МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

КАЗАНСКИЙ (ПРИВОЛЖСКИЙ) ФЕДЕРАЛЬНЫЙ
УНИВЕРСИТЕТ

ИНСТИТУТ ВЫЧИСЛИТЕЛЬНОЙ МАТЕМАТИКИ И
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
Кафедра системного анализа и информационных технологий

Долгов Дмитрий Александрович

ВВЕДЕНИЕ В ТЕОРИЮ КОДИРОВАНИЯ. ЧАСТЬ 1

Методическое пособие

КАЗАНЬ, 2020

УДК 519.725
ББК 22.1, 32.811.4

Рецензенты:
заведующий кафедры системного анализа и информационных технологий КФУ, профессор, доктор технических наук **Р.Х. Латыпов**;
кандидат физико-математических наук, доцент кафедры алгебры и математической логики КФУ **М.М. Ямалеев**

Долгов Д.А.
Введение в теорию кодирования. Часть 1: Методическое пособие / Д.А. Долгов. – Казань: КФУ, 2020. – 27 с.

Методическое пособие предназначено для проведения практических занятий по курсу «Теория кодирования информации» для студентов, обучающихся по направлениям «Фундаментальная информатика и информационные технологии», «Информационная безопасность». Методическое пособие дает основы алгебры, необходимой для современной алгебраической теории кодирования. Изучаются основные алгебраические структуры, их свойства и используемые операции, в частности дается введение в поля Галуа. Изучаются основы теории линейных кодов. Методическое пособие содержит большое количество теоретическое материала, примеров и задач для самопроверки.

Содержание

1. Введение

Коды появились в глубокой древности фактически с появлением системы знаков для записи слов, звуков, информации, которые позднее развились в различные языки. Каждый язык представляет сложную систему кодирования, которая включает в свою конструкцию алфавит, слова, и, конечно, грамматику. Язык позволяет в окружающем шуме передавать информацию по возможности быстро, надежно, с большой долей избыточности.

Появление в 1948 и 1949 гг. классических работ Шеннона вызвало большой поток исследований, посвященных построению эффективных схем кодирования информации для передачи по реальным каналам с шумами. Основные усилия направлялись на построение легко реализуемых схем кодирования и декодирования. Новый подход к решению этой проблемы был найден в важных работах Хоквингема [1959], Боуза и Чоудхури [1960], Рида и Соломона [1960] и других авторов. Они выбрали в качестве алфавита кода поле Галуа. Эти работы послужили основой алгебраической теории кодирования.

Данное методическое пособие дает основы алгебры, необходимой для современной алгебраической теории кодирования. Изучаются основные алгебраические структуры, их свойства и используемые операции, в частности дается введение в поля Галуа. Методическое пособие содержит большое количество теоретическое материала, примеров и задач для самопроверки.

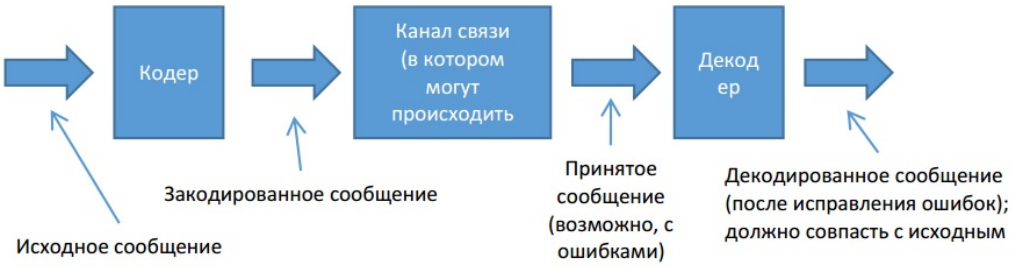
2. Коды, исправляющие ошибки

Подробное изложение информации можно найти в [6, 7].

Теория кодирования изучает модели хранения и передачи «дискретной» информации и предлагает способы оптимального её кодирования. Основные требования, которые предъявляются к способам кодирования:

- Однозначность. По закодированному сообщению нужно уметь однозначно восстанавливать исходное. Это требование обязательно.
- Минимальная избыточность. Закодированное сообщение должно при прочих равных условиях иметь как можно меньший объём для скорейшей передачи по каналам связи.
- Устойчивость к ошибкам. Возможность расшифровать закодированное сообщение даже при возникновении ошибок при его передаче.

В курсе «Теория кодирования информации» упор делается на коды, исправляющие ошибки. Введем модель канала с ошибками:



Пусть на вход кодеру приходит сообщение $m = (m_0, m_1, \cdots, m_k)$. Ради надежной передачи информации, вместо k символов исходного сообщения приходится передавать $n > k$ символов, т.е вводится избыточность. Сопоставление некоторым способом n символов заданным k символам вектора называют *кодированием*. Отношение k/n называется скоростью передачи. Восстановление закодированных k символов по n переданным символам, каждый из которых мог подвергнуться искажению с вероятностью, называется *декодированием*. При этом декодирование может быть ошибочным.

Теорема 1 (Шеннон). *Существует кодирование, позволяющее добиться сколь угодно достоверной передачи сообщения, лишь бы скорость передачи не превосходила некоторой величины, которая называется пропускной способностью канала.*

Чаще всего рассматривают следующие типы ошибок:

1) Ошибки замещения: торт → порт
   - Симметричные (если символ x может замениться на y, и обратно)
   - Несимметричные
2) Ошибки стирания: торт → то?т
3) Ошибки выпадения: торт → тор
4) Ошибки вставки: торт → торты
5) Комбинации перечисленных типов

Пусть A_q — кодовый алфавит, алфавит канала, и пусть $|A_q| = q$. Будем называть q-ичным кодом любое подмножество $C \subseteq {A_q}^n$, где n — длина кода (длина кодовых слов), $|C|$ — мощность кода (число кодовых слов). Мы будем рассматривать двоичные коды, т.е. когда $q = 2$ и $A_q = \{0, 1\}$. Тогда, любой код $C \in {A_2}^n$. Таким же важным является случай, когда A_q является полем. В этих случаях для произвольного слова a будем через $||a||$ обозначать вес этого слова, то есть величину $\#\{i : a_i \neq 0\}$.

