7.11. Доказать, что число примитивных элементов поля Галуа $GF(p^m)$ равно $\varphi(p^m-1)$, где $\varphi(x)$ — функция Эйлера числа x.

• С помощью неприводимого над $GF(p)$ многочлена $g(x)$ степени m можно построить поле Галуа следующим образом: $GF(p^m)$ есть фактор-кольцо кольца $F[x]$ по модулю многочлена $g(x)$.

Многочлен $x^{p^m}-x$ равен произведению всех нормированных неприводимых над $GF(p)$ многочленов, степени которых делят m.

7.12. Найти элемент, обратный по умножению к элементу $x+3$ поля Галуа, построенного с помощью неприводимого над $GF(5)$ многочлена x^2+4x+2. Поле Галуа не строить.

7.13. Пусть β — элемент поля Галуа $GF(2^3)$, построенного по модулю неприводимого многочлена x^3+x+1. Доказать, что элементы $\beta^4+\beta^2+\beta$ и $\beta^3+\beta^5+\beta^6$ всегда принадлежат простому подполю $GF(2)$, и выяснить, в каких случаях они равны нулю поля, а в каких случаях — единице.

7.14. Построить поле Галуа $GF(2^2)$, используя неприводимый многочлен x^2+x+1. Найти таблицы сложения и умножения элементов поля.

7.15. Построить два представления поля Галуа $GF(5^2)$, используя неприводимые многочлены x^2-1 и x^2+x+1. Указать изоморфизм этих представлений поля $GF(5^2)$.

• Функция Мёбиуса целого положительного числа m определяется следующим образом:

$$\mu(m)=\begin{cases} 1, & \text{если } m=1;\\ (-1)^r, & \text{если } m \text{ — произведение } r \text{ различных простых чисел;}\\ 0, & \text{в остальных случаях.}\end{cases}$$

7.16.* Доказать, что число нормированных неприводимых многочленов над $GF(p)$ степени m равняется

$$\frac{1}{m}\sum_{d,\,d|m}\mu(d)p^{m/d}.$$

7.17. Найти число неприводимых многочленов над $GF(2)$ степени 4.

7.18. Построить два представления поля Галуа $GF(2^3)$, используя один и тот же неприводимый многочлен x^3+x+1, но разные примитивные элементы. Указать изоморфизм этих двух представлений поля Галуа $GF(2^3)$.

7.19. Построить поля Галуа:

a) $GF(2^3)$, используя неприводимый многочлен x^3+x^2+1. Показать изоморфизм между построенным полем и полем из задачи 7.18;

b) $GF(3^2)$, используя неприводимый многочлен x^2+x+2;

c) $GF(3^3)$, используя неприводимый многочлен x^3+2x+1.

7.20. Построить поле Галуа $GF(3^2)$, используя неприводимый многочлен x^2+2x+2. Построить таблицы сложения и умножения элементов в поле Галуа. В поле найти элемент, обратный 2α, где α – примитивный элемент.

7.21.* Доказать, что автоморфизмы поля $GF(p^m)$ образуют циклическую группу порядка m.

7.22. Найти группы автоморфизмов полей $GF(2^4)$, $GF(2^5)$, $GF(2^6)$. Решить задачу без использования явных представлений полей Галуа.

7.23.* Показать, что существует автоморфизм (невырожденное линейное преобразование) векторного пространства $GF(q)^n$ порядка $q^n - 1$.

8. Минимальный многочлен

• *Минимальным многочленом* элемента β из $GF(p^m)$ называется приведенный многочлен $M(x)$ над полем $GF(p)$ наименьшей степени такой, что $M(\beta) = 0$.

• **Свойства минимального многочлена $M(x)$ элемента β из $GF(p^m)$.**

1. Многочлен $M(x)$ неприводим над $GF(p)$.
2. Если $f(x)$ — некоторый многочлен такой, что $f(\beta) = 0$, то $M(x)$ делит $f(x)$.
3. Многочлен $M(x)$ делит $x^{p^m} - x$.
4. Степень многочлена $M(x)$ не превосходит m.
5. Многочлен $M(x)$ минимальный для элементов β и β^p.

Множество целых чисел по модулю $p^m - 1$ следующим образом распадается на подмножества, называемые *циклотомическими классами по модулю* $p^m - 1$: циклотомический класс, содержащий s, имеет вид $C_s = \{s, ps, p^2s, p^3s, \ldots, p^{m_s-1}s\}$, где m_s — наименьшее положительное целое число такое, что $p^{m_s} \cdot s \equiv s \pmod{p^m - 1}$.
Пусть $M^{(i)}(x)$ — минимальный многочлен элемента α^i из $GF(p^m)$, где α — примитивный элемент поля.

6. Если i лежит в классе C_s, то справедливо $M^{(i)}(x) = \prod\limits_{j \in C_s} (x - \alpha^j)$.

• Из теоремы Ферма следует равенство

$$x^{p^m-1} - 1 = \prod_s M^{(s)}(x),$$

где s пробегает все множество представителей циклотомических классов по модулю $p^m - 1$.

8.1.^{0} Пусть α — элемент поля $GF(p^m)$, $m \leq 2$. Когда многочлен $x - \alpha$ является минимальным для α?

8.2. Найти циклотомические классы по модулям 7, 8, 15, 31.

8.3. Пусть поле Галуа $GF(2^3)$ задано с помощью неприводимого многочлена

$$x^3 + x^2 + 1.$$

Найти выражения для минимальных многочленов всех элементов поля $GF(2^3)$.

8.4. Найти явный вид минимального многочлена $M^{(1)}(x)$ примитивного элемента α поля $GF(2^4)$, если поле Галуа построено по модулю многочлена $x^4 + x + 1$.

8.5. Пусть поле $GF(3^2)$ задано с помощью неприводимого многочлена $x^2 + x + 2$. Найти выражения для минимальных многочленов всех элементов поля $GF(3^2)$.

8.6. Разложить многочлены a) $x^8 - x$, b) $x^{16} - x$ в произведение минимальных многочленов элементов a) поля Галуа $GF(2^3)$; b) поля Галуа $GF(2^4)$ соотвественно.

8.7. Найти разложение многочлена $x^{10} - x$ на неприводимые многочлены над $GF(2)$.

8.8. Найти разложение $x^5+x^4+x^3+2x^2+1$ на неприводимые многочлены над $GF(3)$.

8.9. Найти минимальные многочлены элементов поля Галуа $GF(2^4)$. Какие из них являются порождающими многочленами кода Хэмминга?

8.10. Доказать, что для произвольного элемента β из $GF(p^m)$ минимальный многочлен $M_\beta(x)$ существует и единствен.

8.11. Пусть β — произвольный элемент поля $GF(p^m)$. Доказать, что если для некоторого многочлена $f(x) \in F[x]$ выполнено $f(\beta) = 0$, то минимальный многочлен $M_\beta(x)$ делит $f(x)$.

8.12. Доказать, что минимальный многочлен $M_\beta(x)$ произвольного ненулевого элемента β из $GF(p^m)$ делит многочлен $x^{p^m-1} - 1$.

8.13. Доказать, что степень минимального многочлена любого элемента поля $GF(p^m)$ не превосходит m.

8.14. Доказать, что степень минимального многочлена примитивного элемента поля $GF(p^m)$ равна m.

8.15. Доказать, что если i лежит в классе C_s, то справедливо

$$M^{(i)}(x) = \prod_{j \in C_s} (x - \alpha^j).$$

9. Циклические коды

• Линейный код длины n называется *циклическим*, если для любого кодового слова $(x_1, x_2, \ldots, x_n)$ слово $(x_2, \ldots, x_n, x_1)$ также является кодовым. Подкольцо I кольца $F[x]/(x^n - 1)$ называется *идеалом*, если для любых многочленов $u(x) \in F[x]/(x^n - 1)$ и $c(x) \in I$ многочлен $u(x) \cdot c(x)$ принадлежит I.

Теорема. *Подпространство кольца $F[x]/(x^n - 1)$ является циклическим кодом тогда и только тогда, когда оно образует идеал.*

Приведенный многочлен наименьшей степени, принадлежащий циклическому коду, называется *порождающим* многочленом кода.

• Код длины n размерности k над $GF(q)$ называется *систематическим*, если после вычеркивания некоторых $n - k$ столбцов из его кодовой матрицы остаются в точности все различные векторы длины k из E_q^k.

Теорема (Граница БЧХ). *Пусть C — циклический код с таким порождающим многочленом $g(x)$, что для некоторых целых чисел $b \geq 0$, $\delta > 1$ выполняется*

$$g(\alpha^b) = g(\alpha^{b+1}) = \ldots = g(\alpha^{b+\delta-2}) = 0,$$

т. е. $\delta - 1$ последовательных степеней примитивного элемента α поля Галуа $GF(p^m)$ являются нулями кода. Тогда кодовое расстояние кода не меньше δ.

9.1.^{0} Выяснить, являются ли следующие коды циклическими:

a) двоичный код $\{(1,0,0),(0,1,0),(0,0,1)\}$;

b) троичный код, состоящий из всех троичных векторов длины 4;

c) двоичный линейный код длины 15, наименьший ненулевой степени кодовый многочлен которого равен x.

9.2. Построить циклический код длины 7 с кодовым расстоянием 3. Найти порождающий многочлен кода.

9.3. Является ли циклическим код, полученный из циклического добавлением общей проверки на четность?

9.4. Является ли циклическим двоичный код с порождающей матрицей

$$\begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \end{pmatrix}.$$

Найти параметры кода.

9.5. Используя задачу 8.6 а), рассмотреть разложение многочлена $x^8 - x$ в произведение минимальных многочленов и выяснить:

a) какие элементы поля $GF(2^3)$, построенного с помощью неприводимого многочлена $x^3 + x + 1$, им отвечают;

b) сколько двоичных циклических кодов длины 7 можно построить;

c) найти порождающие и проверочные матрицы этих кодов.

9.6. Найти проверочный многочлен циклического кода Хэмминга с порождающим многочленом $g(x) = x^4 + x + 1$.

9.7. Найти два систематических кодера кода длины 7 с порождающим многочленом $g(x) = x^3 + x + 1$. Закодировать с их помощью вектор (1101).

9.8. Найти проверочную матрицу циклического кода длины 5 с порождающим многочленом $g(x) = x + 1$.

9.9. Найти проверочную и порождающую матрицы кода длины 7 с порождающим многочленом $g(x) = (x + 1)(1 + x + x^3)$. Построить код, найти кодовое расстояние, указать проверочную матрицу ортогонального кода.

9.10. Найти систематический кодер для кода из задачи 9.9, декодировать полученные слова (1,0,1,1,0,1,1) и (1,1,1,0,0,1,1).

9.11. Пусть двоичный код задан проверочной матрицей

$$\begin{pmatrix} 1 & \alpha & \alpha^2 & . & . & . & \alpha^{14} \\ 1 & \alpha^3 & \alpha^6 & . & . & . & \alpha^{3\times 14} \end{pmatrix},$$

где α есть вектор-столбец, представляющий примитивный элемент поля Галуа $GF(2^4)$, заданного неприводимым многочленом $f(x) = x^4 + x + 1$.

a) Каково минимальное расстояние кода?

b) Пусть полученное слово имеет синдром $\begin{pmatrix} \alpha^7 \\ \alpha^{14} \end{pmatrix}$. Каков наиболее вероятный вектор ошибки?

9.12. Доказать, что в группе симметрий произвольного двоичного кода Хэмминга длины n существует симметрия порядка n.

9.13. Найти нециклический двоичный код Хэмминга длины 7.

9.14. Доказать, что если для порождающего многочлена $g(x)$ циклического кода над $GF(p)$ выполняется $g(1) \neq 0$, то единичный вектор принадлежит коду. Найти условие, когда верно обратное.

9.15. Доказать, что если в двоичном циклическом коде содержится вектор нечетного веса, то единичный вектор принадлежит коду. Найти условие, когда верно обратное.

9.16.* Доказать, что в любом q-значном циклическом коде C длины n, (n, q)=1, есть единственная *единица* для C, т. е. такой многочлен $c(x)$, что $c(x)c'(x) = c'(x)$ для любого кодового многочлена $c'(x)$.

9.17. Найти единицу двоичного циклического кода длины 15 с порождающим многочленом $g(x) = x^2 + x + 1$.

9.18. Найти все *идемпотенты*, т. е. все многочлены $c(x)$ со свойством $c^2(x) = c(x)$, двоичного циклического кода длины 15 с порождающим многочленом $g(x) = x^{10} + x^5 + 1$.

10. Коды БЧХ

• *Кодом БЧХ над полем* $GF(p)$ длины $n = p^m - 1$ с конструктивным расстоянием $\delta > 1$ называется циклический код с порождающим многочленом, нулями которого являются элементы

$$\alpha^b, \alpha^{b+1}, \ldots, \alpha^{b+\delta-2},$$

где α — примитивный элемент поля $GF(p^m)$ и b — некоторое неотрицательное целое число. Приведем другое эквивалентное определение.

• *Код БЧХ над полем* $GF(p)$ длины $n = p^m - 1$ — это циклический код с порождающим многочленом

$$g(x) = \{M^{(b)}(x), M^{(b+1)}(x), \ldots, M^{(b+\delta-2)}(x)\},$$

где b — некоторое неотрицательное число. При $b = 1$ коды БЧХ называются *кодами БЧХ в узком смысле.*

Теорема о коде БЧХ. Код БЧХ над $GF(p)$ длины $n = p^m - 1$ с конструктивным расстоянием $\delta > 1$ имеет параметры $[n = p^m - 1, k \geq n - (\delta - 1)m, d \geq \delta]$.

10.1. Найти кодовые слова, проверочную и порождающую матрицы кода БЧХ длины 8 над $GF(3)$ с конструктивным расстоянием 2.

10.2. Найти выражения для порождающих многочленов всех кодов БЧХ длины 8 над $GF(3)$.

10.3. Найти выражения для всех порождающих многочленов, а также параметры всех двоичных кодов БЧХ в узком смысле длины 7.

10.4. Найти порождающие матрицы, кодовые слова и параметры кодов БЧХ в узком смысле длины 15, исправляющих 1, 3 и 5 ошибок.

10.5. Найти все кодовые слова минимального веса, содержащие 1 в первой координатной позиции, кода БЧХ с параметрами [15,7,5]. Поле Галуа представимо многочленом $f(x) = x^4 + x^3 + x^2 + x + 1$.

10.6. Сколько существует кодовых слов минимального веса в коде БЧХ длины 15, исправляющего 2 ошибки. Поле Галуа построено по модулю многочлена $f(x) = x^4 + x + 1$. Найти эти кодовые слова.

10.7. Доказать, что код Рида – Соломона с параметрами $[3, 2, 2]_4$ допускает двойную проверку на четность. Найти порождающие и проверочные многочлены этого кода, построить все три кода.

10.8. Пусть H — проверочная матрица кода Рида – Соломона с параметрами $[n, k, d]_q$. Доказать, что он допускает две проверки на четность, где первая проверка определяется как обычно, а вторая следующим образом: $\left(\begin{array}{cccccc|c} 1 & 1 & 1 & . & . & 1 & 1 \\ . & . & . & H & . & . & 0 \\ \alpha_1^{q-k} & . & . & . & . & \alpha_{q-1}^{q-k} & 1 \end{array}\right)$. Найти параметры кодов, полученных с помощью этих проверок.

10.9. Эквивалентны ли коды, заданные следующими проверочными матрицами:

$$\begin{pmatrix} 1 & \alpha & \alpha^2 & . & . & . & \alpha^{14} \\ 1 & \alpha^3 & \alpha^6 & . & . & . & \alpha^{3\times 14} \end{pmatrix} \text{ и}$$

$$\begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 & \alpha^8 & \alpha^9 & \alpha^{10} & \alpha^{11} & \alpha^{12} & \alpha^{13} & \alpha^{14} \\ \alpha^{12} & \alpha^9 & \alpha^6 & \alpha^3 & 1 & \alpha^{12} & \alpha^9 & \alpha^6 & \alpha^3 & 1 & \alpha^{12} & \alpha^9 & \alpha^6 & \alpha^3 & 1 \end{pmatrix}.$$

10.10. Найти параметры двоичного циклического кода длины 15 с порождающим многочленом a) $M^{(1)}(x)M^{(2)}(x)$; b) $M^{(1)}(x)M^{(3)}(x)$.

10.11. Пусть дан код БЧХ длины 15 с порождающим многочленом

$$g(x) = 1 + x^2 + x^5 + x^6 + x^8 + x^9 + x^{10},$$

поле Галуа $GF(2^4)$ построено по модулю многочлена $x^4 + x^3 + 1$. Сколько ошибок исправляет код?

10.12. Пусть дан код БЧХ длины 15 с порождающим многочленом

$$g(x) = 1 + x^2 + x^5 + x^6 + x^8 + x^9 + x^{10},$$

поле Галуа $GF(2^4)$ построено по модулю многочлена $x^4 + x^3 + 1$. Декодировать полученные ниже векторы, в каждом случае описать процедуры декодирования, найти векторы ошибок:

a) $x = (0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0)$;

b) $y = (0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0)$;

c) $z = (0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 1, 0, 0)$.

10.13. Пусть для передачи информации использован код из задачи 10.12. Декодировать полученные ниже векторы, в каждом случае описать процедуры декодирования, найти векторы ошибок:

a) $x = (0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1)$;

b) $y = (1, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0)$;

c) $z = (1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0)$.

10.14. Пусть C — циклический код длины n с таким порождающим многочленом $g(x)$, что для некоторых целых чисел $b \geq 0$, $\delta > 1$ выполняется

$$g(\alpha^b) = g(\alpha^{b+r}) = \ldots = g(\alpha^{b+(\delta-2)r}) = 0,$$

где числа r и n взаимно просты, α — примитивный элемент поля Галуа $GF(p^m)$. Доказать, что кодовое расстояние циклического кода не меньше δ.

11. Блок-схемы и коды

• $t-(n,k,\lambda)$ *блок-схемой* называется набор k-элементных подмножеств (именуемых блоками) n-элементного множества, такой что всякое t-элементное подмножество содержится ровно λ раз в k-элементных подмножествах.

• *Системой троек* $STS(n)$ *(четверок) Штейнера* ($SQS(n)$ соответственно) порядка n называется $2-(n,3,1)$ схема ($3-(n,4,1)$ схема соответственно).

• *Группой автоморфизмов* $t-(n,k,\lambda)$ *блок-схемы* называется максимальная группа подстановок n-элементного множества, стабилизирующая множество блоков схемы.

11.1. Доказать, что множество всех векторов веса 3 в двоичном (расширенном) совершенном коде длины n, содержащем нулевой вектор, образует систему троек (четверок) Штейнера порядка n.

11.2. Доказать, что множество всех векторов веса 3 в двоичном коде Хэмминга длины 7 образует проективную плоскость Фано.

11.3. Найти число различных систем троек Штейнера порядка 7.

11.4. Показать, что всякая система троек Штейнера порядка 7 вложима в совершенный код длины 7.

11.5. Доказать, что $STS(7)$ единственна с точностью до подстановки.

11.6. Найти все системы троек Штейнера порядка 7, не пересекающиеся с заданной.

11.7. Построить систему троек Штейнера порядка 9. Доказать ее единственность.

11.8. Найти порядки групп автоморфизмов $STS(7)$ и $STS(9)$.

11.9. Доказать, что множество всех векторов веса 3 в E^9 можно разбить на системы троек Штейнера порядка 9. Найти все эти системы.

11.10. Доказать, что $t-(n,k,\lambda)$ блок-схема является $(t-1)-(n,k,\lambda(n-t+1)/(k-t+1))$ блок-схемой.

11.11. Доказать, что для $t-(n,k,\lambda)$ блок-схемы с $n>k\geq 2$ имеет место *неравенство Фишера*: $|D|\geq n$.

11.12. Доказать, что не существует системы троек Штейнера порядка 12.

11.13. Доказать, что если система троек Штейнера существует, то ее порядок сравним с 1 и 3 по модулю 6.

11.14. Доказать, что если система четверок Штейнера существует, то ее порядок сравним с 2 и 4 по модулю 6.

11.15. Построить систему четверок Штейнера порядка 8, описать ее группу автоморфизмов.

11.16. Получить описание конструкции системы троек Штейнера порядка n, образованной кодовыми словами веса 3 в коде Васильева длины n.

11.17. Описать группу автоморфизмов системы троек Штейнера порядка n, образованной кодовыми словами минимального веса кода Хэмминга длины n. Привести подобное описание для систем четверок Штейнера порядка N, образованных кодовыми словами расширенного совершенного кода Хэмминга длины N.

11.18. Доказать, что если существуют системы троек Штейнера порядков n и m, то существует система троек Штейнера порядка nm, содержащая подсистемы, изоморфные системам порядков n и m. Найти эту систему.

• Код, у которого все кодовые слова имеют одинаковый вес, называется *равновесным*. Максимально возможная мощность двоичных равновесных кодов обозначается в литературе через $A(n,d,w)$, где n — длина кода, d — кодовое расстояние, а w — вес кодовых слов.

11.19. Доказать:

a) $A(n,2\delta-1,w)=A(n,2\delta,w)$;

b) $A(n,2\delta,w)=A(n,2\delta,n-w)$;

c) $A(n,2\delta,w)=1$, если $w<\delta$;

d) $A(n,2\delta,w)=\lfloor n/\delta\rfloor$;

e) $A(n,2,w)=C_n^w$.

11.20.* Доказать, что справедлива оценка Джонсона:

$$A(n,2\delta,w)=\left\lfloor\frac{\delta n}{w^2-wn+\delta n}\right\rfloor$$

при условии, что $w^2-wn+\delta n>0$.

11.21. Доказать справедливость оценок Джонсона:

a) $A(n,2\delta,w)\le\frac{n}{w}A(n-1,2\delta,w-1)$;

b) $A(n,2\delta,w)\le\frac{n}{n-w}A(n-1,2\delta,w)$.

11.22. Доказать $A(n,2\delta,w)\le\lceil\frac{n}{w}\lceil\frac{n-1}{w-1}\lceil\ldots\lceil\frac{n-w-\delta}{\delta}\rceil\ldots\rceil\rceil$.

11.23. Доказать, что справедливо $A(10,6,3)=3$, $A(10,6,4)=5$, $A(10,6,5)=6$, $A(11,6,4)=6$, $A(11,6,5)=11$, $A(12,6,4)=9$.

11.24.* Пусть $A(n,2\delta,w)=M$. Пусть целые числа k и t определены из равенства

$$wM=nk+t,0\le t<n.$$

Доказать справедливость оценки

$$nk(k-1)+2kt\le(w-\delta)M(M-1).$$

11.25. Найти $A(9,6,4)$ и $A(8,6,4)$.

11.26. Доказать, что справедливо $A(20,8,7)\le 80$.

11.27.* Доказать справедливость оценки Джонсона:

$$A(n,2\delta+1)(1+C_n^1+\ldots+C_n^\delta+\frac{C_n^{\delta+1}-C_{2\delta+1}^{\delta}A(n,2\delta+2,2\delta+1)}{\lceil\frac{n}{\delta+1}\rceil})\le 2^n.$$

11.28.* Доказать, что $A(12, 6, 5) = 12$.

11.29.* Доказать, что $A(13, 6, 5) = 18$.

11.30. Оценить сверху $A(12, 5)$.

11.31. Для четного n показать, что $A(n, 3) \leq 2^n/(n + 2)$.

11.32.* Доказать максимальность кода Препараты, т. е. показать, что двоичный код с параметрами $(n = 4^m, M = 2^n/m^2, d = 6)$, $m \geq 2$, является максимальным по мощности кодом длины $n = 4^m$, исправляющим 2 ошибки и обнаруживающим 3 ошибки.

