Министерство образования Республики Беларусь
Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

Институт информационных технологий

Кафедра информационных систем и технологий

А. И. Митюхин, В. И. Пачинин

ЭЛЕМЕНТЫ АЛГЕБРАИЧЕСКИХ СТРУКТУР ТЕОРИИ КОДИРОВАНИЯ

Методическое пособие по курсам
«Теория кодирования»
и «Специальные математические методы и функции»
для студентов специальностей «Промышленная электроника»,
«Программное обеспечение информационных технологий», «Радиосвязь,
радиовещание и телевидение» вечерней и заочной форм обучения

Минск БГУИР 2012

УДК [519.72+621.391](076)
ББК 32.811я73
М67

Р е ц е н з е н т:
профессор кафедры сетей и устройств телекоммуникаций
учреждения образования «Белорусский государственный университет
информатики и радиоэлектроники», доктор технических наук,
профессор В. К. Конопелько

Митюхин, А. И.

М67 Элементы алгебраических структур теории кодирования : метод. пособие по курсам «Теория кодирования» и «Специальные математические методы и функции» для студ. спец. «Промышленная электроника», «Программное обеспечение информационных технологий», «Радиосвязь, радиовещание и телевидение» веч. и заоч. форм обуч. / А. И. Митюхин, В. И. Пачинин. – Минск : БГУИР, 2012. – 64 с. : ил.
ISBN 978-985-488-702-9.

Рассмотрены элементарные сведения теории множеств, групп, колец, полей Галуа, лежащих в основе теории прикладного помехоустойчивого и криптографического кодирования информации, теории дискретных унитарных и теоретико-числовых преобразований, цифровой обработки сигналов.

Представлены примеры практического использования понятий конечных алгебраических структур для кодирования информации в цифровых системах и устройствах радиоэлектроники, при разработке и проектировании эффективных систем передачи, обработки, хранения и распределения информации. Приведены примеры решения задач, упражнения, контрольные вопросы и задачи.

УДК [519.72+621.391](076)
ББК 32.811я73

ISBN 978-985-488-702-9

Введение

Основой построения наиболее важных известных кодов, корректирующих ошибки, является их алгебраическая структура. Существование особых структурных закономерностей в строении таких кодов желательно по двум причинам:
– они облегчают изучение свойств кода;
– обеспечивают возможность практической реализации кодов на аппаратно-программном уровне.

В современной дискретной математике под алгеброй понимается наука о множествах произвольных математических объектов, между которыми установлены алгебраические операции.

1. ТЕОРИЯ МНОЖЕСТВ

1.1. Понятие множества

Под множеством понимается некоторая определенная совокупность объектов или элементов. Конечные множества можно описывать, перечисляя их элементы. Например, $G = \{a, b, c\}$ есть множество, содержащее буквы a, b, c. При перечислении множества часто используется описание характеристического свойства элементов этого множества. Например, $H = \{a^0, a^1, a^2, \dots, a^{n-1}\}$ описывает множество степеней элемента a, где $\{0,1, 2, \dots, n\}$ – множество положительных целых чисел.

Множество задается путем указания характеристического свойства, т. е. свойства, которому удовлетворяют элементы этого множества. Для задания множества используют запись $\{x: x$ обладает свойством$\}$ – множество содержит только те элементы, которые обладают свойством H.

Определение 1.1. Если a есть один из объектов множества G, говорят: a принадлежит G. Принадлежность a множеству G записывается как $a \in G$. Если a не является элементом G, это записывается как $a \notin G$. Например, $a^2 \in \{a^0, a^1, a^2, \dots, a^{n-1}\}$, но $a^n \notin G$.

Определение 1.2. Множество H есть подмножество множества (обозначается $H \subseteq G$), если каждый элемент H принадлежит множеству G, т. е. если $x \in H$, то $x \in G$. Если H не является подмножеством G, то это записывается как $H \not\subseteq G$.

Например, $\{0, 3\} \subseteq \{0, 1, 2, 3, 4, 5\}$, но $\{0, 3, 6\} \not\subseteq \{0, 1, 2, 3, 4, 5\}$.
Множества равны, если они содержат одни и те же элементы.

Определение 1.3. Пусть G и H – некоторые множества. $G = H$, если для любого x имеем: $x \in G$ тогда и только тогда, когда $x \in H$.

Замечания:

1) порядок перечисления элементов множества роли не играет. Например, {0, 1, 2, 3, 4, 5} = {0, 2, 1, 3, 4, 5};

2) каждый элемент множества может входить во множество не более одного раза.

Определение 1.4. Пустое множество есть множество, которое не содержит элементов (обозначается $\emptyset$).

Определение 1.5. Универсальное множество, или универсум, обозначаемое U, есть множество, обладающее таким свойством, что все рассматриваемые множества являются его подмножествами.

Например, множество всех целых или натуральных чисел есть универсальное множество. В математическом анализе универсальное множество есть множество действительных чисел. В теории кодирования множество всех векторов *n*-мерного пространства образуют универсальное множество.

1.2. Операции над множествами

Определение 1.6. Пересечением множеств G и H называется множество, состоящее из тех и только тех элементов, которые принадлежат и G, и H. Пересечение множеств обозначается $G \cap H$. Определение записывается как $G \cap H = \{x: x \in G \text{ и } x \in H\}$.

Например, если G ={0, 1, 2, 3, 4, 5} и H ={0, 3, 6}, то $G \cap H$={0, 3}.

Замечание. В описании пересечения множеств G и H использована связка «И». Символу $\cap$ соответствует символ логической схемы «И» – &. Пересечение множеств в общем случае определяется следующим образом.

Определение 1.7. Если $I = \{1, 2, \ldots, r\}$, то
$\cap_{i \in I} A_i = A_1 \cap A_2 \cap A_3 \cap \ldots \cap A_r = \{x: x \in A_i \text{ для всех i} \in I\}$.

Определение 1.8. Объединением множеств G и H называется множество, состоящее из всех элементов, которые принадлежат хотя бы одному из множеств G или H. Объединение множеств G и H обозначается $G \cup H$. Определению соответствует запись $G \cup H = \{x: x \in G \text{ или } x \in H\}$.

Например, если G ={0, 1, 2, 3, 4, 5} и H ={0, 3, 6}, то $G \cup H$={0, 1, 2, 3, 4, 5, 6}.

Замечание. В описании объединения множеств G и H использована связка «ИЛИ». Символу $\cup$ соответствует символ логической схемы «ИЛИ» – 1.

Объединение множеств в общем случае определяется следующим образом.

Определение 1.9. Если $I = \{1, 2, \ldots, r\}$, то

$$\bigcup_{i \in I} A_i = A_1 \cup A_2 \cup A_3 \cup \ldots \cup A_r = \{x: x \in A_i \text{ для всех i} \in I\}.$$

Определение 1.10. Пусть G и H множества. Разностью множеств G и H называется множество всех тех элементов G, которые не содержатся в H,

$$G - H = \{x: x \in G \text{ и } x \notin H\}.$$

Например, если $G = \{0, 1, 2, 3, 4, 5\}$ и $H = \{0, 3, 6\}$, то $G - H = \{1, 2, 4, 5\}$.

Определение 1.11. Симметрическая разность множеств G и H (обозначается $G \Delta H$) есть множество $(G - H) \cup (H - G)$.

Например, если $G = \{0, 1, 2, 3, 4, 5\}$ и $H = \{0, 3, 6\}$, то $G - H = \{1, 2, 4, 5\}$, $(H - G) = \{6\}$, $G \Delta H = \{1, 2, 4, 5, 6\}$. Симметрическая разность множеств G и H состоит из тех элементов, которые принадлежат или множеству G, или H.

Замечание. В описании симметрической разности множеств G и H использована связка «ИЛИ». Символу Δ соответствует символ логической схемы «ИСКЛЮЧАЮЩЕЕ ИЛИ» – $\oplus$.

Определение 1.12. Дополнение множества G, обозначаемое $\bar{G}$, – это множество элементов универсума, которые не принадлежат G:

$$\bar{G} = U - G = \{x: x \in U \text{ и } x \notin G\}.$$

Например, если U – множество положительных целых чисел, а $G = \{2, 4, 6, \ldots\}$ – множество четных положительных чисел, то $\bar{G} = \{1, 3, 5, \ldots\}$ – множество нечетных положительных чисел.

Теорема 1.1. Пусть A, B и C – подмножества универсального множества U. Справедливы следующие равенства.

1. Законы идемпотентности

$$A \cap A = A,$$
$$A \cup A = A.$$

2. Свойства коммутативности

$$A \cap B = B \cap A,$$
$$A \cup B = B \cup A.$$

3. Свойства ассоциативности

$$A \cap (B \cap C) = (A \cap B) \cap C,$$
$$A \cup (B \cup C) = (A \cup B) \cup C.$$

4. Свойства дистрибутивности

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C),$$
$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$$

5. Двойное дополнение

$$\bar{\bar{A}} = A.$$

6. Свойства тождества

$$A \cup \emptyset = A,$$
$$A \cap U = A.$$

7. Свойства дополнения

$$A \cup \bar{A} = U,$$
$$A \cap \bar{A} = \emptyset.$$

8. Законы де Моргана

$$\overline{(A \cup B)} = \bar{A} \cap \bar{B},$$
$$\overline{(A \cap B)} = \bar{A} \cup \bar{B}.$$

Определение 1.13. Декартово произведение множеств (прямое произведение множеств) X и Y, обозначаемое $X \times Y$, есть множество $\{(x,y): x \in X \text{ и } y \in Y\}$. Объект (x,y) называется упорядоченной парой с первой компонентой x и второй компонентой y.

Множество $X \times Y$ состоит из всех упорядоченных пар (x,y), при этом имеет значение порядок компонент. Если элементы множеств X и Y представляют собой действительные числа, то $X \times Y$ есть декартова плоскость. Если X содержит k элементов, а Y содержит n элементов, то множество $X \times Y$ состоит из kn элементов.

Пример 1.1. Пусть $X = \{1,2,3,4\}, Y = \{1,2\}$. Декартово произведение равно:

1) $X \times Y = \{(1,1),(1,2),(2,1),(2,2),(3,1),(3,2),(4,1),(4,2)\}$,
2) $Y \times X = \{(1,1),(1,2),(1,3),(1,4),(2,1),(2,2),(2,3),(2,4)\}$,
3) $Y \times Y = \{(1,1),(1,2),(2,1),(2,2)\}$.

1.3. Отношения

Определение 1.14. Подмножество R декартова произведения $A \times B$ множеств A и B называется бинарным отношением на паре множеств A, B. Если $(a \text{ и } b) \in R$ (записывают как aRb), то говорят, что элемент a связан с элементом b отношением R. Если $A = B$, то отношение есть подмножество $A \times A$.

Пример 1.2. Пусть $A = \{1,2,3,4\}, B = \{1,2\}$. Декартово произведение множеств A и B равно

$A \times B = \{(1,1),(1,2),(2,1),(2,2),(3,1),(3,2),(4,1),(4,2)\}$.

Выпишем упорядоченные пары на множествах A, B, принадлежащие отношению

$$R = \{(x,y) : x + y = 5\}.$$

Тогда $R = \{(3, 2), (4,1)\}$ есть отношение множеств A и B.

Множество $A \times B$ содержит восемь элементов, поэтому существует 2^8= 256 подмножеств множества $A \times B$. Следовательно, имеется 256 отношений на $A \times B$.

Пример 1.3. Выписать упорядоченные пары, принадлежащие отношению на множествах $A = \{1, 3, 5, 7\}$ и $B = \{2, 4, 6\}$, если $R = \{(x, y): x < y\}$.

Решение. $R = \{(1, 2), (1, 4), (1, 6), (3, 4), (3, 6), (5, 6)\}$ – есть отношение множеств A и B.

1.3.1. Свойства отношений

Рассмотрим отношения, заданные на одном множестве A.

Определение 1.15. Отношение R на множестве $A \times A$:

– рефлексивно, если $(a, a) \in R$ для всех a из A;

– антирефлексивно, если из $(a, b) \in R$ следует $a \neq b$;

– симметрично, если для каждой пары a и b, принадлежащей A, из $(a, b) \in R$ следует, что $(b, a,) \in R$;

– транзитивно, если для всех a, b и c, принадлежащих A, из того что $(a, b) \in R$ и $(b,c) \in R$, следует, что $(a, c) \in R$.

Пример 1.4. Пусть $A = \{1, 2, 3, 4, 5, 6\}$ и отношение $R \subseteq A \times A$ есть подмножество $R = \{(1, 1), (2, 2), (3, 3), (4, 4), (5, 5), (6, 6), (1, 2), (1, 4), (2, 1), (2,4), (3,5), (4,1), (4, 2), (5,3)\}$.

Отношение R рефлексивно, т. к. для каждого $a \in A$, $(a, a) \in R$.

Отношение R симметрично, т. к. $(1, 2) \in R$ и $(2, 1) \in R$; $(1, 4) \in R$ и $(4, 1) \in R$; $(3, 5) \in$ R и $(5, 3) \in$ R.

Отношение R транзитивно. Рассмотрев все возможные случаи, можно показать, что в каждом из них, когда $(a, b) \in R$ и $(b, c) \in R$, следует, что $(a, c) \in R$. Например, $(1, 2) \in R$ и $(2, 4) \in R$, получаем $(1, 4) \in R$.

1.3.2. Отношения эквивалентности

Определение 1.16. Отношение R на A есть отношение эквивалентности, если оно рефлексивно, симметрично и транзитивно.

В примере 1.4 было показано, что отношение R на A, определенное как R = {(1, 1), (2, 2), (3, 3), (4, 4), (5, 5), (6, 6), (1, 2), (1, 4), (2, 1), (2, 4), (3, 5), (4, 1), (4, 2), (5, 3)}, рефлексивно, симметрично и транзитивно, следовательно, R есть отношение эквивалентности.

Определение 1.17. Отношение эквивалентности R на множестве A разбивает его на подмножества, элементы которых эквивалентны друг другу и не эквивалентны элементам других подмножеств. Эти подмножества называются классами эквивалентности по отношению R.

Определение 1.18. Пусть $a \in A$, и R – отношение эквивалентности на $A \times A$. Пусть $[a]$ обозначает множество $\{x : xRa\} = \{x : (x, a) \in R\}$, называемое классом эквивалентности, содержащим a.

Пример 1.5. Пусть A = {1, 2, 3, 4, 5, 6} и отношение $R \subseteq A \times A$ есть подмножество R = {(1, 1), (2, 2), (3, 3), (4, 4), (5, 5), (6, 6), (1, 2), (1, 4), (2, 1), (2, 4), (3, 5), (4, 1), (4, 2), (5, 3)}. Ранее в примере 1.4 было показано, что отношение R на множестве A есть отношение эквивалентности. Построим классы эквивалентности каждого элемента A по отношению R.

Для элемента 1 множества A получаем

$$[1] = \{x : (x, 1) \in R\} = \{1, 2, 4\},$$

где $1 \in [1]$, поскольку $(1, 1) \in R$, $2 \in [1]$, т. к. $(2, 1) \in R$ и $4 \in [1]$, т. к. $(4, 1) \in R$.