Определение 2.1. *Блоковый код- код, в котором все слова имеют одинаковую длину.*

Пусть a и b — слова в алфавите канала. Обозначим через $\widetilde{d}(a, b)$ минимальное число ошибок, в результате которых a может перейти в b. Способ кодирования позволяет обнаруживать k ошибок, если для любых различных кодовых сообщений a' и a'' при передаче в канал a' на выходе из канала не может получиться a'' (если в канале произошло не более k ошибок). Иначе говоря, $\widetilde{d}(a', a'') > k$.

Способ кодирования позволяет исправлять k ошибок, если при передаче в канал различных кодовых сообщений a' и a'' на выходе из канала будут получаться различные сообщения (при условии, что с каждым отдельным сообщением в канале происходит не более k ошибок).

Определение 2.2. $\widetilde{d}$ *является метрикой, если:*

- $\forall a, b\ \widetilde{d}(a, b) = \widetilde{d}(b, a)$ *(симметричность)*
- $\forall a \neq b\ \widetilde{d}(a, b) > 0$

- $\forall a\ \widetilde{d}(a,a) = 0$
- $\forall a,b,c\ \widetilde{d}(a,b) \leqslant \widetilde{d}(a,c) + \widetilde{d}(c,b)$ *(неравенство треугольника)*

Так бывает не всегда. Например, если в канале могут происходить лишь ошибки вставки, то при $a \neq b$ $\widetilde{d}(a,b)$, $\widetilde{d}(b,a)$ вовсе не определена.

Определение 2.3. *Пусть* $\widetilde{d}(\cdots,\cdots)$ *– метрика и* C *– код. Величина* $\widetilde{d}(C)$ *называется кодовым расстоянием кода* C*, если*

$$\widetilde{d}(C) = \min_{\substack{a \neq b \\ a,b \in C}} \widetilde{d}(a,b)$$

Хеммингово расстояние $d(a,b)$ опреляется как число координат, в которых отличаются n-мерные вектора, является метрикой. Здесь и далее будем рассматривать метрику Хемминга. Кодовое расстояние равно минимальному расстоянию Хемминга между различными кодовыми словами. О связи кодового расстояния с устойчивостью к ошибкам расскажет следующее

Предложение 2.1. *Код* C

1) *исправляет все независимые ошибки кратности* t *и менее, или обнаруживает все независимые ошибки кратности* $2t$ *и менее при* $d \geqslant 2t+1$*;*
2) *исправляет все независимые ошибки кратности* t *и менее, и одновременно обнаруживает все независимые ошибки кратности* $t+1$ *при* $d \geqslant 2t+2$*.*

Основная задача теории кодов, исправляющих ошибки: строить коды, для которых число кодовых слов как можно больше, кодовое расстояние как можно больше, а длина кодовых слов как можно меньше.

Если C — q-ичный код с длиной слов n, числом слов M и кодовым расстоянием d, то пишут: «C является (n, M, d) q-кодом». Если код двоичный, то символ q не указывают.

3. Алгебраические основы теории кодирования

3.1. Основные алгебраические структуры

Подробное изложение информации можно найти в [1, 2, 3, 4].

Определение 3.1. *Пусть S — произвольное множество. Бинарной (алгебраической) операцией на S называется произвольное (но фиксированное) отображение $\tau : S \times S \to S$ декартова квадрата $S^2 = S \times S$ в S.*

Таким образом, любой упорядоченной паре (a, b) элементов $a, b \in S$ ставится в соответствие однозначно определённый элемент $\tau(a, b)$ того же множества S. Аналогично определяются n-арные операции. Иногда вместо $\tau(a, b)$ пишут $a\tau b$, а ещё чаще бинарную операцию на S обозначают каким-нибудь специальным символом: $*, \times, \circ, \bullet$ или $+$. Будем обозначать ab произведением, а $a + b$ — суммой элементов $a, b \in S$.

Определение 3.2. *Множество S называется замкнутым относительно бинарной операции $\circ$, если $a \circ b \in S$ $\forall a, b \in S$.*

Определение 3.3. *Бинарным отношением R на множестве S называется любое множество упорядоченных пар, т.е $R \subset S \times S$.*

Определение 3.4. *Алгебраической структурой (алгебраической системой) называется упорядоченная тройка $\mathbb{AS} = (S, \Omega, \Omega_0)$. где S – непустое множество, Ω – множество операций на S и Ω_0 – множество отношений на S.*

Определение 3.5. *Алгеброй называется упорядоченная пара $\mathbb{A} = (S, \Omega)$, где S – непустое множество и Ω – множество операций на S.*

Не трудно видеть, что алгебра – алгебраическая структура с $\Omega_0 = \emptyset$. Здесь и далее при обозначении алгебраической структуры в случае $\Omega_0 = \emptyset$ будем указывать только множество S и заданные операции Ω.

Определение 3.6. *Группой $(G, \circ)$ называется множество G с операцией $\circ$, обладающей следующими свойствами:*

1) $a \circ (b \circ c) = (a \circ b) \circ c$ $\forall a, b, c \in G$ *(ассоциативность);*

2) $\exists e \in G$ *(единица), что* $a \circ e = e \circ a = a$ $\forall a \in G$.

3) $\forall a \in G\ \exists a^{-1} \in G$ *(обратный элемент), что* $a \circ a^{-1} = a^{-1} \circ a = e$.

Для краткости группу будем обозначать G. Группа G называется абелевой или коммутативной, если $a \circ b = b \circ a\ \forall a, b \in G$. Если задана операция умножения $\cdot$, то группу называют группой по умножению или мультипликативной группой, пишут $a \cdot b$ или ab. Если задана операция сложения $+$, то группу называют группой по сложению или аддитивной группой. Группа, содержащая конечное число элементов, называется конечной, и бесконечной в противном случае. Порядком группы называется число ее элементов. Для бесконечной группы ее порядок также считают бесконечным. Пример алгебры — группа.

Примеры.

1) Числовые множества $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ образуют абелевы группы по сложению.

2) $(\{0\}, +)$ — одноэлементная абелева группа.

3) $(\mathbb{N}, +)$ не является группой, так как в нем нет нейтрального элемента: $\nexists e$: $a + e = a\ \forall a \in \mathbb{N}$.

4) $\mathbb{Q}\backslash\{0\}, \mathbb{R}\backslash\{0\}, \mathbb{C}\backslash\{0\}$ образуют коммутативные группы по умножению. Множества $\mathbb{Q}^{>0}$ и $\mathbb{R}^{>0}$ также образуют коммутативные группы по умножению.

5) $(\{1\}, \cdot)$, $(\{1, -1\}, \cdot)$ образуют коммутативные группы по умножению первого и второго порядка соответственно.