12. Преобразование Адамара. Другие коды (коды Адамара, коды Рида – Маллера)

• *Матрицей Адамара* порядка n называется $(n \times n)$-матрица H, элементами которой являются $+1$ и -1, такая, что

$$H \cdot H^T = nE_n,$$

где E_n — единичная матрица размера $n \times n$.

12.1.^{0} Доказать, что любые две строки матрицы Адамара ортогональны (над полем действительных чисел).

12.2. Доказать, что для матрицы Адамара справедливо $\det H \cdot H^T = (\det H)^2 = n^n$.

12.3.^{0} Доказать, что матрицы Адамара порядков 2 и 4 единственны с точностью до эквивалентности.

12.4. Доказать, что если существует матрица Адамара порядка n, то n равно 1, 2 или кратно 4.

• *Прямым*, или *кронекеровым*, произведением двух матриц

$$A = (a_{ij}) \text{ порядка } m \times m \text{ и } B = (b_{ij}) \text{ порядка } n \times n$$

называется матрица $A \times B$ порядка $(mn \times mn)$:

$$A \times B = \begin{bmatrix} a_{11}B & a_{12}B & \dots & a_{1m}B \\ \cdot & \cdot & \cdot & \cdot \\ a_{m1}B & a_{m2}B & \dots & a_{mm}B \end{bmatrix}.$$

12.5. Доказать, что если существуют матрицы Адамара порядков m и n, то их прямое (кронекерово) произведение является матрицей Адамара порядка mn.

12.6. Для любого допустимого порядка построить матрицу Адамара по типу Сильвестра.

12.7. Найти связь между кодом Хэмминга и кодом Адамара, построенным из матрицы Адамара по типу Сильвестра.

12.8. Найти группу автоморфизмов кода Адамара, построенного из матрицы Адамара по типу Сильвестра.

• *Двоичный код Рида – Маллера* $\mathcal{RM}(r, m)$ порядка r, $0 \leq r \leq m$, – это совокупность векторов длины 2^m, отвечающих полиномам от m переменных степени не больше r.

12.9. Доказать, что код Рида – Маллера $\mathcal{RM}(1, m)$ первого порядка ортогонален расширенному коду Хэмминга и совпадает с кодом Адамара $\mathcal{B}_m$.

12.10. Доказать, что расширенный код Хэмминга является кодом Рида – Маллера $\mathcal{RM}(m-2, m)$ порядка $m-2$.

12.11. Найти размерность кода Рида – Маллера $\mathcal{RM}(r, m)$ порядка r.

12.12. Доказать, что код Рида – Маллера $\mathcal{RM}(r,m)$ любого порядка r, $0 \le r \le m$, может быть описан с помощью конструкции Плоткина.

12.13. Минимальное расстояние кода Рида – Маллера $\mathcal{RM}(r,m)$ порядка r, $0 \le r \le m$, равно $d = 2^{m-r}$.

12.14. Доказать, что для любых $r, 0 \le r \le (m-1)$, код Рида – Маллера $\mathcal{RM}(m-r-1,m)$ ортогонален коду Рида – Маллера $\mathcal{RM}(r,m)$.

12.15.* Доказать, что существует широкий класс кодов с параметрами кода Рида – Маллера, который можно получить применением конструкции Васильева.

• Пусть F — действительнозначный вектор длины $n = 2^m$, а H — матрица Адамара порядка n по типу Сильвестра. *Дискретным преобразованием Фурье - Адамара* (кратко *преобразованием Фурье – Адамара*) вектора F называется вектор

$$\hat{F} = FH,$$

где H — матрица Адамара. Часто удобно рассматривать матрицу Адамара по типу Сильвестра (матрицу Сильвестра).

12.16. Доказать, что матрица Сильвестра порядка $n = 2^m$ имеет следующее представление:

$$H_n = \{h_{ij}\}_{n\times n}, \text{ где } h_{ij} = (-1)^{\mathbf{uv}},$$

а $\mathbf{u}, \mathbf{v} \in E^m$.

12.17. Доказать формулу обращения для преобразования Фурье – Адамара:

$$F = \frac{1}{n}\hat{F}H.$$

• Пусть $f: E^m \to \{0,\ 1\}$ – произвольная булева функция, заданная на E^m. Этой функции отвечает двоичный вектор $\mathbf{f}$ длины $n = 2^m$, компоненты которого индексированы векторами из E^m: в позиции $\mathbf{u}$ стоит $f(\mathbf{u})$. Введем вектор $\mathbf{F}$, получающийся из $\mathbf{f}$ заменой 1 на –1 и 0 на 1. Таким образом, координата вектора $\mathbf{F}$, соответствующая вектору $\mathbf{u}$ из E^m, равна

$$F(\mathbf{u}) = (-1)^{f(\mathbf{u})},\ \mathbf{u} \in E^m.$$

Преобразование Фурье – Адамара вектора $\mathbf{F}$ примет вид

$$\hat{F}(\mathbf{u}) = \sum_{\mathbf{v}\in E^m} (-1)^{\mathbf{uv}} F(\mathbf{v}) = \sum_{\mathbf{v}\in E^m} (-1)^{\mathbf{uv}+f(\mathbf{v})},\ \mathbf{u} \in E^m.$$

Формула обращения примет вид

$$F(\mathbf{v}) = \frac{1}{2^m} \sum_{\mathbf{u}\in E^m} (-1)^{\mathbf{uv}} \hat{F}(\mathbf{u}),\ \mathbf{v} \in E^m.$$

12.18. Пусть $m = 2$, рассмотрим булеву функцию $f(v_1, v_2) = v_1 v_2$. Найти вектор $\mathbf{F}$, его преобразование Фурье – Адамара $\hat{F}$ и обращение этого преобразования.

12.19. Доказать, что коэффициенты преобразования Фурье – Адамара некоторого вектора F с координатами ± 1 удовлетворяют следующему свойству ортогональности:

$$\sum_{\mathbf{u}\in\mathbf{E^m}} \hat{F}(\mathbf{u})\hat{F}(\mathbf{u}+\mathbf{v}) = \begin{cases} 2^{2m}, & \text{если } \mathbf{v}=\mathbf{0}; \\ 0, & \text{если } \mathbf{v}\neq\mathbf{0}. \end{cases}$$

12.20. Доказать равенство Парсеваля:

$$\sum_{\mathbf{u}\in\mathbf{E^m}} \hat{F}^2(\mathbf{u}) = 2^{2m}.$$

12.21. Показать, что код Рида – Маллера первого порядка $R(1,m)$ состоит из всех векторов

$$\sum_{i=1}^{m} u_i\mathbf{v_i},\ u_i + u_0\mathbf{1} = 0 \text{ или } 1,$$

соответствующих линейным булевым функциям, определенным на E^m. Здесь через $\mathbf{v_i}$ обозначен вектор значений функции $f(x_1,x_2,\ldots,x_m)=x_i$ на множестве E^m.

12.22. Пусть $\mathcal{A}_m$ — линейный $[2^m, m, 2^{m-1}]$-код, состоящий из векторов вида $\sum\limits_{i=1}^{m} u_i\mathbf{v_i}$, $u_i \in \{0,\ 1\}$. Показать, что $R(1,m) = \mathcal{A}_m \cup \{1+\mathcal{A}_m\}$.

12.23. Доказать, что весовой спектр смежного класса по коду $R(1,m)$, содержащего вектор $\mathbf{f}$, равен

$$\frac{1}{2}\{2^m \pm \hat{\mathbf{F}}(\mathbf{u})\},\ \mathbf{u}\in E^m.$$

12.24. Пусть булевы функции от m переменных f и g связаны аффинным преобразованием, т. е. для некоторой двоичной обратимой матрицы $\mathbf{B}$ и некоторого булевого вектора $\mathbf{b}$ выполняется

$$g(\mathbf{v}) = f(\mathbf{Bv}+\mathbf{b}).$$

Доказать, что смежные классы, содержащие $\mathbf{f}$ и $\mathbf{g}$, имеют одинаковые весовые спектры.

12.25. Пусть C — двоичный линейный $[n,k]$-код, $C^\perp$ — ортогональный ему код, а f — произвольное вещественнозначное отображение, определенное на E^n. Доказать справедливость

$$\sum_{\mathbf{v}\in C^\perp} f(\mathbf{v}) = \frac{1}{|C|}\sum_{\mathbf{u}\in C}\hat{f}(\mathbf{u}).$$

12.26. Доказать справедливость соотношения

$$\prod_{i=1}^{n}(a_i+b_i) = \sum_{\mathbf{v}\in E^n}\prod_{i=1}^{n} a_i^{1-v_i}b_i^{v_i},$$

где $a_i, b_i \in \{0,1\}$.

12.27. Доказать теорему МакВильямс для линейных кодов: пусть C — двоичный линейный $[n,k]$-код. Тогда справедливо

$$W_{C^\perp}(x,y) = \frac{1}{|C|}W_C(x+y, x-y).$$

12.28. Доказать $W_C(x,y) = \frac{1}{|C^\perp|} W_{C^\perp}(x+y, x-y)$.

12.29. Найти явное выражение для весовой функции кода из задачи 12.18.

12.30. Найти явное выражение для весовой функции кода Хэмминга длины 7.

12.31. Найти явное выражение для весовой функции кода Хэмминга произвольной допустимой длины n.

• Многочлен $P_k(x,n) = \sum\limits_{j=0}^{k} \binom{x}{j} \binom{n-x}{k-j}$, $k = 0,1,2,\ldots$, от переменной x называется *многочленом Кравчука.*

12.32. Найти первые четыре многочлена Кравчука.

12.33. Доказать, что производящая функция многочленов Кравчука $P_k(x,n)$ имеет вид

$$(x+y)^{n-i}(x-y)^i = \sum_{k=0}^{n} P_k(i) x^{n-k} y^k.$$

12.34. Доказать, что весовой спектр дуального кода к линейному коду определяется следующими соотношениями:

$$A'_k = \frac{1}{|C|} \sum_{i=0}^{n} A_i P_k(i).$$

13. APN-функции

• Пусть $F : E^m \to E^m$ — функция, удовлетворяющая условию $F(0^m) = 0^m$. Функция F называется *APN-функцией* (*почти совершенно нелинейной*), если для любого $a \in E^m \setminus \{0^m\}$ и каждого $b \in E^m$ уравнение

$$F(x) + F(x + a) = b$$

имеет не более двух решений в E^m.

• Определим параметр $\delta(F)$ следующим образом:

$$\delta(F) = \max_{b \in E^m,\, a \in E^m \setminus \{0^m\}} |\{x \in E^m : F(x) + F(x + a) = b.$$

• Пусть $F : E^m \to E^m$ — функция. Для любого $a \in E^m$ *производная* F *по* a есть функция D_aF из E^m в E^m, определенная как

$$D_aF(x) = F(x) + F(x + a) \text{ для любого } x \in E^m.$$

13.1.^{0} Доказать, что $\delta(F) \geq 2$ для любой функции $F : E^m \to E^m$, удовлетворяющей условию $F(0^m) = 0^m$. Доказать, что функция, для которой достигается $\delta(F) = 2$, является APN-функцией.

13.2. Доказать, что функция $F : E^m \to E^m$, удовлетворяющая условию $F(0^m) = 0^m$, является APN-функцией, если ее ограничение до любой двумерной плоскости (т. е. аффинного подпространства) в E^m не является аффинным.

13.3. При каких m функция $F : E^m \to E^m$, удовлетворяющая $F : x \to x^3$, является APN-функцией? Какому коду отвечает эта функция?

13.4. Пусть функция $F : E^m \to E^m$ удовлетворяет $F(0^m) = 0^m$, $m \geq 4$. Пусть C_F — двоичный линейный код с проверочной матрицей

$$H_F = \begin{pmatrix} H_m \\ H_m^{(F)} \end{pmatrix} = \begin{pmatrix} \cdots & x & \cdots \\ \cdots & F(x) & \cdots \end{pmatrix},$$

где $x \in E^m$, $x \neq 0^m$, а H_m — проверочная матрица кода Хэмминга с m проверками на четность. Доказать, что размерность k кода C_F удовлетворяет неравенству $n - 2m \leq k \leq n - m$.

13.5. Является ли функция, отвечающая линейному коду с проверочной матрицей

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \end{pmatrix},$$

APN-функцией?

13.6. Доказать, что кодовое расстояние d_{C_F} кода C_F, определенного в задаче 13.4, удовлетворяет неравенствам $3 \leq d_{C_F} \leq 5$.

13.7.* Доказать, что функция F является APN-функцией тогда и только тогда, когда кодовое расстояние кода C_F, определенного в задаче 13.4, равно 5.

13.8.* Доказать, что если функция F является APN-функцией, то код C_F, определенный в задаче 13.4, имеет размерность $n - 2m$.

• Для любого двоичного кода C *радиус покрытия* ρ_C определяется как

$$\rho_C = \max_{x \in E^n} \min_{c \in C} \{d(x, C)\}.$$

13.9.* Доказать, что если функция F является APN-функцией, то код C_F, определенный в задаче 13.4, имеет радиус покрытия $\rho_C \in \{3, 4\}$.

• Введем отношение частичного порядка $\preceq$ на множестве функций $F : E^m \to E^m$ следующим образом: $F' \preceq F$, если код C'_F является подкодом кода C_F.

13.10. Пусть функция F является APN-функцией. Тогда любая функция F', удовлетворяющая $F' \preceq F$, является APN-функцией.

13.11. Пусть функция F является APN-функцией. Тогда единичный вектор не является кодовым словом кода $C_F^{\perp}$.

13.12. Доказать, что линейный код, заданный своей проверочной матрицей

$$\begin{pmatrix} 1 & \alpha & \alpha^2 & . & . & . & \alpha^{2^m-2} \\ 1 & \alpha^3 & \alpha^6 & . & . & . & \alpha^{3\times(2^m-2)} \end{pmatrix},$$

задает подстановочную APN-функцию для нечетного m, т. е. вторая строка этой матрицы является перестановкой первой. Доказать, что для каждого четного m код также задает APN-функцию, которая уже не является подстановочной функцией.

Глава II

Криптология

14. Элементы теории чисел

• *Функция Эйлера* $\varphi(n)$ определяется как количество чисел от 1 до n, взаимно простых с n. Если число n имеет каноническое разложение $n = p_1^{s_1} p_2^{s_2} \dots p_k^{s_k}$, то справедлива формула

$$\varphi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right).$$

Теорема (малая теорема Ферма). Если p — простое и a не делится на p, то

$$a^{p-1} \equiv 1 \pmod{p}.$$

Теорема (Эйлер). Если натуральные числа x и n взаимно просты и $n > 1$, то выполняется

$$x^{\varphi(n)} \equiv 1 \pmod{n}.$$

Теорема (китайская теорема об остатках). Если натуральные числа $m_1, m_2, \dots, m_k$ попарно взаимно просты, то система сравнений

$$x \equiv a_1 \pmod{m_1},\ x \equiv a_2 \pmod{m_2},\ \dots\ ,\ x \equiv a_k \pmod{m_k}$$

имеет единственное решение по модулю $n = m_1 m_2 \dots m_k$ при любых целых числах $a_1, a_2, \dots, a_k$.

14.1. Найти остатки от деления $1534^5 - 1$ на 9.

14.2. Найти остатки от деления:

a) 19^{10} на 66;

b) 19^{14} на 70;

c) 17^9 на 48;

d) $14^{14^{14}}$ на 100.

14.3. Пусть p — простое число. Доказать, что если $a \equiv b \pmod{p^n}$, то $a^p \equiv b^p \pmod{p^{n+1}}$.

14.4. Вычислить $128^{343} \pmod{527}$.

14.5. Пусть $(m, n) = 1$. Доказать, что сравнение $a \equiv b \pmod{mn}$ равносильно одновременному выполнению двух сравнений $a \equiv b \pmod{m}$ и $a \equiv b \pmod{n}$.

14.6. Доказать следующий *вариант теоремы Эйлера*: если p и q — простые числа, $p \neq q$, то $a^{k\varphi(pq)+1} \pmod{pq} = a$.

14.7. Доказать, что для любого нечетного числа n существует такое натуральное число m, что $2^m - 1$ делится на n.

14.8. Пусть p — простое число, а α — натуральное число. Чему равна сумма

$$\varphi(1) + \varphi(p) + \varphi(p^2) + \cdots + \varphi(p^\alpha)?$$

14.9. Доказать следующее эквивалентное малой теореме Ферма утверждение: если p — простое число, то для любого натурального a справедливо сравнение $a^p \equiv a \pmod{p}$.

14.10. Доказать, что если p и q — простые отличные друг от друга числа, то

$$p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}.$$

14.11. Решить сравнение:

a) $3x \equiv 8 \pmod{13}$;

b) $156x \equiv 41 \pmod{221}$;

c) $271x \equiv 25 \pmod{119}$.

14.12. Решить систему сравнений:

$$\begin{cases} 3x \equiv 1 \pmod{10}; \\ 4x \equiv 3 \pmod{5}; \\ 2x \equiv 7 \pmod{9}. \end{cases}$$

14.13. Решить в целых числах уравнение $45x - 37y = 25$.

15. Криптосистема Диффи и Хеллмана

Как открытое распределение ключей Диффи и Хеллмана, так и криптосистема Шамира базируются на сложности решения задачи дискретного логарифмирования.

• Пусть $y = \alpha^x \pmod p$ — показательная функция в конечном поле Галуа $GF(p)$. Функция *дискретного логарифма* определяется как $x = \log_\alpha y$, где $y \in GF(p)$.

Алгоритм формирования общего секретного ключа с помощью криптосистемы Диффи и Хеллмана

Для работы алгоритма обе стороны совместно устанавливают открытые параметры p и g (обычно значения p и g выбираются на одной стороне и передаются другой), где p является случайным простым числом, а g — примитивным элементом поля Галуа $GF(p)$.

1. Алиса выбирает произвольное натуральное число x_A такое, что $1 < x_A < p - 1$.
2. Боб выбирает произвольное натуральное число x_B такое, что $1 < x_B < p - 1$.
3. Алиса вычисляет открытый ключ $y_A = g^{x_A} \pmod p$ и передает его Бобу по открытому каналу связи.
4. Боб вычисляет открытый ключ $y_B = g^{x_B} \pmod p$ и передает его Алисе по открытому каналу связи.
5. Алиса с помощью полученного открытого ключа y_B вычисляет общий секретный ключ $K = y_B^{x_A} \pmod p$.
6. Боб с помощью полученного открытого ключа y_A вычисляет общий секретный ключ $K = y_A^{x_B} \pmod p$.

В практических реализациях в качестве чисел x_A и x_B используются числа порядка 10^{100} и p порядка 10^{300}. Число g не обязано быть большим и обычно имеет значение в пределах первого десятка.

15.1. Найти дискретный логарифм числа 7 по основанию 2 в группе $G = Z_{19}$.

15.2. Пусть $\alpha \in GF(3^2)$ — примитивный элемент поля $GF(3^2)$, построенного с помощью неприводимого многочлена $x^2 - x - 1$. Найти дискретный логарифм элемента -1 по основанию α.

15.3. Можно ли в алгоритме открытого распределения ключей Диффи и Хеллмана вместо $GF(p)$ брать $GF(p^k)$?

15.4. Доказать криптостойкость открытого распределения ключей Диффи и Хеллмана.

15.5. Пусть открытый ключ равен $\{GF(37), 2\}$. Каким образом Алиса и Боб создадут секретный ключ?

15.6. Пусть открытый ключ $\{GF(3^3), \alpha\}$, где α — корень примитивного многочлена $f(x)$. Используя открытое распределение ключей Диффи и Хеллмана, получить общий секретный ключ, если Алиса задумала число 7, а Боб — число 5. Даны следующие многочлены:

a) $f(x) = x^3 + x^2 - 1$;

b) $f(x) = x^3 - x^2 + 1$.

15.7. Описать алгоритм открытого распределения ключей на основе использования двух коммутативных подполугрупп некоторой некоммутативной полугруппы G большого порядка. Открытый ключ $\{G, \sigma\}$, где σ — элемент полугруппы G. Обосновать сложность вычисления общего ключа.

16. Криптосистема Шамира

Алгоритм шифрования криптосистемы Шамира

Для работы алгоритма на основе задачи дискретного логарифмирования обе стороны совместно устанавливают общий открытый ключ p, где p является случайным простым числом. Сообщения m представляются целыми числами из интервала $1 < m < p$.

1. Алиса выбирает натуральные взаимно обратные по модулю $p-1$ числа x_A и y_A, принадлежащие интервалу $1 < x_A < p$, $1 < y_A < p$, т. е. удовлетворяющие условию $x_A \cdot y_A \equiv 1 \pmod{p-1}$.

2. Боб аналогично и независимо выбирает натуральные взаимно обратные по модулю $p-1$ числа x_B и y_B из интервала $1 < x_B < p$, $1 < y_B < p$, т. е. удовлетворяющие условию $x_B \cdot y_B \equiv 1 \pmod{p-1}$.

3. Для передачи сообщения m Алиса вычисляет $x_1 = m^{x_A} \pmod{p}$ и передает его Бобу по открытому каналу связи.

4. Боб вычисляет $x_2 = x_1^{x_B} \pmod{p}$ и передает его Алисе по открытому каналу связи.

5. Алиса вычисляет $x_3 = x_2^{y_A} \pmod{p}$ и снова передает его Бобу по открытому каналу связи.

6. Боб вычисляет
$$x_4 \equiv x_3^{y_B} \pmod{p}.$$

16.1. Доказать, что для криптосистемы Шамира $x_4 \equiv m \pmod{p}$.

16.2. Передать секретно сообщение m, используя криптосистему Шамира, если задан открытый ключ p:

a) $m = 2$, $p = 13$;

b) $m = 17$, $p = 23$;

c) $m = 20$, $p = 31$.

16.3. Описать алгоритм Шамира для конечной циклической группы G с порождающим элементом g.

16.4. Можно ли задать алгоритм Шамира для:

a) группы вычетов по модулю простого числа;

b) группы эллиптических кривых простого порядка;

c) циклических подгрупп большого порядка в Z_n, где n — составное?

16.5. Обосновать криптостойкость алгоритма Шамира.

16.6. В чем состоят положительные и отрицательные свойства криптосистемы Шамира?

17. Криптосистема Эль-Гамаля

Схема Эль-Гамаля является криптосистемой с открытым ключом, основанной на трудности вычисления дискретного логарифма в конечном поле. Криптосистема включает алгоритм шифрования и алгоритм цифровой подписи. Схема была предложена Тахером Эль-Гамалем в 1984 г. и лежит в основе стандартов электронной цифровой подписи в США (DSA) и России (ГОСТ Р 34.10-94).

Алгоритм шифрования криптосистемы Эль-Гамаля

Процесс генерации ключей заключается в следующих действиях.

1. Генерируется случайное простое число p.
2. Выбирается случайный примитивный элемент g поля $\mathbb{Z}_p$.
3. Выбирается случайное целое число x такое, что $1 < x < p - 1$.
4. Вычисляется $y = g^x \pmod{p}$.

В результате публичным ключом является тройка (p, g, y), а секретным ключом — число x. Далее сообщение m шифруется следующим образом.

5. Выбирается сессионный ключ — случайное целое число k такое, что $1 < k < p - 1$.
6. Вычисляются числа $a = g^k \pmod{p}$ и $b = y^k \cdot m \pmod{p}$.

Пара чисел (a, b) является шифротекстом.

Зная секретный ключ x, исходное сообщение можно вычислить из шифротекста (a, b) по формуле $m = b \cdot (a^x)^{-1} \pmod{p}$.