Классы эквивалентности остальных элементов множества A по отношению R :

$$[2] = \{x : (x, 2) \in R\} = \{2, 1, 4\};$$
$$[3] = \{x : (x, 3) \in R\} = \{3, 5\};$$
$$[4] = \{x : (x, 4) \in R\} = \{4, 1, 2\};$$
$$[5] = \{x : (x, 5) \in R\} = \{5, 3\};$$
$$[6] = \{x : (x, 6) \in R\} = \{6\}.$$

Таким образом, имеется всего три различных класса эквивалентности:

$$[1] = [2] = [4] = \{1, 2, 4\},$$
$$[3] = [5] = \{3, 5\},$$

[6] ={6}.

Множество всех классов эквивалентности множества A по отношению R запишется как

$$[A_R] = \{[1], [3], [6]\} = \{\{1, 2, 4\},\{3, 5\}, \{6\}\}.$$

Выводы:

– каждый элемент класса эквивалентности порождает (представляет) класс эквивалентности, т. е. если $b \in [a]$, то $a \in [b]$;

– каждый класс эквивалентности содержит по крайней мере один элемент;

– никакой элемент не может принадлежать двум различным классам эквивалентности;

– совокупность классов эквивалентности разделяет множество A на непересекающиеся подмножества. Такое разделение множества называется его разбиением.

Определение 1.19. Пусть $R \subseteq A \times B$ – отношение на $A \times B$, а $S \subseteq B \times C$ – отношение на $B \times C$. Композицией отношений S и R называется отношение $T \subseteq A \times C$, для которого справедливо:

$T = \{(a, c)$: существует такой элемент b из B, что $(a, b) \in R$ и $(b, c) \in S\}$. Это подмножество множества $A \times C$ обозначается $T = S \circ R$.

Пример 1.6. Пусть R и S – бинарные отношения на множестве положительных целых чисел, заданных в виде $R = \{(x, x^2)$: x – положительное целое число$\}$ и $S = \{(x, x + 2)$: x – положительное целое число$\}$. Тогда $S \circ R$ = = $\{x, (x^2 + 2)\}$. Поскольку $x^2 = b \in R$, то $c = b + 2 = (x^2 + 2) \in S$.

Для R = {(1, 1), (2, 4), (3, 9), (4, 16),…} и S = {(1, 3), (2, 4), (3, 5), (4, 6), (5, 7), (6, 8), (7, 9), (8, 10), (9, 11)…} получаем отношение $T = \{(a, c)\}$ ={1, 3), (2, 6), (3, 11), (4, 18), (5, 27) …}. Действительно, существует элемент b = 4 из B, такой, что (2, 4) $\in R$ и элемент b = 4, такой, что (4, 6) $\in S$. Имеем композицию из элементов отношений R и S.

1.4. Сравнения и вычеты

Определение 1.20. Рассмотрим два целых числа a, b и некоторое целое число M. Если a и b дают при делении на M один и тот же остаток, то говорят, что a сравнимо с b по модулю M, что обозначается $a \equiv b \bmod M$.

Например, $4 \equiv 1 \bmod 3$.

Теорема 1.2. Отношение $R = \{(a, b)$: $a \equiv b \bmod M\}$ для фиксированного M является отношением эквивалентности на множестве целых чисел, т. к. оно рефлексивно, симметрично и транзитивно.

Следовательно, справедливы следующие выражения:

1) $a \equiv a \bmod M$;

2) если $a \equiv b \bmod M$, то $b \equiv a \bmod M$;

3) если $a \equiv b \bmod M$ и $b \equiv c \bmod M$, то $a \equiv c \bmod M$.

Все числа, которые сравнимы между собой по модулю M, образуют класс эквивалентности по модулю M. Всем числам этого класса соответствует один и тот же остаток. Любое число в классе называется вычетом по модулю M по отношению ко всем числам того же класса.

Всего имеется M остатков: $\{0, 1, 2, \ldots, M-1\}$. Поэтому существует M классов эквивалентности.

Определение 1.21. Пусть M – целое число. Множество всех классов эквивалентности по модулю M называется множеством классов вычетов по модулю M.

Например, для $M = 4$ существует 4 различных класса эквивалентности (класса вычетов).

2. АЛГЕБРАИЧЕСКИЕ СТРУКТУРЫ

Теория групп, колец, полей – это те понятия конечной алгебры, которые являются основой для поиска хороших кодов, контролирующих ошибки. Эти же алгебраические структуры используются при технической реализации методов криптографической защиты информации, алгоритмов криптоанализа. Математические основы названных понятий широко применяются в алгоритмах дискретных преобразований цифровой обработки сигналов и изображений.

2.1. Элементы теории конечных групп

2.1.1. Арифметика конечных групп

Определение 2.1. Группа – это алгебраическая структура или множество элементов G с заданной на нем основной алгебраической операцией.

Замечания:

1. В большей части это те же операции, которые применимы к числовым системам.

2. Для теории кодирования наибольшее значение имеют бинарные операции.

Элементы множества произвольной природы обозначают как $G = \{a, b, c\}$, а результат операции символически записывают в виде $c = f(a, b)$. Говорят: на множестве G задана бинарная операция f. Чтобы подчеркнуть аб-

страктность операции применяют символы $*$ или $\circ$. При операции сложения пишут $c = a + b$, а при операции умножения $c = a \cdot b$.

Замечание. Операции вычитания и деления – это неосновные операции, т. к. они являются обратными для сложения и умножения.

Алгебраические операции могут задаваться таблицами Кэли. Первые строка и столбец таблицы состоят из элементов множества G. Результат операции записывается в ячейке таблицы с координатами, задаваемыми элементами множества. Например, для множества элементов $G = \{a, b\}$ операцию можно представить в виде таблицы

f	a	b
a	a	b
b	b	a

В группе должны выполняться следующие аксиомы:

1) замкнутость – любой паре a, b элементов из множества G ставится в однозначное соответствие третий элемент $c \in G$, т. е. $a*b = c$;

2) ассоциативность – для всех элементов множества $G = \{a,b,c\}$ выполняется $a*(b*c)=(a*b)*c= a*b*c$;

3) существование во множестве G нейтрального элемента e, такого, что выполняется $a*e = e*a = a \in G$;

4) существование для каждого элемента $a \in G$ обратного $\hat{a}$ или $a^{-1} \in G$, такого, что $a * \hat{a} = \hat{a} * a = e$ или $a * a^{-1} = a^{-1} * a = e$;

5) если в группе выполняется аксиома коммутативности, т. е. для любых a и b из группы $a*b = b* a$, то группа называется коммутативной, или абелевой (Н. Абель (1802 – 1829), норвежский математик).

Определение 2.2. Если группа содержит конечное число элементов, то она называется конечной группой, а число элементов в группе называется порядком группы. Если порядок группы бесконечен, то она называется бесконечной.

Замечания:

1. Аддитивная абелева группа в качестве нейтрального элемента e имеет 0, $a + \hat{a} = e = 0$.

2. Мультипликативная абелева группа в качестве нейтрального элемента e имеет 1, $a \cdot \hat{a} = e = 1$.

Теорема 2.1. Единичный элемент в группе является единственным. Для каждого элемента группы обратный элемент также является единственным.

Примеры абелевых групп

2.1. Рациональные числа относительно операции сложения $< R; + >$.

2.2. Натуральные числа относительно операции умножения $< N; \cdot >$.

2.3. Совокупность действительных чисел относительно операции сложения $< D; + >$.

2.4. Группа из одного элемента (единичного) $< e; * >$, например, $< 0; + >$ – аддитивная, $< 1; \cdot >$ – мультипликативная..

2.5. Группа второго порядка. Ее таблица Кэли имеет вид

f	e	a
e	e	a
a	a	e

Здесь $a * a = e$, т. к. $a * \hat{a} = e$ и $(a * a)$ не может быть равным a. В группе может быть только один нейтральный элемент.

На множестве из двух элементов групповая операция задается не более чем одним способом:

1) аддитивная абелева группа второго порядка:
$< \{0,1\}; +; 0 >$; $1 + \hat{1} = 0$; поэтому для 0 обратным является 0; для 1 обратным является 1; таблица Кэли примет форму

+	0	1
0	0	1
1	1	0

2) мультипликативная абелева группа второго порядка:
$< \{1, -1\}; \cdot; 1 >$; $1 \cdot \hat{1} = 1$; поэтому для 1 обратным является 1; для (–1) обратным является (– 1), т. к. (–1)·(–1) = 1, таблица Кэли примет форму

·	1	–1
1	1	–1
–1	–1	1

2.6. Группа третьего порядка:

1) $<\{e, a, b\}; +; e>$. Операция в группе задается таблицей Кэли (табл. 2.1).

Таблица 2.1

+	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

2) $<\{0, 1, 2\}; +; 0>$. Операция в группе задается таблицей Кэли (табл. 2.2).

Таблица 2.2

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Обратные элементы группы:

– для 1 обратным является элемент 2, т. к. $1+\hat{1} = 1+2 = 0$;

– для 2 обратным является элемент 1, т. к. $2+\hat{2} = 2+1 = 0$.

На множестве из трех элементов групповая операция задается не более чем одним способом. Табл. 2.1 обладает следующими свойствами:

1) из однозначности разрешимости уравнения $a * x = e$ (у каждого элемента a из множества G существует единственный обратный элемент) следует, что в каждой строке (в каждом столбце) содержатся все элементы группы по одному разу;

2) строки и столбцы ее являются перестановками последовательности (e, a, b);

3) все строки (столбцы) различны.

С точки зрения конечной алгебры рассмотренные группы (см. табл. 2.1 и 2.2) следует считать однотипными. Этот факт приводит к очень важному понятию алгебры – понятию изоморфизма (из этого понятия строятся изоморфные коды).

2.7. Совокупность двоичных n-разрядных чисел с операцией сложения по модулю 2 (mod 2) образует группу $x < \{a = (1110010),\ b = (1100101)\}; \oplus; 0 >$. Например, $a \oplus b = (0010111)$. В такой группе e = (0000000). Обратный элемент равен самому себе, т. к. $a \oplus \hat{a} = e$ = (0000000). Для $a = (1110010)$ обратный элемент $\hat{a} = (1110010)$.

2.8. Пример неабелевой группы. Совокупность невырожденных матриц порядка n относительно матричного умножения $A \cdot B \neq B \cdot A$.

Замечания:

1) существует матрица порядка n, которая коммутирует с любой матрицей такого же порядка. При умножении на нее действие аналогично умножению на нейтральный элемент (единичный элемент), т.е. $A \cdot I = A = A$. Это будет иметь место в том случае, когда I будет единичной матрицей. Например, для n = 4 матрица I имеет вид

$$I=\begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 1\end{bmatrix};$$

2) перестановка строк матрицы. Рассмотрим следующее произведение матриц $E \cdot B = C$:

$$C=\begin{bmatrix}0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\\ 0 & 1 & 0 & 0\\ 1 & 0 & 0 & 0\end{bmatrix}\cdot\begin{bmatrix}1 & 2 & 3 & 4\\ -1 & -2 & -3 & -4\\ 2 & 1 & 0 & 1\\ -2 & 0 & 1 & 1\end{bmatrix}=\begin{bmatrix}-2 & 0 & 1 & 1\\ 2 & 1 & 0 & 1\\ -1 & -2 & -3 & -4\\ 1 & 2 & 3 & 4\end{bmatrix}.$$

Матрица E осуществляет перестановку строк матрицы B. Подобные перестановки широко используются для реализации факторизации матриц, упрощения матриц, для преобразования матриц, например, в каноническую форму, обратную и др.

2.1.2. Особые свойства мультипликативной группы

Для мультипликативной группы $< G; \bullet >$ вводится понятие натуральной степени элемента группы

$$a^0, a, a\,a, \ldots, a\,a\,\ldots a = a^0, a, a^2 \ldots, a^n,$$

где n – ноль или натуральное число.

Определение 2.3. Группа называется циклической, порожденной элементом a, если каждый элемент группы есть некоторая степень a^j.

Теорема 2.2. Пусть $< G; \bullet >$ – группа и a элемент G такой, что $a^s = 1$ для некоторого целого s. Если N – наименьшее положительное целое число, такое, что $a^N = 1$, то $N \mid s$. Целое число N называется порядком a.

Пример 2.9. Задана мультипликативная группа $< \{1, -1, j, -j\}; \bullet; 1>$. Каков порядок элемента j? Каков порядок (–1)? Какой элемент может быть использован в качестве a?

Решение. $j^1 = j, j^2 = -1, j^3 = -j, j^4 = 1$. Порядок элемента j равен 4. Элемент (– 1) имеет порядок, равный 2, т. к. $(-1)^1 = -1$, $(-1)^2 = 1$. Порядок элемента $(-j)$ также равен 4. Данная мультипликативная группа является циклической, порожденной элементом j.

Определение 2.4. Группа называется бесконечной, если все натуральные степени порождающего элемента a различны, т. е. $a^n \neq a^m$ при $m \neq n$. В этом случае говорят, что элемент a имеет бесконечный порядок.

Определение 2.5. Циклическая группа конечна и имеет порядок N, если при некотором N выполняется равенство $a^N = 1$ и N – наименьшее положительное число с таким свойством. Обозначение циклической группы

$$G = <\{ a^0 = 1, a^1, a^2, \ldots, a^N\}; \bullet>,$$

где N – порядок элемента α (число элементов группы).

Определение 2.6. Натуральное число $p > 1$ называется простым, если оно делится только на 1 и на себя. Натуральное число, большее 1, называется составным, если оно не является простым.

Замечание. По определению целое число 1 не является ни простым, ни составным. Число 2 – единственное четное простое число.

Теорема 2.3. Всякая группа простого порядка p (p – простое число) является циклической. Всякая циклическая группа является абелевой, при этом

$$a^m a^n = a^{m+n}; \quad (a^m)^n = a^{mn}.$$

Определение 2.7. Если все элементы циклической группы G могут быть представлены в виде натуральных степеней некоторого элемента $\alpha \in G$, то такой элемент называется примитивным.

В примере 2.9 элемент j – примитивный.

Определение 2.8. Целые числа a и b называются взаимно-простыми, если наибольший общий делитель (НОД) $d = (a, b) = 1$.

Теорема 2.4. (Эйлера), (Леонард Эйлер (1707–1783), швейц. математик) Если a и M взаимно-простые числа, то

$$a^{\varphi(M)} \equiv 1 \bmod M,$$

где $\varphi(M)$ – функция Эйлера, равная количеству всех натуральных чисел меньших M и взаимно-простых с M.

Примеры

2.10. Пусть задано множество целых чисел G = {1, 2, 3, 4, 5, 6}. Найти $\varphi(7)$. Решение. $\varphi(7)$ = 6.

2.11. Задано множество целых чисел G = {1, 2, 3, 4, 5, 6, 7, 8}. Найти $\varphi(9)$.

Решение. $\varphi(9)$ = 6.