6) Множество $\mathbb{Z}$ по умножению не группа, так как хотя операция умножения ассоциативна и имеется нейтральный по умножению элемент 1, но обратимы лишь 1 и -1.

Предложение 3.1. *Для произвольной группы* $G = (G, \circ)$ *имеем:*

1) В G *существует единственная единица.*

2) $\forall a \in G\ \exists a^{-1} \in G$.

3) В G *однозначно разрешимы уравнения* $ax = b$, $xa = b\ \forall a, b \in G$, *а именно* $x = a^{-1}b$, $x = ba^{-1}$.

4) $(a^{-1})^{-1} = a\ \forall a \in G$.

Как проверить является ли алгебраическая структура $(G, \circ)$ группой? Нужно проверить наличие бинарной операции, действующей для всех элементов множества G, проверить замкнутость G, а также проверить выполнимость трех основных операций и при необхомости условие коммутативности. Аналогично проверяется принадлежность и к другим алгебраическим структурам с учетом условий и введенных бинарных операций.

Определение 3.7. *Кольцом $\langle R, +, \cdot \rangle$ называется непустое множество R с заданными на нем двумя бинарными операциями, называемыми сложением $+$ и умножением $\cdot$ и удовлетворяющими следующим условиям:*

а) $(R, +)$ *— абелева группа;*

б) $a(bc) = (ab)c \ \forall a, b, c \in R$ *(ассоциативность по умножению).*

в) $a(b + c) = ab + ac \ \forall a, b, c \in R$ *(левая дистрибутивность).*

г) $(a + b)c = ac + bc \ \forall a, b, c \in R$ *(правая дистрибутивность).*

Для краткости кольцо будем обозначать R. $(R, +)$ называется аддитивной группой кольца. Отметим, что в теории колец рассматриваются структуры, в которых ассоциативность умножения не требуется. При этом в ситуации, когда она отсутствует, такие структуры называют неассоциативными кольцами, а при ее наличии — ассоциативными. У нас по умолчанию будут только ассоциативные кольца. Кольцо R называется коммутативным, если умножение коммутативно, т. е. $ab = ba \ \forall a, b \in R$. В отличие от групп, коммутативное кольцо не принято называть абелевым. Кольцо называется кольцом с единицей, если $\exists e \in R \ \forall a \in R \ ae = ea = a$. Единичный элемент кольца принято обозначать обычной единицей 1.

Примеры.

1) Нулевое кольцо. Пусть $R = \{0\}$, $0 + 0 = 0$, $0 \cdot 0 = 0$. Тогда $\langle R, +, \cdot \rangle$ — коммутативное кольцо с единицей, которая совпадает с нулем. Такое кольцо называют нулевым кольцом.

2) Кольцо с нулевым умножением. Пусть $G = (G, +)$ — абелева группа по сложению, содержащая по крайней мере два элемента. Определим в G умножение, положив $ab = 0 \ \forall a, b \in G$. Тогда $\langle G, +, \cdot \rangle$ будет коммутативным кольцом без 1, которое называется кольцом с нулевым умножением.

3) $\langle \mathbb{Z}, +, \cdot \rangle$, $\langle \mathbb{Q}, +, \cdot \rangle$, $\langle \mathbb{R}, +, \cdot \rangle$ — коммутативные кольца с единицей.

4) $\langle \mathbb{Z}_p, +, \cdot \rangle$ — кольцо классов вычетов по модулю p. Это коммутативное кольцо с единицей.

5) $\langle 2\mathbb{Z}_p, +, \cdot \rangle$ — коммутативное кольцо без единицы.

6) Кольцо целых гауссовых чисел. $\langle \mathbb{Z}[i], +, \cdot \rangle$, где $\mathbb{Z}[i] = a + bi : a, b \in \mathbb{Z} \subset \mathbb{C}$. Это коммутативное кольцо с единицей $1 = 1 + 0i$.

Предложение 3.2. *Пусть $\langle R, +, \cdot \rangle$ — кольцо. Тогда справедливы следующие утверждения:*

1) Значение конечной суммы элементов кольца не зависит от порядка выполнения суммирования (обобщенная ассоциативность) и порядка слагаемых (обобщенная коммутативность).

2) Нуль в кольце единственный.

3) Для любого элемента кольца противоположный к нему — единственный.

4) $-(-a) = a \ \forall a \in R$.

5) Если в кольце имеется единица, то она единственна.

6) Если в кольце с единицей элемент обратим, то обратный для него единственен.

7) Если R — кольцо с единицей и $a_1, ..., a_n$ — его обратимые элементы, то элемент $a_1 a_2 \cdots a_n$ также обратим, при этом $(a_1 \cdot a_2 \cdots a_n)^{-1} = {a_1}^{-1} {a_2}^{-1} \cdots {a_n}^{-1}$.

8) $a \cdot 0 = 0 \cdot a = 0 \ \forall a \in R$.

9) Если R — кольцо с единицей 1 и $0 = 1$, то R — нулевое кольцо.

10) В кольце выполняются правила знаков: $(-a)b = -ab$, $a(-b) = -ab$, $(-a)(-b) = ab \ \forall a, b \in R$.

Определение 3.8. *Z_p — кольцо вычетов по модулю p, состоящее из наименьших неотрицательных остатков деления натуральных чисел на p, т.е. $Z_p = \{0, 1, 2, \cdots, p-1\}$.*

Предложение 3.3. *Множество $\mathbb{Z}_p$ всех обратимых элементов кольца $\mathbb{Z}$ образует коммутативную мультипликативную группу, состоящую в точности из тех элементов $a^{-1} \in \mathbb{Z}_p$, что a и p взаимно просты, и поэтому $|{\mathbb{Z}_p}^*| = \phi(p)$, где $\phi(p)$ — функция Эйлера.*

В кольце $\mathbb{Z}_p$ классов вычетов мы встречаемся с новым явлением, не встречавшимся ранее. Наименьшее натуральное n, для которого в кольце R выполняется равенство

$$\underbrace{1+1+1+1+\cdots+1}_{n}=0$$

называется характеристикой кольца R и обозначается $\mathrm{char}\ R$. Если такого n не существует, то говорят, что R — кольцо нулевой (или бесконечной) характеристики. Таким образом, характеристика кольца с единицей — это порядок единицы в аддитивной группе кольца. Ненулевой элемент a кольца R является делителем нуля, если существует ненулевое b такое, что $ba = 0$ и $ab = 0$.