17.1. Доказать, что длина шифротекста в схеме Эль-Гамаля вдвое длиннее исходного сообщения.

17.2. Обосновать криптостойкость алгоритма шифрования Эль-Гамаля.

17.3. Описать алгоритм дешифрования криптосистемы Эль-Гамаля. Обосновать криптостойкость.

17.4. Пусть $K_{open} = \{p = 29, g = 3\}$ и $K_{B.,secret} = \{c_B = 13\}$. Как Алиса передаст сообщение $m = 11$ Бобу (пусть для шифрования она выбирает $k = 2$, где $1 < k < p - 1$)?

17.5. Провести шифрование с помощью схемы Эль-Гамаля при следующих значениях параметров:

a) $p = 11$, $g = 2$;

b) $p = 23$, $g = 5$.

17.6. Доказать, что, применяя алгоритм дешифрования схемы Эль-Гамаля, получатель восстановит исходное сообщение.

Электронная подпись на криптосистеме Эль-Гамаля

Использование электронной подписи позволяет осуществлять контроль целостности передаваемого документа, защиту от изменений или подделки документа, невозможность отказа от авторства, а также подтверждение авторства документа.

Подпись сообщений

Для подписи сообщения m выполняются следующие операции.

1. Выбирается случайное число $1 < k < p-1$ взаимно простое с $p-1$ и вычисляется $r = g^k \pmod{p}$.
2. Вычисляется число $s = (m - xr)k^{-1} \pmod{p-1}$.

Подписью сообщения m является пара (r, s).

17.7. Обосновать криптостойкость электронной подписи на основе криптосистемы Эль-Гамаля.

17.8. Описать и обосновать процедуру проверки подписи сообщения для криптосистемы Эль-Гамаля.

17.9. Сформировать электронную подпись на основе схемы Эль-Гамаля при заданных параметрах p и g с помощью секретного ключа x. Осуществить проверку подлинности сообщения m:

a) $p = 23$, $g = 5$, $x = 7$, $m = 3$;

b) $p = 29$, $g = 7$, $x = 3$, $m = 2$.

18. Криптосистема RSA

RSA — криптографический алгоритм с открытым ключом, основывающийся на вычислительной сложности задачи факторизации больших целых чисел. Аббревиатура RSA образована из первых букв фамилий трех ученых R. Rivest, A. Shamir и L. Adleman, разработавших данную систему шифрования в 1978 г.

Алгоритм шифрования криптосистемы RSA

Алгоритм шифрования RSA основан на следующей процедуре.

1. Генерация двух различных простых чисел p и q.
2. Вычисление числа $n = p \cdot q$ и функции Эйлера $\varphi(n) = (p-1) \cdot (q-1)$.
3. Поиск целого числа e, $1 < e < \varphi(n)$, такого, чтобы НОД$(e, \varphi(n)) = 1$.

Сообщение в этой системе представлено в виде числа, принадлежащего интервалу $[0, n-1]$. Шифруемый текст произвольным обратимым способом преобразовывается в сообщения (числа, принадлежащие интервалу $[0, n-1]$). Чтобы зашифровать текст, для каждого сообщения m необходимо вычислить $c = m^e \pmod{n}$.

18.1. Описать алгоритм дешифрования криптосистемы RSA.

18.2. Доказать, что, применяя алгоритм дешифрования криптосистемы RSA, получатель восстановит исходное сообщение. Обосновать криптостойкость данной криптосистемы.

18.3. Провести шифрование в системе RSA при следующих значениях параметров:

a) $p = 7$, $q = 11$;

b) $p = 11$, $q = 13$.

18.4. Для передачи секретной информации выбрана криптосистема RSA. Используя открытый ключ $\{n, e\}$, передать Алисе секретное сообщение m. Дешифровать его с помощью секретного ключа. Даны следующие параметры криптосистемы:

a) $p = 11$, $q = 17$, $e = 9$, $m = 3$;

b) $p = 17$, $q = 31$, $e = 7$, $m = 2$;

c) $p = 5$, $q = 11$, $e = 3$, $m = 9$;

d) $p = 3$, $q = 11$, $e = 3$, $m = 8$.

18.5. Доказать, что в системах RSA с модулями $n_1 = 21$ и $n_2 = 35$ все возможные ключи шифрования e совпадают с ключами дешифрования d.

18.6. При шифровании в системе RSA $(n = pq, e, d)$ оказалось, что повторное шифрование всегда приводит к исходному тексту. В чем причина? Привести пример конечного простого поля, в котором это свойство выполнено для любого числа e.

Электронная подпись на криптосистеме RSA

Отметим, что схема RSA обладает двумя дополнительными очень полезными свойствами.

1. Множество исходных сообщений S совпадает с множеством закодированных сообщений T. В качестве этого множества используется кольцо вычетов по модулю n, где n — произведение двух больших простых чисел (десятичная запись числа n имеет длину не меньше 200 символов).

2. Не только $e \cdot d = 1$, но и $d \cdot e = 1$! Таким образом, владелец секретного ключа d может применять его не только для дешифрования, но и для шифрования. При этом любой может декодировать это сообщение, используя открытый ключ e, но послать его может только владелец секретного ключа d. Такая «обратная» схема применения открытого ключа позволяет удостоверить отправителя сообщения. В практических применениях для аутентификации отправителя обратная схема даже более важна, чем прямая.

18.7. Для электронной подписи используется криптосистема RSA. Секретный ключ банкира Боба составляют числа p_B и q_B, а секретный ключ вкладчика Алисы — числа p_A и q_A. Пусть открытыми ключами Боба и Алисы являются пары $\{n_B = p_B \cdot q_B, e_B\}$ и $\{n_A = p_A \cdot q_A, e_A\}$ соответственно, где $(e_B, \varphi(n_B)) = (e_A, \varphi(n_A)) = 1$. Необходимо передать Бобу секретное поручение m от Алисы, а также удостовериться в подлинности данного сообщения. Даны следующие значения параметров криптосистемы:

a) $p_A = 11$, $q_A = 23$, $e_A = 31$, $p_B = 7$, $q_B = 13$, $e_B = 5$, $m = 41$;

b) $p_A = 7$, $q_A = 11$, $e_A = 7$, $p_B = 3$, $q_B = 5$, $e_B = 7$, $m = 13$;

c) $p_A = 11$, $q_A = 2$, $e_A = 3$, $p_B = 5$, $q_B = 3$, $e_B = 7$, $m = 3$.

18.8. Алиса и Боб используют различные системы RSA с общим модулем n и публичными экспонентами шифрования e_A и e_B (держат в секрете свои экспоненты дешифрования d_A и d_B).

1. Доказать, что Алиса может дешифровывать сообщения, посланные Бобу.

2. Кроме того, показать, что криптоаналитик Ева может дешифровывать сообщения, посланные Алисе и Бобу, если НОД$(e_A, e_B) = 1$.

Открытые сообщения

При использовании алгоритма криптосистемы RSA существуют такие значения e и m, что $m^e \pmod n = m$. Сообщения m, для которых $m^e \pmod n = m$, называются *открытыми*. Проблема выбора e состоит в том, что не должно быть слишком много открытых сообщений.

Пример 18.1. Пусть $p = 19$ и $q = 37$. Тогда $n = 19 \cdot 37 = 703$ и $\varphi(n) = 18 \cdot 36 = 648$. Если выберем $e = 181$, то, несмотря на то, что НОД$(181, 648) = 1$, окажется, что все возможные сообщения m $(0 \leq m \leq n - 1)$ будут открытыми после вычисления $m^e \pmod n$.

Для любого верного выбора e существуют некоторые открытые сообщения. Важно, чтобы число таких открытых сообщений было минимальным.

18.9. Задача из проекта Эйлера № 182[1]**.** Дано: $p = 1009$ и $q = 3643$. Найдите сумму всех значений e, $1 < e < \varphi(p \cdot q)$ и НОД$(e, \varphi(p \cdot q)) = 1$, для которых число открытых сообщений будет минимальным.

18.10. Показать, что число открытых сообщений равно

$$(1 + \text{НОД}(p-1)(e-1))(1 + \text{НОД}(q-1)(e-1)).$$

Какие рекомендации могут быть выработаны для правильного выбора параметров p, q и e?

18.11. Нерешенная проблема. Существует гипотеза, подтвержденная некоторыми косвенными соображениями, что задача RSA на самом деле легче задачи факторизации. В настоящее время проверка этой гипотезы — один из открытых вопросов криптологии.

[1]URL: `http://projecteuler.net/index.php?section=problems&id=182`

19. Криптосистема Меркля – Хеллмана

Ранцевая криптосистема Меркла – Хеллмана, основанная на «задаче о рюкзаке», была разработана Ральфом Мерклем и Мартином Хеллманом в 1978 г.

Условие «задачи о рюкзаке» заключается в следующем: зная подмножество грузов, уложенных в ранец, легко подсчитать суммарный вес рюкзака, но, зная вместимость рюкзака, непросто определить подмножество грузов, наполняющих его.

Генерация ключей

1. Алиса выбирает супервозрастающую последовательность из n ненулевых натуральных чисел $w = (w_1, w_2, \ldots, w_n)$, т. е. такую, что каждый последующий член последовательности больше суммы всех предыдущих.

2. Далее Алиса случайным образом выбирает целые взаимно простые числа q и r такие, что $q > \sum_{i=1}^{n} w_i$.

3. Алиса вычисляет последовательность $a = (a_1, a_2, \ldots, a_n)$, где каждый член последовательности определяется по формуле $a_i = r \cdot w_i \pmod{q}$.

Таким образом, открытым ключом будет последовательность a. Секретным ключом является набор (w, q, r).

Шифрование сообщения

Пусть Бобу необходимо передать Алисе сообщение $m = (m_1, m_2, \ldots, m_n)$, представленное в виде двоичного вектора длины n.

$\star$ Боб вычисляет шифротекст $s = \sum_{i=1}^{n} a_i m_i$ и передает его Алисе.

19.1. Пусть вектор груза w и вес рюкзака S, найти вектор a, удовлетворяющий $S = wa$:

a) $w = (171, 197, 459, 1191, 2410)$, $S = 3798$;

b) $w = (2, 3, 7, 15, 31)$, $S = 24$.

19.2. Описать алгоритм дешифрования сообщения для криптосистемы Меркля – Хеллмана.

19.3. Пусть элементами открытого текста являются буквы латинского алфавита от 0 до 25, которым отвечают двоичные числа от $0 = (0, 0, 0, 0, 0)$ до $25 = (1, 0, 0, 1, 1)$ соответственно. Пусть секретный ключ дан выше, см. задачу 19.1 b). Пусть $q = 61$, что удовлетворяет $q > \sum_{i=1}^{5} W_i$, пусть $r = 17$. Найти секретный и открытый ключ Алисы и описать передачу сообщения «WHY».

19.4. Пусть для передачи информации используется криптосистема, основанная на «задаче о рюкзаке». Часть вашего секретного ключа составляют супервозрастающий вектор $w = (1, 2, 4, 9, 17, 34)$, число $q = 69$ и число $r = 31$. Каждая буква русского алфавита (без буквы «ё») кодируется двоичным набором длины 6, соответствующим порядковому номеру буквы (буква «а» имеет номер 1). Считаем, что первый бит в наборе является старшим. При шифровании, используя открытый ключ, отправитель каждой букве сопоставил целое число.

a) Найти открытый и полный секретный ключи.

b) Дешифровать сообщение $x = 62, 19, 81, 121, 58, 180$. Определить переданное слово.

19.5. Пусть для передачи информации используется криптосистема, основанная на «задаче о рюкзаке». Часть вашего секретного ключа составляют супервозрастающий вектор $w = (3, 5, 9, 19, 45)$, число $q = 100$ и число $r = 21$. Каждая буква русского алфавита (без буквы «ё») кодируется двоичным набором длины 6, соответствующим порядковому номеру буквы (буква «а» имеет номер 1). Считаем, что первый бит в наборе является старшим. При шифровании, используя открытый ключ, отправитель каждой букве сопоставил целое число.

a) Найти открытый и полный секретный ключи.

b) Дешифровать сообщение $x = 193, 104, 162, 301, 45, 63, 167$. Определить переданное слово.

19.6. Пусть для передачи информации используется криптосистема, основанная на «задаче о рюкзаке». Часть вашего секретного ключа составляют супервозрастающий вектор $a' = (1, 2, 4, 9, 18, 35)$, число $q = 80$, а число $r = 29$. Каждая буква русского алфавита (без буквы «ё») кодируется двоичным набором длины 6, соответствующим порядковому номеру буквы (буква «а» имеет номер 1). Считаем, что первый бит в наборе является старшим. При шифровании, используя открытый ключ, отправитель каждой букве сопоставил целое число.

a) Найти открытый и полный секретный ключи.

b) Дешифровать сообщение $x = 55, 97, 21, 79, 100, 155$. Определить переданное слово.

19.7. В чем состоит слабость криптосистемы Меркля – Хэллмана?

20. Криптосистема на эллиптических кривых

В криптографии с использованием эллиптических кривых все значения вычисляются по модулю p, где p является простым числом. Элементами эллиптической кривой являются пары неотрицательных целых чисел, которые меньше p и удовлетворяют частному виду уравнения эллиптической кривой: $y^2 = x^3 + ax + b \pmod p$. Такую кривую будем обозначать $E_p(a, b)$. При этом числа a и b должны быть меньше p и удовлетворять условию $4a^3 + 27b^2 \pmod p \neq 0$. Множество точек на эллиптической кривой вычисляется следующим образом.

1. Для каждого такого значения x, что $0 \leq x \leq p$, вычисляется $x^3+ax+b \pmod p$.
2. Для каждого из полученных на предыдущем шаге значений выясняется, имеет ли это значение квадратный корень по модулю p. Если нет, то в $E_p(a, b)$ нет точек с этим значением x. Если корень существует, имеется два значения y, соответствующих операции извлечения квадратного корня (исключением является случай, когда единственным значением оказывается $y = 0$). Эти значения (x, y) и будут точками кривой $E_p(a, b)$.

Множество точек $E_p(a, b)$ обладает следующими свойствами.

1. $P + 0 = P$.
2. Если $P = (x, y)$, то $P + (x, -y) = 0$. Точка $(x, -y)$ является отрицательным значением точки P и обозначается $-P$. Заметим, что $(x, -y)$ лежит на эллиптической кривой и принадлежит $E_p(a, b)$.
3. Если $P = (x_1, y_1)$ и $Q = (x_2, y_2)$, где $P \neq Q$, то $R = P+Q = (x_3, y_3)$ определяется по следующим формулам:

$$x_3 = \lambda^2 - x_1 - x_2 \pmod p,$$

$$y_3 = \lambda(x_1 - x_3) - y_1 \pmod p,$$

где

$$\lambda = \begin{cases} (y_2 - y_1)/(x_2 - x_1), & \text{если } P \neq Q, \\ (3x_1^2 + a)/2y_1, & \text{если } P = Q. \end{cases}$$

Число λ есть угловой коэффициент секущей, проведенной через точки $P = (x_1, y_1)$ и $Q = (x_2, y_2)$. При $P = Q$ секущая превращается в касательную, чем и объясняется наличие двух формул для вычисления λ.

Задача, которую должен решить в этом случае атакующий, является своего рода задачей *дискретного логарифмирования на эллиптической кривой*, и формулируется она следующим образом. Даны точки P и Q на эллиптической кривой $E_p(a, b)$. Необходимо найти коэффициент $k < p$ такой, что $P = [k]Q$. Точку P по данным k и Q вычислить относительно легко, но довольно трудно вычислить k, зная точки P и Q.

20.1. Описать аналог алгоритма Диффи – Хеллмана на эллиптических кривых.

20.2. Описать процедуру шифрования и дешифрования с использованием эллиптических кривых.

20.3.^{0} Даны точки P, Q и R на эллиптической кривой $E_{751}(-1,1)$. Найти точку $[2]P+[3]Q-R$:

a) $P=(58,139)$, $Q=(67,667)$, $R=(82,481)$;

b) $P=(73,72)$, $Q=(56,332)$, $R=(85,35)$;

c) $P=(62,379)$, $Q=(53,474)$, $R=(110,622)$.

20.4.^{0} Дана точка P на эллиптической кривой $E_{751}(-1,1)$ и натуральное число n. Найти точку $[n]P$:

a) $P=(62,372)$, $n=128$;

b) $P=(33,355)$, $n=111$;

c) $P=(73,72)$, $n=103$.

Теорема (Хассе, 1934 г.) Число точек $\#E_p(a,b)$ эллиптической кривой $E_p(a,b)$ удовлетворяет неравенству

$$p-1+2\sqrt{p}\le \#E_p(a,b)\le p+1+2\sqrt{p}.$$

20.5.^{0} Найти все точки эллиптической кривой

a) $E_7(2,6)$;

b) $E_{11}(5,7)$.

20.6. Дана эллиптическая кривая $E_{11}(2,9)$ и принадлежащая ей точка $G=(1,1)$. Передать секретно сообщение $m=5$ от Алисы Бобу при условии, что выбраны секретные ключи $c_A=3$ и $c_B=4$.

20.7. Пусть эллиптическая кривая $E_{11}(2,9)$ над $GF(2^4)$ (поле задано многочленом x^4+x^3+1) определена уравнением $y^2=x^3+\alpha x+1$. Лежит ли точка (α^2,α^{14}) на эллиптической кривой? Сколько точек лежит на этой кривой?

20.8. Рассмотрим кривую $y^2+xy=x^3+x^2+1$ над полем $GF(2^5)$, заданным многочленом x^5+x^2+1. Убедиться, что точка $P=(00101,10110)$ лежит на эллиптической кривой. Найти ее порядок. Найти k, где $kP=(01101,00101)$.

20.9. Поле $GF(2^m)$ задано посредством многочлена $f(x)$, $g=x$ — примитивный элемент поля $GF(2^m)$. Найти множество точек эллиптической кривой $y^2+xy=x^3+ax^2+b$, где:

a) $m=3$, $f(x)=x^3+x+1$, $a=g^3$, $b=g^0=1$;

b) $m=4$, $f(x)=x^4+x+1$, $a=g^4$, $b=g^0=1$.

20.10. Для задачи 20.9 b) придумать открытый ключ, открытый и секретный ключи Боба. Передать сообщение $(0,1,1,0)$ Бобу. Как он дешифрует это сообщение?

20.11. Для задачи 20.9 b) пусть открытый ключ имеет вид $K_{open}=\{GF(2^4), a=g^4=(0,0,1,1), b=g^0=(0,0,0,1), (.)G=(g^5,g^3)\}$, $K_{Bsecret}=\{c_B=3\}$. Найти открытый ключ Боба и передать сообщение $(0,0,1,0)$ Бобу. Дешифровать это сообщение.

Электронная подпись на эллиптических кривых

Для электронной подписи сообщений с помощью криптосистемы на эллиптических кривых, как и в случае использовния других криптосистем, необходимы открытый и секретный ключи. При этом секретным ключом должен обладать только тот, кто подписывает сообщение, в то время как открытый ключ должен быть в свободном доступе для любого желающего удостовериться в подлинности сообщения. Следует отметить, что, несмотря на свободный доступ к открытому ключу, средства его публикации не должно вызывать сомнений в его происхождении. Также общедоступными являются параметры самого алгоритма, т. е. эллиптическая кривая $E_p(a,b)$ и точка этой кривой G.

Допустим, что владельцем криптосистемы является Алиса, а задача Боба убедиться в подлинности сообщения m от Алисы. При формировании криптосистемы Алиса выбрала свой секретный ключ и опубликовала открытый ключ $D = [c]G$.

Подпись сообщений

Для подписи сообщения m выполняются следующие операции.

1. Алиса выбирает случайное число $0 < k < q$, взаимно простое с $q-1$, где простое число q — порядок циклической подгруппы, порожденной точкой G, группы точек эллиптической кривой $E_p(a,b)$.

2. Алиса вычисляет точку $[k]G = (x,y)$ и число $r = x \pmod q$.

3. Алиса вычисляет число $s = (m + cr)k^{-1} \pmod q$.

Подписью сообщения m является пара (r,s). Заметим, что если число r или s получилось равным нулю, то необходимо выполнить все процедуры заново, выбрав новое число k.

20.12. Обосновать криптостойкость электронной подписи на основе криптосистемы на эллиптических кривых.

20.13. Описать и обосновать процедуру проверки электронной подписи сообщения для криптосистемы на эллиптических кривых.

20.14. Вычислить электронную подпись сообщения m и проверить его подлинность с помощью криптосистемы на эллиптической кривой $E_p(a,b)$ при условии, что Алиса выбрала секретный ключ c и порождающую точку G, а также задан порядок q группы точек.

a) Параметры кривой: $a = 1$, $b = 1$, $p = 11$. Порядок подгруппы точек: $q = 7$. Точка $G = (0,1)$. Секретный ключ $c = 4$. Случайное число Алисы $k = 5$. Сообщение $m = 5$.

b) Параметры кривой: $a = 2$, $b = 6$, $p = 11$. Точка $G = (10,5)$. Секретный ключ $c = 5$. Случайное число Алисы $k = 4$. Сообщение $m = 10$.

c) Параметры кривой: $a = 2$, $b = 7$, $p = 11$. Точка $G = (7,10)$. Секретный ключ $c = 6$. Случайное число Алисы $k = 5$. Сообщение $m = 2$.

21. Криптосистема Мак-Элиса

В основе криптосистемы Мак-Элиса, разработанной в 1978 г. Робертом Мак-Элисом, лежит теория линейных кодов. Это была первая схема, использующая рандомизацию в процессе шифрования. Алгоритм основан на сложности декодирования линейных кодов (общая задача декодирования является NP-сложной).

Для описания закрытого ключа выбран линейный код, исправляющий t ошибок, для которого известен эффективный алгоритм декодирования. Алгоритм использует двоичные коды Гоппы, которые эффективно декодируются благодаря алгоритму Питерсона. Открытый ключ получается при помощи маскировки выбранного кода как произвольного линейного кода с данными параметрами. Для этого порождающая матрица умножается на две случайные невырожденные матрицы S и P над полем $GF(q)$ (см. схему шифрования).

Алгоритм шифрования криптосистемы Мак-Элиса

Пользователи системы совместно используют параметры безопасности: n — длина кода; k — размерность кода; t — число исправляемых кодом ошибок. Все вычисления осуществляются в k-мерном подпространстве n-мерного векторного пространства $\mathbb{F}_2^n$ над полем Галуа $GF(2)$.

Генерация ключей

1. Алиса выбирает двоичный $[n, k]$-линейный код C, исправляющий t ошибок. Для кода C выбирается произвольная порождающая матрица G.
2. Для того чтобы исходный код было сложно восстановить, Алиса генерирует случайную $(k \times k)$-невырожденную матрицу S.
3. Алиса генерирует случайную $(n \times n)$-матрицу перестановки P.
4. Алиса вычисляет $(k \times n)$-матрицу $G' = SGP$.

Таким образом, открытым ключом является пара (G', t), а секретным ключом — набор (S, G, P).

Шифрование сообщения

Пусть Боб хочет передать Алисе сообщение m, представленное в виде двоичного вектора длины k.

1. Боб вычисляет вектор $c' = mG'$.
2. Боб генерирует случайный вектор ошибок z длины n, имеющий вес не более t.
3. Боб вычисляет шифротекст как $c = c' + z$ и передает его Алисе.

21.1. Описать алгоритм дешифрования сообщения с помощью криптосиситемы Мак-Элиса.

21.2. Доказать корректность алгоритма дешифрования криптосистемы Мак-Элиса.

21.3. Пусть для передачи информации используется криптосистема Мак-Элиса. Ваш секретный ключ составляют невырожденная матрица S, порождающая матрица G и матрица P, соответствующая перестановке π.