Если в циклической группе выполняется условие

$$\varphi(M) = N,$$

то для примитивного элемента циклической группы α справедливо

$$\alpha^{\varphi(M)} \equiv 1 \bmod M, \quad \alpha^N \equiv 1. \tag{2.1}$$

Но α не единственный примитивный элемент циклической группы. Примитивным всегда является элемент α^{N-1}. Разделив (2.1) на α, получим

$$\alpha^{-1} \equiv \alpha^{N-1} \bmod M,$$

$$\alpha^{-1} \equiv \alpha^{\varphi(M)-1} \bmod M. \tag{2.2}$$

Следовательно, примитивным является элемент, обратный α.

Замечание. Для циклической мультипликативной группы, числовых полей и колец обратные элементы можно найти:

1) перебором;

2) по теореме Эйлера;

3) по алгоритму Евклида.

Количество примитивных элементов определяется функцией Эйлера $\varphi(M-1)$.

Пример 2.12. Задана мультипликативная абелева группа G = <{a_0 =1, a_1 =2, a_2 =3, a_3 =4}$_5$;•;1>. Построить возможные циклические группы. Определить число примитивных элементов.

Решение. $\varphi(5)$ = 4. Число примитивных элементов равно $\varphi(4)$ = 2. Примитивным является элемент

$$a_1 = 2, \text{ т. к. } 2^4 = 16 \equiv 1 \bmod 5.$$

Циклическую группу образует множество

$$G = <\{ 2^0 = 1, 2^1, 2^2, 2^3 \equiv ((3)), 2^4 \equiv ((1))\};\bullet>.$$

Примитивным будет также элемент

$$a_2 = a_1^{-1} = a_1^{4-1} \bmod 5 = 2^3 = 8 \equiv ((3)).$$

Циклическую группу образует множество

$$G = <\{ 3^0 = 1, 3^1, 3^2 \equiv ((4)), 3^3 \equiv ((2))\};\bullet>$$

Замечание. Элемент a_3= 4 не является примитивным элементом заданной мультипликативной группы, т. к. имеет порядок 2, ({$4^0 = 1, 4^1, 4^2 \equiv ((1))$}).

2.1.3. Теорема Лагранжа

К свойству конечной аддитивной группы также относится следующее: в любой группе множество G всех элементов по операции сложения образует циклическую аддитивную группу $< \{G\}; +; 0 >$, а элемент 1 порождает множество вида $\{1; 1+1; 1+1+1; \ldots\}$. Так как число элементов в группе конечно, то в этом ряду найдется сумма p единиц, равная нулевому элементу группы.

Определение 2.9. Порядок каждого элемента аддитивной группы a_j определяется по числу этих элементов в последовательности вида
$a, a + a, a + a + a, \ldots, a + a + \ldots\ a = 0 = e$.

Пример 2.13. Определить порядок каждого элемента аддитивной группы $G = < \{0,1,2,3,4,5\}_6; +; 0 >$ порядка 6, задаваемой таблицей Кэли.

Решение. По определению 2.9 представим все элементы группы следующим образом:

1) 0: 0 = e, следовательно, порядок элемента 0 равен 1;

2) 1: 1 + 1 + 1+ 1 + 1+ 1 = $6 \equiv 0 \bmod 6$, следовательно, порядок элемента 1 равен 6;

3) 2: 2 + 2 + 2 = $6 \equiv 0 \bmod 6$, порядок элемента 2 равен 3;

4) 3: 3 + 3 = $6 \equiv 0 \bmod 6$, порядок элемента 3 равен 2;

5) 4: 4 + 4 + 4 = $12 \equiv 0 \bmod 6$, порядок элемента 4 равен 3;

6) 5: 5 + 5 + 5 + 5 + 5 + 5 = $30 \equiv 0 \bmod 6$, порядок элемента 5 равен 6.

Теорема 2.5. (Лагранжа), (Ж. Л. Лагранж (1736 – 1813), франц. математик). Порядок любого элемента a_j произвольной конечной группы, а не только циклической является делителем порядка группы N (числа элементов группы).

2.1.4. Подгруппа

Пусть $< G; * >$ – группа, а $H \subseteq G$ – подмножество, являющееся группой относительно той же групповой операции. Тогда H называется подгруппой группы G. Подгруппа H всегда содержит нейтральный элемент группы. Для того чтобы определить, является ли H подгруппой, достаточно проверить выполнение аксиом замкнутости и существования обратных элементов.

Примеры подгрупп

2.14. Множество E всех четных чисел является подмножеством целых чисел $Z = \{0, \pm 1, \pm 2, \ldots\}$. Тогда $< E; \pm >$ – подгруппа группы $< Z; \pm >$.

2.15. Множество $\{0, 1, 2\}$ принадлежит подмножеству целых чисел Z, но группа, задаваемая табл. 2.2, не является подгруппой группы < Z; + >, т. к. они определяются разными операциями.

2.16. Пусть G = < {0, 1, 2, 3}$_4$; +; 0> – группа порядка 4, задаваемая табл. 2.3.

Таблица 2.3

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Тогда H = <{0, 2}; +; 0> – подгруппа группы G с операцией (табл. 2.4)

Таблица 2.4

+	0	2
0	0	2
2	2	0

Теорема 2.6. Пусть a – элемент порядка N группы G, тогда H = <{ a^1, a^2,…, a^{N-1}}; •; 1> – циклическая подгруппа.

Пример 2.17. Пусть G = < {1, 2, 3, 4}$_5$; •; 1>. H = <{ $4^1 = 4$, $4^2 = 1$}; •; 1>. Порядок N элемента 4 равен 2. Подмножество H – циклическая подгруппа группы G.

Следствие теоремы 2.6. Во всякой мультипликативной группе натуральные степени a^j любого элемента a образуют подгруппу.

Теорема 2.7 (Теорема Ж. Л. Лагранжа). Порядок любой подгруппы конечной группы является делителем порядка группы.

Следствие теоремы 2.7. Порядок каждого элемента конечной подгруппы является делителем порядка группы.

2.1.5. Определение смежного класса по подгруппе

Для заданных конечной группы G и подгруппы H существует операция, которая устанавливает взаимосвязь между G и H и называется разложением

группы G на смежные классы по подгруппе H. Обозначим элементы группы G через $\{g_1, g_1, \dots, g_n\}$, а элементы подгруппы H группы G через $\{h_1, h_2, \dots, h_m\}$.

Построим следующим образом таблицу:

1) запишем элементы подгруппы H в строку с нейтральным элементом в качестве первого элемента строки;

2) выберем произвольным способом элемент группы g_i , не принадлежащий подгруппе H, и запишем его первым элементом столбца;

3) просуммировав g_i со всеми элементами H, получим вторую строку таблицы;

4) далее, выбрав произвольным способом элементg_j, не принадлежащий ни первой, ни второй строке таблицы, и просуммировав его со всеми элементами H, получим третью строку и т. д. для всех элементов группы. Построение заканчивается тогда, когда после некоторой итерации оказывается, что каждый элемент группы G записан в некоторой ячейке таблицы. В результате получается таблица (табл. 2.5):

Таблица 2.5

$h_1 = e$	h_2	h_3	$\cdots$	h_m
$g_1 + h_1$	$g_1 + h_2$	$g_1 + h_3$	$\cdots$	$g_1 + h_m$
$g_2 + h_1$	$g_2 + h_2$	$g_2 + h_3$	$\cdots$	$g_2 + h_m$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$g_r + h_1$	$g_r + h_2$	$g_r + h_3$	$\cdots$	$g_r + h_m$

Подобным способом построенная таблица называется таблицей смежных классов. Строки таблицы называются смежными классами по подгруппе H. Элементы первого столбца называются образующими смежных классов (лидерами смежных классов).

Пример 2.18. Заданы группа G и подгруппа H группы G:
$G = <\{0,1, 2, 3, 4, 5\}_6; +; 0>$, $H = <\{0, 3\}_6; +; 0>$. Построить таблицу смежных классов.

Решение. Группа G и подгруппа H задаются таблицами (табл. 2.6 и 2.7)

Обозначим смежный класс $(g + H)$. Первый смежный класс $(0 + H)$ есть множество элементов подгруппы $H = \{0, 3\}$. Далее получим смежные классы, порожденные всеми элементами группы G:

$$(1 + H) = \{1, 4\},$$
$$(2 + H) = \{2, 5\}.$$

Таблица 2.6

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Таблица 2.7

+	0	3
0	0	3
3	3	0

Таблица смежных классов имеет вид табл. 2.8.

Таблица 2.8

0	3
1	4
2	5

Теорема 2.8. Каждый элемент группы принадлежит одному и только одному смежному классу.

Утверждение 2.1. Два смежных класса не пересекаются. Объединение всех смежных классов совпадает с множеством группы G.

Утверждение 2.1 примера 2.18 соответствует следующим операциям над подмножеством H группы G:

$$(0+H)\cap(1+H)\cap(2+H)=\emptyset,$$
$$(0+H)\cup(1+H)\cup(2+H)=G.$$

Следствие теоремы 2.8. Если H – подгруппа конечной группы G, то число элементов в H делит число элементов в G. Доказательство следует из прямоугольности таблицы смежных классов. Следовательно,
(Порядок G) = (Порядок H) × (Число смежных классов разложения G по H).

Пример 2.19. Заданы n-разрядная группа двоичных чисел $G=<\{G\};\oplus;0>$, $n=4$ и подгруппа H группы G

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

Построить таблицу смежных классов.

Решение. Таблица смежных классов будет иметь следующий вид (табл. 2.9):

Таблица 2.9

0000	1011	0110	1101
1000	0011	1110	0101
0100	1111	0010	1001
0001	1010	0111	1100

Замечание. Таблицы смежных классов используются для декодирования помехоустойчивых кодов. Декодирование основывается на анализе стандартного расположения элементов таблицы.

Упражнение 2.1. Показать, что группа G = <{0,1, 2, 3, 4, 5}$_6$; +; 0> содержит подгруппы порядков: 1, 2, 3 и 6.

2.2. Кольцо

Определение 2.10. Кольцо – это алгебраическая структура или множество элементов R, в котором определены две основные операции (сложение и умножение) и операция, обратная первой из них (вычитание).

В кольце должны выполняться следующие аксиомы:

– <R; +> – абелева группа;

– <R; ·> – полугруппа;

– дистрибутивность (для любых элементов множества R ={ a, b, c }, $a \cdot (b + c) = a \cdot b + a \cdot c$).

Кольцо можно определить и так: кольцо R является группой относительно операции сложения и полугруппой относительно операции умножения.

Определение 2.11. Множество G с заданной на нем бинарной операцией и выполнением аксиом замкнутости и ассоциативности называется полугруппой.

Примеры полугрупп

2.20. <N; +> – аддитивная полугруппа натуральных чисел.

2.21. Пусть q– это конечный набор символов (алфавит). Например, q – множество символов белорусского алфавита, или q – двоичное множество {0, 1}. Пусть слово символов из множества имеет вид $a_1\, a_2 \ldots a_n$, где $a_i \in q$. G обозначает множество слов алфавита q. Введем бинарную операцию ○, называемую конкатенацией над G, следующим образом: если $a_1\, a_2 \ldots a_n$ и $b_1\, b_2 \ldots \ldots b_m \in G$, то $a_1\, a_2 \ldots a_n \circ b_1\, b_2 \ldots b_m = a_1\, a_2 \ldots a_n\, b_1\, b_2 \ldots \ldots b_m$.

Например, если q = {0, 1}, то 11011 ○ 1010110 =110111010110.

Пусть $a_1\ a_2\ \dots\ a_n$, $b_1\ b_2\ \dots\ b_m$ и $c_1\ c_2\ \dots\ c_t \in G$. Тогда $(a_1\ a_2\ \dots\ a_n \circ b_1\ b_2 \dots\ \dots\ b_m) \circ (c_1\ c_2\ \dots\ c_t) = (a_1\ a_2\ \dots\ a_n\ b_1\ b_2\ \dots\ b_m) \circ c_1\ c_2\ \dots\ c_t = a_1\ a_2 \dots\ \dots\ a_n\ b_1\ b_2 \dots\ b_m\ c_1\ c_2\ \dots\ c_t$. Бинарная операция конкатенации ассоциативна на множестве G и это множество вместе с операцией конкатенации образует полугруппу.

Замечания:

1. В кольце для операции умножения могут не выполняться аксиомы существования нейтрального и обратного элементов группы.

2. Если в кольце существует нейтральный элемент относительно умножения, то кольцо называется кольцом с единицей.

3. Кольцо называется коммутативным, если коммутативна операция умножения, т.е. $ab = ba$.

Примеры колец

2.22. Все действительные числа образуют кольцо относительно операций сложения и умножения.

2.23. Алгебраическая система целых чисел $< Z; +; \cdot >$.

2.24. Множество квадратных матриц размером $n \times n$. Нейтральным элементом относительно операции умножения в кольце матриц является единичная матрица.

2.25. Кольцо целых чисел по модулю M. Например, $M = 14$. Тогда система $< \{0, 1, 2, \dots, 13\}; +; \cdot; 0; 1 >$ – кольцо, в котором для элемента 2 не существует обратного элемента, т. к. $2 \cdot 2^{-1} \neq 1 \bmod 14$.

2.2.1. Идеал кольца

Определение 2.12. Пусть R – кольцо, а R' есть подкольцо − подмножество множества R, являющееся кольцом относительно той же операции.

Примеры подколец

2.26. Целые числа образуют подкольцо кольца рациональных чисел

$$R' < \{Z = 0, \pm 1, \pm 2, \dots, \}; +; \cdot; 0; 1 >.$$

2.27. Рациональные числа образуют подкольцо кольца действительных чисел.

2.28. Действительные числа образуют подкольцо кольца комплексных чисел.

2.29. Множество квадратных матриц размером $n \times n$ с целыми значениями элементов образуют подкольцо кольца матриц размером $n \times n$ с рациональными элементами.

Определение 2.13. Подмножество I элементов кольца R называется идеалом в R, если выполняются следующие условия:

– I является подкольцом кольца R, т. е. для любого множества $\{a, b\} \in I$ выполняется $(a + b) \in I$ и $a \cdot b \in I$;

– для любого элемента $a \in I$ и любого элемента $r \in R$ произведения $a \cdot r$ и $r \cdot a$ принадлежат I.

Упражнение 2.2. Показать, что множество $R' = \{0, 2, 4\}$ – это подкольцо кольца $\{Z_6 = 0, 1, 2, 3, 4, 5\}_6; +; \cdot; 0; 1 >$.

2.2.2. Главный идеал

Определение 2.14. Пусть R – коммутативное кольцо. Идеал I кольца R называется главным идеалом, порожденным элементом a (обозначается $< a >$), если I состоит из всех произведений a на элементы кольца R, т. е. $I = < a > = \{a \cdot r: r \in R\}$.

Теорема 2.9. Совокупность целых чисел образует главный идеал тогда и только тогда, когда она состоит из всех чисел, кратных некоторому числу.

Пример 2.30. Множество целых чисел $Z = \{0, 1, 2, 3\}_4$ является коммутативным кольцом с единицей. Найти главный идеал кольца Z.