Предложение 3.4. *Характеристика кольца R с единицей без делителей нуля, если она положительна, всегда является простым числом.*

Определение 3.9. *Подмножество S кольца $\langle R, +, \cdot\rangle$ называется подкольцом этого кольца, если оно замкнуто относительно операций $+$, $\cdot$ и образует кольцо относительно этих операций.*

Определение 3.10. *Подмножество J кольца R называется (двусторонним) идеалом этого кольца, если оно является подкольцом кольца R и для всех $a \in J$, $r \in R$ выполняется $ar \in J$, $ra \in J$.*

$a, b \in R$ принадлежат одному и тому же классу вычетов по модулю J. Множество классов вычетов кольца R по модулю идеала J образует кольцо относительно операций $+$, $\cdot$, определяемых равенствами

$$(a + J) + (b + J) = (a + b) + J \tag{1}$$

$$(a + J)(b + J) = ab + J \tag{2}$$

Определение 3.11. *Кольцо классов вычетов кольца R по модулю идеала J относительно операций (1) и (2) называется фактор-кольцом кольца R по идеалу J и обозначается R/J.*

Определение 3.12. *Поле $(R, +, \cdot)$ — это коммутативное кольцо с единицей $1 \neq 0$, в котором каждый ненулевой элемент обратим. Группа R^* называется мультипликативной группой поля.*

Теорема 2. *$\mathbb{Z}_p$ будет являться полем только в случае простого p.*

Для краткости будем обозначать поле нулевой характеристики как F. Поле представляет из себя гибрид двух абелевых групп - аддитивной $(R, +)$ и мультипликативной $(R \setminus \{0\}, \cdot)$, связанных одним законом дистрибутивности ввиду коммутативности мультипликативной группы. Поле, содержащее бесконечное (конечное) число элементов, называется бесконечным (конечным). Конечное поле $\mathbb{Z}_p$ будем дальше обозначать как $\mathbb{F}_p$ или $GF(p)$ и называть полем Галуа. Следует иметь в виду, что существует конечное поле $GF(p^n)$ с p^n элементами, где — простое, а n — любое целое положительное число. К этому интересному вопросу мы вернёмся в следующей главе.

Примеры.

1) $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ — поля.

2) $\mathbb{Z}$ не является полем, т.к. в нём обратимы только 2 элемента -1, 1.

3) $Z_5 = 0, 1, 2, 3, 4$ является полем, т.к. каждый ненулевой элемент обратим. Операции в Z_5 можно задать таблицами:

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\times$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

4) Z_4 не является полем, т.к. есть делители нуля $2 \times 2 = 4 = 0 \mod 4$.

5) $char\ \mathbb{Z}_n = n$, $char\ \mathbb{Z} = char\ \mathbb{Q} = char\ \mathbb{R} = 0$.

Задачи.

1) Выясните, образует ли группу

   1. $(\mathbb{Z}, \circ)$, где $a \circ b = a + b - m$ при фиксированном $m \in \mathbb{Z}$.
   2. $(\mathbb{N}, \circ)$, где $a \circ b = (a, b)$, НОД — наибольший общий делитель чисел a и b.
   3. $(\mathbb{N}, \circ)$, где $a \circ b = (a, b)$, НОК — наименьшее общее кратное чисел a и b.
   4. $(2\mathbb{Z}, +)$.

5. $(2\mathbb{Z}, \cdot)$.
6. $(\mathbb{Q}, \circ)$, где $a \circ b = 2ab$.
7. $(\mathbb{R}, \circ)$ где $a \circ b = \sqrt[3]{a^3 + b^3}$.

2) Множество всех $n \times n$ матриц с вещественными коэффициентами и отличным от нуля определителем назовем $GL(\mathbb{R})_n$. Доказать, что $(GL(\mathbb{R}_n), \cdot)$ — группа.

3) Выясните, образует ли кольцо

1. множество вещественных чисел $x + y\sqrt{2}$ $x, y \in \mathbb{Q}$.
2. $\langle R, +, \circ \rangle$, если $\langle R, +, \cdot \rangle$ является кольцом и $a \circ b = ba$ $\forall a, b \in R$.

4) Пусть $\langle R, +, \cdot \rangle$ — кольцо с единицей 1 и R^* — множество всех обратимых элементов этого кольца. Доказать, что $(R^*, \cdot)$ — группа.

5) Пусть R — кольцо. Справедлив ли для R бином Ньютона? Да, нет, почему?

6) В кольце Z_6 решите уравнения

1. $4x = 5$
2. $5x = 1$
3. $4x = 1$

7) Какие свойства кольца выполняются, а какие нет для

1. $\langle \mathbb{Z}, +, \circ \rangle$, где $a \circ b = b$, $\forall a, b \in \mathbb{Z}$.
2. $\langle \mathbb{Z} \times \mathbb{Z}, +, \circ \rangle$, где $(a, b) + (c, d) = (a + c, b + d)$, $(a, b) \circ (c, d) = (ac, b + d)$.

8) Докажите, что кольцо многочленов $F[x]$ над произвольным полем F не будет полем.

9) Пусть F — поле. Докажите, что char $F[x]$= char F.

10) Докажите, что в конечном поле из равенства $a^x = a^y$ не следует равенства $x = y$.

11) Докажите, что в поле характеристики $p > 0$ из равенства $a^p = a^p$ следует $a = b$.

3.2. Многочлены и конечные поля

Подробное изложение информации можно найти в [5, 6].

Определение 3.13. *Многочленом f над кольцом R называется выражение вида*

$$f(x) = \sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n,$$

где a_i — элементы кольца R, x — некоторый символ, не принадлежащий кольцу R.

Здесь мы рассматриваем многочлены от одной переменной. Многочлены можно складывать, умножать, а также сравнивать друг с другом. Пусть есть 2 многочлена над кольцом R $f(x)$, $g(x)$. Сложение: $f(x)+g(x) = \sum_{i=0}^{n}(a_i+b_i)x^i$. Умножение: $f(x)g(x) = \sum_{k=0}^{n+m} c_k x^k$, $c_i = \sum_{i+j=k}^{n+m} a_i b_j$, если $f(x) = \sum_{i=0}^{n} a_i x^i$, $g(x) = \sum_{j=0}^{m} b_j x^j$. Многочлены с такими операциями образуют кольцо. Если кольцо R имеет 1 и старший коэффициент равен 1, то многочлен называется нормированным.