Секретная информация представлена двоичными блоками длины 3.

a) Найти открытый ключ криптосистемы. Дешифровать полученное сообщение $x = (101100)$ и восстановить секретную информацию при условии, что ваш секретный ключ составляют матрицы

$$S = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}, G = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

и перестановка $\pi = (142536)$.

b) Передать секретную информацию $m = (100)$ при условии, что ваш секретный ключ составляют матрицы

$$S = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \end{pmatrix}, G = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$$

и перестановка $\pi = (1346752)$.

21.4. Передать секретно сообщение $m = (1101)$ с помощью криптосистемы Мак-Элиса, если для ее построения необходимо использовать порождающую матрицу кода Хэмминга длины 7, заданную в канонической форме, а также перестановку $\pi = (4152763)$ и невырожденную матрицу

$$S = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix}.$$

21.5. Пусть для передачи информации используется криптосистема Мак-Элиса. Ваш секретный ключ составляют невырожденная матрица S, порождающая матрица G:

$$S = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \; G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$$

и матрица P, соответствующая подстановке $\pi = (13578642)$. Секретная информация кодируется с помощью открытого ключа двоичными блоками длины 4. Каждый блок представляет собой двоичную запись некоторого числа от 0 до 15.

a) Найти открытый ключ криптосистемы.

b) Дешифровать полученное сообщение $x = (10111100)$ и восстановить секретную информацию.

21.6. Описать генерацию ключей и алгоритмы шифрования и дешифрования сообщений с помощью криптосистемы Мак-Элиса, используя произвольный q-значный код, исправляющий достаточно большое количество ошибок t.

21.7. Описать передачу информации с помощью криптосистемы Мак-Элиса, используя код Хэмминга длины 6 над $GF(5)$. Сообщение m, невырожденную матрицу S, перестановочную и диагональную матрицы выбрать по своему усмотрению. Описать процедуру дешифрования.

21.8. Описать передачу информации с помощью криптосистемы Мак-Элиса, используя двоичный код БЧХ длины 15 с кодовым расстоянием 7. Сообщение m, невырожденную матрицу S и перестановку выбрать по своему усмотрению. Описать процедуру дешифрования.

22. Криптосистема Нидеррайтера

Пользователи системы совместно используют параметры безопасности: n — длина кода; k — размерность кода; t — число исправляемых кодом ошибок. Все вычисления осуществляются в k-мерном подпространстве n-мерного векторного пространства $\mathbb{F}_q^n$ над полем Галуа $GF(q)$, где q — степень просто числа.

Генерация ключей

1. Алиса выбирает линейный $[n,k]$-код C, исправляющий t ошибок. Для кода C выбирается произвольная проверочная матрица размера $r \times n$, где $r = n - k$.

2. Для того чтобы исходный код было сложно восстановить, Алиса генерирует случайную невырожденную $(r \times r)$-матрицу S над полем Галуа $GF(q)$.

3. Алиса генерирует случайную диагональную $(n \times n)$-матрицу D над полем Галуа $GF(q)$.

4. Алиса генерирует случайную $(n \times n)$-матрицу перестановки P над полем Галуа $GF(2)$.

5. Алиса вычисляет $r \times n$ матрицу $H' = SHDP$.

Таким образом, открытым ключом является пара (H', t), а секретным ключом — набор (S, H, D, P).

22.1. Описать процедуру шифрования сообщения с помощью криптосистемы Нидеррайтера.

22.2. Описать алгоритм дешифрования сообщения с помощью криптосистемы Нидеррайтера.

22.3. Доказать корректность алгоритма дешифрования криптосистемы Нидеррайтера.

22.4. Пусть для передачи информации используется криптосистема Нидеррайтера. Ваш секретный ключ составляют невырожденная матрица S, проверочная матрица H линейного кода, исправляющего 1 ошибку, и матрица P, соответствующая перестановке π.

Секретная информация представлена двоичными блоками веса 1.

а) Найти открытый ключ криптосистемы, зашифровать сообщение $m = (0100000)$ и дешифровать полученный шифротекст при условии, что ваш секретный ключ составляют матрицы

$$S = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}, \; H = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

и перестановка $\pi = (2143567)$.

b) Найти открытый ключ криптосистемы, зашифровать сообщение $m = (00010000)$ и дешифровать полученный шифротекст при условии, что ваш секретный ключ составляют матрицы

$$S = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix}, \; H = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

и перестановка $\pi = (78465312)$.

22.5. Пусть дан троичный код Хэмминга длины 4 с проверочной матрицей

$$H = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 2 & 0 & 1 \end{pmatrix}.$$

Пусть

$$P = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \; S = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}, \; D = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Найти открытый ключ криптосистемы, зашифровать сообщение $x = (1000)$ и дешифровать полученный шифротекст.

Глава III

Сжатие данных

23. Энтропия, ее свойства. Теорема Шеннона

• Пусть $f(x)$ — выпуклая вверх функция, заданная на положительной полуоси. Для произвольных положительных чисел β_i, $i = 1, \ldots, k$, таких, что $\sum_{i=1}^{k} \beta_i = 1$, и любых $x_1, \ldots, x_k$ из участка выпуклости функции $f(x)$ выполняется *неравенство Йенсена*

$$\sum_{i=1}^{k} \beta_i f(x_i) \leq f\left(\sum_{i=1}^{k} \beta_i x_i\right),$$

причем равенство имеет место тогда и только тогда, когда

$$x_1 = \ldots = x_k.$$

• *Энтропия по Шеннону* $\mathcal{H}(A)$ источника A определяется следующим образом:

$$\mathcal{H}(A) = -\sum_{i=1}^{k} p_i \log p_i.$$

Энтропия — мера неопределенности опыта, понятие, противоположное понятию *информация*, которое понимается как степень или мера знания об опыте, объекте. В определенной выше энтропии $\mathcal{H}(x)$ для двоичного симметричного канала связи (см. разд. 6.) имели два исхода с вероятностями p и $1 - p$ соответственно.

23.1.^{0} Какова энтропия опыта с k равновероятными исходами?

23.2.^{0} Сколько максимальных бит информации могло бы приходиться на одну букву текста, использующего кириллицу?

23.3. В первой урне содержится 25 красных, 7 синих и 3 зеленых шара, во второй урне — 11 красных, 15 синих и 9 зеленых шаров. Из каждой урны извлекают по одному шару. Исход какого из этих двух опытов более неопределен?

23.4. Согласно прогнозу gismeteo.ru вероятность того, что завтра в Новосибирске будет жаркая погода равна 0,3. Согласно прогнозу на yandex.ru завтра с вероятностью 0,5 будет жаркая сухая погода, а с вероятностью 0,1 будет прохладно и дождь. Какой прогноз более достоверен?

23.5. Доказать, что энтропия $\mathcal{H}(A)$ источника Бернулли A неотрицательна и равна 0 тогда и только тогда, когда одна из вероятностей букв равна 1, а остальные вероятности равны 0.

23.6. Дан источник Бернулли A с вероятностями букв $\{p_1, \ldots, p_k\}$, где $\sum_{i=1}^{k} p_i = 1$. Доказать, что справедливо неравенство $\mathcal{H}(A) \leq \log k$. Выяснить условия, при которых $\mathcal{H}(A) = \log k$.

23.7. Дан источник Бернулли с вероятностями букв $\{p_1, \ldots, p_k\}$, где $\sum_{i=1}^{k} p_i = 1$. Доказать, что для любых неотрицательных чисел q_i, $i = 1, \ldots, k$, таких что $\sum_{i=1}^{k} q_i = 1$, выполняется неравенство $-\sum_{i=1}^{k} p_i \log q_i \geq -\sum_{i=1}^{k} p_i \log p_i$.

23.8. Найти оценку сверху стоимости побуквенного кодирования через энтропию, гарантируемую кодированием Шеннона.

• Через A^N обозначим произведение N источников A, определяемое как

$$A^N = H = \begin{pmatrix} (a_{i_1}, \ldots, a_{i_N}) \\ p_{i_1} \cdots p_{i_N} \end{pmatrix}, \; a_{i_j} \in A, \; j \in \{1, \ldots, N\}.$$

• *Стоимость блочного кодирования* (A) источника A^N определяется следующим образом:

$$C(A) = \sum_{i=1}^{n^N} p(u_i) l_i,$$

где $p(u_i)$ — вероятность блока $p(u_i) = (a_{i_1}, \ldots, a_{i_N})$, а l_i — длина его кодового слова.

23.9. Найти стоимость кодирования на букву сообщения, используя определение стоимости блочного кодирования.

23.10. Доказать, что для любых случайных опытов A и B справедливо

$$\mathcal{H}(AB) \leq \mathcal{H}(A) + \mathcal{H}(B),$$

причем равенство достигается только тогда, когда опыты A и B независимы.

23.11. Доказать, что для любых случайных опытов $A_1, A_2, \ldots, A_N$ справедливо

$$\mathcal{H}(A_1 A_2 \cdots A_N) \leq \mathcal{H}(A_1) + \ldots \mathcal{H}(A_N).$$

Доказать, что для бернуллиевских источников справедливо

$$\mathcal{H}(A^N) = N \cdot \mathcal{H}(A)$$

для любого натурального N.

23.12. Найти среднюю длину количества символов выходного алфавита, приходящихся на букву сообщения, используя определение стоимости блочного кодирования.

23.13. Доказать, что для блочного кодирования Шеннона справедливо

$$C_{Shannon}^{(N)} < \mathcal{H}(A) + \varepsilon_N,$$

где $\varepsilon_N \longrightarrow 0$ при $N \longrightarrow \infty$.

23.14. Доказать, что для данного источника A стоимость любого разделимого блочного кодирования при любом N удовлетворяет оценке $C^{(N)} \geq \mathcal{H}(A)$.

23.15. Найти оценку:

a) сверху для биномиального коэффициента C_N^m через функцию энтропии;

b) сверху полиномиального коэффициента $\frac{N!}{m_1!m_2!\cdots m_k!}$ через функцию энтропии

$$\mathcal{H}(\frac{m_1}{N},\ldots,\frac{m_k}{N}) = -\sum_{i=1}^{k}\frac{m_i}{N}\log\frac{m_i}{N},$$

где $\sum_{i=1}^{k}\frac{m_i}{N} = 1$.

23.16.* Доказать следующий частный случай неравенства Йенсена: пусть $y = f(x)$ — выпуклая функция на некотором интервале. Пусть $x_1, x_2, \ldots, x_k$ — некоторые k значений в этом интервале, не все равные между собой. Тогда

$$\frac{f(x_1)+f(x_2)+\cdots+f(x_k)}{k} < f(\frac{x_1+x_2+\cdots+x_k}{k}).$$

23.17.* Доказать неравенство Йенсена.

24. Префиксное и разделимое кодирование. Графы Маркова

• Рассмотрим k-буквенный алфавит $A = \{a_1, \ldots, a_k\}$, $B = \{0, \ldots, q-1\}$ — *кодирующий алфавит*. Через B^* обозначим множество всех слов конечной длины в алфавите B. Отображение $\Sigma : A \to B^*$ называется *алфавитным кодированием*. Пусть l_i — *длина* i-го кодового слова, т. е. $l_i = |\Sigma(a_i)|$.
• Кодирование Σ называется *разделимым*, если из равенства

$$\Sigma(a_{i_1}) \ldots \Sigma(a_{i_m}) = \Sigma(a_{j_1}) \ldots \Sigma(a_{j_n})$$

следует, что $m = n$ и $i_t = j_t$ для всех $t = 1, \ldots, m$ (другими словами, любая последовательность кодовых слов единственным образом разделима на кодовые слова).
• Кодирование Σ называется *префиксным*, если никакое кодовое слово не является началом (префиксом) никакого другого кодового слова. Любой префиксный код, очевидно, является разделимым. Обратное неверно.
• Выполнение *неравенства Крафта – Макмиллана*

$$\sum_{i=1}^{k} q^{-l_i} \leq 1$$

является необходимым и достаточным условием для существования q-значных префиксного и разделимого кодов с заданным набором длин L.
• Для разделимости заданного кодирования Σ необходимо и достаточно наличие хотя бы одной цепи в *графе Маркова* кодирования Σ, проходящей через вершину, соответствующую пустому символу.

24.1. Привести конструкцию префиксного кода k-буквенного алфавита для произвольного заданного k.

24.2. Пусть кодом каждого из данных чисел является его двоичное представление наименьшей возможной длины (без нулей слева), например, $1 \to 1, 2 \to 10, 4 \to 100$ и т. д. Является ли кодирование разделимым?

a) $L = \{1, 2, 4, 9, 50\}$;

b) $L = \{1, 2, 4, 17, 98\}$.

24.3. Построить двоичный префиксный код с заданной последовательностью длин кодовых слов:

a) $L = \{1, 2, 3, 3\}$;

b) $L = \{1, 2, 4, 4, 4\}$;

c) $L = \{1, 2, 3, 3, 4, 4, 4, 4\}$.

24.4. Может ли набор чисел L быть набором длин кодовых слов разделимого кода в q-значном алфавите?

a) $L = \{1, 2, 2, 3\}$;

b) $L = \{2, 2, 2, 4, 4, 4\}$.

24.5. Пусть в алфавитном двоичном коде C таком, что $|C| > 2^n$, каждое слово имеет длину, не превышающую n. Может ли код C быть разделимым?

24.6. Префиксное q-значное кодирование Σ называется *полным*, если для любого слова v в кодирующем алфавите справедливо одно из следующих условий:

1) слово v является префиксом (необязательно собственным) некоторого слова из кода Σ;

2) некоторое слово из Σ является собственным префиксом слова v.

Доказать, что префиксный код с q-значным кодирующим алфавитом полный тогда и только тогда, когда выполняется равенство $\sum_{i=1}^{r} q^{-l_i} = 1$, где $l_1, \ldots, l_r$ — длины кодовых слов.

24.7. По заданному алфавитному коду $\Sigma(A)$ построить граф Маркова G_Σ и выяснить, является ли код разделимым:

a) $\Sigma(A) = \{ab, dc, a, bcadd, ca\}$;

b) $\Sigma(A) = \{ddac, dd, cddab, a, cddd, b\}$;

c) $\Sigma(A) = \{abc, abb, bcc, ccaa, bcabbbcc, bbccaaabca, abcabbabbbcca\}$.

24.8. Перечислить все неоднозначно декодируемые последовательности кодовых слов:

a) $\Sigma = \{0, (10)^{2013}, (01)^{2014}\}$;

b) $\Sigma = \{010, 101, 01010, (01)^{2014}\}$;

c) $\Sigma = \{0, 10, 11, (101)^k\}$.

25. Оптимальность. Коды Фано, Хаффмена и Шеннона

• Дан источник Бернулли $A = \{a_1, \ldots, a_k\}$ с вероятностями букв $P = \{p_1, \ldots, p_k\}$. *Стоимостью кодирования* $\Sigma : A \to B^*$ называется величина $C(\Sigma) = \sum_{i=1}^{k} p_i \cdot l_i$.
• Кодирование Σ *оптимально* в некотором классе кодов, если его стоимость кодирования является наименьшей среди всех кодов этого класса.

Теорема Хаффмена. *Код Хаффмена является оптимальным в классе разделимых кодов.*

Теорема Шеннона. *Для заданного источника A имеют место следующие оценки:*

$$H(A) \leq C_{ш}(A^N)/N < H(A) + (1/N),$$

где $C_{ш}(A^N)$ есть стоимость кодирования Шеннона источника A^N.

При построении кода Шеннона требуется найти q-ичное представление десятичного числа, не превосходящего 1, для поиска которого удобно пользоваться следующим алгоритмом.

1. Пусть x — исходное число, $i = 1$.
2. Вычисляется $x * q$, имеющее целую часть x' и дробную часть x''.
3. Число x' есть i-й знак после запятой в q-ичном разложении. Если x'' равно 0, то q-ичное представление найдено, иначе — x равным x'', i увеличивается на 1 и алгоритм переходит на шаг 1.

25.1. Построить коды Фано, Хаффмена и Шеннона, найти и сравнить стоимости кодов источников Бернулли с вероятностями букв:

a) $P = \{0,5; 0,2; 0,1; 0,09; 0,08; 0,03\}$;

b) $P = \{0,4; 0,2; 0,1; 0,1; 0,1; 0,1\}$;

c) $P = \{0,4; 0,3; 0,1; 0,07; 0,06; 0,04; 0,03\}$.

25.2. Доказать, что кодирование Фано префиксное.

25.3. Для источников Бернулли с вероятностями букв

$$P = \{0,35; 0,15; 0,15; 0,15; 0,1; 0,05; 0,05\},$$

построить двоичный и троичный коды Хаффмена, найти их стоимости.

25.4. Построить оптимальный код для q-значного источника Бернулли с данными вероятностями букв:

a) $P = \{0,3; 0,2; 0,2; 0,2; 0,05; 0,05\}, q = 3$;

b) $P = \{0,4; 0,2; 0,1; 0,1; 0,1; 0,05; 0,05\}, q = 3$.

25.5. Для заданного q указать набор вероятностей P, при котором существует q-значный префиксный код с заданным набором длин кодовых слов L, являющийся оптимальным. Построить этот код.

a) $q = 2, L = \{1, 3, 3, 3, 4, 4\}$;

b) $q = 3, L = \{1, 2, 2, 3, 3, 3\}$.

25.6. Доказать, что коды Фано и Хаффмена совпадают для источника Бернулли с суперубывающим набором вероятностей (т. е. для любого i $p_i \geq \sum_{j>i} p_j$).

25.7. С помощью теоремы Крафта доказать, что существует кодирование любого источника Бернулли A, стоимость которого не превосходит $\mathcal{H}(A) + 1$.

25.8. Построить двоичные и троичные коды Шеннона для источника Бернулли с заданными распределениями вероятностей букв:

a) $P = \{0,6; 0,1; 0,09; 0,08; 0,07; 0,06\}$;

b) $P = \{0,4; 0,4; 0,1; 0,03; 0,03; 0,02; 0,02\}$;

c) $P = \{0,34; 0,18; 0,17; 0,16; 0,15\}$;

d) $P = \{1/3; 1/3; 1/6; 1/6\}$;

e) $P = \{4/15; 1/3; 1/5; 2/15; 1/15\}$.

Найти стоимости кодирований.

25.9. Найти q-ичное представление дроби s/t, $(s, t) = 1$, если:

a) $(t, q) = 1$;

b) $(t, q) = m, m > 1$.

25.10. Построить коды Фано, Хаффмена и Шеннона для источников A, A^2 и A^3, если $P(A) = \{0,4; 0,3; 0,3\}$. Найти $C_{\text{Ш}}(A^1), C_{\text{Ш}}(A^2)/2, C_{\text{Ш}}(A^3)/3$ — среднее число символов, затрачиваемых каждым из кодов для кодирования одного символа исходного алфавита A. Сравнить результаты с теоретическими данными.

25.11. Доказать, что код Шеннона префиксный.

25.12. Доказать, что коды, оптимальные в классе префиксных и разделимых для одного и того же источника, имеют одинаковую стоимость.

26. Адаптивное кодирование

• Источник $A = \{a_1, a_2, \ldots, a_k\}$ называется *монотонным*, если вероятности букв упорядочены по невозрастанию, т. е. $p_1 \geq p_2 \geq \ldots \geq p_k$.

26.1. Пусть дан алфавит $A = \{1, 2, 3\}$. Передать слово $\omega = 221312233112$ с помощью кода «стопка книг». Декодировать полученное слово.

26.2. Пусть дан алфавит $A = \{a, b, c, d\}$. Передать слово ω с помощью кода «стопка книг». Декодировать полученное слово:

a) $\omega = cbbacccdbb$;

b) $\omega = ccabbaaccc$.

26.3. При каких условиях, наложенных на передаваемые сообщения, эффективен метод кода «стопка книг»?

• Определим $n^{(0)} = 0,\ n^{(i)} = 2^{n^{(i-1)}}$, $i = 1, 2, \ldots$.
Определим также при $x \geq 0$ целочисленную функцию $\log^* x$, полагая

$$\log x = i, \text{ если } n^{(i)} \leq x < n^{(i+1)}.$$

Функция $\log^* x$ является медленно растущей.
Слово $Bin'x$ определяется из двоичного слова $Binx$ удалением первой цифры, равной единице, например, $Bin'2 = 0$, $Bin'3 = 1$.
• *Код Левенштейна* $Lev(x)$ определяется следующим образом:

$$Lev(x) = 1^{\log^* x} 0 \prod_{i=1}^{\log^* x} Bin' \lfloor \log^{(\log^* x - i)} x \rfloor.$$

26.4.^{0} Найти $n^{(i)}, i = 1, 2, \ldots, 6$.

26.5. Найти $\log^* 37$, $\log^* 100$, $\log^* 2^{10^4}$.

26.6.^{0} Найти $\log^* 37$, $\log^* 100$, $\log^* 2^{10^4}$.

26.7.^{0} Чему равна длина $Bin'(x)$?

26.8. Найти

a) $Lev(37)$;

b) $Lev(57)$.

26.9. Описать процедуру декодирования кода Левенштейна. Декодировать слово 111100100010111101001.

26.10. Найти длину кода Левенштейна.

26.11. Доказать префиксность кода Левенштейна.

26.12. Передать сообщение ω с помощью метода Лемпела – Зива LZ77 с заданным размером окна. Декодировать полученное слово:

a) $\omega = (abbaabbb)aabcab$;

b) $\omega = (abcabbcc)cabbaabd$;

c) $\omega = (01200211)300213013$.

26.13. Найти код сообщения ω с помощью метода Лемпела – Зива LZ78:

a) $\omega = babaababababaaabab$;

b) $\omega = aaababaabaaabab$.

26.14. Пусть дан источник Бернулли A с распределением вероятностей P. Найти код последовательности ω с помощью арифметического кодирования:

a) $A = \{a_1, a_2, a_3, a_4\}$, $P = \{0,1; 0,4; 0,2; 0,3\}$, $\omega = a_3a_2a_3a_1$;

b) $A = \{a_1, a_2, a_3, a_4\}$, $P = \{0,2; 0,3; 0,1; 0,4\}$, $\omega = a_4a_2a_2a_1$.

26.15. Доказать префиксность арифметического кода.

26.16. Найти с помощью адаптивного кода Хаффмана код сообщения

$$\omega = a_1a_1a_4a_3a_1a_1a_2a_4a_3a_3.$$

Декодировать полученное слово.

26.17. Декодировать слово 111 с помощью адаптивного кода Хаффмана, если окно имеет вид $(a_1a_1a_4a_3a_1a_1a_2a_4) = (00101110011010)$.

Решения, ответы, указания

Ответы по теории кодирования

Булев куб. Расстояние Хэмминга

1.7. a) Число пар соседних векторов в пространстве E^n равно $n2^{n-1}$.

1.9. a) Число неупорядоченных пар векторов в пространстве $\in E^n$ на расстоянии k равно $C_n^k 2^{n-1}$.

1.10. a) 2^m; b) $C_m^{\frac{m+k-r}{2}} C_{n-m}^{\frac{k-m+r}{2}}$; c) $\sum_{j=0}^{k} C_m^{\frac{m+r-j}{2}} C_{n-m}^{\frac{j-m+r}{2}}$;
d) $\sum_{j=0}^{k} \sum_{i=0}^{m-r+k} C_m^{\frac{m+r-j}{2}+i} C_{n-m-1}^{\frac{j-m+r}{2}-i}$.

1.13. a) Число баз в пространстве E^n равно $\frac{(2^n-1)(2^n-2)\ldots(2^n-2^{n-1})}{n!}$.

1.15. a) $n!$, $n!2^n$.