Решение. Если a – минимальное целое число из I, то по определению идеала $b = r \cdot a$. Выберем в качестве $a = 2$, т. е. $I = < 2 >$. Тогда множество всех чисел, кратных a, запишем в виде

$$I = \{0 \cdot 2 = 0; 1 \cdot 2 = 2; 2 \cdot 2 = ((0))_4; 3 \cdot 2 = ((2))_4\} = \{0, 2\}.$$

Пример 2.31. Рассмотрим кольцо целых чисел и два главных идеала, порожденных целыми числами 8 и 12:

$< 8 >$ = $\{8r: r \in Z\}$ = {…, – 32, – 24, – 16, – 8, 0, 8, 16, 24, 32, …};

$< 12 >$ = $\{12r: r \in Z\}$ = {…, – 36, – 24, – 12, 0, 12, 24, 36, …}.

Найти главный идеал пересечения множеств $< 8 > \cap < 12 >$.

Решение. Пересечение множеств $< 8 > \cap < 12 >$ есть множество {…, – 48, – 24, 0, 24, 48,…}. Главный идеал порождается числом 24, которое является наименьшим общим кратным чисел 8 и 12. В общем случае

$$< a > \cap < b > = < НОК(a, b) >.$$

2.2.3. Полиномиальные формы кольца

2.2.3.1. Сравнения и вычеты полиномов

Рассмотрим два полинома $c(x), f(x)$ и некоторый полином $p(x)$. Если $c(x)$ и $f(x)$ при делении на $p(x)$ дают один и тот же остаток, то говорят, что

$c(x)$ сравним с $f(x)$ по модулю $p(x)$. Полином $p(x)$ называется модулем. Записывается $(x) \equiv f(x) \bmod p(x)$.

Все полиномы, сравнимые по модулю $p(x)$, образуют класс полиномов по модулю $p(x)$. Всем полиномам этого класса соответствует один и тот же остаток. Любой полином в классе называется вычетом по модулю $p(x)$ по отношению ко всем полиномам того же класса. Взяв от каждого класса по одному вычету, получим множество классов вычетов по модулю полинома $p(x)$.

Определение 2.15. Пусть R – коммутативное кольцо с единицей и пусть $R(x)$ – это множество полиномов (многочленов) над кольцом R. Символ x обозначает переменную над кольцом R. Произвольный элемент $c(x) = c_0 + c_1x + + c_2x^2 + + \ldots c_nx^{n-1}$ множества $R(x)$ называется полиномом над кольцом R. Функция $degc(x)$ называется степенью полинома. Если $c_{n-1} \neq 0$ и $degc(x) = n-1$, то c_{n-1} называется старшим коэффициентом полинома. Если $c_{n-1} = 1$, то полином c называется нормированным. Полином степени 0 называется константой.

Например, если $c(x) = 1 + x + x^3$, то $degc(x) = 3$. Если $c(x) = 1$, то $degc(x) = 0$.

Замечание. Множество полиномов $R(x)$ относительно операций сложения и умножения образуют n-мерное векторное пространство над R.

Рассмотрим кольцо вида $R_n = \frac{R(x)}{x^n-1}$, состоящее из класса вычетов кольца полиномов $R(x)$ по модулю полинома $x^n - 1$.

Определение 2.16. Идеалом I_n кольца R_n называется линейное подмножество полиномов от x, такое, что если $c(x) \in I_n$, то $r(x) \cdot c(x) \in I_n$ для всех $r(x) \in R_n$.

Пример 2.32. Пусть $n = 3$. Подмножество полиномов вида $I_n = \{0, (1 + x), (x + x^2), (1 + x^2)\}$ есть идеал в R_3. Действительно, подмножество замкнуто относительно сложения (линейно). Например, $(1 + x) + (1 + x^2) = (x + x^2)$. Кроме того, выполняется условие $r(x) \cdot c(x) \in I_n$. Например, $x^2(1 + x^2) = (x^2 + x^4) \equiv \equiv (x + x^2) mod(x^3 - 1)$, $(x + x^2) \in I_n$.

2.2.3.2. Алгебраическое описание циклических корректирующих кодов

Теория линейных циклических кодов основывается на полиномиальном представлении, когда построение кода осуществляется с помощью операций сложения, вычитания и умножения полиномов по модулю полинома $x^n - 1$. Множество слов циклического кода $C = \{c(x)\}$ попадает в класс вычетов многочленов в степени не больше $(n-1)$, т. е. $\{c(x)\} \in R(x)$.

Сопоставим каждому вектору $c = c_0\, c_1\, c_2 \ldots c_{n-1}$ многочлен $c(x) = c_0 + c_1x + + c_2x^2 + \ldots + c_{n-1}x^{n-1}$. Умножая в кольце R_n многочлен $c(x)$ на x, получаем

$$xc(x) = c_0x + c_1x^2 + \cdots + c_{n-1}x^n = c_{n-1} + c_0x + c_1x^2 + \cdots + c_{n-2}x^{n-1}. \quad (2.3)$$

В кольце R_n имеет место равенство $x^n - 1 \equiv 0 \mod x^n - 1$, отсюда ((x^n)) ≡ 1. Многочлену (2.3) соответствует вектор $(c_{n-1}\ c_0\ c_1 \ldots c_{n-2})$. Следовательно, в кольце R_n операция умножения на x эквивалентна операции циклического сдвига элементов вектора. Пусть n = 4, $p(x) = x^4 - 1$, $c(x) = (x + x^3)$. Умножая x на полином $(x + x^3)$, получаем

$$x\,(x + x^3) \equiv (1 + x^2) \bmod (x^4 - 1).$$

В векторном представлении полученное выражение соответствует циклическому сдвигу вектора (0101).

Определение 2.17. Циклический код $C = \{c(x)\}$ длиной n есть ненулевой идеал I_n в кольце многочленов R_n по модулю многочлена $x^n - 1$.

Утверждение 2.2. Если $c(x) \in I_n$ то $x\,c(x) \in I_n$. Любое, кратное многочлену c(x) ∈ I_n, опять лежит в I_n.

2.2.3.3. Порождающий многочлен циклического кода

Рассмотрим главные идеалы <$g(x)$>, состоящие из всевозможных произведений элементов R_n, некоторый фиксированный многочлен $g(x)$ – порождающий многочлен.

Теорема 2.10. Пусть $C = \{c(x)\}$ − ненулевой идеал кольца R_n, т. е. циклический код длиной n. Тогда справедливо:

1) в C имеется единственный нормированный многочлен $g(x)$ наименьшей степени в коде;

2) C = <$g(x)$> ,т. е. $g(x)$ – порождающий многочлен идеала C;

3) $g(x) \mid (x^n - 1)$,т. е. ($g(x)$ делит($x^n - 1$));

4) любой многочлен c(x) ∈ C в кольце $R(x)$ однозначно записывается в виде

$$c(x) = f(x)g(x), \quad (2.4)$$

где $f(x) \in R(x)$ – кодируемый (информационный) многочлен.

Формула (2.4) – это правило формирования кодового слова сообщения $f(x)$;

5) степень порождающего многочлена $\deg g(x) = n - k$, где k – определяет степень информационного многочлена $\deg f(x) \leq (k-1)$.

Пусть n = 7, $g(x)$ = 1 + $x + x^3$, $f(x) = 1 + x + x^2$. Получим кодовое слово $c(x) =$ (1 + x + x^2)(1+ x + x^3) = 1 + x^2 + x^3 + x^4 + x^5. Таким образом, если на вход кодера подается сообщение f = (1 1 1 0), на выходе его формируется вектор c = (1 0 1 1 1 1 0).

2.3. Поле

Определение 2.18. Полем называется коммутативное кольцо с единицей, каждый элемент которого имеет обратный элемент относительно умножения.

Определение 2.19. Поле – это множество элементов, над которыми заданы две бинарные операции (сложение, умножение) и для них существуют обратные операции (кроме деления на ноль), причем умножение дистрибутивно относительно сложения, т. е.

$$(a + b)c = ac + bc, \quad c(a + b) = ca + cb.$$

Поле – это алгебра <{G}; +; ·; −;:; 0; 1>.

Примеры полей

2.33. Множество рациональных чисел.

2.34. Множество действительных чисел.

2.35. Множество целых чисел простого порядка p, где p – простое число.

При построении кодов различного назначения наибольший интерес представляют конечные алгебры – поля Галуа (Galois Feld). Эта алгебра названа в честь Эвариста Галуа ((1811 – 1832), франц. математик). Конечные поля $GF(q^m)$ имеют порядок поля q^m, где простое число q – это характеристика поля, натуральное число m – размерность поля. Порядок поля $GF(q^m)$ равен числу элементов поля.

Определение 2.20. Поле $GF(q)$ называется подполем поля $GF(q^m)$, если оно содержится в поле $GF(q^m)$ и имеет те же операции. Поле $GF(q^m)$ называется расширением поля $GF(q)$ (простого поля).

Например, поле из двух элементов $GF(2)$ – простое поле порядка 2, а $GF(2^7) = GF(128)$ – его расширение; поле действительных чисел является расширением поля рациональных чисел.

Замечания:

1. Алгебра (школьная) рациональных чисел – это пример бесконечного поля.

2. Целые числа бесконечных множеств не образуют поле (результат операции деления двух целых чисел необязательно является целым числом).

3. При $m = 1$ имеем простое поле $GF(q)$ с модулярными операциями сложения и умножения, т.е. операциями по $\mathrm{mod}\ q$.

Для каждого простого q существует только одно поле, т. е. правила сложения и умножения, удовлетворяющие всем нужным аксиомам, можно задать только одним способом. Для заданного простого q элементами поля являются числа 0, 1, …, $(q - 1)$.

Наименьшее число элементов, образующих поле, равно 2. Это является следствием того, что должно быть два нейтральных элемента относительно операции сложения и умножения.

Поле $GF(2)$ задается таблицами Кэли (табл. 2.10 и 2.11).

Таблица 2.10

+	0	1
0	0	1
1	1	0

Таблица 2.11

·	0	1
0	0	0
1	0	1

Поле $GF(3)$ задается таблицами Кэли (табл. 2.12 и 2.13).

Таблица 2.12

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Таблица 2.13

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Таблицы сложения и умножения для $GF(5)$ имеют вид табл. 2.14 и 2.15.

Таблица 2.14

+	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

Таблица 2.15

·	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

Для выполнения вычитания или деления следует, используя таблицы, найти соответствующий обратный элемент, а затем выполнить сложение или умножение.

Пример 2.36. Вычислить в поле $GF(5)$:

1) 3 – 4;

2) $3/4$.

Решение

1) $3 - 4 = 3 + (-4) = 3 + ((-4 + 5)) = 3 + 1 = 4$, т.к. $4 + (-4) \equiv 0 \bmod 5$;

2) $3/4 = 3 \cdot 4^{-1} = ((3 \cdot 4)) = 2$, т. к. $4 \cdot 4^{-1} \equiv 1 \bmod 5$.

В любом поле множество G всех элементов по операции сложения образует циклическую аддитивную группу.

В любом поле множество G ненулевых элементов по операции умножения образует циклическую мультипликативную группу.

Теорема 2.11. В конечных полях, так же как и циклических мультипликативных группах, существуют примитивные (генераторные) элементы α (по крайней мере один). Все ненулевые элементы β поля могут быть представлены в виде натуральных степеней α^j элемента α, т. е.

$$\beta = \alpha^j,$$

где j – логарифм элемента α.

Пример 2.37. Имеется поле $GF(5)$. Элемент 2 поля является примитивным, поскольку: $2^1 = 2; 2^2 = 4; 2^3 = 3; 2^4 = 1$.

Если a и M взаимно-простые числа, для поля, так же как и для циклических мультипликативных групп, справедлива теорема Эйлера:

$$a^{\varphi(M)} \equiv 1 \bmod M.$$

Количество примитивных элементов определяется функцией Эйлера $\varphi(M-1)$. Примитивным всегда является элемент α^{N-1}, где N – порядок элемента α.

В примере 2.37 $\varphi(M-1) = \varphi(5-1) = \varphi(4) = 2$. Примитивным элементом будет элемент 3, поскольку

$$2^{4-1} = 2^3 = 8 \equiv 3 \bmod 5.$$

2.3.1. Корректирующие коды

Среди корректирующих (помехоустойчивых) кодов находят применение линейные коды с символами из группы или поля Галуа $GF(q)$.

Определение 2.21. Линейный $[n,k,d]$-код есть подпространство размерностью k линейного n-мерного пространства над $GF(q)$. Подмножество, состоящее из последовательностей длиной n, называется q-ичным блоковым кодом длиной n.

Замечания:

1. Если $q = \{0,1\}$, векторное пространство кода над полем $GF(2)$ образует аддитивную подгруппу группы всех двоичных последовательностей длиной n.

2. Так как операция суммирования является линейной операцией, то и код называется линейным.

Определение 2.22. Длина кода n (значность) – число символов кодового слова. Последовательности элементов (символов) длиной n называются кодовыми словами или кодовыми векторами. Говорят, что слово $c = (c_0\, c_1\, \ldots c_{n-1})$ имеет длину n.

Определение 2.23. Размерность кода k – число информационных элементов (позиций) кодового слова.

Определение 2.24. Расстояние Хэмминга между двумя векторами (степень удаленности любых кодовых последовательностей друг от друга) – d_x. Если $X = (x_0\, x_1\, x \ldots x_{n-1})$ и $Y = (y_0\, y_1\, \ldots y_{n-1})$ – кодовые векторы, то расстояние Хэмминга равно числу позиций, в которых они различаются. Расстояние Хэмминга может обозначаться и как dist (X,Y). Например, dist $(cc\,acg\,a, acgccg) = 4$; dist $(0122, 2212) = 3$.

Замечание. С позиции теории кодирования d_x показывает, сколько символов в слове надо исказить, чтобы перевести одно кодовое слово в другое.

Определение 2.25. Наименьшее значение расстояния Хэмминга для всех пар кодовых последовательностей кода G называют кодовым расстоянием d (минимальное расстояние кода),

$$d = \min\{\text{dist}\,(X, Y)\},\ \text{где}\ X \in G;\ Y \in G;\ X \neq Y.$$

Кодовое расстояние d характеризует корректирующую способность кода

$$t = f(d).$$

Определение 2.26. Код значностью n, размерностью k и расстоянием d называется $[n, k, d]$-кодом.

Например, множество

$$G = \begin{Bmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{Bmatrix}$$

используем для кодирования 2-битовых двоичных чисел, используя следующее (произвольное) соответствие:

$$00 \leftrightarrow 1011;$$
$$10 \leftrightarrow 0000;$$
$$01 \leftrightarrow 0110;$$
$$11 \leftrightarrow 1101.$$

Вычислим кодовое расстояние этого кода:

dist (1011, 0110) = 3;
dist (1011, 1101) = 2;
dist (0110, 1101) = 3.

Следовательно, для этого кода d = min{dist(X, Y)} = 2.