Определение 3.14. *Кольцо, образованное многочленами над кольцом R, называется кольцом многочленов и обозначается $R[x]$.*

Нулевой многочлен — многочлен с коэффициентами равными нулю. Степень многочлена f — степень при x старшего отличного от нуля коэффициента, обозначается $\deg(f)$.

Теорема 3. *Пусть $f, g \in R[x]$, тогда*

$$\deg(f+g) \leqslant \max(\deg(f), \deg(g)),$$

$$\deg(fg) \leqslant \deg(f) + \deg(g)$$

Если R — коммутативное кольцо с 1 без делителей нуля (целостное кольцо или область целостности), то

$$\deg(fg) = \deg(f) + \deg(g)$$

Как и в кольце целых чисел, в многочленах над полем существует деление с остатком. Многочлены над полем обозначим $F[x]$, многочлены над конечным полем F_p обозначим $F_p[x]$. $F[x]$, $F_p[x]$ — кольца многочленов.

Теорема 4. *Пусть $g \neq 0$ — многочлен из $F[x]$, F — поле. Тогда, $\forall f(x) \in F[x]$ $\exists g(x), r(x) \in F[x]$: $f = gq + r$,*

Пример.

$f(x) = 2x^5 + x^4 + 3$, $g(x) = 3x^2 + 1$, $f, g \in F_5[x]$. Найдем $q, r \in F_5[x]$, используя обычное деление.

$$
\begin{array}{l|l}
2x^5 + x^4 + 4x + 3 & 3x^2 + 1 \\
\cline{2-2}
-\ 2x^5 + 4x^3 & 4x^3 + 2x^2 + 2x + 1 \\
\cline{1-1}
x^4 + x^3 + 4x + 3 & \\
-\ x^4 + 2x^2 & \\
\cline{1-1}
x^3 + 3x^2 + 4x + 3 & \\
-\ x^3 + 2x & \\
\cline{1-1}
3x^2 + 2x + 3 & \\
-\ 3x^2 + 1 & \\
\cline{1-1}
2x + 2 &
\end{array}
$$

$q(x) = 4x^3 + 2x^3 + 2x + 1$, $r(x) = 2x + 2$, $\deg(r) < \deg(g)$.

Теорема 5. *Пусть $f_1, \cdots, f_n$ — многочлены из $F[x]$, не равные 0. Тогда существует однозначно определенный нормированный многочлен $d \in F[x]$, обладающий следующими свойствами:*

1) *d делит каждый многочлен f_i, $1 \leqslant i \leqslant n$;*

2) *любой многочлен $g \in F[x]$, который делит каждый из многочленов f_i, $1 \leqslant i \leqslant n$, делит и многочлен d.*

Пусть $d_1, \cdots, b_n \in F[x]$, многочлен d может быть представлен в виде

$$d = b_1 f_1 + \cdots + b_n f_n$$

Нормированный многочлен d называется *наибольшим общим делителем* многочленов $f_1, \cdots, f_n$ и обозначается НОД$(f_1, \cdots, f_n)$. Если НОД$(f_1, \cdots, f_n)$=1, то многочлены $f_1, \cdots, f_n$ называются взаимно простыми.

НОД двух многочленов f, $g \in F[x]$ можно найти при помощи алгоритма Евклида. Пусть g отличен от нуля и не делит многочлен f. Тогда, применяя многоратно алгоритм деления, получим

$$
\begin{aligned}
f &= q_1 g + r_1,\ 0 \leqslant \deg(r_1) < deg(g), \\
g &= q_2 r_1 + r_2,\ 0 \leqslant \deg(r_2) < deg(r_1), \\
r_1 &= q_3 r_2 + r_3,\ 0 \leqslant \deg(r_3) < deg(r_2),
\end{aligned}
$$

$$\cdots\cdots\cdots$$

$$r_{s-2} = q_s r_{s-1} + r_s,\ 0 \leqslant \deg(r_s) < deg(r_{s-1}),$$

$$r_{s-1} = q_{s+1} r_s$$

Здесь $q_1, \cdots, q_{s+1}$ и $r_1, \cdots, r_s$ — многочлены из $F[x]$. Так как $deg(g)$ конечна, то процедура должна закончиться после конечного числа шагов. Если старший коэффициент последнего ненулевого остатка r_s равен b, то НОД(f,g)=$b^{-1}r_s$.

Пример.

$f(x) = 2x^6 + x^3 + x^2 + 2$, $g(x) = x^4 + x^2 + 2x$ из $F_3[x]$. Применим алгоритм Евклида:

$2x^6 + x^3 + x^2 + 2 = (2x^2 + 1)(x^4 + x^2 + 2x) + x + 2$, $x^4 + x^2 + 2x = (x^3 + x^2 + 2x + 1)(x + 2) + 1$, $x + 2 = (x + 2) \cdot 1$. Значит, НОД(f,g)=1, а значит многочлены взаимно просты.

Определение 3.15. *Многочлен $f \in F[x]$ называется неприводимым (над полем F или в кольце $F[x]$), если f имеет положительную степень и равенство $f = gh$, $g, h \in F[x]$, может выполняться лишь в том случае, когда либо g, либо h является постоянным многочленом.*

Таким образом, многочлен положительной степени неприводим над F, если он допускает лишь тривиальные разложения на множители. Если многочлен допускает нетриальные разложения, то он называется *приводимым*. Неприводимость и приводимость многочлена зависит от того, в каком кольце (или над каким полем) мы его рассматриваем.

Теорема 6. *Для неприводимости многочлена $f(x) \in F[x]$ степени 2 или 3 необходимо и достаточно, чтобы он не имел корней в поле F.*

Примеры.

1) Многочлен $x^2 - 2 \in \mathbb{Q}[x]$ неприводим над $Q[x]$, но приводим над $\mathbb{R}$,

$$x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$$

2) $x^2 + 1$ неприводим в $Z[x]$, и приводим в $F_2[x]$, т.к.

$$x^2 + 1 = (x + 1)(x + 1),\ deg(x + 1) = 1,$$

но в кольце $F_3[x]$ он снова неприводим, т.к. его разложение с неопределенными коэффициентами $a, b \in F_3[x]$

$$x^2 + 1 = (x + a)(x + b)$$

приводит к несовместной в поле F_3 системе уравнений:

$$\begin{cases} a + b = 0 \\ a \cdot b = 1 \end{cases}$$

3) Над полем F_2 существует единственный неприводимый многочлен степени два: $x^2 + x + 1$.