Линейные коды

2.5. a) Число различных линейных двоичных кодов длины n размерности k равно

$$\frac{(2^n-1)(2^n-2)\cdots(2^n-2^{k-1})}{(2^k-1)(2^k-2)\cdots(2^k-2^{k-1})}.$$

2.6. a) Число различных линейных двоичных кодов длины n размерности k с информационными символами в первых k координатах равно $2^{(n-k)k}$.

2.7. a) Число различных линейных двоичных кодов длины n размерности k, содержащих фиксированный вектор x, с информационными символами в первых k координатах равно $2^{(n-k)(k-1)}$.

2.8. С помощью теоремы о связи проверочной и порождающей матриц, заданных в каноническом виде, мы находим

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}.$$

Кодовое слово с требуемым свойством есть $(1,1,0)G = (110110)$.

2.9. *Указание.* Можно использовать теорему о связи проверочной и порождающей матриц.

2.10. Коды неэквивалентны, первый код имеет четное кодовое расстояние, а второй — равное 1.

2.11. b) Например, можно преобразовать проверочную матрицу к каноническому виду, затем использовать теорему о связи проверочной и порождающей матриц и воспользоваться обратным преобразованием. Свойство матрицы быть проверочной

матрицей одного и того же кода не изменится, если с ее строками произвести невырожденные линейные преобразования. Например, умножив вторую строку матрицу

$$H = \begin{pmatrix} 0 & 2 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 2 & 2 \\ 2 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

на 2, получим проверочную матрицу

$$\widetilde{H} = \begin{pmatrix} 0 & 2 & 1 & 0 & 1 & 0 \\ 2 & 2 & 0 & 0 & 1 & 1 \\ 2 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

того же кода. Пусть H' получена из $\widetilde{H}$ перестановкой столбцов, заданную следующим циклом $\pi = (3465)$. Заметим, что H', равная

$$\begin{pmatrix} 0 & 2 & 1 & 1 & 0 & 0 \\ 2 & 2 & 1 & 0 & 1 & 0 \\ 2 & 0 & 0 & 0 & 0 & 1 \end{pmatrix},$$

будет проверочной матрицей кода C', эквивалентного (возможно, неравного) коду C с проверочной матрицей H. Матрица H' в каноническом виде, поэтому порождающую матрицу G' кода C' можно легко найти, используя теорему о связи проверочной и порождающей матриц, заданных в каноническом виде. Чтобы получить порождающую матрицу

$$G = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 2 & 1 & 0 & 2 \end{pmatrix}$$

кода C, достаточно переставить столбцы матрицы

$$G' = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 2 & 2 & 0 \end{pmatrix}$$

с помощью перестановки $\pi^{-1} = (3564)$. 3^3 кодовых слов кода C получаются всевозможными линейными комбинациями строк G.

2.25. Число векторов, ортогональных данному ненулевому вектору из E^n, равно 2^{n-1}.

2.29. Код с повторением имеет параметры $[n, 1, n]$. Кодом, ортогональным данному коду, является полный четновесовой код $[n, n-1, 2]$.

2.33. Порядок полной линейной группы $GL(k, q)$ удовлетворяет равенству

$$|GL(k, q)| = (q^k - 1)(q^k - q)(q^k - q^2) \dots (q^k - q^{k-1}).$$

2.34. Матрица GP является порождающей матрицей линейного кода C тогда и только тогда, когда отвечающая матрице P подстановка принадлежит группе симметрий линейного кода C. С другой стороны, матрица GP может быть получена из матрицы G невырожденным линейным преобразованием посредством некоторой невырожденной матрицы M.

Границы объемов двоичных кодов

3.1. *Указание.* Рассмотреть геометрическую модель процедуры декодирования кода с минимальным расстоянием d.

3.13. Многократно применяя задачу 3.12, получаем
$N(k,d) \geq d + N(k-1, \rceil d/2 \lceil) \geq d + \rceil d/2 \lceil + N(k-2, \rceil d/4 \lceil) \geq \ldots \geq$
$\geq \sum_{i=0}^{k-2} \rceil d/2^i \lceil + N(1, \rceil d/2^{k-1} \lceil) \geq \sum_{i=0}^{k-1} \rceil d/2^i \lceil)$.

3.14. $N(5,7) = 15$, существует $[15,5,7]$-код БЧХ, о существовании таких кодов см. раздел 10.

3.15. $N(k, 2^{k-1}) = 2^{k-1} + 2^{k-2} + \ldots + 2 + 1 = 2^k - 1$, существует код с параметрами $[2^k - 1, k, 2^{k-1}]$, на котором достигается эта граница.

3.16. Подсчитаем число пар (y,x) таких, что $y \in E^n$, $x \in C$, $d(y,x) = 2$. С одной стороны, число пар равно $|C| \cdot C_n^2$. С другой стороны, для фиксированного $y \in E^n$ найдется ровно $2C_n^2/n$ векторов с попарным расстоянием хотя бы 2 между собой. Сопоставляя эти два значения, получаем требуемое.

Совершенные коды

4.19. *Указание.* Доказать по индукции, используя представление кода Хэмминга с помощью конструкции Васильева для совершенных кодов.

4.20. a) Порядок группы автоморфизмов двоичного кода Хэмминга длины 7 равен 2688.

4.21. Порядок группы автоморфизмов троичного кода $\{000, 111, 222\}$ равен 12.

4.22. Порядок группы автоморфизмов троичного кода Хэмминга длины 4 равен 48, из них 24 перестановки координатных позиций.

4.34– 4.36. *Указание.* Использовать формулу Стирлинга.

4.39. Использовать связь размерности кода, двойственного совершенному двоичному коду C с размерностью ядра и с рангом кода C.

4.40. *Указание.* Использовать теорему Симониса, см. задачу 2.24.

Способы построения кодов

5.6. *Указание.* Воспользоваться теоремой о столбцах проверочной матрицы. Например, в качестве такой матрицы можно взять матрицу

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

5.8. *Указание.* Код имеет 8 кодовых слов. Для построения кода рассмотрим все кодовые слова веса 3 кода Хэмминга длины 7, затем расширим код общей проверкой на четность и добавим нулевое кодовое слово. Остается доказать максимальность кода.

Декодирование

6.11. a) Слово (1110000) находится на расстоянии 2 от следующих кодовых слов: (1100100), (0110001), (0111000), (1100100), все остальные кодовые слова находятся на расстоянии, большем 2. Поэтому (1110000) по принципу максимума правдоподобия можно декодировать в любое из вышеперечисленных кодовых слов.

b) Слово (1010101) является кодовым и поэтому в исправлении ошибок не нуждается.

6.16. *Указание.* Использовать формулу Стирлинга.

6.17. *Указание.* Использовать формулу бинома Ньютона.

6.20. $P_i = \sum_{y \in E^n} P(y \neq x^i | x^i)$.

Поля Галуа

7.1. Неприводимые над $GF(2)$ многочлены степени, не превышающей 3, следующие: $0, 1, x, x+1, x^2+x+1, x^3+x^2+1, x^3+x+1$.

7.2. Найдем непосредственным испытанием делимости на многочлены степени, не превышающей 2, являющиеся неприводимыми над $GF(2)$.

7.3.

a) $x^5 + x^4 + x^2 + x = x(x+1)^2(x^2+x+1)$;

b) $x^{16} - x = x(x+1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1)$.

7.6. *Указание.* Воспользоваться биномом Ньютона.

7.9. Предположим, что $\beta\gamma$ — элемент порядка k. Имеем $k|mn$ по задаче 7.8. Так как $\beta^k = \gamma^{-k}$, то $\beta^{km} = \gamma^{-km} = 1$, откуда вновь по задаче 7.8 получаем, что порядок n элемента γ делит km. Учитывая, что $(n, m) = 1$, имеем $n|k$. Аналогично показывается, что $m|k$. Следовательно, $k = mn$.

7.11. Пусть α — примитивный элемент поля Галуа $GF(p^m)$, т. е. порождающий элемент мультипликативной группы G порядка $p^m - 1$, которая является циклической. Если i и $p^m - 1$ имеют общие делители, то группа, порожденная α^i, будет собственной подгруппой G. В противном случае α^i порождает G. Действительно, иначе найдется $k, k < p^m - 1$, такое, что $\alpha^{ik} = 1$, $k < p^m - 1$ и, следовательно, $p^m - 1 | ik$, чего не может быть, поскольку i и $p^m - 1$ взаимно просты.

7.12. Многочлен $x + 1$.

7.13. *Указание.* Чтобы доказать, что $\beta^4 + \beta^2 + \beta$ и $\beta^3 + \beta^5 + \beta^6$ принадлежат простому подполю, достаточно применить теорему Ферма. Воспользовавшись методом неопределенных коэффициентов для $\beta = a_0 + a_1 x + a_2 x^2$, несложно установить, что $\beta^4 + \beta^2 + \beta = a_0$, а $\beta^3 + \beta^5 + \beta^6 = a_0 + a_2$.

7.14. Любой элемент $GF(2^2)$, отличный от нуля и единицы, является примитивным элементом поля $GF(2^2)$. Например, элемент $\alpha = x$, степени которого задают все различные ненулевые элементы поля: $\alpha^2 = x + 1$, $\alpha^3 = 1$.

7.15. *Указание.* Элемент $\alpha = 2x + 1 \pmod{x^2 + x + 1}$ удовлетворяет сравнению $\alpha^2 \equiv 2 \pmod{x^2 + x + 1}$. Нетрудно проверить, что отображение $ax + b \pmod{x^2 - 2} \to a(2x+1) + b \pmod{x^2 + x + 1}$ есть искомый изоморфизм.

7.17. Число неприводимых многочленов над $GF(2)$ степени 4 равно 3.

7.18. *Указание.* В качестве изоморфизма рассмотреть отображение, переводящее примитивный элемент одного представления поля в другой.

7.19. a) В качестве примитивного элемента конечного поля $GF(2)[x]/(x^3+x^2+1)$ можно выбрать $\alpha = x$. Действительно, $\alpha^2 = x^2$, $\alpha^3 = x^2+1$, $\alpha^4 = x^2+x+1$, $\alpha^5 = x+1$, $\alpha^6 = x^2 + x$, $\alpha^7 = 1$.

b), c) В качестве примитивного элемента можно взять любой многочлен первой степени.

7.21. *Указание.* Порождающим группы будет автоморфизм, определяемый по правилу $\alpha \to \alpha^p$, называемый *Фробениусовым автоморфизмом* для любого элемента α поля $GF(p^m)$. Помимо этого, всякий автоморфизм поля сохраняет каждый элемент простого подполя на месте.

7.22. По задаче 7.21, группы автоморфизмов полей Галуа $GF(2^4)$, $GF(2^5)$, $GF(2^6)$ являются циклическими группами Z_4, Z_5, Z_6 порядков $4, 5, 6$ соответственно.

7.23. *Указание.* Рассмотрим мультипликативную группу поля $GF(q^n)$, полученного доопределением бинарной операции умножения в векторном пространстве $GF(q)^n$. Порождающий этой группы α задает требуемый автоморфизм векторного пространства $GF(q)^n$: $\alpha(x) = \alpha * x$.

Минимальный многочлен

8.3. Найдем циклотомические классы по модулю 7: $C_0 = \{0\}$, $C_1 = \{1, 2, 4\}, C_3 = \{3, 6, 5\}$. Отсюда получаем следующие выражения для минимальных многочленов:
$M^0(y) = y + 1$,
$M^1(y) = M^2(y) = (y - \alpha)(y - \alpha^2)(y - \alpha^4) = y^3 + y^2(\alpha + \alpha^2 + \alpha^4) + y(\alpha^3 + \alpha^5 + \alpha^6) + \alpha^7$,
$M^3(y) = (y - \alpha^3)(y - \alpha^6)(y - \alpha^5) = y^3 + y^2(\alpha^3 + \alpha^6 + \alpha^5) + y(\alpha + \alpha^2 + \alpha^4) + \alpha^7$,
где α — примитивный элемент поля Галуа $GF(2^3)$, построенного по модулю x^3+x^2+1. В качестве примитивного элемента поля Галуа рассмотрим $\alpha = x$, что дает следующие выражения для неизвестных коэффициентов многочленов M^1 и M^3 (см. задачу 7.19): $\alpha + \alpha^2 + \alpha^4 = 0$, $\alpha^3 + \alpha^6 + \alpha^5 = 1$. Отсюда получаем, что $M^0(y) = y + 1, M^1(y) = y^3 + y + 1, M^3(y) = y^3 + y^2 + 1$. Заметим, что если взять в качестве примитивного элемента $\alpha = x + 1$, то выражения для многочленов M^1 и M^3 поменяются местами.

8.5. В данном случае минимальные многочлены проще всего получить, отобрав многочлены над $GF(3)$ степени не больше 2, обладающие свойством неприводимости. Если воспользоваться представлением $GF(3^2)$ как фактор-кольца по идеалу, порожденному $x^2 + x + 2$ с примитивным элементом $\alpha = x$ (см. 7.19), то при использовании шестого свойства минимальных многочленов выражения для минимальных многочленов будут следующими: $M^0(y) = y + 2, M^1(y) = M^3(y) = y^2 + y + 2, M^2(y) = M^6(y) = y^2 + 1, M^4(y) = y + 1, M^5(y) = M^7(y) = y^2 + 2y + 2$.

8.6. a) $x^8 - x = x(x + 1)(x^3 + x^2 + 1)(x^3 + x + 1)$;
b) $x^{16} - x = x(x + 1)(x^2 + x + 1)(x^4 + x + 1)(x^4 + x^3 + 1)(x^4 + x^3 + x^2 + x + 1)$.

8.7. $x^{10} - x = x(x + 1)(x^2 + x + 1)(x^6 + x^3 + 1)$.

8.13. Рассмотрим следующие суммы: $a_0 + a_1\beta + a_2\beta^2 + \ldots + a_m\beta^m$, где a_i — элементы простого подполя $GF(p)$. Если сумма равна 0 для некоторого набора $(a_i : i = 0, \ldots, m)$, то β является корнем многочлена $f(x) = \sum_{i=0,\ldots,m} a_i$, следовательно, по задаче 8.11 степень минимального многочлена β не превосходит m.

Рассмотрим случай, когда $a_0 + a_1\beta + a_2\beta^2 + \ldots + a_m\beta^m$ не равно нулю ни при каких $a_i \in GF(p)$. Тогда, в силу алгебраической замкнутости простого подполя, имеем две отличных друг от друга суммы, т. е. $a_0 + a_1\beta + a_2\beta^2 + \ldots + a_m\beta^m \neq a'_0 + a'_1\beta + a'_2\beta^2 + \ldots + a'_m\beta^m$, если соответствующие им упорядоченные наборы $(a_i : i = 0, \ldots, m)$ и $(a'_i : i = 0, \ldots, m)$ различны. Иными словами, это означает, что в $GF(p^m)$ не менее p^{m+1} элементов. Противоречие.

8.15. *Указание.* Воспользоваться задачей 7.6, чтобы показать, что
$M^{(i)}(x^p) = (M^{(i)})^p(x)$.

Циклические коды

9.4. Нет, данный линейный $(6, 3, 1)$-код не является циклическим, так как все его кодовые слова имеют ноль в последней координатной позиции.

9.6. Известно, что параметры кода Хэмминга выражаются через число проверок r следующим образом: $n = 2^r - 1, k = n - r$. Так как степень порождающего многочлена $g(x)$ циклического кода равна числу проверок, то в данном случае речь идет о коде Хэмминга длины $n = 2^4 - 1 = 15$. Поэтому проверочный многочлен этого кода равен $h(x) = (x^{15} - 1)/(x^4 + x + 1) = x^{11} + x^8 + x^7 + x^5 + x^3 + x^2 + x + 1$.

9.8. $H = (1, 1, 1, 1, 1)$, $h(x) = 1 + x + x^2 + x^3 + x^4$.

9.11. a) Минимальное расстояние кода равно 5;

b) вектор $e_7 + e_{11}$ является наиболее вероятным вектором ошибки.

9.13. Известно, что для любой допустимой длины n существует циклическое представление кода Хэмминга, в группе симметрий которого, очевидно, есть циклическое преобразование, имеющее порядок n. Так как все коды Хэмминга длины n эквивалентны (более того, они изоморфны), то в группе симметрий всякого кода Хэмминга найдется симметрия порядка n.

9.13. *Указание.* Достаточно, например, задать проверочную (или порождающую) матрицу так, чтобы код содержал кодовое слово $(1, 1, 1, 0, 0, 0, 0)$. Очевидно, циклический сдвиг такого кодового слова не будет кодовым словом.

9.14. Пусть $g(1) \neq 0$. Поскольку код циклический, то многочлен $g(x)$ делит многочлен $x^n - 1$, т. е. $x^n - 1 = g(x)q(x)$ для некоторого многочлена $q(x)$. Подставляя $x = 1$, получим $g(1)q(1) = 0$ и, поскольку $g(1) \neq 0$, имеем $q(1) = 0$. Следовательно, по теореме Безу выполняется $q(x) = (x-1)u(x)$. Отсюда $x^n - 1 = (x-1)(1+x+x^2+\ldots+x^{n-1}) = (x-1)g(x)u(x)$. Из последнего равенства получаем, что многочлен $1+x+x^2+\ldots+x^{n-1}$, которому отвечает единичный вектор, представим в виде произведения кодового многочлена $g(x)$ на многочлен $u(x)$, т. е. многочлен $1+x+x^2+\ldots+x^{n-1}$ является кодовым. Обратное утверждение выполняется только, когда длина кода n не делит характеристику поля p.

9.15. *Указание.* Использовать задачу 9.14. Обратное утверждение выполняется только, когда длина кода n является нечетной.

9.16. Переформулируем свойство быть единицей циклического кода с заданным порождающим многочленом $g(x)$. Несложно видеть, что кодовый многочлен $f(x)g(x)$ — единица тогда и только тогда, когда $f(x)g^2(x) = g(x)$. Пусть $g(x)$ — порождающий многочлен циклического кода C длины n. Тогда $g(x)|x^n - 1$. Так как $(q, n) = 1$, то многочлен $x^n - 1$ не имеет кратных делителей. Следовательно, $(g^2(x), x^n - 1) = g(x)$, т. е. найдутся $a(x)$ и $b(x) : (x^n - 1)a(x) + g^2(x)b(x) = g(x)$. Рассматривая равенство в $F_q[x]$, получаем, что $g^2(x)b(x) = g(x)$, т. е. $g(x)b(x)$ — единица кода C.

9.17. $x^{14} + x^{13} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^2 + x$. Чтобы найти явный вид единицы $f(x)g(x)$ кода с порождающим многочленом $g(x)$, можно или воспользоваться решением задачи 9.16 и взять в качестве $f(x)$ многочлен $b(x)$: $(x^n - 1)a(x) + g^2(x)b(x) = g(x)$, или применить метод неопределенных коэффициентов к равенству $f(x)g^2(x) = g(x)$.

9.18. Все идемпотенты кода имеют вид $(x^{10} + x^5 + 1)(f_0 + f_1(x + x^2 + x^3 + x^4))$ для некоторых двоичных f_0 и f_1.

10.14. Поскольку $(r, n) = 1$, то элемент $\beta = \alpha^r$ также является примитивным элементом поля Галуа $GF(p^m)$. Следовательно, найдется такое число k, что $\alpha^b = \beta^k$, и циклический код имеет $\delta - 1$ подряд идущих степеней примитивного элемента β:

$$g(\beta^k) = g(\beta^{k+1}) = \ldots = g(\beta^{k+\delta-2}) = 0.$$

Далее остается применить теорему о границе БЧХ.

Коды БЧХ

10.5. Имеется 18 кодовых слов минимального веса, содержащих 1 в первой координатной позиции.

10.9. Да, коды эквивалентны.

10.11. Данный код исправляет три ошибки.

10.12.
a) Вектор ошибки e_{15}, кодовое слово $x + e_{15}$.
b) Вектор ошибки $e_1 + e_2$, кодовое слово $y + e_1 + e_2$.
c) Вектор ошибки $e_3 + e_4 + e_5$, кодовое слово $z + e_3 + e_4 + e_5$.
10.13.
a) Вектор ошибки e_2, кодовое слово $x + e_2$.
b) Вектор ошибки $e_{11} + e_{13}$, кодовое слово $y + e_{11} + e_{13}$.
c) Вектор ошибки $e_6 + e_7 + e_9$, кодовое слово $z + e_6 + e_7 + e_9$.

Блок-схемы и коды

11.6. *Указание.* Существует 2 непересекающиеся системы.
11.8. $|Aut(STS(7))| = 168$.
11.21. a) Выкалывая единичную координату у всех кодовых слов, имеющих единицу в i-й координате, получим код длины $n-1$ с расстоянием не менее 2δ веса $w-1$. Мощность такого кода не более $A(n-1, 2\delta, w-1)$. С учетом общего числа единиц в первоначальном коде получим не более

$$nA(n-1, 2\delta, w-1)$$

кодовых слов. С другой стороны, общее число единиц равно $wA(n, 2\delta, w)$, поскольку каждое кодовое слово имеет вес w, а кодовых слов в первоначальном коде было $A(n, 2\delta, w)$. Отсюда получаем оценку

$$wA(n, 2\delta, w) \leq nA(n-1, 2\delta, w-1),$$

из которой следует требуемая оценка.

b) *Указание.* Используя задачу 11.19 b), получить требуемое неравенство, при этом в отличие от случая a) считать не единицы, а нули.

11.22. *Указание.* Применить последовательно оценки из задачи 11.21, затем использовать оценку из задачи 11.19 d), получить требуемое неравенство, при этом в отличие от случая a) считать не единицы, а нули.

11.25. *Указание.* Использовать комбинации оценок из задач 11.20 и 11.24, получить $A(9, 6, 4) = 3$ и $A(8, 6, 4) = 2$.

11.26. *Указание.* Последовательно применить два раза оценку из задачи 11.21 a), затем оценки из задач 11.20 и 11.24.

11.30. $A(12, 5) \leq 39$. Использовать задачи 11.27 и 11.28.

11.31. Использовать задачу 11.27 и известную оценку

$$A(n, 4, 3) = \begin{cases} \left\lceil \frac{n}{3} \left\lceil \frac{n-1}{2} \right\rceil \right\rceil - 1 & \text{для } n \equiv 5 \pmod 6, \\ \left\lceil \frac{n}{3} \left\lceil \frac{n-1}{2} \right\rceil \right\rceil & \text{в противном случае.} \end{cases}$$

11.32. *Указание.* Для доказательства этого утверждения (теорема Додунекова и Зиновьева) использовать границу Джонсона из задачи 11.27.

Другие коды (преобразование Адамара, матрицы Адамара, коды Адамара, коды Рида – Маллера)

12.2. Имеем

$$H^{-1} \cdot H \cdot H^T = nH^{-1},$$

отсюда $H^T = nH^{-1}$ и $H^T \cdot H = nH^{-1} \cdot H = nE_n$, следовательно, $H^T \cdot H = nE_n$, откуда следует требуемое.

12.4. Без ограничения общности предположим, что H представлена в нормализованном виде и пусть $n > 2$. Найдется матрица, эквивалентная матрице H, первые три строки которой имеют вид

$$\underbrace{\begin{array}{cccc|cccc|cccc|cccc} 1 & 1 & \cdots & 1 & 1 & 1 & \cdots & 1 & 1 & 1 & \cdots & 1 & 1 & 1 & \cdots & 1 \\ 1 & 1 & \cdots & 1 & 1 & 1 & \cdots & 1 & -1 & -1 & \cdots & -1 & -1 & -1 & \cdots & -1 \\ 1 & 1 & \cdots & 1 & -1 & -1 & \cdots & -1 & 1 & 1 & \cdots & 1 & -1 & -1 & \cdots & -1 \end{array}}_{i \qquad\qquad j \qquad\qquad k \qquad\qquad l}.$$

Тогда из ортогональности строк имеем следующую систему уравнений:

$$\begin{cases} i+j+k+l=n; \\ i+j-k-l=0 \quad \text{(умножая 1 и 2-ю строки)}; \\ i-j-k+l=0 \quad \text{(умножая 2 и 3-ю строки)}; \\ i-j+k-l=0 \quad \text{(умножая 1 и 3-ю строки)}. \end{cases}$$

Решая эту систему, получаем $i = j = k = l = n/4$, откуда следует, что 4 делит n.