Определение 2.27. Вес Хэмминга вектора $X = (x_0\, x_1\, x \ldots x_{n-1})$ равен числу ненулевых позиций x_i, обозначается $wt(X)$.

Например, $wt(X) = wt(1\ 0\ a\ b) = 3$. Используя определение веса Хэмминга, получим очевидное выражение

$$\text{dist}\,(X, Y) = wt(X - \mathrm{Y}). \qquad (2.5)$$

Пусть элементами поля $GF(3)$ является множество $\{0, 1, 2\}$. Для векторов $X = (1\ 2\ 0\ 2)^T$ и $Y = (2\ 0\ 1\ 2)^T$

$$\text{dist}\,(X, Y) = wt\left\{\begin{bmatrix}1\\2\\0\\2\end{bmatrix} - \begin{bmatrix}2\\0\\1\\2\end{bmatrix}\right\} = wt\begin{bmatrix}2\\2\\2\\0\end{bmatrix} = 3.$$

3 3 3

Из выражения (2.5) следует, что минимальное расстояние Хэмминга равно

d = min{dist (X, Y)} = min $\{wt(X - \mathrm{Y})\}$, где $X \in G$; $Y \in G$; $X \neq Y$.

Определение 2.28. Число проверочных (избыточных) позиций кодового слова $r = n - k$.

Например, n = 7, k = 4. Тогда на длине слова из семи символов – три избыточных, r = 3.

Определение 2.29. Кратность ошибки t. Параметр t указывает, что все конфигурации из t или менее ошибок в любом кодовом слове могут быть исправлены.

Предположим, что по каналу передается или хранится в памяти кодовое слово $X = (x_0\, x_1\, x \ldots x_{n-1})$, а принимается или считывается из памяти вектор $Y = (y_0\, y_1\, \ldots y_{n-1})$. Вектор $E = Y - X = (e_0\, e_1\, \ldots e_{n-1})$ называется вектором ошибок, где $e_i \in GF(q)$. Если ошибок не произошло, то $E = 0$. Вектор ошибок указывает место и значение ошибок.

Теорема 2.12. При необходимости обнаруживать ошибки кратностью t кодовое расстояние кода должно быть

$$d \geq t + 1.$$

Теорема 2.13. Для исправления ошибок кратностью t кодовое расстояние должно удовлетворять соотношению

$$d \geq 2\mathrm{t} + 1. \qquad (2.6)$$

Используя эту формулу, можно записать

$$t = \lceil (d - \lceil l \rceil)/2 \rceil,$$

где $\lceil l \rceil$ обозначает целую часть числа l. Если d четное, то код может исправлять $t = (d - 2)/2$ ошибок.

Примером линейного группового кода является двоичный код Хэмминга.

Определение 2.30. Для каждого целого положительного числа m существует код Хэмминга с параметрами $[2^m - 1, 2^m - 1 - m, 3]$, $t = 1$.

2.3.2. Граница Синглтона

Теорема 2.14. Кодовое расстояние любого линейного $[n, k, d,]$-кода удовлетворяет неравенству

$$d \leq 1 + n - k.$$

Доказательство. Ненулевое слово минимального веса в коде имеет вес

$$d = \min\{wt(X)\}, \text{ где } X \neq 0, X \in G.$$

Кодовое слово кода с одним ненулевым информационным символом и $r = (n - k)$ проверочными символами не может иметь вес, больший $(1 + n - k)$. Следовательно, минимальный вес кода не может быть больше

$$\min\{wt(X)\} \leq 1 + n - k.$$

Тогда

$$d \leq 1 + n - k. \qquad (2.7)$$

Граница Синглтона показывает, что для исправления t ошибок код должен иметь не менее $2t$ проверочных символов и что линейные коды с $r = d - 1$ существуют. Из формул (2.6) и (2.7) следует

$$1 + n - k \geq 2t + 1;\ n - k \geq 2t;\ r \geq 2t.$$

Определение 2.31. Любой код с кодовым расстоянием, удовлетворяющим равенству

$$d = 1 + n - k = r + 1, \qquad (2.8)$$

называется кодом с максимальным расстоянием.

Коды с максимальным расстоянием имеют точно два проверочных символа на ошибку, т. е. $r = 2t$.

Упражнения

2.3. Построить поле Галуа $GF(4)$, если задано множество элементов $G = \{0, 1, a, b\}$.

2.4. Построить поле Галуа $GF(4)$ для числового множества $G = \{0, 1, 2, 3\}$.

2.5. Показать, что поле $GF(2)$ содержится в поле $GF(4)$.

2.6. Показать, что поле $GF(2)$ не содержится в поле $GF(3)$.

2.3.3. Полиномиальные формы поля

Определение 2.32. Если операции сложения и умножения коэффициентов полиномов рассматриваются как операции в поле, полиномы называются полиномами над полем.

Операции с полиномами над полем задаются через приведение результата операции по модулю неприводимого полинома $p(x)$ степени m. Например,

$$((c(x)) + ((f(x))) = ((c(x) + (f(x))),$$
$$((c(x)) \cdot ((f(x))) = ((c(x) \cdot (f(x))).$$

Определение 2.33. Если q^m– есть степень простого числа, то элементами поля полиномов являются все полиномы степени $(m - 1)$ или менее, коэффициенты которых лежат в простом поле $GF(q)$.

Определение 2.34. Поле, образованное полиномами над полем $GF(q)$ по модулю неприводимого полинома $p(x)$ степени m, называется расширением поля степени m над полем $GF(q)$.

Неприводимый полином обладает тем свойством, что его нельзя разложить на множители, используя полиномы с коэффициентами из поля $GF(q)$.

Замечания:

1. Аналог неприводимого полинома $p(x)$ – простое число.

2. Как и простые числа, неприводимые полиномы находятся методом перебора. Таблицы неприводимых полиномов над полем $GF(2)$ имеются в книге У. Питерсона и Э. Уэлдона (Коды, исправляющие ошибки) [15].

Пример 2.38. Найти неприводимый полином второй степени над полем $GF(2)$.

Решение. Здесь $m = 2$, $q = 2$. Действуя методом перебора, определяем:

1) $p(x) = x^2$– приводимый полином над полем $GF(2)$, т. к. $x^2 = x \cdot x$;

2) $p(x) = (x^2 + 1) = (x + 1)(x + 1) = (x^2 + x + x + 1) = (x^2 + x(1 + 1) + 1) = (x^2 + 1)$ – приводимый полином над полем $GF(2)$;

3) $p(x) = (x^2 + x + 1)$ – единственный вариант неприводимого полинома второй степени над полем $GF(2)$.

Пример 2.39. Заданы два полинома поля $GF(2^3)$: $f_1(x) = 1 + x + x^2$ и $f_2(x) = 1 + x^2$. Выполнить операции сложения и умножения в поле, если $p(x) = (x^3 + x + 1)$ – неприводимый полином третьей степени над полем $GF(2)$.

Решение

1) $f_1(x) + f_2(x) = (1 + x + x^2) + (1 + x^2) = x;$

2) $f_1(x) \cdot f_2(x) = (1 + x + x^2) \cdot (1 + x^2) = 1 + x^2 + x + x^3 + x^2 + x^4 \equiv (1 + x + x^3 + x^4 mod(x^3 + x + 1) = ((x^2 + x)).$

2.3.4. Представление элементов поля Галуа $GF(q^m)$

Удобное описание многих вычислительных алгоритмов, процессов помехоустойчивого и криптографического кодирования и декодирования реализуется с помощью степенного, полиномиального, векторного и логарифмического представления элементов расширенного поля Галуа.

Элементы поля $GF(q^m)$ могут интерпретироваться как класс вычетов полиномов от x с коэффициентами из $GF(q)$ по модулю неприводимого над $GF(q)$ полинома степени m.

Пример 2.40. Определим основные операции в поле неприводимого над полем $GF(2)$ полинома $p(x) = 1 + x + x^2$.

Операция сложения в поле $GF(2^2)$, элементы которого записываются в виде полиномов, задается в виде табл. 2.16.

Таблица 2.16

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

Записывая коэффициенты полиномов, получим следующее соответствие между полиномами и двоичными векторами (табл. 2.17):

Таблица 2.17

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

Таблица Кэли в поле $GF(2^2)$, элементы которого записываются в виде двоичных чисел, имеет вид табл. 2.18:

Таблица 2.18

+	0 0	1 0	0 1	1 1
0 0	0 0	1 0	0 1	1 1
1 0	1 0	0 0	1 1	0 1
0 1	0 1	1 1	0 0	1 0
1 1	1 1	0 1	1 0	0 0

Аналогично построим таблицы умножения элементов поля $GF(2^2)$. Операция умножения в поле $GF(2^2)$, элементы которого записываются в виде полиномов, задается в виде табл. 2.19.

Таблица 2.19

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

Таблица умножения, представленная двоичными векторами, имеет вид табл. 2.20.

Таблица 2.20

	0 0	1 0	0 1	1 1
0 0	0 0	0 0	0 0	0 0
1 0	0 0	1 0	0 1	1 1
0 1	0 0	0 1	1 1	1 0
1 1	0 0	1 1	1 0	0 1

Например, элемент таблицы 10 с координатами (01, 11) получен следующим образом.

1. Воспользуемся обычным умножением в «столбик» со старшим разрядом числа слева:

$$\begin{array}{r} 1\ 0 \\ 1\ 1 \\ 1\ 0 \\ \underline{1\ 0\ \ } \\ 1\ 1\ 1\ 0. \end{array}$$

2. Результат умножения приведем по модулю полинома $p(x)$ (в этом представлении полиному $p(x) = 1 + x + x^2$ соответствует вектор коэффициентов (111)):

$$\begin{array}{l} \underline{1\ 1\ 0|}\ \underline{1\ 1\ 1} \\ \underline{1\ 1\ 1}\ \ 1 \\ 0\ \ 0\ 1. \end{array}$$

3. Выполним инверсию двоичного числа: 0 0 1|1 0 0. Получим вектор 1 0.

Теорема 2.15. В расширенном поле полиномов $GF(q^m)$ существует примитивный элемент α порядка $(q^m - 1)$, т. е.

$$\alpha^{(q^m - 1)} = 1.$$

Каждый элемент β поля $GF(q^m)$ может быть представлен как некоторая степень α, т. е. $\beta = \alpha^i$.

Теорема 2.16. Если α – примитивный элемент поля, то α^κ тоже примитивный элемент, если κ и q^m – взаимно-простые числа. Тогда в поле $GF(q^m)$ имеется $\varphi(q^m - 1)$ примитивных элементов.

Пример 2.41. Пусть $GF(2^3)$ – расширенное поле Галуа. Найти примитивные элементы поля.

Решение. Примитивным элементом поля является элемент α^κ, где κ и $q^m = 2^3 = 8$ – взаимно-простые числа. Взаимно-простыми числами с числом 8 будут числа 3, 5, 7. (НОД) d = (8, 3) = (8, 5) = 1. Тогда α^3 и α^5 – примитивные элементы.

Определение 2.35. Неприводимый над полем $GF(q)$ полином степени m называется примитивным, если его корнем является примитивный элемент α поля $GF(q^m)$.

Пример 2.42. Полином $p(x) = 1 + x + x^2$ неприводим над полем $GF(2)$. Этот полином примитивный, т. к. примитивный элемент α поля $GF(q^m)$ является корнем $p(x)$. Действительно, в поле $GF(2^2)$ выполняется $p(\alpha) = 1 + \alpha + \alpha^2 = 0$, т. к. $x^2 \equiv (1 + x) \bmod 1 + x + x^2$. Тогда $p(\alpha) = 1 + \alpha + \alpha^2 = 1 + \alpha + 1 + \alpha = 0$.

В табл. 2.21 приведены четыре формы представления элементов поля $GF(2^2)$. Поле образовано полиномами над полем $GF(2)$ по модулю неприводимого полинома $p(x) = 1 + x + x^2$ Порядок элемента α равен 3, т. к. $\alpha^{(2^2 - 1)} = \alpha^3 \equiv$ $\equiv 1 \bmod (1 + \alpha + \alpha^2)$.

Таблица 2.21

В виде степени примитивного элемента	В виде полинома	В виде двоичного числа	В виде логарифма
–	0	0 0	–
α^0	1	1 0	0
α^1	α	0 1	1
α^2	$1 + \alpha$	1 1	2

Используя разные формы элементов поля, можно эффективно производить алгебраические операции в поле $GF(q^m)$.

1. Умножение с представлением элементов поля в виде степеней примитивного элемента выполняется следующим образом:

$$\beta_1 \cdot \beta_2 = \alpha^i \cdot \alpha^j = \alpha^{i+j} = ((\alpha^{Rest\left[\frac{i+j}{N}\right]})),$$

где $Rest\left[\frac{i+j}{N}\right]$ – остаток от деления $(i + j)$ на порядок N примитивного элемента α поля $GF(q^m)$. Например, используя табл. 2.21, имеем

$$\alpha^2 \cdot \alpha^2 = \alpha^4 = \alpha^1.$$

2. Деление на элемент поля.

Теорема 2.17. Если полином $p(x)$ степени m неприводим над поле $GF(q)$, то каждый ненулевой полином $c(\alpha)$ степени не более $(m - 1)$ имеет единственный обратный полином $c(\alpha)^{-1}$, такой, что

$$c(\alpha) \cdot c(\alpha)^{-1} \equiv 1 \bmod p(\alpha).$$

Нахождение обратных элементов легко выполнять, если воспользоваться представлением элементов поля в виде степеней примитивного элемента или логарифмов. Пусть $C = c(\alpha)$ – произвольный элемент поля $GF(q^m)$ с коэффициентами из поля $GF(q)$, т. е.

$$C = c(\alpha) = c_0 + c_1\alpha + c_2\alpha^2 + \cdots + c_{m-1}\alpha^{m-1}.$$

Требуется разделить элемент C на элемент поля

$$B = b_0 + b_1\alpha^1 + b_2\alpha^2 + \cdots + b_{m-1}\alpha^{m-1}.$$

Для того чтобы найти C/B, вычислим обратный элемент $B^{-1} = 1/B$, а затем представим

$$C/B = C \cdot B^{-1}.$$

Пример 2.43. Поле образовано полиномами над полем $GF(2)$ по модулю неприводимого полинома $p(x) = 1 + x + x^2$. Вычислить $\alpha/(1 + \alpha)$.

Решение. Полиному (1+ α) соответствует α^2. Тогда $\alpha/(1+\alpha) = \frac{\alpha}{\alpha^2} =$ $= \alpha^{-1} = \alpha^3\alpha^{-1} = \alpha^2 = 1 + \alpha$.

Поле образовано полиномами над полем $GF(2)$ по модулю неприводимого полинома $p(x) = 1 + x + x^3$. Вычислить $\sqrt{110}$.

Решение. Вектору (110) соответствует элемент поля α^3. Квадратный корень $\sqrt{\alpha^3} = \sqrt{1\alpha^3} = \sqrt{\alpha^7\alpha^3} = \sqrt{\alpha^{10}} = \alpha^5 = 111$.