4) Неприводимые многочлены степени 3 над полем F_2: $x^3 + x + 1$, $x^3 + x + 1$.

Теорема 7. *Каждый многочлен положительной степени $f \in F[x]$ (F — поле) может быть однозначно представлен в виде произведения*

$$f = a{f_1}^{e_1}{f_2}^{e_2} \cdots {f_k}^{e_k},$$

где $a \in F$, $f_1, \cdots, f_k \in F[x]$ — нормированные неприводимые многочлены, $e_1, \cdots, e_k \in \mathbb{N}$.

Теорема 8. *Произвольный неприводимый многочлен над полем F_2 делит многочлен $x^n + 1$, где $n = 2^m - 1$ и m есть степень многочлена.*

Основным вопросом для многочленов из $F[x]$ является вопрос о приводимости и неприводимости. Для приложений полезны многочлены над конечным полем F_p. Существует p^n многочленов степени n над F_p.

Теорема 9. *Пусть $F_p[x]$ – кольцо многочленов над полем F_p, где p – простое число, и многочлен $g(x) \in F_p[x]$. Фактор-кольцо $F_p[x]/(g)$ кольца $F_p[x]$ по модулю главного идеала (g) является полем тогда и только тогда, когда $g(x)$ – неприводимый многочлен в кольце $F_p[x]$.*

Пусть $g(x)$ – неприводимый в кольце $F_p[x]$ многочлен. Тогда по теореме фактор-кольцо $F_p[x]/(g)$ является полем. Элементы этого поля – классы вычетов $[f]_{(g)}$, $f(x) \in F_p[x]$, по модулю идеала (g), т.е.

$$[f]_{(g)} = \{f(x) + g(x) \cdot h(x) | h(x) \in F_p[x]\}$$

В каком случае два многочлена $f_1(x)$, $f_2(x) \in F_p[x]$ принадлежат одному классу вычетов $[f](g)$? В том и только в том случае, когда у них

одинаковые остатки при делении на многочлен $g(x)$. Следовательно, элементов в поле $F_p[x]/(g)$ столько, сколько различных остатков при делении на многочлен $g(x)$. Если $\deg(g) = n$, то возможных остатков будет p^n. А значит, p^n элементов в поле $F_p[x]/(g)$. Конечные поля мощности p^n обозначаются через $GF(p^n)$ и называются полями Галуа в честь открывшего и описавшего их математика Эвариста Галуа.

Теорема 10. *Для любого простого числа p и всякого натуральноо числа n существует конечное поле, содержащее p^n элементов.*

Операции сложения и умножения в поле $F_p[x]/(g)$:

$$[r1] + [r2] = [r1 + r2]$$

$$[r1] \cdot [r2] = [r1 \cdot r2]$$

с возможным приведением по модулю многочлена $g(x)$.

Пример.

Рассмотрим фактор-кольцо $F_2[x]/(x^2+x+1)$ являющееся полем. Элементами этого поля служат всевозможные остатки от деления на $x^2 + x + 1$:

$$F_4 = GF(2^2) = \{0, 1, x, x + 1\}$$

В поле F_4 четыре элемента-многочлена; алгебраические действия над ними производятся по модулю неприводимого многочлена x^2+x+1, при этом операции над коэффициентами выполняются по модулю простого числа 2. $[0] = 0$ – нулевой и $[1] = 1$ – единичный элементы. Следующие таблицы показывают примеры сложения и умножения элементов.

+	0	1	x	x+1
0	0	1	x	x+1
1	1	0	x+1	x
x	x	x+1	0	1
x+1	x+1	x	1	0

×	0	1	x	x+1
0	0	0	0	0
1	0	1	x	x+1
x	0	x	x+1	1
x+1	0	x+1	1	x

Дадим другой способ задания поля Галуа. Обозначим через α тот класс вычетов в кольце $F_p[x]/(g)$, который содержит x. Тогда, так как $g(x)$ — это многочлен, по модулю которого построено поле $GF(p^n)$, то $g(\alpha) = 0$. Таким образом, α оказывается корнем уравнения $g(x) = 0$ в поле $GF(p^n)$. Благодаря этому $GF(p^n)$ состоит из многочленов от α степени, не превосходящей n над $GF(p)$. Говорится, что поле $GF(p^n)$ образовано из поля $GF(p)$ присоединением к нему корня α многочлена $g(x)$.

В нашем случае многочлен $g(x)$ неприводим, а значит, не имеет корней в поле $GF(p)$. "Назначив" его корнем элемент α, мы получили расширение исходного поля $GF(p)$. Многочлены можно представлять в виде вектора коэффициентов. Например, многочлен $x^4 + x + 1$ это $(1, 1, 0, 0, 1)$, т.к. в начале идет коэффициент при x^0, потом коэффициент при x^1, потом коэффициент при x^2 и т.д.

Пример.

Пусть $p = 2$, $n = 4$. Построим $GF^*(2^4)$ по модулю многочлена $g(x) = x^4 + x + 1$, при условии $g(\alpha) = 0$, или, что то же $\alpha^4 = \alpha + 1$.

$\alpha^0 = 1$	=(1,0,0,0)	$\alpha^8 = 1 + \alpha^2$	=(1,0,1,0)
$\alpha^1 = \alpha$	=(0,1,0,0)	$\alpha^9 = \alpha + \alpha^3$	=(0,1,0,1)
$\alpha^2 = \alpha^2$	=(0,0,1,0)	$\alpha^{10} = 1 + \alpha + \alpha^2$	=(1,1,1,0)
$\alpha^3 = \alpha^3$	=(0,0,0,1)	$\alpha^{11} = \alpha + \alpha^2 + \alpha^3$	=(0,1,1,1)
$\alpha^4 = \alpha + 1$	=(1,1,0,0)	$\alpha^{12} = 1 + \alpha + \alpha^2 + \alpha^3$	=(1,1,1,1)
$\alpha^5 = \alpha + \alpha^2$	=(0,1,1,0)	$\alpha^{13} = 1 + \alpha^2 + \alpha^3$	=(1,0,1,1)
$\alpha^6 = \alpha^2 + \alpha^3$	=(0,0,1,1)	$\alpha^{14} = 1 + \alpha^3$	=(1,0,0,1)
$\alpha^7 = 1 + \alpha + \alpha^3$	=(1,1,0,1)	$\alpha^{15} = 1$	=(1,0,0,0)

Чтобы получить поле $GF(2^4)$ осталось только добавить вектор $(0, 0, 0, 0)$.