12.5. Пусть H_m и H_n — две матрицы Адамара порядков m и n соответственно. Тогда

$$(H_m \times H_n)(H_m \times H_n)^T = (H_m \times H_n)(H_m^T \times H_n^T) =$$
$$= H_m \cdot H_m^T \times H_n \cdot H_n^T = mE_m \times nE_n = mnE_{mn}.$$

12.11. Из определения кода Рида – Маллера порядка r вытекает, что он состоит из всех линейных комбинаций векторов, соответствующих произведениям

$$1, x_1, \ldots, x_m,\ x_1x_2,\ \ldots,\ x_{m-1}x_m,\ \ldots,\ x_{m-r+1}x_{m-r+2}\ldots x_m.$$

Эти произведения задают базис кода Рида – Маллера порядка r. Отсюда следует, что размерность кода равна

$$k = 1 + \binom{m}{1} + \cdots + \binom{m}{r},$$

все кодовые слова имеют четный вес.

12.12. *Указание.* По индукции доказать, что справедливо

$$\mathcal{RM}(r+1, m+1) = \{\, (u, u+v) \mid u \in \mathcal{RM}(r+1, m), v \in \mathcal{RM}(r, m) \,\}.$$

12.13. *Указание.* Доказать индукцией по m, используя задачу 12.12.

12.14. Рассмотрим произвольные векторы $f \in \mathcal{RM}(m-r-1, m)$ и $g \in \mathcal{RM}(r, m)$. Из определения кодов Рида – Маллера вытекает, что степени многочленов f и g от m переменных не превосходят $m-r-1$ и r соответственно. Отсюда степень многочлена $f(x_1, \ldots, x_m) \cdot g(x_1, \ldots, x_m)$ не превосходит $m-1$ и отвечающий этому многочлену вектор принадлежит коду $\mathcal{RM}(m-1, m)$. Поскольку в коде $\mathcal{RM}(m-1, m)$ все вершины имеют четный вес, т. е. скалярное произведение векторов f и g равно нулю, то получаем $\mathcal{RM}(m-r-1, m) \subseteq \mathcal{RM}(r, m)^\perp$. Обозначим через $\dim(C)$ размерность кода C. Справедливо

$$\dim\mathcal{RM}(m-r-1, m) + \dim\mathcal{RM}(r, m) = 2^m,$$

откуда следует, что

$$\mathcal{RM}(m-r-1, m) = \mathcal{RM}(r, m)^\perp,$$

что требовалось доказать.

12.16. Покажем, что матрицу H_n можно представить следующим образом: строки и столбцы матрицы помечены всевозможными булевыми векторами длины m, а элемент, стоящий на пересечении строки, помеченной вектором $\mathbf{u}$ и столбца, помеченного вектором $\mathbf{v}$, равен в точности $(-1)^{\mathbf{uv}}$. Доказательство проведем индукцией по m. При $m = 1$, т. е. $n = 2$, утверждение верно:

$$H_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} (-1)^{(0)(0)} & (-1)^{(0)(1)} \\ (-1)^{(1)(0)} & (-1)^{(1)(1)} \end{pmatrix}.$$

Допустим, что утверждение верно для $n = 2^{m-1}$, т. е. $H_{\frac{n}{2}} = \{h_{ij}\}_{\frac{n}{2}\times\frac{n}{2}}$, где $h_{ij} = (-1)^{\mathbf{xy}}$, $\mathbf{x}, \mathbf{y} \in E^{m-1}$. Покажем истинность утверждения для $n = 2^m$.

По построению матрицы Сильвестра выполняется

$$H_n = \begin{pmatrix} H_{\frac{n}{2}} & H_{\frac{n}{2}} \\ H_{\frac{n}{2}} & -H_{\frac{n}{2}} \end{pmatrix}.$$

При этом метки строк (столбцов) матрицы H_n могут быть получены из меток $H_{\frac{n}{2}}$ следующим образом: метка строки (столбца) H_n с номером от 0 до $2^{m-1} - 1$ имеет вид $(0\mathbf{u})$, где $\mathbf{u}$ — метка одноименной строки (столбца) матрицы $H_{\frac{n}{2}}$. Метка строки (столбца) с номером i от 2^{m-1} до $2^m - 1$ имеет вид $(1\mathbf{u})$, где $\mathbf{u}$ – метка строки (столбца) под номером $i - 2^{m-1}$ матрицы $H_{\frac{n}{2}}$. В силу $(0\mathbf{u})(0\mathbf{v}) = (0\mathbf{u})(1\mathbf{v}) = (1\mathbf{u})(0\mathbf{v}) = \mathbf{uv}$ и $(1\mathbf{u})(1\mathbf{v}) = \mathbf{uv} + 1$ получаем искомое.

12.17. Формула обращения $F = \frac{1}{n}\hat{F}H$ для преобразования Фурье – Адамара вытекает из определения матрицы Адамара, а именно из $H^2 = nE$ и того факта, что $H^{\perp} = H$ для симметрической матрицы H:

$$\hat{F}H = FH^2 = nF \Rightarrow \; F = \frac{1}{n}\hat{F}H,$$

.

12.18. Рассмотрим булеву функцию $f(v_1, v_2) = v_1 v_2$, $m = 2$. Найдем вектор $\mathbf{F}$, его преобразование Фурье – Адамара $\hat{F}$ и обращение этого преобразования.

Функция f отлична от нуля только в точке $(1, 1)$, поэтому вектор $\mathbf{F}$ будет иметь вид $(1, 1, 1, -1)$. Тогда

$$\hat{F} = FH_4 = \begin{pmatrix} 1 & 1 & 1 & -1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 2 & 2 & -2 \end{pmatrix}.$$

Непосредственной проверкой убеждаемся, что $F = \frac{1}{n}\hat{F}H$. Действительно,

$$\frac{1}{n}\hat{F}H = \frac{1}{4}\begin{pmatrix} 2 & 2 & 2 & -2 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} = \frac{1}{4}\begin{pmatrix} 4 & 4 & 4 & -4 \end{pmatrix} = F.$$

12.19.

$$\sum_{\mathbf{u}\in\mathbf{E^m}} \hat{F}(\mathbf{u})\hat{F}(\mathbf{u}+\mathbf{v}) = \sum_{\mathbf{u}\in\mathbf{E^m}} \sum_{\mathbf{y}\in\mathbf{E^m}} (-1)^{\mathbf{uy}} F(\mathbf{y}) \sum_{\mathbf{x}\in\mathbf{E^m}} (-1)^{(\mathbf{u}+\mathbf{v})\mathbf{x}} F(\mathbf{x}) =$$

$$= \sum_{\mathbf{y},\ \mathbf{x}\in\mathbf{E^m}} (-1)^{\mathbf{vx}} F(\mathbf{y})F(\mathbf{x}) \sum_{\mathbf{u}\in\mathbf{E^m}} (-1)^{\mathbf{u(x+y)}}.$$

Обозначим $\mathbf{x}+\mathbf{y}$ через $\mathbf{z}$ и рассмотрим подробнее сумму $\sum\limits_{\mathbf{u}\in\mathbf{E^m}} (-1)^{\mathbf{uz}}$. Очевидно, при $\mathbf{z}=\mathbf{0}$ все слагаемые равны 1, и поэтому сумма равна 2^m. Пусть вектор $\mathbf{z}$ отличен от нуля. В этом случае существуют векторы, как ортогональные, так и неортогональные $\mathbf{z}$: $\mathbf{U_1}=\{\mathbf{u}|\ \mathbf{uz}=1\}$, $\mathbf{U_0}=\{\mathbf{u}|\ \mathbf{uz}=0\}$. Зафиксируем $i\in \operatorname{supp}(\mathbf{z})$, через $\mathbf{e_i}$ обозначим i-й координатный орт. Заметим, что множества $\mathbf{U_1}$ и $\mathbf{U_0}$ образуют разбиение E^m и мощности их одинаковы (если $\mathbf{u}\in\mathbf{U_0}$, то $\mathbf{e_i}+\mathbf{u}\in\mathbf{U_1}$, и наоборот). Это означает, что

$$\sum_{\mathbf{u}\in\mathbf{E^m}} (-1)^{\mathbf{uz}} = \sum_{\mathbf{u}\in\mathbf{U_0}} (-1)^0 + \sum_{\mathbf{u}\in\mathbf{U_1}} (-1)^1 = 2^{m-1} - 2^{m-1} = 0.$$

Поэтому сумма $\sum\limits_{\mathbf{u}\in\mathbf{E^m}} (-1)^{\mathbf{u(x+y)}}$ принимает значение 2^m при $\mathbf{x}=\mathbf{y}$ и 0 в противном случае. Следовательно,

$$\sum_{\mathbf{u}\in\mathbf{E^m}} \hat{F}(\mathbf{u})\hat{F}(\mathbf{u}+\mathbf{v}) = 2^m \sum_{\mathbf{y}\in\mathbf{E^m}} (-1)^{\mathbf{vy}} F^2(\mathbf{y}) = 2^m \sum_{\mathbf{y}\in\mathbf{E^m}} (-1)^{\mathbf{vy}} = \begin{cases} 2^{2m}, & \text{если } \mathbf{v}=\mathbf{0}; \\ 0, & \text{если } \mathbf{v}\neq\mathbf{0}. \end{cases}$$

12.23. Действительно, значение $\hat{F}(\mathbf{u})$ равно разности между числом нулей и единиц в двоичном векторе $\mathbf{f}+\sum\limits_{i=1}^{m} u_i\mathbf{v_i}$. Число единиц в векторе $\mathbf{x}+\mathbf{y}$ равно расстоянию от $\mathbf{x}$ до $\mathbf{y}$, поэтому число нулей в $\mathbf{f}+\sum\limits_{i=1}^{m} u_i\mathbf{v_i}$ есть не что иное, как $2^m - d\{\mathbf{f},\ \sum\limits_{i=1}^{m} u_i\mathbf{v_i}\}$, а число единиц — это $d\{\mathbf{f},\ \sum\limits_{i=1}^{m} u_i\mathbf{v_i}\}$, здесь d обозначает расстояние между векторами. Таким образом, верно соотношение

$$\hat{F}(\mathbf{u}) = (2^m - d\{\mathbf{f},\ \sum_{i=1}^{m} u_i\mathbf{v_i}\}) - d\{\mathbf{f},\ \sum_{i=1}^{m} u_i\mathbf{v_i}\} = 2^m - 2d\{\mathbf{f},\ \sum_{i=1}^{m} u_i\mathbf{v_i}\}.$$

Или

$$d\{\mathbf{f},\ \sum_{i=1}^{m} u_i\mathbf{v_i}\} = \frac{1}{2}\{2^m - \hat{F}(\mathbf{u})\}.$$

Аналогично получаем, что

$$d\{\mathbf{f},\ \mathbf{1}+\sum_{i=1}^{m} u_i\mathbf{v_i}\} = \frac{1}{2}\{2^m + \hat{F}(\mathbf{u})\}.$$

Поэтому расстояние от нуля до вектора $\mathbf{f}+u_0\mathbf{1}+\sum\limits_{i=1}^{m} u_i\mathbf{v_i}$ из класса $\mathbf{f}+R(1,m)$ равно $\frac{1}{2}\{2^m-\hat{F}(\mathbf{u})\}$, если $u_0=0$, и $\frac{1}{2}\{2^m+\hat{F}(\mathbf{u})\}$, если $u_0=1$.

12.24. Согласно задаче 12.23 достаточно показать, что множества $\{\pm\hat{G}(\mathbf{u})|\ \mathbf{u}\in E^m\}$ и $\{\pm\hat{F}(\mathbf{u})|\ \mathbf{u}\in E^m\}$ совпадают. Действительно,

$$\hat{G}(\mathbf{u}) = \sum_{\mathbf{v}\in E^m} (-1)^{\mathbf{uv}} G(\mathbf{v}) = \sum_{\mathbf{v}\in E^m} (-1)^{\mathbf{uv}} F(\mathbf{Av}+\mathbf{b}).$$

Положим $\mathbf{v} = \mathbf{B^{-1}x} + \mathbf{B^{-1}b}$. Тогда

$$\hat{G}(\mathbf{u}) = \sum_{\mathbf{x}\in E^m} (-1)^{\mathbf{uB^{-1}x}}(-1)^{\mathbf{uB^{-1}b}}F(\mathbf{x}) = \pm \sum_{\mathbf{x}\in E^m} (-1)^{\mathbf{uB^{-1}x}}F(\mathbf{x}) = \pm\hat{F}(\mathbf{uB^{-1}}).$$

12.25. Верна следующая последовательность равенств:

$$\sum_{\mathbf{u}\in C} \hat{f}(\mathbf{u}) = \sum_{\mathbf{u}\in C}\sum_{\mathbf{v}\in E^n} (-1)^{\mathbf{uv}} f(\mathbf{v}) =$$

$$\sum_{\mathbf{v}\in E^n} f(\mathbf{v})\sum_{\mathbf{u}\in C} (-1)^{\mathbf{uv}} = \sum_{\mathbf{v}\in C^\perp} f(\mathbf{v})\sum_{\mathbf{u}\in C} (-1)^{\mathbf{uv}} + \sum_{\mathbf{v}\notin C^\perp} f(\mathbf{v})\sum_{\mathbf{u}\in C} (-1)^{\mathbf{uv}}.$$

По определению дуального кода первое слагаемое равно $|C|\sum\limits_{\mathbf{v}\in C^\perp} f(\mathbf{v})$. Рассмотрим подробнее второе слагаемое. Зафиксируем некоторый вектор $\mathbf{v} \notin C^\perp$ и вычислим внутреннюю сумму. Код C разбивается на два подмножества: C_0, состоящее из векторов, ортогональных $\mathbf{v}$ (например нулевого), и C_1, включающее векторы, не ортогональные $\mathbf{v}$ (это множество также непусто, иначе $\mathbf{v}$ попадал бы в $C^\perp$). Выберем произвольный элемент $\mathbf{y} \in C_1$:

$$\mathbf{y} + C_0 \subseteq C_1 \Rightarrow |C_0| \le |C_1|,\ \mathbf{y} + C_1 \subseteq C_0 \Rightarrow |C_1| \le |C_0|.$$

Значит, $|C_0| = |C_1|$ и внутренняя сумма содержит одинаковое число единиц и минус единиц. Следовательно, второе слагаемое равно нулю, откуда следует требуемое.

12.26. Доказательство проведем индукцией по n. При $n = 1$ это верно: $a_1 + b_1 = \sum\limits_{v=0}^{1} a_1^{1-v}b_1^v$. Допустим, что утверждение истинно для $n-1$. Тогда

$$\prod_{i=1}^{n}(a_i + b_i) = (a_n{+}b_n)\prod_{i=1}^{n-1}(a_i + b_i) = (a_n{+}b_n)\sum_{\mathbf{v}\in E^{n-1}}\prod_{i=1}^{n-1} a_i^{1-v_i}b_i^{v_i} = \sum_{\mathbf{v}\in E^{n-1}} a_n\prod_{i=1}^{n-1} a_i^{1-v_i}b_i^{v_i} +$$

$$+ \sum_{\mathbf{v}\in E^{n-1}} b_n\prod_{i=1}^{n-1} a_i^{1-v_i}b_i^{v_i} = \sum_{\substack{\mathbf{v}\in E^n\\ v_n=0}}\prod_{i=1}^{n} a_i^{1-v_i}b_i^{v_i} + \sum_{\substack{\mathbf{v}\in E^n\\ v_n=1}}\prod_{i=1}^{n} a_i^{1-v_i}b_i^{v_i} = \sum_{\mathbf{v}\in E^n}\prod_{i=1}^{n} a_i^{1-v_i}b_i^{v_i}.$$

12.27. Рассмотрим отображение $f(\mathbf{v}) = x^{n-w(\mathbf{v})}y^{w(\mathbf{v})}$.

$$\hat{f}(\mathbf{u}) = \sum_{\mathbf{v}\in E^n} (-1)^{\mathbf{uv}} x^{n-w(\mathbf{v})}y^{w(\mathbf{v})} = \sum_{\mathbf{v}\in E^n} (-1)^{u_1v_1+u_2v_2+\cdots+u_nv_n}\prod_{i=1}^{n} x^{1-v_i}y^{v_i} =$$

$$= \sum_{\mathbf{v}\in E^n}\prod_{i=1}^{n} (-1)^{u_iv_i}x^{1-v_i}y^{v_i} = \prod_{i=1}^{n}(x + (-1)^{u_i}y).$$

Последнее равенство следует из задачи 12.26, примененной в случае $a_i = x$ и $b_i = (-1)^{u_i}y$. Если $u_i = 1$, то внутренняя сумма равна $x - y$. В случае же $u_i = 0$ она равна $x + y$. Поэтому последовательность равенств можно продолжить:

$$\hat{f}(\mathbf{u}) = \prod_{i=1}^{n}(x + (-1)^{u_i}y) = \prod_{i|\ u_i=0}(x + y)\prod_{i|\ u_i=1}(x - y) = (x + y)^{n-w(\mathbf{u})}(x - y)^{w(\mathbf{u})}.$$

Воспользовавшись теперь задачей 12.25, получим

$$\sum_{\mathbf{u}\in C^\perp} x^{n-w(u)}y^{w(u)} = \frac{1}{|C|}\sum_{\mathbf{u}\in C}(x+y)^{n-w(\mathbf{u})}(x-y)^{w(\mathbf{u})},$$

т. е. справедливо требуемое.

12.28. Для доказательства достаточно применить задачу 12.27 к коду $C^\perp$ и использовать свойство $(C^\perp)^\perp = C$.

12.29. Применим задачу 12.27 к коду из задачи 12.18: имеем $W_C(x,y) = x^3+3xy^2$. Тогда

$$\frac{1}{|C|}W_C(x+y,x-y) = \frac{1}{4}((x+y)^3+3(x+y)(x-y)^2) = x^3+y^3 = W_{C^\perp}(x,y).$$

12.30. Применим задачу 12.27 к коду из задачи 12.19: имеем $W_C(x,y) = x^3+3xy^2$. Тогда для кода Хэмминга $W_{H^7}(x,y) = x^7+7x^4y^3+7x^3y^4+y^7$. Отсюда

$\frac{1}{|H^7|}W_{H^7}(x+y,x-y) = \frac{1}{16}((x+y)^7+7(x+y)^4(x-y)^3+7(x+y)^3(x-y)^4+(x-y)^7) =$
$= \frac{1}{16}((x+y)^7+(x-y)^7+7(x+y)^3(x-y)^3(x+y+x-y)) = \frac{1}{8}x((x+y)^6+(x-y)^6-$
$-(x+y)(x-y)((x+y)^4+(x-y)^4)+(x+y)^2(x-y)^2((x+y)^2+(x-y)^2)+6(x+y)^3(x-y)^3) =$
$= \frac{1}{8}x((2x^2+2y^2-x^2+y^2)((x+y)^4+(x-y)^4)+6(x+y)^3(x-y)^3) = \frac{1}{8}x(((x+y)(x^2+3y^2)+$
$+3(x-y)^3)(x+y)^3+((x-y)(x^2+3y^2)+3(x+y)^3)\times(x-y)^3) =$
$= \frac{1}{8}x((4x^3-8x^2y+12xy^2)(x+y)^3+(4x^3+8x^2y+12xy^2)(x-y)^3) =$
$= \frac{1}{2}x^2((x^2+3y^2)\times((x+y)^3+(x-y)^3)-2xy((x+y)^3-(x-y)^3)) =$
$= x^3((x^2+3y^2)^2-2y^2(3x^2+y^2)) = x^7+7x^3y^4.$

Таким образом, действительно

$$\frac{1}{|H^7|}W_{H^7}(x+y,x-y) = W_{(H^7)^\perp}(x,y).$$

12.31. Рассмотрим код $(H^n)^\perp$. Его порождающей матрицей (обозначим ее G) является проверочная матрица кода H^n, столбцы которой — все ненулевые векторы куба E^m. Пометим столбцы векторами из $E^m\backslash\mathbf{0}$. Тогда строку i можно рассматривать как значения функции x_i на множестве $E^m\backslash\mathbf{0}$: действительно, элемент $G(i,\mathbf{u}) = 1$ в том и только том случае, когда i-я координата вектора $\mathbf{u}$ равна единице. Таким образом, код $(H^n)^\perp$ можно отождествить с множеством линейных функций, определенных на $E^m\backslash\mathbf{0}$. Возьмем произвольную нетривиальную функцию f из этого множества и рассмотрим множества ее нулей U_0 и единиц U_1. Они непусты в силу нетривиальности f, а значит, образуют разбиение множества $E^m\backslash\mathbf{0}$. Если бы f была определена на всем E^m, то мощности U_0 и U_1 были бы равны: так как для каждого вектора $\mathbf{u}\in U_1$ выполнялось бы

$$\mathbf{u}+U_0\subseteq U_1 \Rightarrow\ |U_0|\le|U_1| \text{ и } \mathbf{u}+U_1\subseteq U_0 \Rightarrow\ |U_1|\le|U_0|.$$

В данном случае мощность множества U_0 будет на единицу меньше, так как ноль не принадлежит области определения f. Поэтому $|U_0| = 2^{m-1}-1$ и $|U_1| = 2^{m-1}$. Это означает, что все нетривиальные кодовые слова из $(H^n)^\perp$ имеют одинаковый вес, равный $|U_1| = 2^{m-1} = \frac{n+1}{2}$. Код $(H^n)^\perp$ содержит $2^m = n+1$ кодовых слов, следовательно, можно выписать его весовой спектр: $A'_0 = 1$, $A'_{\frac{n+1}{2}} = n$, все остальные A'_i равны нулю. Таким образом,

$$W_{(H^n)^\perp}(x,y) = x^n + nx^{\frac{n-1}{2}}y^{\frac{n+1}{2}}.$$

Отсюда с учетом задачи 12.28 имеем

$$W_{H^n}(x,y)=\frac{1}{n+1}((x+y)^n+n(x+y)^{\frac{n-1}{2}}(x-y)^{\frac{n+1}{2}}).$$

12.32. Первые четыре многочлена Кравчука выглядят следующим образом:
$P_0(x,n)=1$;
$P_1(x,n)=n-2x$;
$P_2(x,n)=\begin{pmatrix} n \\ 2 \end{pmatrix}-2xn+2x^2$;
$P_3(x,n)=\begin{pmatrix} n \\ 3 \end{pmatrix}-(n^2-n+2/3)x+2nx^2-4x^3/3$.