2.3.5. Способы задания линейных кодов

Линейные коды задаются с помощью:

а) порождающей матрицы G размером $k \times n$;

б) проверочной матрицы H размером $(n-k) \times n$.

Матрицы связаны основным уравнением кодирования

$$G \times H^T = 0.$$

Из уравнения следует, что для всякой матрицы G существует матрица H, удовлетворяющая этому равенству. И наоборот, заданной матрице H будет соответствовать только одна матрица G. В качестве строк матрицы G выбираются линейно независимые кодовые слова длиной n, отстоящие друг от друга на заданное кодовое расстояние d. Проверочную матрицу кода можно построить, используя примитивный элемент расширенного поля Галуа $GF(2^m)$. Например, матрица H кода Хэмминга (определение 2.30) представляется как

$$H = [\alpha^0, \alpha^1, \alpha^2, \ldots, \alpha^{2^m-2}],$$

где α примитивный элемент поля $GF(2^m)$.

Пусть $\alpha \in GF(2^3)$ – корень уравнения $1 + \alpha + \alpha^3 = 0$. Двоичный код Хэмминга длиной $n = 2^3 - 1 = 7$ имеет проверочную матрицу

$$H = [1, \alpha^1, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6].$$

Все элементы поля $\beta = \alpha^j$ могут быть представлены как различные ненулевые двоичные векторы. Если каждый элемент α^j заменить на вектор столбец, получающийся операцией транспонирования вектор-строки (двоичного представления элемента поля α^j), то проверочная матрица двоичного [7, 4, 3] – кода Хэмминга примет вид

$$H = \begin{matrix} 1 & \alpha^1 & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \end{matrix}$$
$$\begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}. \qquad (2.9)$$

2.3.5.1. Двоичный код Боуза – Чоудхури – Хоквингема (БЧХ-код), исправляющий две ошибки

Определение 2.36. БЧХ-код, исправляющий две ошибки, – это блоковый циклический код над полем $GF(2)$ с параметрами: $n = 2^m - 1$, $k = n - 2m$, $d \geq 5$, $m \geq 3$, с проверочной матрицей

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{2^m-2} \\ 1 & \alpha^3 & \alpha^6 & \dots & \alpha^{3(2^m-2)} \end{bmatrix},$$

где α – примитивный элемент поля $GF(2^m)$. Элемент α является корнем неприводимого порождающего полинома поля $GF(2^m)$.

Пусть α – примитивный элемент поля $GF(2^3)$ есть корень уравнения $1+ \alpha + \alpha^3 = 0$. Проверочная матрица двоичного [7, 1, 5] БЧХ-кода, исправляющего две ошибки, записывается в виде

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & \alpha^{15} & \alpha^{18} \end{bmatrix}. \quad (2.10)$$

С учетом свойства периодичности элементов поля для примитивного элемента, когда $\alpha^7 \equiv ((1))$, матрица (2.10) преобразуется к виду

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ 1 & \alpha^3 & \alpha^6 & \alpha^2 & \alpha^5 & \alpha^1 & \alpha^4 \end{bmatrix}. \quad (2.11)$$

Замечание. Элемент α действительно является примитивным элементом поля, т. к. и во второй строке матрицы (2.11) появляются все степени α.

Используя двоичное представление элементов поля (2.9), получаем проверочную матрицу БЧХ-кода:

$$H_{7,1} = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix}.$$

Определение 2.37. Проверочная матрица двоичного БЧХ-кода, исправляющего t независимых ошибок, записывается как

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{(n-1)} \\ 1 & \alpha^3 & \alpha^6 & \dots & \alpha^{3(n-1)} \\ . & . & . & \dots & . \\ 1 & \alpha^{2t-1} & \alpha^{2(2t-1)} & \dots & \alpha^{(n-1)(2t-1)} \end{bmatrix},$$

где каждый элемент поля $\beta = \alpha^j \in \mathrm{GF}(2^m)$ должен быть заменен соответствующим двоичным вектором.

Упражнения

2.7. Найти все примитивные элементы расширенного поля Галуа $GF(2^4)$.

2.8. Привести четыре формы представления элементов поля $GF(2^4)$. Поле образовано неприводимым над полем $GF(2)$ полиномом $p(x) = 1 + x + x^4$.

2.9. Поле образовано полиномами над полем $GF(2)$ по модулю неприводимого полинома $p(x) = 1 + x + x^3$. Вычислить:

а) полином , обратный полиному $A = 1 + \alpha + \alpha^2$;

б) полином , обратный полиному $B = \alpha + \alpha^2$;

в) A / B;

г) $\sqrt{\alpha + \alpha^2}$;

д) $(111)^{-1}$.

2.10. Построить проверочную матрицу двоичного БЧХ-кода длиной 15, исправляющего трехкратные ошибки.

2.4. Вычисления в конечном поле Галуа

2.4.1. Описание структурных схем для выполнения операций в поле $GF(q^m)$.

Алгебру полей Галуа можно технически реализовать с помощью логических (арифметических) цепей и схем запоминания элементов поля.

1. Умножитель на скаляр (константу), показанный на рис. 2.1, реализует функцию одной переменной. Умножает входную переменную (входной символ) на константу, которой может быть элемент поля $GF(q)$. Введение в схему умножителя константы $h = 1$ эквивалентно соединению. Константа $h = 0$ эквивалентна отсутствию соединения.

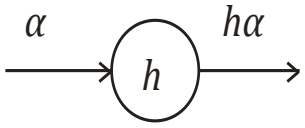

Рис. 2.1

2. Сумматор (рис. 2.2) реализует функцию двух переменных, принадлежащих полю Галуа $GF(q)$. Если $q = 2$, сумматор – схема «Исключающее ИЛИ».

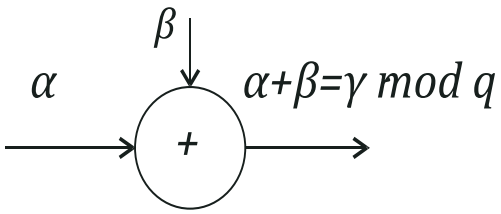

Рис. 2.2

3. Умножитель, показанный на рис. 2.3, реализует функцию двух переменных, принимающих значение из поля $GF(q)$. Для $q = 2$ умножитель – это схема «Логическое И».

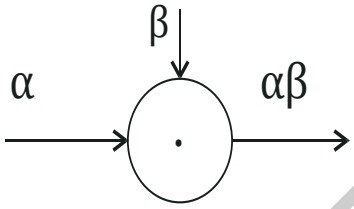

Рис. 2.3

4. Цепи записи (хранения) двоичных элементов поля элементов поля Галуа $GF(2^m)$ представляют собой m-битовые последовательные и параллельные схемы на основе регистров сдвига и хранения.

Определение 2.38. Символ Y на выходе ячейки памяти (элемента задержки) может быть записан в форме

$$Y = DX,$$

где X – входной символ, а D – оператор задержки или отношение выходной величины задержки к входной задержке.

Символ D^i является алгебраическим оператором задержки, действие которого заключается в задержке входного символа на i тактов.

Схемы, состоящие из различных сочетаний элементов, изображенных на рис. 2.1 – 2.3, называются линейными переключательными схемами. Символ, появляющийся на выходе такой схемы, может зависеть только от одного символа, который присутствует на входе, или от нескольких символов, которые появились на входе в данный и предыдущий момент времени. В первом случае схема будет однотактной, а во втором – многотактной.

2.4.2. Линейная многотактная переключательная схема

Функциональную зависимость между выходными и входными символами многотактной переключательной схемы можно выразить как

$$Y = f(X). \tag{2.12}$$

Ограничимся только линейной логической функциональной зависимостью выход – вход. Многотактная переключательная схема называется линейной, если выходной символ равен сумме по модулю q некоторых входных символов. Для такой схемы применим аппарат линейной алгебры. Для двоичного случая, когда $q = 2$, выходной символ схемы есть сумма по модулю 2 множества входных сигналов.

Рассмотрим принцип работы многотактной переключательной схемы, изображенной на рис. 2.4. Пусть все константы h равны 1.

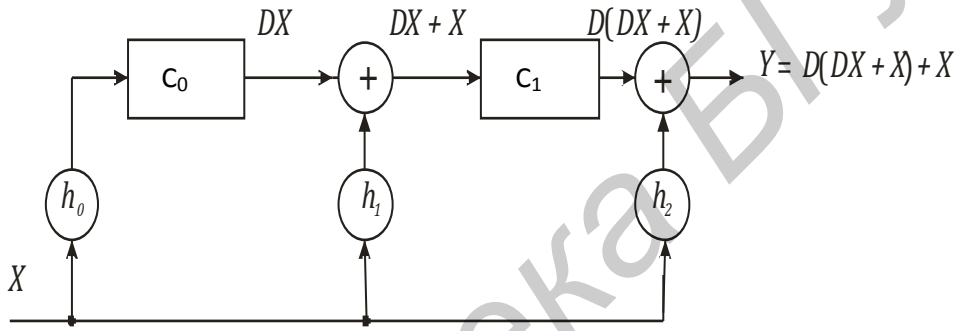

Рис. 2.4

Зависимость между входной и выходной последовательностями определяется выражением

$$Y = D(DX + X) + X. \tag{2.13}$$

Отношение выходной последовательности к входной называется передаточной функцией $P(D)$ схемы. Запишем уравнение (2.13) в другой форме:

$$Y = D^2X + DX + X = X(D^2 + D + 1), \tag{2.14}$$

где $1 = D^0$– это тождественный или единичный оператор.

Передаточная функция многотактной переключательной схемы (линейного фильтра), показанной на рис. 2.4, равна

$$P(D) = \frac{Y}{X} = D^2 + D + 1. \tag{2.15}$$

Видно, что передаточная функция представляет собой полином задержки, записанный в порядке возрастания степеней оператора D.

Вывод. Передаточная функция однозначно определяет свойства линейной многотактной переключательной схемы (устройства преобразования входных последовательностей).

Пример 2.45. Пусть на входе схемы (рис. 2.4) имеется единичное воздействие X = (1 0 0 0…). Изменения состояний ячеек памяти регистра в тактовые моменты времени приведены в табл. 2.22.

Таблица 2.22

№ такта	Вход X	c_0	c_1	Выход Y
0	1	0	0	1
1	0	1	1	1
2	0	0	1	1
3	0	0	0	0
⋮	⋮	⋮	⋮	⋮

На выходе получим импульсную реакцию Y = (1 1 1 0…). Положение единицы в импульсной реакции соответствует степеням оператора D в передаточной функции. Импульсная реакция затухает через два такта. Здесь выходная последовательность является функцией только последовательности входных символов (формула (2.12)).

Далее рассмотрим случай, когда выход является функцией не только символов входной последовательности, но и выходной. Функциональную зависимость между выходными и входными символами такой многотактной переключательной схемы можно выразить как

$$Y = f(X, Y). \tag{2.16}$$

Из выражения (2.16) возникает вопрос, при каких условиях возможно появление выходных символов Y, если на схему не поступают входные символы X. Разрешим уравнение (2.15) относительно входной последовательности

$$X = \frac{Y}{(D^2+D+1)}. \tag{2.17}$$

Если принять, что Y– это входная последовательность, а X– выходная, то передаточная функция примет вид

$$\frac{1}{(D^2+D+1)}.$$

Схемная реализация такой многотактной схемы показана на рис. 2.5.

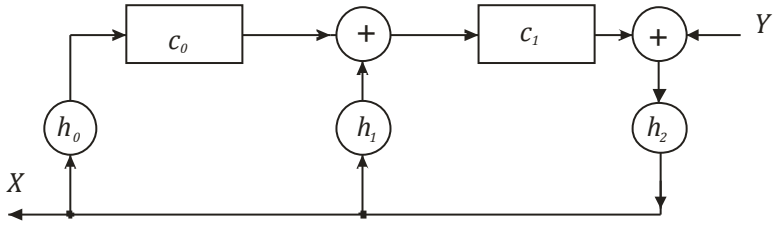

Рис. 2.5

Схема рис. 2.5 отличается от схемы, приведенной на рис. 2.4, тем, что вход и выход поменялись местами, и изменилось направление прохождения входного символа. Поскольку в схеме имеются обратные связи, при определенных условиях можно получить выходную последовательность при отсутствии входной. Этот режим формирования вытекает из решения уравнения

$$X = \frac{Y}{(D^2+D+1)}, \text{ когда } Y = 0.$$

$$X(D^2 + D + 1) = 0.$$

Напомним, для рассматриваемой схемы X означает выходную последовательность. Таким образом, схема рис. 2.5 при определенных условиях может генерировать псевдослучайные последовательности двоичных символов. Чтобы началась генерация, достаточно записать в элемент памяти единицу.

2.4.3. Генератор псевдослучайной последовательности

На рис. 2.6 изображена линейная генераторная схема на основе регистра сдвига (РС) с обратной связью.

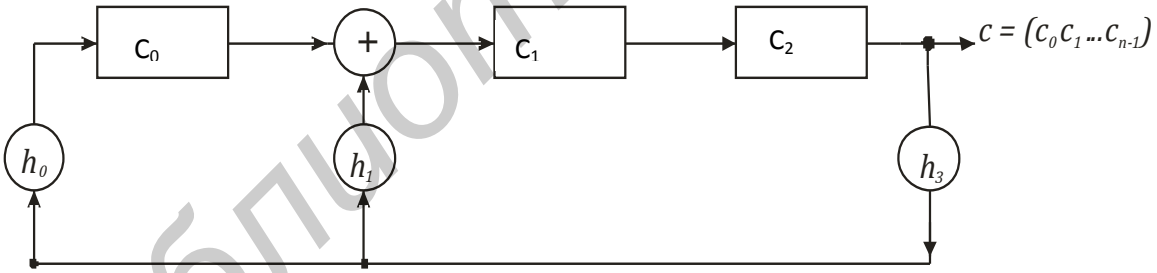

Рис. 2.6

Структура линейных обратных связей описывается проверочным полиномом $h(x) = 1 + x + x^3$. Так же, как и передаточная функция $P(D)$, проверочный полином $h(x)$ однозначно определяет свойства линейной схемы генератора.

Обозначим состояния содержимого РС $(c_0 c_1 c_2 \ldots c_m)$. Начальное состояние РС примем равным $c_0 = 1,\ c_1 = 0,\ c_2 = 0, \ldots, c_m = 0$. Изменение состояний РС после $(n + 1)$ тактов приведено в табл. 2.23.