Задачи.

1) Докажите, что НОД(x^{n-1},x^{m-1})=x^d-1, d =НОД(n,m) в кольце многочленов $F[x]$ над некоторым полем F.

2) Найти НОД многочленов $f(x)$, $g(x)$

   1. $f(x) = x^5 + 2x^3 + 2x + 1$, $g(x) = x^3 + 4x^2 + 3$, $f(x), g(x) \in \mathbb{Z}[x]$.
   2. $f(x) = x^5 + 2x^3 + 2x + 1$, $g(x) = x^3 + 4x^2 + 3$, $f(x), g(x) \in \mathbb{F}_7[x]$.

3) Доказать, что для многоченов $f_1, \cdots, f_n$ справедливо соотношение НОД($f_1, \cdots, f_n$)=НОД(НОД($f_1, \cdots, f_{n-1}$), f_n).

4) Проверить на неприводимость многочлен

   1. $x^3 + x^2 + x + 1$ над F_2.
   2. $2x^3 + 2x + 1$ над F_3.

5) Построить таблицы сложения и умножения для фактор кольца $F_2[x]/(x^3 + x^2 + x)$. Будет ли это кольцо полем?

6) Построить поле $GF(2^3)$ двумя способами, неприводимый многочлен $g(x) = x^3 + x + 1$.

3.3. Расширенный алгоритм Евклида для многочленов

Мы еще не рассмотрели как искать обратные элементы. Это можно сделать с помощью расширенного алгоритма Евклида. $u(x)f(x) + v(x)g(x) = d(x)$, где $u(x)$, $v(x)$ – вспомогательные многочлены, $d(x)$ – НОД($f(x)$,$g(x)$). Также как и для чисел вначале идет прямой ход, а потом обратный ход для вычисления вспомогательных многочленов $u(x)$, $v(x)$. Начальные значения: $u_i(x) = 0$, $v_i(x) = 1$. Общие формулы вычисления $u(x)$, $v(x)$:

$$u_i(x) = v_{i+1}(x), v_i(x) = u_{i+1}(x) - v_{i+1}(x)\lfloor f_i(x)/(g_i(x))\rfloor$$

Пример.

Найти обратный элемент к x^2 над F_2, если неприводимый многочлен над F_2 равен $x^3 + x + 1$.

$f_i(x)$	$g_i(x)$	$\lfloor \frac{f_i(x)}{g_i(x)} \rfloor$	$f_i(x) \mod g_i(x)$	$u_i(x)$	$v_i(x)$
$x^3 + x + 1$	x^2	x	$x + 1$	$x + 1$	$x^2 + x + 1$
x^2	$x + 1$	x	x	1	$x + 1$
$x + 1$	x	1	1	1	1
x	1	x	0	0	1

Задачи.

1) Решить сравнение

   1. $(x^2 + 1)f(x) = 1 \mod (x^3 + 1)$ в $F_3[x]$.
   2. $(x + 2)f(x) = 1 \mod (x^3 + 1)$ в $F_3[x]$.

2) Найти обратный многочлен к $x + 1$ в $GF(8)$, неприводимый многочлен над F_2 $x^3 + x + 1$.

4. Линейные коды

Подробное изложение информации можно найти в [6, 7, 8].

Пусть p — степень простого числа и символы кодовых слов — элементы конечного поля F_p. $(n, M, d)_p$ -код C называется линейным, если он является линейным подпространством пространства ${F_p}^n$, то есть линейная комбинация кодовых слов также является кодовым словом. Если $\dim C = k$, то говорят, что задан линейный $[n, k, d]_p$-код. Таким образом, линейный код – непустое множество последовательностей длины n над F_p, называемых кодовыми словами, такое, что сумма двух кодовых слов является кодовым словом, произведение кодового слова на элемент поля также является кодовым словом.

Предложение 4.1. *Для любого линейного кода C имеем*

$$d(C) = \min_{\substack{a \in C \\ a \neq 0}} ||a||$$

Пример линейного двоичного кода — код с проверкой чётности:

$$C = \{(a_1, \cdots, a_n) \in {F_2}^n : \sum a_i = 0\}$$

Один из базисов этого кода:

$$\begin{gathered}(1, 0, 0, \cdots, 0, 1)\\(0, 1, 0, \cdots, 0, 1)\\(0, 0, 1, \cdots, 0, 1)\\\cdots\\(0, 0, 0, \ldots, 1, 1)\end{gathered}$$

Если выписать базис линейного $[n, k, d]_p$-кода построчно в виде матрицы размера $k \times n$, получим порождающую матрицу кода. Итак, для задания $[n, k, d]_p$-кода достаточно указать его порождающую матрицу $G \in {F_p}^{k \times n}$. Число линейных комбинаций k базисных векторов с коэффициентами из F_p равно p^k, поэтому каждый $[n, k, d]_p$-код является $[n, p^k, d]_p$-кодом.

Пусть порядок кода C будет p^k. Тогда базис кода как подпространства содержит k линейно независимых векторов. Пусть $v_1 = (a_{11}, \cdots, a_{1n})$, $v_2 = (a_{21}, \cdots, a_{2n})$, $\cdots$, $v_k = (a_{k1}, \cdots, a_{kn})$ суть k выбранных векторов базиса. Расположим их в виде строк матрицы:

$$G = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{k1} & a_{k2} & \cdots & a_{kn} \end{pmatrix} \tag{3}$$

Эта матрица называется порождающей матрицей кода C. Если бы при передаче по каналу связи не было опасности возникновения ошибок, то каждое из p^k сообщений можно было бы передавать посредством вектора $u = (u_1, u_2, \cdots, u_k)$ длины k. Однако ради создания нужного нам расстояния между кодовыми векторами вектор u должен быть подвергнут некоторому преобразованию. Оно состоит в том, что вектор u задаёт линейную комбинацию строк матрицы G. Именно, вектор $v \in C$, соответствующий вектору u, который в отсутствие помех должен был бы передаваться по каналу связи, получается следующим образом, $v \in {F_p}^n$:

$$v = uG$$

Если закодированное сообщение $a \in {F_p}^n$ было принято без ошибок, декодируем его, решая, например, методом Гаусса систему $uG = a$.