12.33. *Указание.* Из свойств биномиальных рядов производящая функция многочленов Кравчука $P_k(x,n)$ имеет вид

$$(x+y)^{n-i}(x-y)^i=\sum_{k=0}^{n}P_k(i)x^{n-k}y^k.$$

12.34. По теореме МакВильямс (см. задачу 12.27) соотношение между весовыми функциями представляет собой равенство многочленов, его можно использовать для обнаружения связи между весовыми спектрами $\{A_i\}$ и $\{A'_i\}$ взаимно дуальных кодов. Тогда

$$\frac{1}{|C|}W_C(x+y,x-y)=\frac{1}{|C|}\sum_{i=0}^{n}A_i(x+y)^{n-i}(x-y)^i=\frac{1}{|C|}\sum_{i=0}^{n}A_i\sum_{k=0}^{n}P_k(i)x^{n-k}y^k=$$

$$=\sum_{k=0}^{n}\left(\frac{1}{|C|}\sum_{i=0}^{n}A_iP_k(i)\right)x^{n-k}y^k=\sum_{k=0}^{n}A'_kx^{n-k}y^k.$$

Таким образом, весовой спектр дуального кода определяется следующими соотношениями:

$$A'_k=\frac{1}{|C|}\sum_{i=0}^{n}A_iP_k(i),\ k=0,1,2,\ldots$$

APN-функции

13.3. Функция $F:E^m\to E^m$, удовлетворяющая $F:x\to x^3$, является APN-функцией при любых натуральных m. Эта функция отвечает БЧХ-коду, исправляющему две ошибки при $m\equiv 1 \pmod 2$.

13.4. Проверочная матрица H_F имеет $2m$ строк, отсюда $k\geq n-2m$. Поскольку матрица H_F содержит в качестве подматрицы проверочную матрицу кода Хэмминга H_m с m проверками на четность, получаем $k\leq n-m$.

13.5. Да, эта функция является APN-функцией.

13.6. Для любого отображения F размерность k кода C_F удовлетворяет $k\geq n-2m$ (см. задачу 13.4). Поскольку любые два столбца в H_F различны, имеем $d_{C_F}\geq 3$. Пусть $d_{C_F}\geq 6$. Из существования линейного $[n,k,d]$-кода выкалыванием любой координатной позиции получается код с параметрами $[n-1,k,d-1]$. Следовательно, из линейного кода с параметрами $[n=2^m-1,k,d=6]$ получим код с параметрами $[n=2^m-2,k,d=5]$. Но по теореме Додунекова и Зиновьева (см. задачу 11.32) такой код не существует.

13.8. *Указание.* Использовать 13.4 и теорему Додунекова и Зиновьева (см. задачу 11.32).

13.9. *Указание.* Использовать теорему о существовании совершенных кодов и теорему Додунекова и Зиновьева (см. задачу 11.32).

13.10. Пусть это не так и функция F' не является APN-функцией. Тогда по задаче 13.7 имеем $d_{C'_F} \geq 4$. Поскольку код C'_F является подкодом кода C_F, то выполняется $d_{C_F} \geq 4$. Последнее противоречит тому, что функция F является APN-функцией.

13.11. Так как функция F' является APN-функцией, то по задаче 13.7 имеем $d_{C_F} = 5$. Следовательно, код C_F содержит кодовые слова веса 5. Очевидно, единичный вектор не может быть ортогонален ни одному кодовому слову нечетного веса.

Ответы по криптологии

Элементы теории чисел

14.1. Поскольку $1534^5 \equiv 4^5 \pmod 9 \equiv 2^{10} \pmod 9 \equiv 1024 \pmod 9 \equiv 7 \pmod 9$, то, вычитая из этого сравнения тривиальное сравнение $1 \equiv 1 \pmod 9$, получим $1534^5 - 1 \equiv 6 \pmod 9$.

14.2. a) Обозначим остаток от деления 19^{10} на 66 через r. Из сравнений $19 \equiv 1 \pmod 2$, $19 \equiv 1 \pmod 3$, $19 \equiv -2 \pmod{11}$ следует, что $r \equiv 1 \pmod 2$, $r \equiv 1 \pmod 3$, $r \equiv (-2)^{10} \pmod{11}$. По малой теореме Ферма $(-2)^{10} \equiv 1 \pmod{11}$. Отсюда $r = 1$.

b) 11;

c) 17;

d) 36.

14.3. Из $a = b \pmod{p^n}$ имеем $a = b + kp^n$ для некоторого натурального k. Следовательно,

$$a^p = (b + kp^n)^p = b^p + pb^{p-1}kp^n + \ldots + k^p p^{pn} = b^p + b^{p-1}kp^{n+1} + \ldots + k^p p^{pn},$$

откуда следует $a^p \equiv b^p \pmod{p^{n+1}}$.

14.4. *Указание.* Сначала разложить 343 по степеням двойки, затем применить теорию. *Ответ.* 2.

14.7. В качестве m можно взять, например, $\varphi(n)$.

14.8. Сумма равна p^α.

14.9. *Указание.* Использовать индукцию.

14.10. *Указание.* Использовать малую теорему Ферма.

14.11. a) *Указание.* Поскольку $(3, 13) = 1$, можно применить метод Эйлера для сравнения $ax \equiv b \pmod n$, где $(a, n) = 1$: решение (единственное) ищем в виде $x = ba^{\varphi(n)-1} \pmod n$. Подставляя значения a, b и n, преобразовывая, получим $x = 7 \pmod{13}$.

b) Нет решения, поскольку $(156, 221) = 13$.

c) *Указание.* Упростить и применить метод непрерывных дробей.

14.12. $x = 17 \pmod{90}$.

14.13. *Указание.* Решить систему с помощью сравнений.

Ответ.

$$\begin{cases} x &= 17 + 37t \\ y &= 20 + 45t. \end{cases}$$

Криптосистема Диффи и Хеллмана

15.1. Дискретный логарифм числа 7 по основанию 2 в группе $G = Z/19Z$ равен 6.

15.2. Дискретный логарифм элемента -1 по основанию α равен 4.

15.6. a) Найдем $K = (\alpha^5)^7 = (\alpha^7)^5 = \alpha^{35} = \alpha^9$, поскольку в поле Галуа $GF(3^3$ для примитивного элемента α выполняется $\alpha^{26} = 1$. В силу $\alpha^3 + \alpha^2 - 1 = 0$ имеем $\alpha^9 = (1 - \alpha^2)^3 = 1 - 3\alpha^2 + 3\alpha^4 - \alpha^6 = 1 - \alpha^6 = 1 - (\alpha^3)^2 = 1 - (1 - \alpha^2)^2 = 2\alpha^2 - \alpha^4 = 2\alpha^2 - \alpha(1 - \alpha^2) = 2\alpha^2 - \alpha + \alpha^3 = 2\alpha^2 - \alpha + 1 - \alpha^2 = \alpha^2 + 2\alpha + 1$.

15.7. Криптостойкость алгоритма основана на сложности вычисления следующей задачи (В. М. Сидельников, М. А. Черепнев, В. В. Ященко, 1993 г.): по известным

элементам g_a и g_b из полугруппы G, допускающим разложения вида $g_a = h_a \cdot \sigma \cdot r_a$ и $g_b = h_b \cdot \sigma \cdot r_b$ (сами разложения неизвестны!), найти неизвестный элемент g вида $g = h_a \cdot g_a \cdot r_a = h_b \cdot g_b \cdot r_b$.

16.1. $x_4 = x_3^B \pmod p = m^{x_A x_B y_A y_B} \pmod p = m^{x_A y_A x_B y_B} \pmod p = m^{1+e\cdot\varphi(p)} \pmod p = m \cdot m^{e\varphi(p)} \pmod p = m \pmod p$, где e — некоторое целое число, а $\varphi(p)$ — функция Эйлера.

16.2. а) Найдем функцию Эйлера числа 13: $\varphi(13) = 12$. Алиса, решая сравнение $5x \equiv 1 \pmod{12}$, находит $x = 5$. Аналогично Боб, решая сравнение $7y \equiv 1 \pmod{12}$, находит $y = 7$. Далее имеем следующие действия Алисы (А.) и Боба (В.):

А.: $m_1 = 2^5 \pmod{13} = 32 \pmod{13} = 6 \pmod{13}$;

В.: $m_2 = 6^7 \pmod{13} = 279936 \pmod{13} = 7 \pmod{13}$;

А.: $m_3 = 7^5 \pmod{13} = 16807 \pmod{13} = 11 \pmod{13}$;

В.: $m_4 = 11^7 \pmod{13} = 19487171 \pmod{13} = 2 \pmod{13}$, $m_4 = m$.

Криптосистема Эль-Гамаля

17.3. Зная секретный ключ x, исходное сообщение можно вычислить из шифротекста (a, b) по формуле $m = b \cdot (a^x)^{-1} \pmod p$.

17.4. Алиса посылает Бобу информацию $(9, 27)$.

17.8.

Генерация ключей

1. Выберем $x = 8$ — случайное целое число x такое, что $1 < x < p - 1$.
2. Вычислим $y = g^x \pmod p = 2^8 \pmod{11} = 3$.

Итак, открытым ключом является тройка $(p, g, y) = (11, 2, 3)$, а закрытым ключом — число $x = 8$. Допустим, что нужно передать сообщение $m = 5$.

Шифрование

1. Выбираем случайное целое число k такое, что $1 < k < p - 1$. Пусть $k = 9$.
2. Вычисляем число $a = g^k \pmod p = 2^9 \pmod{11} = 512 \pmod{11} = 6$.
3. Вычисляем число $b = y^k \cdot m \pmod p = 3^9 \cdot 5 \pmod{11} = 19683 \cdot 5 \pmod{11} = 9$.

Полученная пара $(a, b) = (6, 9)$ является шифротекстом.

Дешифрование

1. Получаем сообщение m по известному шифротексту $(a, b) = (6, 9)$ и секретному ключу $k = 9$.
2. Вычисляем m по формуле $m = b \cdot (a^x)^{-1} \pmod p = 9 \cdot (6^8)^{-1} \pmod{11} = 5$. Получим исходное сообщение $m = 5$.

Электронная подпись на криптосистеме Эль-Гамаля

17.8. При известном открытом ключе (p, g, y) и подписи (r, s) сообщения m проверка проводится следующим образом.

1. Проверяется выполнимость условий $0 < r < p$ и $0 < s < p - 1$. Если хотя бы одно из них не выполняется, то подпись считается недействительной.
2. Подпись считается верной, если выполняется сравнение $y^r r^s \equiv g^m \pmod p$.

17.9.

а) Для подписи сообщения $m = 3$ выполняются следующие операции.

1. Выбирается случайное число $1 < k < p - 1$ такое, что $(p - 1, k) = 1$, например, $k = 5$.

2. Вычисляется число $r = g^k \pmod p = 5^5 \pmod{23} = 20$.

3. Вычисляется число
$s = (m - xr)k^{-1} \pmod{p-1} = (3 - 7 \cdot 20) \cdot 5^{-1} \pmod{22} = (-137) \cdot 9 \pmod{22} = 21$.

Подписью сообщения $m = 3$ является пара $(r, s) = (20, 21)$.

Зная открытый ключ (p, g, y), где $y = g^x \pmod p = 5^7 \pmod{23} = 17$, осуществляем проверку подписи (r, s) сообщения m.

1. Проверяется выполнимость условий $0 < r < p$ и $0 < s < p - 1$. Условия выполнены.

2. Проверяется сравнение $y^r r^s \equiv g^m \pmod p$.
$L = y^r r^s \pmod p = 17^{20} \cdot 20^{21} \pmod{23} = 8^5 \cdot 19^7 \pmod{23} = 16 \cdot 15 \pmod{23} = 10$.
$$R = g^m \pmod p = 5^3 \pmod{23} = 10.$$

Поскольку левая L и правая R части равны, подлинность сообщения $m = 3$ проверена.

Криптосистема RSA

18.1. Для дешифровки текста выполняется следующая процедура.

1. Найти такое d, чтобы $e \cdot d \equiv 1 \pmod{\varphi(n)}$.

2. Затем для каждого зашифрованного сообщения c вычислить $m = c^d \pmod n$.

18.3. Вычислим $n = p \cdot q = 77$ и функцию Эйлера $\varphi(n) = 60$. Выберем открытый ключ $e = 37$, для которого выполняется условие взаимной простоты $(37, 60) = 1$.

Вычислим секретный ключ $d = e^{-1} \pmod{\varphi(n)} = 13$. Выберем исходное сообщение $m = 2$. Вычислим шифротекст на основе открытого ключа

$$c = m^e \pmod n = 2^{37} \pmod{77} = 51.$$

Заметим, что вычисление остатка по модулю 77 можно провести вручную или с помощью калькулятора. Аналогичным образом происходит процесс дешифрования с помощью секретного ключа

$$m = 51^{13} \pmod{77} = 2.$$

18.4. а)

1. Алиса формирует свои секретный и открытый ключи:

$$\begin{aligned} n &= p \cdot q = 11 \cdot 17 = 187, \\ \varphi(n) &= 10 \cdot 16 = 160, \\ d &= e^{-1} \pmod{\varphi(n)} \Rightarrow d = 89. \end{aligned}$$

2. Таким образом, получены открытый и секретный ключи Алисы:

$$\begin{aligned} K_{A,pub} &= \{n = 187, e = 9\}; \\ K_{A,priv} &= \{p = 11, q = 17, d = 89\}. \end{aligned}$$

3. Для передачи сообщения $m = 3$ Боб выполняет процедуру шифрования с помощью открытого ключа Алисы:

$$x = m^e \pmod{n} = 3^9 \pmod{187} = 48.$$

4. Далее Боб передает шифротекст $x = 48$ Алисе по открытому каналу связи.

5. Алиса для прочтения шифротекста $x = 48$ выполняет процедуру дешифрования с помощью своего секретного ключа:

$$m = x^d \pmod{n} = 48^{89} \pmod{187} = 3.$$

6. Таким образом, Боб секретно передал Алисе свое сообщение.

Электронная подпись на криптосистеме RSA

18.7. а)

1. Алиса формирует свой секретный ключ:

$$\begin{aligned} n_A &= p_A \cdot q_A = 11 \cdot 23 = 253; \\ \varphi(n_A) &= 10 \cdot 22 = 220; \\ d_A &= e_A^{-1} \pmod{\varphi(n_A)} \Rightarrow d_A = 71. \end{aligned}$$

2. Аналогично Боб формирует свой секретный ключ:

$$\begin{aligned} n_B &= p_B \cdot q_B = 7 \cdot 13 = 91; \\ \varphi(n_B) &= 6 \cdot 12 = 72; \\ d_B &= e_B^{-1} \pmod{\varphi(n_B)} \Rightarrow d_B = 29. \end{aligned}$$

3. Таким образом, имеются открытые ключи Алисы и Боба:

$$\begin{aligned} K_{A,pub} &= \{n_A = 253, e_A = 31\}; \\ K_{B,pub} &= \{n_B = 91, e_B = 5\}. \end{aligned}$$

А также секретные ключи Алисы и Боба:

$$\begin{aligned} K_{A,priv} &= \{p_A = 11, q_A = 23, d_A = 71\}; \\ K_{B,priv} &= \{p_B = 7, q_B = 13, d_B = 29\}. \end{aligned}$$

4. Для передачи распоряжения $m = 41$ от Алисы Бобу с возможностью аутентификации отправителя Алиса выполняет следующие процедуры.

   ⋆ Шифрование поручения открытым ключом Боба:

$$m_1 = m^{e_B} \pmod{n_B} = 41^5 \pmod{91} = 6.$$

   ⋆ Подпись шифротекста поручения секретным ключом Алисы:

$$m_2 = m_1^{d_A} \pmod{n_A} = 6^71 \pmod{253} = 94.$$

5. Далее Алиса отправляет Бобу шифротекст с подписью $\{m_1 = 6, m_2 = 94\}$.

6. При получении зашифрованного поручения Боб выполняет следующие процедуры.

   ⋆ Аутентификация отправителя шифротекста: проверяется совпадение шифротекста с подписью, к которой применяется алгоритм дешифровки с помощью открытого ключа Алисы

   $$m_3 = m_2^{e_A} \pmod{n_A} = 94^31 \pmod{253} = 6.$$

   Совпадение m_1 и m_3 проверено, значит, распоряжение действительно отправлено Алисой.

   ⋆ Дешифрование распоряжения m_1 с помощью секретного ключа Боба

   $$m_4 = m_1^{d_B} \pmod{n_B} = 6^29 \pmod{91} = 41.$$

7. Таким образом, Боб убедился в подлинности отправителя, а Алиса секретно передала свое поручение.

b) Поручение Алисы — 13, подпись — 7.
c) Поручение Алисы — 3, подпись — 48.

Криптосистема Меркля – Хеллмана

19.1. a) Пусть вектор груза $w = (171, 197, 459, 1191, 2410)$ и вес рюкзака $S = 3798$, найдем вектор a, удовлетворяющий $S = wa$: очевидно, что координата a_5 должна быть равна 1, так как в противном случае, даже если все остальные координаты вектора a равны 1, имеем $wa < 3798$. Таким образом, $a_5 = 1$ и $S - w_5 = 3798 - 2410 = 1387$. Аналогично $a_4 = 1$. Действуя таким образом далее, получим $a = (0, 1, 0, 1, 1)$.

19.2. Алгоритм дешифрования сообщения для криптосистемы Меркля – Хеллмана выглядит следующим образом.

После получения сообщения s Алиса выполняет следующие действия для его дешифрования.

1. Алиса вычисляет мультипликативное обратное по модулю q к числу r. Поскольку r взаимно просто с q, найти r^{-1} возможно с использованием расширенного алгоритма Евклида.

2. Алиса вычисляет число
   $s' = sr^{-1} \pmod{q} = \sum_{i=1}^{n} a_i m_i r^{-1} \pmod{q} = \sum_{i=1}^{n} w_i m_i \pmod{q} = \sum_{i=1}^{n} w_i m_i$.

3. Из последнего равенства Алиса вычисляет сообщение m, и эта задача не является сложной, поскольку последовательность w супервозрастающая. Для вычисления m используется «жадный» алгоритм.

19.4. a) Открытый ключ $a = (31, 62, 55, 3, 44, 19)$.
Полный секретный ключ $w = (1, 2, 4, 9, 17, 34)$, $q = 69$, $r = 31$, $r^{-1} = 49$.
b) После преобразования с помощью секретного ключа получается сообщение $y = 2, 34, 36, 64, 13, 57$, переданное слово есть «ПАРОЛЬ».

19.5. a) Открытый ключ $a = (63, 5, 89, 99, 45)$. Полный секретный ключ $w = (3, 5, 9, 19, 45)$, $q = 100$, $r = 21$, $r^{-1} = 81$.

b) После преобразования с помощью секретного ключа получается сообщение $y = 33, 24, 22, 81, 45, 3, 27$, переданное слово есть «ОКТЯБРЬ».

19.6. a) Открытый ключ $a = (29, 58, 36, 21, 42, 55)$.

Полный секретный ключ $a' = (1, 2, 4, 9, 18, 35)$, $m = 80$, $\omega = 29$, $\omega^{-1} = 69$

b) После преобразования секретного ключа получается сообщение

$$y = 35, 53, 9, 11, 20, 55,$$

переданное слово есть «АВГУСТ».

Криптосистема на эллиптических кривых

20.1. Аналог алгоритма Диффи – Хеллмана на эллиптических кривых выглядит следующим образом.

Обмен ключами с использованием эллиптических кривых может быть выполнен следующим образом.

1. Выбирается достаточно большое простое число p и параметры a и b для уравнения эллиптической кривой. Это задает множество точек $E_p(a, b)$.

2. Затем в $E_p(a, b)$ выбирается генерирующая точка $G = (x_1, y_1)$. При выборе G важно, чтобы наименьшее значение n, при котором $[n]G = 0$, оказалось очень большим простым числом. Параметры кривой $E_p(a, b)$ и точка G являются публичным ключом криптосистемы, известным всем участникам.

3. Далее происходит обмен ключами между абонентами Алисой и Бобом. В качестве закрытого ключа Алиса выбирает целое число c_A, меньшее n. Затем она вычисляет открытый ключ $D_A = [c_A]G$, который представляет собой некоторую точку на $E_p(a, b)$.

4. Аналогично Боб выбирает закрытый ключ c_B и вычисляет открытый ключ $D_B = [c_B]G$.

5. Участники обмениваются открытыми ключами, после чего вычисляют общий секретный ключ K.

Алиса: $K = [c_A]D_B$. Боб: $K = [c_B]D_A$.

Следует заметить, что общий секретный ключ представляет собой пару чисел. Если данный ключ предполагается использовать в качестве сеансового ключа для алгоритма симметричного шифрования, то из этой пары необходимо создать одно значение.

20.2. Процедура шифрования и дешифрования с использованием эллиптических кривых выглядит следующим образом.

Требуется зашифровать сообщение $0 < m < p$. Как и в случае обмена ключом, в системе шифрования/дешифрования в качестве параметров рассматривается эллиптическая кривая $E_p(a, b)$ и точка G на ней. Боб выбирает закрытый ключ c_B и вычисляет открытый ключ $D_B = [c_B]G$. Чтобы зашифровать сообщение m, используется открытый ключ получателя Боба D_B. Алиса выбирает случайное целое положительное число c_A и вычисляет точки $D_A = [c_A]G$ и $R = [c_A]D_B = (x, y)$. Зашифрованным сообщением является следующая пара:

$$C_m = \{D_A, e = mx \pmod p\}.$$

Чтобы дешифровать сообщение, Боб умножает полученную точку D_A на свой закрытый ключ: $R = [c_B]D_A = (x, y)$, а далее вычисляет исходное сообщение $m = ex^{-1} \pmod p$.

Алиса зашифровала сообщение, применяя к нему $[c_A]D_B$. Никто не знает значения c_A, поэтому, хотя D_B и является открытым ключом, никто не знает $[c_A]D_B$. Злоумышленнику для восстановления сообщения придется вычислить c_A, зная точки G и $[c_A]G$. Сделать это будет нелегко.

Боб также не знает c_A, но ему в качестве подсказки посылается $[c_A]G$. Умножив $[c_A]G$ на свой закрытый ключ, Боб получит значение, которое было применено Алисой к незашифрованному сообщению. Тем самым Боб, не зная c_A, но имея свой закрытый ключ, может восстановить исходное сообщение.

20.3. a) $(446, 227)$;
b) $(326, 675)$;
c) $(109, 200)$.

20.4. a) $(188, 658)$;
b) $(33, 396)$;
c) $(73, 679)$.

20.5. a) Эллиптическая кривая $E_7(2, 6)$ состоит из 11 точек: $(1, 3)$, $(1, 4)$, $(2, 2)$, $(2, 5)$, $(3, 2)$, $(3, 5)$, $(4, 1)$, $(4, 6)$, $(5, 1)$, $(5, 6)$ и бесконечно удаленная точка.

b) Эллиптическая кривая $E_{11}(5, 7)$ состоит из 14 точек.

20.6. Шифротекст, отправленный Алисой, равен следующей паре: $\{(4, 2); 20\}$.

20.8. Порядок точки P равен 22; $k = 19$.

20.9.

a) Эллиптическая кривая состоит из 10 точек: $(0, 1)$, $(g^2, 1)$, (g^2, g^6), (g^3, g^2), (g^3, g^5), $(g^5, 1)$, (g^5, g^4), $(g^6, 1)$, (g^6, g^5) и бесконечно удаленная точка.

b) Эллиптическая кривая состоит из 16 точек: $(1, g^{13})$, (g^3, g^{13}), (g^5, g^{11}), (g^6, g^{14}), (g^9, g^{13}), (g^{10}, g^8), (g^{12}, g^{12}), $(1, g^6)$, (g^3, g^8), (g^5, g^3), (g^6, g^8), (g^9, g^{10}), (g^{10}, g), $(g^{12}, 0)$, $(0, 1)$ и бесконечно удаленная точка.

20.10. Открытый ключ Боба равен $K_{Bopen} = D_B = [3]G = (g^{10}, g)$. Алиса выполняет следующие действия.