Таблица 2.23

№ такта	c_0	c_1	c_2	ПСП $c = (c_0 c_1 \dots c_{n-1})$	$\beta = \alpha^i$	$\alpha^0 + \alpha^1 + \dots + \alpha^{m-1}$	Дв. вектор
1	1	0	0	0	α^0	α^0	1 0 0
2	0	1	0	0	α^1	α^1	0 1 0
3	0	0	1	1	α^2	α^2	0 0 1
4	1	1	0	0	α^3	$1 + \alpha$	1 1 0
5	0	1	1	1	α^4	$\alpha + \alpha^2$	0 1 1
6	1	1	1	1	α^5	$1 + \alpha + \alpha^2$	1 1 1
7	1	0	1	1	α^6	$1 + \alpha^2$	1 0 1
8	1	0	0	0	α^7	α^0	1 0 0

Если некоторое состояние (фазу) $(c_0 c_1 c_2 \dots c_m)$ регистра выбрать в качестве начального, то регистр принимает $(2^m - 1)$ возможных двоичных состояний, прежде чем состояния начинают повторяться. С выхода третьей ячейки генератора формируется *M*-последовательность *c* = (0 0 1 0 1 1 1). Последовательность символов является периодической с периодом 7. Это максимально возможный период для трех ячеек памяти. Имеется только $2^3 - 1 = 7$ ненулевых состояний. Выходные последовательности значностью 7 представляют собой кодовые слова кода максимальной длины.

Для сравнения в табл. 2.23 также приведены три формы представления элементов расширенного поля Галуа $GF(2^3)$, порождаемого неприводимым полиномом $h(x) = 1 + x + x^3$. Любой элемент поля представляется *m*-разрядным двоичным числом и может храниться в *m*-разрядном регистре памяти. Как видно, двоичные состояния РС эквивалентны степеням примитивного элемента поля α и формам полиномов. Таким образом, схема, показанная на рис. 2.6, является генератором элементов расширенного поля Галуа.

Устройство (рис. 2.6) умножает содержимое РС на элемент α в поле $GF(2^3)$. Например, если в начальный момент времени регистр содержит 1 0 0 $\Leftrightarrow \alpha^0 = 1$, то в последующие моменты времени он будет содержать $\alpha, \alpha^2, \dots, \alpha^7 = ((1))$, так как α – примитивный элемент поля.

Пример 2.46. Умножить $\alpha\beta = \alpha(c_0 + c_1\alpha + c_2\alpha^2)$, где элемент поля $\beta = (c_0 + c_1\alpha + c_2\alpha^2)$ пусть будет начальным содержимым регистра хранения, $c_i \in \{0,1\}$.

Решение. $\alpha\beta = \alpha(c_0 + c_1\alpha + c_2\alpha^2) = c_0\alpha + c_1\alpha^2 + c_2\alpha^3$. Так как $\alpha^3 \equiv (\alpha + 1)\ mod(\alpha^3 + \alpha + 1)$, то $\alpha\beta = c_0\alpha + c_1\alpha^2 + c_2(\alpha + 1)) = (c_0\alpha + c_1\alpha^2 + c_2\alpha + c_2)) = (c_2 + (c_0 + c_2)\ \alpha + c_1\alpha^2)$. На рис. 2.7 показано состояние регистра памяти после умножения на α.

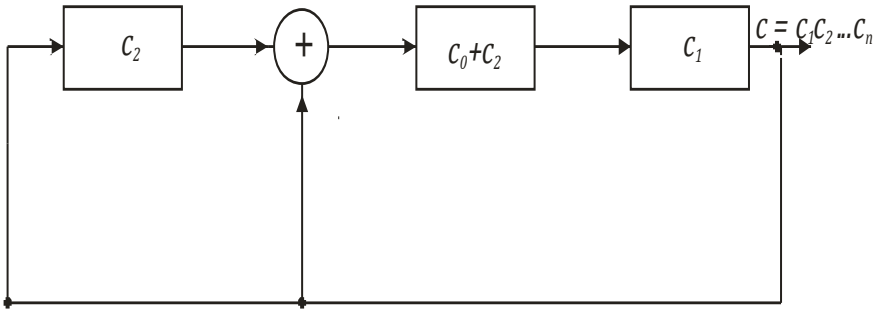

Рис. 2.7

Пример 2.47. Умножение на фиксированный элемент поля.

Задан произвольный элемент поля $GF(2^4)$ поля $\beta = (c_0 + c_1\alpha + c_2\alpha^2 + c_3\alpha^3)$. Его надо умножить на фиксированный элемент поля $(1 + \alpha^2)$.

Решение. $(c_0 + c_1\alpha + c_2\alpha^2 + c_3\alpha^3)(1 + \alpha^2) = c_0 + c_1\alpha + c_2\alpha^2 + c_3\alpha^3 + c_0\alpha^2 + c_1\alpha^3 + c_2\alpha^4 + c_3\alpha^5 = c_0 + c_1\alpha + (c_0 + c_2)\alpha^2 + (c_1 + c_3)\alpha^3 + (1 + \alpha)c_2 + (\alpha + \alpha^2)c_3 = (c_0 + c_2) + (c_1 + c_2 + c_3)\alpha + (c_2 + c_0 + c_3)\alpha^2 + (c_3 + c_1)\alpha^3$.

На рис. 2.8 показана функциональная схема умножения на произвольный элемент поля элемента поля $(1 + \alpha^2)$.

Регистр хранения

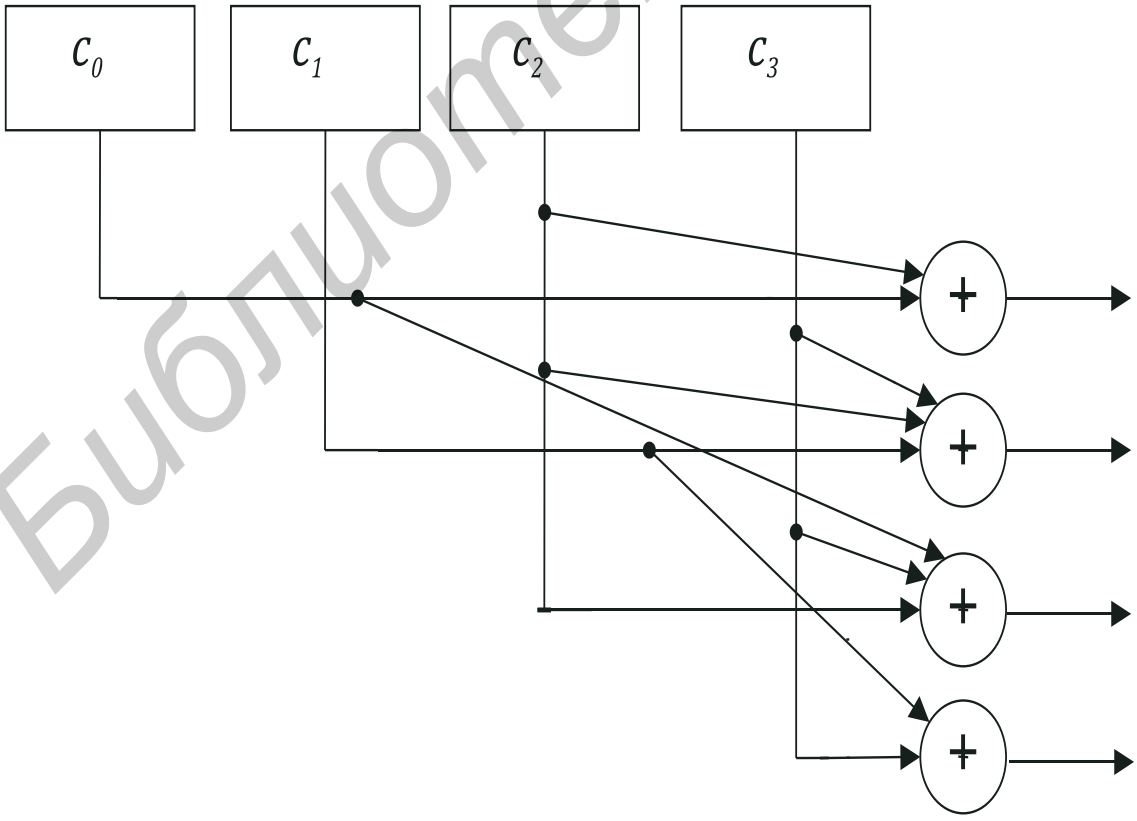

Рис. 2.8

2.4.4. Псевдошумовые последовательности

Определение 2.39. Последовательности, порождаемые неприводимым над полем $GF(2)$ примитивным полиномом

$$h(x) = h_0 + h_1 + h_2x^2 + \cdots + h_mx^m$$

степени m образуют псевдошумовые последовательности.

Псевдошумовая последовательность $c = (c_0\, c_1\, \ldots c_{n-1})$ обладает свойствами, характерными для последовательностей, которые получаются при случайном подбрасывании монеты (2^m-1) раз. Например, число единиц и нолей в c практически равно друг другу, как и должно быть при длительном подбрасывании монеты.

Псевдошумовые последовательности генерируются при помощи регистров сдвига с линейной обратной связью. Состояния регистра сдвига соответствуют элементам расширенного поля Галуа $GF(2^m)$, порожденного примитивным элементом поля α (корнем уравнения $h(x)$). Устройство генерирования псевдошумовой последовательности эквивалентно устройству, выполняющему умножение на α в поле $GF(2^m)$.

Длительность псевдошумовой последовательности

$$T = n\tau_0 = (2^m-1)\tau_0,$$

где τ_0 – длительность элементарного дискрета последовательности c.

Если тактовая частота в сдвигающем регистре равна

$$f = \frac{1}{\tau_0}, \text{ то } \quad T = n\tau_0 = (2^m-1)/f.$$

В табл. 2.24 приведены значения длительности периода псевдошумовой последовательности с тактовой частотой f = 1 МГц для $m \in \{7,8,\ldots,89\}$. Как видно, на практике легко получить бесконечные ключевые последовательности.

В качестве примера использования таких последовательностей можно привести систему связи с непилотируемым межпланетным космическим аппаратом и его управление по программе «Венера 15». С помощью сигналов, кодированными псевдошумовыми последовательностями, обеспечивалось совместное измерение скорости движения и дальности до аппарата. При измерении дальности осуществляется оценка задержки между излученным и принятым сигналами:

$$\tau_\delta = \frac{2Д(t)}{c},$$

где $Д(t)$ – дальность до объекта измерений, c – скорость света.

Таблица 2.24

Регистр длиной m	Длина последовательности	Длительность периода последовательности
7	127	$1{,}27\cdot10^{-4}$ с
8	255	$2{,}55\cdot10^{-4}$ с
9	511	$5{,}11\cdot10^{-4}$ с
10	1023	$1{,}023\cdot10^{-3}$ с
11	2047	$2{,}047\cdot10^{-3}$ с
12	4095	$4{,}095\cdot10^{-3}$ с
13	8191	$8{,}191\cdot10^{-3}$ с
15	32767	$0{,}32767\cdot10^{-1}$с
17	131071	$1{,}31\cdot10^{-1}$ с
19	524287	$5{,}24\cdot10^{-1}$ с
23	8388607	8,388с
27	134217727	13,421 с
31	2147483647	35,8 мин
43	879609302207	101,7 дня
61	2305843009213693951	$7{,}3\cdot10^{4}$ лет
89	618971119642691137449562111 (27 десятичных символов)	$1{,}95\cdot10^{9}$лет

При измерении скорости оценивалось допплеровское приращение частоты

$$F = \frac{2\dot{Д}(t)f}{c},$$

где $\dot{Д}(t)$ – скорость движения объекта; f – несущая частота.

В качестве переносчика информации использовались *M*-последовательности длиной 127, 511 и 32767 двоичных символов. Система должна была обеспечивать связь с космическим аппаратом на расстоянии до 105 млн км и выполнять следующие задачи:

– передавать командную и телеметрическую информацию на борт космического аппарата с Земли;

– передавать технические и научные данные с космического аппарата на Землю;

– обеспечивать автоматическое слежение за частотой Допплера и слежение по угловым координатам.

2.4.5. Кодирование в системе GPS «Navstar»

В глобальной спутниковой навигационной системе «Navstar» используются две периодические псевдошумовые последовательности кода Голда. Пер-

вая последовательность (СА-код) получается за счет сложения по модулю два последовательностей двух 10-разрядных сдвиговых регистров с обратной связью. Вторая кодовая последовательность (Р-код) строится на комбинировании двух *М*-последовательностей, генерируемых 24-разрядными регистрами с соответствующими обратными связями и укороченным циклом. Каждая из *М*-последовательностей задается неприводимым примитивным полиномом степени m.

Структура последовательности *Р*-кода определяется по формуле

$$X = c \oplus D^i v,$$

где c и v – кодовые последовательности, D^i – оператор задержки последовательности v на i тактов ($1 \le i \le 24$).

Длины последовательностей соответственно равны $n_c = 15345000$ и $n_v = 15345047$.

Длительность элементарного дискрета последовательности

$$\tau = \frac{1}{f_{T2}}.$$

Длительность периода последовательности c

$$T_c = n_c\tau = 15345000 \cdot \frac{1}{10{,}23 \cdot 10^6} = 1{,}5 \text{ с.}$$

Период последовательности v имеет несколько большую величину длительности

$$T_v = n_v\tau = 15345047 \cdot \frac{1}{10{,}23 \cdot 10^6} = 1{,}5000045 \text{ с.}$$

При сложении двух двоичных периодических последовательностей с различными длинами получается новая составная последовательность Голда длиной

$$n = n_c n_v = 15345000 \cdot 15345047.$$

Период составной последовательности, выраженный в сутках,

$$T_{cv} = \frac{n}{f_{T2}\,3600 \cdot 24} = 266{,}4 \text{ суток.}$$

7-суточные сегменты *Р*-последовательности приписаны как *Р*-коды различным спутникам системы GPS. Неперекрывающиеся 7-суточные сегменты имеют следующую величину длины кода:

$$n' = 7 \cdot 24 \cdot 3600 \cdot f_{T2} = 7 \cdot 24 \cdot 3600 \cdot 10{,}23 \cdot 10^6 = 6{,}187104 \cdot 10^{12}.$$

Число возможных различных неприводимых полиномов степени m, задающих коды и, следовательно, коды Голда, определяется по формуле

$$L = \frac{\varphi(n)}{m},$$

где $\varphi(n)$ – функция Эйлера. Напомним, если n – простое число, то $\varphi(n) = n - 1$. С ростом m величина L возрастает, как показано в табл. 2.25.

Таблица 2.25

m	3	4	5	6	7	8	9	10	11
L	2	2	6	6	18	16	48	60	176
m	12	13	14	15	16	17	18	19	
L	144	630	756	1800	2048	7710	7776	27594	

Каждый порождающий полином степени m образует *M*-код мощностью

$$M = 2^m - 1.$$

Количество кодовых слов, генерируемых *m*-разрядным РС, достигает величины $M_\Sigma = L(2^m - 1)$.

Например, для m =10, путем изменения структуры обратной связи РС можно сформировать 60 последовательностей максимальной длины разного вида. Каждый порождающий полином степени m образует *M*-код мощностью

$$M = 2^{10} - 1 = 1023.$$

Таким образом, общее количество слов, формируемых одним 10-разрядным РС, $M_\Sigma = L(2^m - 1) = 60 \cdot 1023 = 61380.$ Предполагается, что структура кода Голда может изменяться. Все это говорит о чрезвычайной сложности раскрытия структуры даже С/А-кода, не говоря уже о *P*-коде. На рис. 2.9 показана структурная схема генератора псевдошумовых последовательностей кода Голда (С/А-код Голда).