Порождающую матрицу $G \in {F_q}^{k \times n}$ линейными преобразованиями и перестановками строк и столбцов можно привести к каноническому виду, $\widetilde{G} \in {F_p}^{k \times (n-k)}$:

$$\widetilde{G} = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} \tag{4}$$

В этом случае получится, что исходные k символов останутся неизменными, а в конец добавятся $n - k$ проверочных. Такой код будет называться *систематическим*.

Порождающую матрицу будем изображать следующим образом:

$$H = \begin{pmatrix} h_{11} & h_{12} & \cdots & h_{1n} \\ h_{21} & h_{22} & \cdots & h_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ h_{(n-k)1} & h_{(n-k)2} & \cdots & h_{(n-k)n} \end{pmatrix} \tag{5}$$

Соотношение $vH^T = 0$ проверяет принадлежность вектора v к коду C, и потому матрицу H называют проверочной матрицей кода C. Матрицы G, H связаны соотношением $GH^T = [0]$, где $[0]$ нулевая матрица размера $k \times (n - k)$.

Большинство известных хороших кодов принадлежат классу линейных кодов. Структура линейных кодов облегчает поиск хороших кодов, помогает создавать хорошие кодеры и декодеры.

Задачи.

1) Пусть $u = 011$, $G = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}$. Закодировать u.

2) Зная порождающую матрицу G из задания №1 найти проверочную матрицу H. Является ли 10110 кодом?

4.1. Коды Хэмминга

Коды Хемминга - одни из самых простых нетривиальных линейных кодов. Рассмотренный ранее простейший двоичный код с проверкой чётности $\{(a_1, \cdots, a_n) \in {F_2}^n : \sum a_i = 0\}$ может обнаруживать одну ошибку, т.к. при замене разряда a_i на противоположный, соотношение $\sum a_i = 0$ нарушится. Но исправить ошибку не удастся. Хочется построить двоичный код, исправляющий хотя бы одну ошибку. Для этого вместо «глобального» контроля чётности применим несколько «дихотомических» проверок на чётность.

Код, кодовое расстояние d которого $\geqslant 3$ в силу следствия 3.2.3 из [8] имеет проверочную матрицу, в которой все столбцы ненулевые и различные. Двоичный код Хемминга удобнее всего задавать при помощи проверочной матрицы H. Если H имеет m строк, то каждый столбец оказывается двоичным числом длины m, существует $2^m - 1$ таких столбцов. Таким образом, в матрице H m строк и $2^m - 1$ столбцов, кодовое расстояние $d \geqslant 3$. В результате получаем $(2^m - 1, 2^m - m - 1)$ код, называемый кодом Хемминга. При $m = 3$ матрицы G, H в систематическом виде равны:

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

Пример. $u = 1011$, $uG = 1011010$. Пусть при передаче произошла 1 ошибка, пришло сообщение $v = 1010010$. Тогда, $vH^T = 111$, столбец равный 111 находится на 4 позиции в матрице H. Значит, нужно изменить 4 разряд полученного сообщения v.

Давайте изменим матрицу H, расположив ее столбцы в лексикографическом порядке.

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

Примечательной чертой такого нового расположения столбцов является то, что при любой одиночной ошибке в принятом векторе v результатом умножения vH^T будет в точности двоичный номер искаженного разряда кодового вектора.

Для того, чтобы предложенный выше алгоритм фиксировал наличие двойных ошибок, нужно к полученному коду добавить один дополнительный разряд в конце, который будет отвечать за четность. Рассмотрим систематический (8,4) код Хэмминга, позволяющий исправлять 1 ошибку и находить 2 ошибки. Подобную конструкцию без привязки к конкретным n, k еще называют расширенным кодом Хемминга.

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

В случае одной ошибки изменится четность сообщения. При возникновении двойной ошибки четность не нарушится, но $vH^T \neq 0$.

Пример. $u = 1001$, $uG = 10011001$. Пусть при передаче произошла 1 или 2 ошибки и пришло сообщение $v = 10010001$. Сообщение v имеет нечетное число "1" , поэтому произошла 1 ошибка. $vH^T = 1000$, данный вектор равен 5 столбцу слева, значит, поменяем 5 разряд в v. Исправленное сообщение: 10011001.

Представим теперь, что произошло 2 ошибки и пришло сообщение $v = 10001000$. Сообщение имеет четное число "1", но $vH^T \neq 0$, что означает, что произошло 2 ошибки, но исправить их мы не можем.

Задачи.

1) Дан (7,4) код Хемминга. Пришло сообщение 1001100. Есть ли ошибка? Если есть, то исправить.

2) Дан (8,4) код Хемминга. Пришли сообщения $v_1 = 10000111$, $v_2 = 11001000$, $v_3 = 11011101$. Произошли ли ошибки при передаче? Если да, то сколько? Можно ли их исправить?

Список литературы

[1] Кострикин, А.И. Введение в алгебру. Часть 1. Основы алгебры [Текст] / Алексей Иванович Кострикин. М.: ФИЗМАТЛИТ, 2004. — 272 с.

[2] Куликов, Л.Я. Алгебра и теория чисел: Учеб. пособие для педагогических институтов [Текст] / Леонид Яковлевич Куликов. М.: Высш. школа, 1979. — 559 с.

[3] Вечтомов, Е.М. Абстрактная алгебра. Базовый курс: учебное пособие [Текст] / Евгений Михайлович Вечтомов, Вадим Вениаминович Сидоров. Киров: Изд-во ООО «Радуга-ПРЕСС», 2014. — 260 с.

[4] Лидл, Р., Нидеррайтер Г. Конечные поля [Текст] / Рудольф Лидл, Гаральд Нидеррайтер. М.: Мир, 1988. — 430 с.

[5] Берлекамп, Э. Алгебраическая теория кодирования [Текст] / Элвин Берлекамп. М.: Мир, 1971. — 489 с.

[6] Сагалович, Ю. Л. Введение в алгебраические коды [Текст] / Юрий Львович Сагалович. ИППИ РАН, 2011. — 302 с.

[7] Дайняк, А. Б. Конспект лекций по теории кодирования [URL] / Александр Дайняк. https://www.dainiak.com/teaching/courses/codes/

[8] Питерсон, У.У. Коды, исправляющие ошибки. [Текст] / Уильям Уэсли Питерсон, Э. Дж. Уэлдон. М.: Мир. 1976. 594 с.

Методическое пособие

Долгов Дмитрий Александрович

ВВЕДЕНИЕ В ТЕОРИЮ КОДИРОВАНИЯ. ЧАСТЬ 1