1. $k = 3$.
2. (.) $Q = [k]G = [3]G = (g^{10}, g)$.
3. (.) $R = [k]D_B = [3]D_B = (g^5, g^3)$.
4. $z = mx_R = gg^5 = g^6$.
5. Пару $\{Q, z\}$ Алиса посылает Бобу, т. е. $\{(g^{10}, g), g^6\} \to B$ или

$$\{((0111), (0010)), (1100)\} \to B.$$

20.13. Для того чтобы проверить подлинность сообщения m с помощью подписи (r, s), пользователь Боб должен выполнить следующие процедуры.

1. Проверить выполнимость условий $0 < r < q$ и $0 < s < q$. Если хотя бы одно из них не выполняется, то подпись считается недействительной.
2. Вычислить числа $u_1 = s^{-1}m \pmod q$ и $u_2 = s^{-1}r \pmod q$.
3. Вычислить точку $[u_1]G + [u_2]D = (x_1, y_1)$ и число $v = x_1 \pmod q$.

4. Подпись считается верной, если выполняется равенство $r = v$.

20.14. а) Подпись сообщения $(r, s) = (3, 2)$.

Криптосистема Мак-Элиса

21.1. Алгоритм дешифрования сообщения с помощью криптосиситемы Мак-Элиса выглядит следующим образом.

После получения сообщения c Алиса для его дешифрования выполняет следующие действия.

1. Алиса вычисляет обратную матрицу P^{-1} к матрице перестановки P.

2. Алиса вычисляет вектор $c' = cP^{-1}$.

3. Алиса использует алгоритм декодирования для кода C, чтобы получить информационный блок m' из вектора c'.

4. Алиса осуществляет поправку информационного блока m' с помощью обратной матрицы S^{-1}: $m = m'S^{-1}$.

21.5.
а) Открытый ключ — матрица

$$G' = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \end{pmatrix}.$$

b) Было передано сообщение «11», представленное вектором (1011). При передаче использовался вектор ошибок $e = (10000000)$.

Криптосистема Нидеррайтера

22.1. Процедура шифрования сообщения с помощью криптосистемы Нидеррайтера выглядит следующим образом.

Пусть Бобу необходимо передать Алисе сообщение m, представленное в виде вектора длины n, принадлежащего шару радиуса t с центром в нулевой вершине n-мерного пространства над полем Галуа $GF(q)$.

Боб вычисляет шифротекст как синдром $\sigma = H'm^\top$ и передает его Алисе.

22.2. Алгоритм дешифрования сообщения с помощью криптосистемы Нидеррайтера выглядит следующим образом.

После получения сообщения σ Алиса для его дешифрования выполняет следующие действия.

1. Алиса вычисляет обратную матрицу S^{-1} к обратимой матрице S.

2. Алиса вычисляет вектор $\sigma' = S^{-1}\sigma = S^{-1}H'm^\top = S^{-1}SHDPm^\top = HDPm^\top$.

3. Далее Алиса использует алгоритм декодирования для кода C, чтобы получить вектор ошибок $m'^\top = DPm^\top$ из синдрома σ'.

4. Алиса осуществляет поправку найденного вектора ошибок m' с помощью обратных матриц P^{-1} и D^{-1}: $P^{-1}D^{-1}m'^\top = P^{-1}D^{-1}DPm^\top = m^\top$.

22.4. a) Открытый ключ криптосистемы

$$H' = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \end{pmatrix}.$$

b) Открытый ключ криптосистемы

$$H' = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \end{pmatrix}.$$

Ответы по сжатию данных

Энтропия, ее свойства. Теорема Шеннона

23.1. $\mathcal{H}(A) = \log k$.

23.2. 5 бит информации.

23.3. При извлечении шара из первой урны имеем следующие вероятности: вероятность извлечь красный шар равна $\frac{5}{7}$, синий — $\frac{1}{5}$, зеленый шар — $\frac{3}{35}$. При извлечении шара из второй урны имеем следующие вероятности: вероятность извлечь красный шар равна $\frac{11}{35}$, синий — $\frac{3}{7}$, зеленый шар — $\frac{9}{35}$.

По определению энтропии при первом опыте A_1 имеем

$$\mathcal{H}(A_1) = -\frac{5}{7}\log\frac{5}{7} - \frac{1}{5}\log\frac{1}{5} - \frac{3}{35}\log\frac{3}{35} < 1,11;$$

энтропия второго опыта A_2 равна

$$\mathcal{H}(A_2) = -\frac{11}{35}\log\frac{11}{35} - \frac{3}{7}\log\frac{3}{7} - \frac{9}{35}\log\frac{9}{35} > 1,54.$$

Поскольку $\mathcal{H}(A_2) > \mathcal{H}(A_1)$, то исход второго опыта более неопределен, чем исход первого.

23.4. *Указание.* Необходимо посчитать энтропии обоих опытов и сравнить их. Тот опыт, энтропия которого меньше, более достоверен.

23.5. Действительно, из $0 \le p_i \le 1$ имеем $\frac{1}{p_i} \ge 1$ и $\log\frac{1}{p_i} \ge 0$, т. е. $-\log p_i \ge 0$, отсюда $-p_i \log p_i \ge 0$. Поскольку, по определению, $-p_i \log p_i = 0$ при $p_i = 0$, то для любого $p_i \ge 0$ выполняется $-p_i \log p_i \ge 0$ и, следовательно,

$$\mathcal{H}(A) = -\sum_{i=1}^{k} p_i \log p_i \ge 0.$$

При $\mathcal{H}(A) = 0$ каждое слагаемое равно нулю, а значит, либо $p_i = 0$, либо $\log p_i = 0$, т. е. $p_i = 1$. Так как $\sum_{i=1}^{k} p_i = 1$, то среди вероятностей p_i принять значение 1 может лишь одна, остальные равны нулю. Таким образом, неопределенность события равна нулю тогда и только тогда, когда исход события заранее известен, в остальных случаях энтропия положительна.

23.6. Рассмотрим функцию $f(x) = \log x$. Она выпукла вверх при $x > 0$, поскольку ее вторая производная меньше нуля. Положим $\beta_i = p_i$. Тогда с учетом $\sum_{i=1}^{k} p_i = 1$ и неравенства Йенсена имеем

$$\mathcal{H}(A) = -\sum_{i=1}^{k} p_i \log p_i = \sum_{i=1}^{k} p_i \log\left(\frac{1}{p_i}\right) \le \log\left(\sum_{i=1}^{k} p_i \frac{1}{p_i}\right) = \log k.$$

23.7. Рассмотрим доказательство в случае, когда все p_i положительны (при $p_i = 0$ для некоторого $i = 1, \ldots, k$ доказательство аналогично с некоторыми модификациями). Воспользуемся неравенством Йенсена при $\beta_i = p_i$, $x_i = q_i/p_i$, $i = 1, \ldots, k$, для функции $f(x) = \log x$:

$$\sum_{i=1}^{k} p_i \log\frac{q_i}{p_i} \le \log\left(\sum_{i=1}^{k} p_i \cdot \frac{q_i}{p_i}\right) = \log\left(\sum_{i=1}^{k} q_i\right) = \log 1 = 0.$$

Отсюда имеем

$$\sum_{i=1}^{k} p_i \log q_i - \sum_{i=1}^{k} p_i \log p_i \le 0,$$

откуда вытекает требуемое. Неравенство Йенсена переходит в равенство только тогда, когда $x_1 = \ldots = x_k$, или в нашем случае при $q_1/p_1 = \ldots = q_k/p_k$, т. е. когда векторы $(q_1, \ldots, q_k)$ и $(p_1, \ldots, p_k)$ пропорциональны, и, следовательно, в силу

$$\sum_{i=1}^{k} q_i = \sum_{i=1}^{k} p_i = 1$$

имеем $q_i = p_i$.

23.8. Из неравенства $p_i \le \frac{1}{2^{l_i-1}}$ имеем $2^{l_i-1} \cdot p_i < 1$, откуда следует $2^{l_i-1} < \frac{1}{p_i}$. Логарифмируя, получаем $l_i - 1 < -\log p_i + 1$. Вычислим стоимость $C_{Shannon}$ побуквенного кодирования, гарантируемую кодированием Шеннона:

$$C_{Shannon} = \sum_{i=1}^{k} p_i\, l_i < -\sum_{i=1}^{k} p_i\, \log p_i + \sum_{i=1}^{k} p_i = \mathcal{H}(A) + 1$$

в силу $\sum_{i=1}^{k} p_i = 1$.

23.10. $\mathcal{H}(A) + \mathcal{H}(B) = -\sum_{AB} p(x,y)(\log p(x) + \log p(y)$, где AB — произведение источников A и B и $p(x,y)$ — вероятность появления буквы $(a,b) \in AB$. Поскольку $\sum_{AB} p(x)p(y) = 1$, используя задачу 23.7, имеем

$$-\sum_{AB} p(x,y)(\log(p(x)p(y)) \ge -\sum_{AB} p(x,y)(\log p(x,y) = \mathcal{H}(AB).$$

Доказать, что равенство достигается тогда и только тогда, когда $p(x)p(y) = p(x,y)$, т. е. в случае бернуллиевских источников.

23.11. Применить индукцию, используя задачу 23.10.

23.12. Стоимость кодирования на букву сообщения в данном случае равна среднему числу кодовых символов, затрачиваемых на букву сообщения, т. е. $C^{(N)} = \frac{C(A)}{N} = \frac{1}{N}\sum_{i=1}^{n^N} p(u_i) l_i$.

23.15. a) $C_N^m \le N\mathcal{H}(\frac{m}{N})$.

b) *Указание.* Доказать индукцией по N, что справедливо неравенство

$$\frac{N!}{m_1!\, m_2! \cdots m_k!} \le 2^{N \cdot \mathcal{H}(\frac{m_1!}{N}, \ldots, \frac{m_k!}{N})}.$$

Далее, прологарифмировав это неравенство, после несложных преобразований получить требуемое неравенство.

Префиксное и разделимое кодирование. Графы Маркова

24.8. a) $(0(10)^{2014\times 2013})^*$;

b) любая последовательность слов из множества $01010101010((01)^{2014}010)^*$;

c) любая последовательность слов из множества $(101)^{k-1}10(11)^*0$.

Оптимальность. Коды Фано, Хаффмена и Шеннона

25.5. a) Сначала рассмотрим последовательные редукции набора длин (полученные заменой двух наибольших чисел L в наборе на $L-1$): $\{1,3,3,3,4,4\}$ последовательно редуцируется до $\{1,3,3,3,3\}$, $\{1,3,3,2\}$, $\{1,2,2\}$, $\{1,1\}$. Согласно конструкции

Хаффмена, по этим последовательностям легко восстановить дерево и соответствующий ему оптимальный код, начиная с последнего набора и заканчивающего первым: $\{0,1\}$, $\{0,10,11\}$, $\{0,101,100,11\}$, $\{0,101,100,110,111\}$, $\{0,101,100,110,1110,1111\}$. Набор вероятностей также можно восстановить, анализируя последовательности редукций набора длин. Набору $\{1,1\}$ можно сопоставить любую пару вероятностей с условием невозрастания, например $\{0.6,0.4\}$, далее вероятность 0.4 разбивается на два числа, например, равных 0.2, согласно переходу к предыдущему набору: $\{1,2,2\}$. Продолжая процесс таким образом, получим наборы: $\{0.6,0.2,0.2\}$, $\{0.6,0.1,0.1,0.2\}$, $\{0.6,0.1,0.1,0.1,\ 0.1\}$, $\{0.6,0.1,0.1,0.1,0.05,0.0.5\}$.

b) Например, $\{1/2,1/6,1/6,1/18,1/18,1/18\}$.

25.8. d) Вычислим кумулятивные вероятности источника $\{1/3,1/3,1/6,1/6\}$: $P_1 = 0$, $P_2 = 1/3$, $P_3 = 2/3$, $P_4 = 5/6$. Определим длины слов двоичного кода:

$$l_1 = l_2 = \lceil -log_2(1/3) \rceil = 2,\ l_3 = l_4 = \lceil -log_2(1/6) \rceil = 3.$$

Найдем представления для кумулятивных вероятностей в двоичной системе счисления. Представления чисел $1/3$ и $2/3$ могут быть получены с использованием формулы для бесконечной геометрической прогрессии: $q_0/1-q = 1/3$, где $q_0 = 1/4$ и $1/2$ соответственно. Чтобы получить двоичное представление $5/6$, лучше воспользоваться алгоритмом, описанным в теоретическом разделе задачника. Таким образом, получаем, что $(P_1)_2 = 0.0$, $(P_2)_2 = 0.(01)$, $(P_3)_2 = 0.1(01)$, $(P_4)_2 = 0.1(10)$. Так как по определению кода Шеннона i-е кодовое слово есть l_i знаков после запятой в двоичном разложении P_i, то имеем следующие кодовые слова: $\{00,01,101,110\}$. Стоимость кода равна $7/3$. Длины троичного кода равны: $l_1 = l_2 = 1, l_3 = l_4 = 2$. Рассмотрим кумулятивные вероятности в троичной системе исчисления: $(P_1)_3 = 0.0$, $(P_2)_3 = 0.1$, $(P_3)_3 = 0.2$, $(P_4)_3 = 0.2(1)$. Откуда получаем выражения для кодовых слов: $\{0,1,20,21\}$. Стоимость кода равна $4/3$.

e) Прежде всего, переупорядочим вероятности по невозрастанию: $\{1/3,4/15,1/5,2/15,1/15\}$. Кумулятивные вероятности этого источника равны: $P_1 = 0$, $P_2 = 1/3$, $P_3 = 3/5$, $P_4 = 4/5$, $P_4 = 14/15$. Длины двоичного и троичных кодов равны: $l_1 = 2, l_2 = 2, l_3 = 3, l_4 = 3, l_5 = 4$ и $l_1 = 1, l_2 = 2, l_3 = 2, l_4 = 2, l_5 = 3$ соответственно. Выделяя нужное количество знаков после запятой в двоичном разложении кумулятивных вероятностей, учитывая измененный порядок вероятностей, получим следующие двоичные и троичные коды: $\{01,00,100,110,1110\}$, $\{10,0,12,21,220\}$. Стоимости кодов равны $37/15$ и $9/5$ соответственно.

Адаптивное кодирование

26.1. *Указание.* Для кодирования использовать монотонный код $\{0,10,11\}$. При декодировании использовать такую же «стопку книг», находящуюся в начальный момент времени в начальном состоянии. В дальнейшем над ней провести те же преобразования, что и при кодировании, что гарантирует однозначность восстановления исходной последовательности при отсутствии помех в канале связи.

26.3. Метод «стопка книг» особенно эффективен при кодировании серий одинаковых букв сообщения, поскольку часто встречающиеся буквы сообщения находятся в верхних позициях «стопки» и, следовательно, кодируются более короткими кодовыми словами.

26.4. $n^{(1)} = 1$, $n^{(2)} = 2$, $n^{(3)} = 4$, $n^{(5)} = 16$, $n^{(5)} = 2^{16}$, $n^{(6)} = 2^{2^{16}}$.

26.5. $\log^* 37 = 4$, $\log^* 100 = 4$, $\log^* 2^{10^4} = 5$.

26.6. $\log^* 37 = 4$, $\log^* 100 = 4$, $\log^* 2^{10^4} = 5$.

26.7. Длина $Bin'(x)$ равна $\lfloor \log x \rfloor$.

26.8. а) $Lev(37) = 1111000100101$.

26.9. 75.

26.10. $|Lev(x)| = \log^* x + 1 + \sum_{i=1}^{\log^* x} \log^{(i)} x$.

26.17. Имеем $(a_1a_1a_4a_3a_1a_1a_2a_4)111$. По частоте встречаемости букв несложно видеть, что буква a_1 имеет код 0, буква a_4 — код 10, буква a_2 — код 110, а буква a_3 имеет код 111. Следовательно, $x = a_3$.

Заключение

Настоящий сборник задач не претендует на полноту освещения всех областей теории информации — бурно развивающейся в последние десятилетия науке, включающей теорию кодов, корректирующих ошибки в каналах связи с шумами, криптологию и сжатие информации. Цель задачника — познакомить читателя с азами современной теории информации посредством решения упражнений и задач, подготовить его к чтению специальной научной литературы по теории кодирования, криптологии и сжатию данных. Для понимания изложенного в книге материала достаточно знаний основ теории информации, линейной алгебры, теории групп, теории чисел, комбинаторики и теории вероятностей. Впрочем, все необходимые для понимания основного материала определения и утверждения имеются в тексте. В сборнике задач также приведены некоторые нерешенные проблемы.

Следует подчеркнуть, что выбор материала, изложенного в настоящем пособии, отвечает в некотором смысле вкусам авторов и соответствует тем темам и разделам теории информации, которые излагаются в разных курсах авторов в Новосибирском государственном университете на факультете информационных технологий и механико-математическом факультете. Авторы со всей ответственностью осознают факт отсутствия некоторых разделов теории информации в данном задачнике и в дальнейших переизданиях задачника возможно восполнение этих пробелов и пополнение имеющихся новыми коллекциями задач. Некоторые разделы опущены намеренно, например, криптосистемы с секретными ключами, поскольку имеется достаточное количество доступной и даже популярной литературы по данному разделу.

Пособие написано по многочисленным просьбам студентов математического факультета и факультета информационных технологий Новосибирского государственного университета. Изложенный материал был апробирован при проведении семинарских занятий на факультете информационных технологий, а также при чтении лекций в течение ряда лет в Новосибирском государственном университете на указанных выше факультетах. Помимо студентов математических факультетов и факультетов информационных технологий университетов, задачник также может быть полезен студентам физических и технических факультетов, интересующимся математическими основами проблем передачи данных по каналам связи.

Авторы выражают признательность всем коллегам Института математики СО РАН, аспирантам, студентам, которые помогали шлифовать в дискуссиях презентации многих тем, решений задач. Авторы пользуются случаем выразить благодарность тем студентам, которые придумывали задачи и (или) приняли участие в создании ряда задач. Часть из наиболее сложных и интересных таких задач также включена в настоящий сборник задач.

Список литературы

Книжная полка по теории кодирования

Основная литература

1. Мак-Вильямс Ф. Дж. А.., Слоэн Н. Дж. А. Теория кодов, исправляющих ошибки: Пер. с англ. М.: Связь, 1979. 744 с.

2. Соловьева Ф. И. Введение в теорию кодирования: учеб. пособие. Новосибирск, 2011. 123 с.

3. Сидельников В. М. Теория кодирования. М.: Физматлит, 2008. 324 с.

4. Сагалович Ю. Л. Введение в алгебраические коды: учеб. пособие. М.: Изд. ИППИ РАН, 2010. 302 с.

5. Колесник В. Д. Кодирование при передаче и хранении информации (алгебраическая теория блоковых кодов). М.: Высш. шк., 2009. 550 с.

6. Шоломов Л. А. Основы теории дискретных логических и вычислительных устройств. М.: Наука, 1980. 399 с.

7. Питерсон У., Уэлдон Э. Коды, исправляющие ошибки: Пер. с англ. М.: Мир, 1976. 594 с.

8. Блейхут Р. Теория и практика кодов, контролирующих ошибки: Пер. с англ. М.: Мир, 1986. 576 с.

9. Касами Т., Токура Н., Ивадари Е., Инагаки Я. Теория кодирования: Пер. с яп. М.: Мир, 1978. 576 с.

10. van Lint J. H. Introduction to coding theory: 3rd rev. Springer-Verlag Berlin Heidelberg; N. Y., 1999. 227 p.

Дополнительная литература

11. Шеннон Л. А. Работы по теории информации и кибернетике. М.: ИЛ, 1963. 829 с.

12. Конвей Дж. Н., Слоэн Н. Дж. А. Упаковки шаров, решетки и группы: Пер. с англ. М.: Мир, 1990. Т. 1, 2.

13. Берлекэмп Э. Алгебраическая теория кодирования: Пер. с англ. М.: Мир, 1971. 477 с.

14. Гаврилов Г. П., Сапоженко А. А. Задачи и упражнения по дискретной математике. М.: Физматлит, 2005. 416 с.

15. Цымбал В. П. Теория информации и кодирование. Киев: Вища шк., 1992, 263 с.

16. Solov'eva F. I. On perfect codes and related topics: Lecture Notes. Pohang University of Science and Technology (POSTECH), Republik of Korea, 2004. 80 p.

Книжная полка по криптологии

Основная литература

1. Рябко Б. Я., Фионов А. Н. Основы современной криптографии для специалистов в информационных технологиях. М.: Научный Мир, 2004. 172 с.

2. Рябко Б. Я., Фионов А. Н. Основы современной криптографии и стеганографии. М.: Горячая линия-Телеком, 2010. 232 с.

3. Земор Ж. Курс криптографии. М.–Ижевск: НИЦ «Регулярная и хаотическая динамика»; Ин-т комп. ис-ний, 2006. 256 с.

4. Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В. Основы криптографии. М.: Гелиос АРВ, 2002. 480 с.

5. Нечаев В. И. Элементы криптографии. Основы теории защиты информации. М.: Высш. шк., 1999. 109 с.

6. Ященко В. В. Введение в криптографию. М.: МЦНМО «ЧеРо», 1999.

7. Саломаа А. Криптография с открытым ключом: Пер. с англ. М.: Мир, 1996. 318 с.

8. ван Тилборг Х. К. А. Основы криптологии: Пер. с англ. М.: Мир, 2006. 472 с.

Дополнительная литература

9. Шеннон Л. А. Работы по теории информации и кибернетике. М.: ИЛ, 1963.

10. Введение в криптографию. Под общ. ред. В. В. Ященко. М.: МЦНМО «ЧеРо», 2000. 272 с.

11. Саломаа А. Криптография с открытым ключом: Пер. с англ. М.: Мир, 1996. 318 с.

12. Баричев С., Серов Р. Основы современной криптографии. М., 2001. 121 с.

13. Коблиц Н. Основы теории чисел и криптографии: Пер. с англ. М.: ТВП, 2001. 260 с.

Книжная полка по сжатию данных

Основная литература

1. Кричевский Р. Е. Сжатие и поиск информации. М.: Наука, 1986.
2. Кудряшов Б. Д. Теория информации. СПб.: Питер, 2009. 213 с.
3. Шоломов Л. А. Основы теории дискретных логических и вычислительных устройств. М.: Наука, 1980. 399 с.
4. Потапов В. Н. Теория информации. Кодирование дискретных вероятностных источников. Новосибирск: Изд. центр НГУ, 1999. 71 с.

Дополнительная литература

5. Шеннон Л. А. Работы по теории информации и кибернетике. М.: ИЛ, 1963.
6. Гаврилов Г. П., Сапоженко А. А. Задачи и упражнения по дискретной математике. М.: Физматлит, 2005. 416 с.
7. Цымбал В. П. Теория информации и кодирование. Киев: Вища шк., 1992, 263 с.
8. Яглом А. М., Яглом И. М. Вероятность и информация. М.: Наука, 1973. 511 с.

Интернет-ресурсы

1. Сайт по теории информации в НГУ:

   `http://www.codingtheory.nsu.ru`.

2. Потапов В. Н. Введение в теорию информации. 102 с.

   `http://math.nsc.ru/~potapov/`.

Учебное издание

Соловьева Фаина Ивановна,
Лось Антон Васильевич,
Могильных Иван Юрьевич

СБОРНИК ЗАДАЧ ПО ТЕОРИИ КОДИРОВАНИЯ, КРИПТОЛОГИИ И СЖАТИЮ ДАННЫХ

Учебное пособие

Редактор К. В. Шмугурова
Оригинал-макет авторов

Подписано в печать 16.12.13.
Формат 60×84 1/8. Офсетная печать.
Уч.-изд. л. 12,5. Усл. печ. л. 11,6. Тираж 200 экз.

Заказ №

Редакционно-издательский центр НГУ.
630090, Новосибирск, ул. Пирогова, 2.