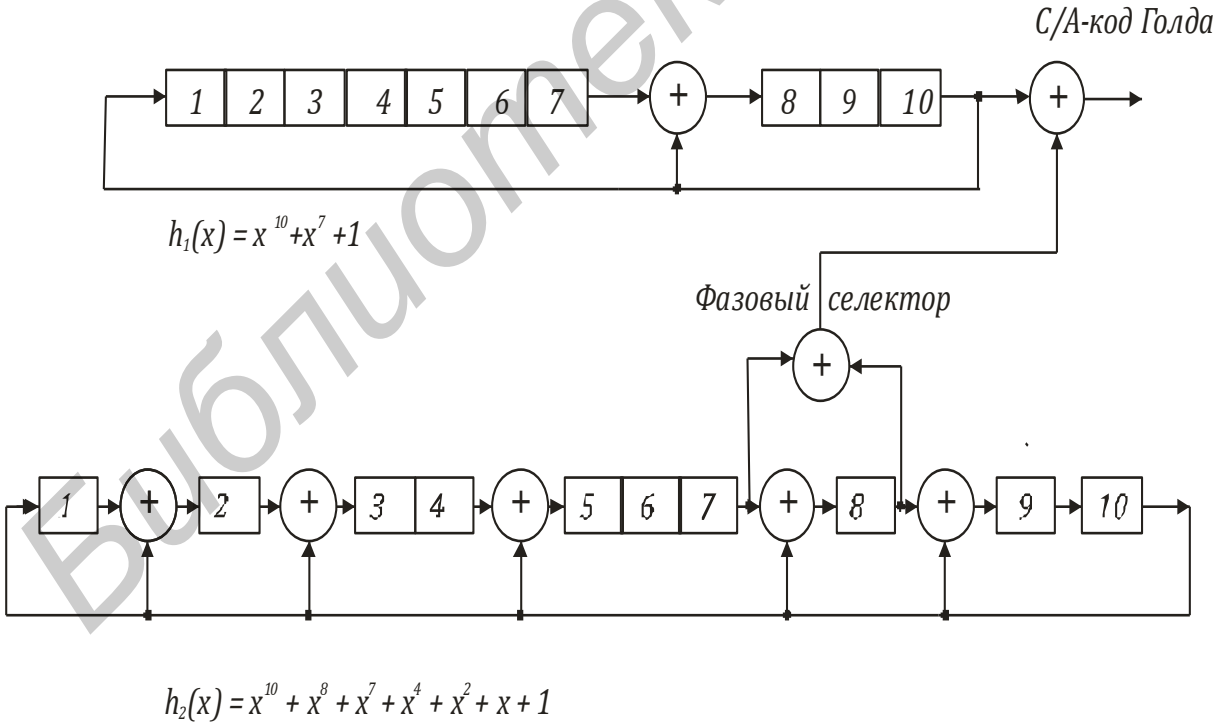

Рис. 2.9

Фазовый селектор позволяет формировать при разных обратных связях для $1 \le i \le 24$ (для всех космических аппаратов) последовательности Голда. Министерство обороны США уполномочило разработчиков GPS предусмотреть и криптозащиту, которая реализована на основе шифра Вернама. В этом случае последовательность *P*-кода суммируется по модулю 2 с секретным ключом в виде *W*-кода. Результатом гаммирования является *Y*-код. Один символ *W*-кода перекрывает 20 символов *P*-кода.

Для взлома ключа перебором пришлось бы протестировать до $2^{\frac{n'}{20}}=2^{\frac{6{,}187104\cdot 10^{12}}{20}} > 2^{10000000000}$ вариантов. По этой причине *Y*-код практически невозможно взломать. Заметим, что для повышения надежности передачи информационного потока применяется кодирование расширенным [32, 26, 4]-кодом Хэмминга.

2.5. Минимальные многочлены

Пусть F – произвольное расширенное поле Галуа $GF(q^m)$порядка q^m. Любое конечное поле содержит q^m элементов для некоторого простого q и некоторого целого $m \ge 1$. Существует только одно такое поле $GF(q^m)$для каждого q и m.

Конечное поле содержит по крайней мере один примитивный элемент α, такой, что все ненулевые элементы поля β могут быть представлены в виде разных степеней α^j.Элементы поля могут быть выражены и через отрицательные степени α, т. к. поле содержит мультипликативный обратный элемент каждого ненулевого элемента.

2.5.1. Теорема Ферма

Каждый элемент β поля $GF(q^m)$ является корнем уравнения

$$x^{q^m} - x = 0 \qquad (2.18)$$

или эквивалентно удовлетворяет множеству

$$\beta^{q^m} = \beta.$$

Это означает, что многочлен (2.18) представляется произведением двучленов вида

$$x^{q^m} - x = \prod_{\beta \in F} (x - \beta).$$

Перепишем уравнение (2.18) как

$$x(x^{q^m-1}) - 1 = 0,$$

для $x \neq 0$ получаем выражение

$$x^{q^m-1} - 1 = 0. \quad (2.19)$$

Многочлену (2.19) также соответствует двучлен

$$x^{q^m-1} - 1 = \prod_{\beta \in F} (x - \beta).$$

Для двоичного случая (простого поля, $q = 2$) каждый элемент β поля $GF(q^m)$ является корнем уравнения

$$x^{2^m-1} - 1 = 0.$$

Во многих приложениях для некоторого целого числа $m \geq 1$ принимают $2^m - 1 = n$, где n определяет значность (длину) кода.

Тогда каждый элемент β поля $GF(q^m)$ является корнем уравнения

$$x^n - 1 = 0. \quad (2.20)$$

Многочлен $x^n - 1$ выражается произведением двучленов вида

$$x^n - 1 = \prod_{\beta \in F} (x - \beta).$$

Если β – корень уравнения (2.20), то

$$\beta^n = \alpha^{jn} = 1,\ 1 \leq j \leq n-1.$$

Известно, что любой многочлен (двучлен) типа (2.18) и (2.20) может быть представлен произведением всех неприводимых многочленов, степени которых являются делителями числа m (от 1 до m включительно).

Согласно теореме Ферма корни уравнений (2.18), (2.20) принадлежат различным неприводимым в поле $GF(q)$ многочленам, на которые разлагается двучлен.

Например, если $q = 2$, $m = 4$. По таблице неприводимых многочленов находим:

$$x^{15} + 1 = (x + 1)(x^2 + x + 1)(x^4 + x + 1)(x^4 + x^3 + 1)(x^4 + x^3 + x^2 + x + 1). \quad (2.21)$$

Заметим, что степени неприводимых многочленов (2.21) – числа 1, 2, 4 – являются делителями числа $m = 4$.

С каждым элементом поля связан неприводимый многочлен, называемый минимальным многочленом. Многие циклические коды в своей основе имеют минимальные многочлены.

Определение 2.40. Минимальным многочленом элемента β над полем $GF(q)$ называется нормированный многочлен $M(x)$ с коэффициентами из $GF(q)$, наименьшей степени, такой, что $M(\beta) = 0$.

Теорема 2.18. Если известен один из корней β неприводимого многочлена степени m, то все другие корни этого многочлена являются степенями β, а именно:

$$\beta, \beta^2, \ldots, \beta^{2^{m-1}}.$$

Например, при $m = 3$ корнями являются элементы поля $\beta, \beta^2, \beta^{2^{3-1}} = \beta^4$.

В этом случае $M^1(x) = M^2(x) = M^4(x)$. Если $M^1(x) = 1 + x + x^3$, то $M^2(x) = M^4 = 1 + x + x^3$. Воспользовавшись данными табл. 2.23, можно проверить вид минимально возможного многочлена $M^2(x)$:

$$M^2(\beta^2) = 1 + \beta^2 + \beta^{2^3} = 1 + \beta^2 + \beta^6 = 1 + \beta^2 + 1 + \beta^2 = 0.$$

Следовательно, $M^2(x) = 1 + x + x^3$.

Пример 2.48. Найти минимальный многочлен $M^3(x)$ элемента $\beta = \alpha^3$, m = 3. Корень α рассматриваем как элемент поля, построенного с использованием неприводимого многочлена $g(x) = x^3+x+1$.

Решение. Многочлен $M^3(x)$может быть представлен в виде

$$M^3(x) = (x-\beta_1)(x-\beta_2)(x-\beta_3),$$

где $\beta_1 = \alpha^3,\ \beta_2 = \alpha^{3^2},\ \beta_3 = \alpha^{3^4}$. Корнями уравнения$M^3(x)$ являются следующие различные элементы: $\beta_1 = \alpha^3,\ \beta_2 = \alpha^6,\ \beta_3 = \alpha^5$. Тогда $M^3(x)$ =$(x-\alpha^3)(x-\alpha^6)(x-$ $-\alpha^5) = (x^2 - x\,\alpha^6 - x\,\alpha^5 - \alpha^9(x - \alpha^5) = (1 + x^2 + x^3)$.

Упражнение 2.11. Показать, что задавая поле $GF(2^4)$ корнем уравнения $\alpha^4 +$ $+ \alpha + 1 = 0$, минимальные многочлены имеют вид:

Элемент	Минимальные многочлены
0	x;
1	$M^0(x) = x + 1$;
$\alpha, \alpha^2, \alpha^4, \alpha^8$	$M^1(x) = M^2(x) = M^4(x) = M^8(x) = 1 + x + x^4$;
$\alpha^3, \alpha^6 \alpha^{12}, \alpha^9$	$M^3(x) = M^6(x) = M^{12}(x) = M^9(x) = 1 + x + x^2 + x^3 + x^4$;
x^4	
$\alpha^5 \alpha^{10}$	$M^5(x) = M^{10}(x) = 1 + x + x^2$;
$\alpha^7, \alpha^{14} \alpha^{13}, \alpha^{11}$	$M^7(x) = M^{14}(x) = M^{13}(x) = M^{11}(x) = 1 + x^3 + x^4$.

2.5.2. Свойства минимальных многочленов

1. Пусть $M(x)$ – минимальный многочлен элемента $\beta \in GF(q^m)$. $M(x)$ – неприводим.

2. Если $c(x)$ – некоторый многочлен с коэффициентами из $GF(q)$, такой что $c(\beta) = 0$, то $M(x) \mid c(x)$, ($M(x)$ делит c(x)).

3. $M(x) \mid x^{q^m} - x$.

4. deg $M(x) \leq m$.

5. Степень минимального многочлена примитивного элемента поля $GF(q^m)$ равна m. Такой многочлен называется примитивным.

6. Минимальные многочлены элементов поля β и β^q равны.

Замечание. Если неприводимый многочлен $p(x)$используется для построения поля $GF(q^m)$ и α является корнем $p(x)$, то многочлен $p(x)$– минимальный.

Пример 2.49. Циклический код Хэмминга задается порождающим многочленом $g(x) = M^1(x)$ идеала.

Из определения 2.16 следует, что любой многочлен $c(x) \in I_n$ в кольце R_n определяется как

$$c(x) = f(x) \cdot g(x) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1} \in I_n. \quad (2.22)$$

В этом случае информация $f(x)$ кодируется посредством использования порождающего многочлена $g(x) = M^1(x)$ идеала. Многочлену $c(x)$ соответствует вектор $c = (c_0 c_1 \ldots c_{n-1})$, где $c_i \in GF(q)$. Вектор $c = (c_0 c_1 \ldots c_{n-1})$ принадлежит циклическому коду Хэмминга $\rightleftarrows$ $c(\alpha) = 0$, где $\alpha \in GF(q^m)$ – корень уравнения, порождающего поле. Из свойства минимальных многочленов и понятия главного идеала (теорема 2.10) следует, что вектор c принадлежит коду тогда и только тогда, когда $g(x)$ делит $c(x)$. Следовательно, $g(x) = M^1(x)$.

2.5.3. Циклотомические классы

Пусть задано поле $GF(2^4)$. Согласно его свойству, 6 минимальных многочленов в этом поле равны минимальным многочленам элементов β и β^2. Например, если $\beta = \alpha^5$, то $M^5(x) = M^{10}(x)$.

Определение 2.41. Элементы поля, минимальные многочлены которых равны, называются сопряженными.

Из определения 2.41 следует, что элементы α^5 и α^{10} будут сопряженными. Из упражнения 2.11 видно, что степени примитивного элемента поля $GF(2^4)$ всех минимальных многочленов образуют непересекающиеся множества сопряженных элементов поля. Эти подмножества множества элементов поля называются циклотомическими классами. Следовательно, совокупность циклотомических классов разделяет множество элементов поля $GF(q^m)$ на непересекающиеся подмножества.

Определение 2.42. Множество целых чисел по модулю $(q^m - 1)$ относительно операции умножения на q разделяется на непересекающиеся подмножества – циклотомические классы.

Циклотомический класс, содержащий целое число s, это подмножество чисел вида

$$\{s, qs, q^2 s, \ldots, q^{m_s - 1} s\}, \tag{2.23}$$

где m_s – наименьшее натуральное число, такое, что

$$q^{m_s} \cdot s \equiv s \bmod q^m - 1. \tag{2.24}$$

Обозначим через C_s – циклотомический класс целого наименьшего числа s в классе. Например, циклотомическими классами по модулю $(2^3 - 1)$ являются:

$C_0 = \{0\};$

$C_1 = \{1, 2, 4\};$

$C_3 = \{3, 6, 5\}.$

В циклотомическом классе C_3 число $s = m_s = 3$ – это наименьшее натуральное число, такое, что выполняются выражения (2.23) и (2.24):

$q^{m_s} \cdot s \equiv 2^3 \cdot 3 \equiv 3 \bmod 2^3 - 1,$

$$q \cdot s = 2 \cdot 3 = 6,$$

$$q^{m_s - 1} \cdot s = 2^{3-1} \cdot 3 = 12 \equiv 5 \bmod 2^3 - 1.$$

Минимальный многочлен элемента α^s равен

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

По определению 2.40 $M^s(x)$ – это нормированный многочлен с коэффициентами из $GF(q)$, наименьшей степени, такой, что $M(\beta = \alpha^s) = 0$. Из теоремы Ферма получаем выражение разложения двучлена вида

$$x^n - 1 = \prod_s M^s(x). \tag{2.25}$$

Формула (2.25) представляет собой разложение многочлена $x^n - 1$ над полем $GF(q)$ на неприводимые множители. Многие конструкции циклических кодов получаются с использованием таблицы циклотомических классов разложения (2.25).

2.5.4. БЧХ-код, исправляющий ошибки кратностью t

Теорема 2.19. БЧХ-код, исправляющий две ошибки, – это циклический код над полем $GF(q)$ с порождающим многочленом $g(x) = M^1(x)M^3(x)$.

Например, для $n = 7$ и $q = 2$ имеем поле $GF(2^3)$. Поле порождается неприводимым над полем $GF(2)$ полиномом $p(x) = 1 + x + x^3$. Корнем уравнения $p(\alpha) = 1 + \alpha + \alpha^3 = 0$ является элемент $\alpha \in GF(2^3)$. Таким образом,

$$M^1(x) = 1 + x + x^3.$$

Воспользовавшись данными примера 2.48 ,

$$M^3(x) = 1 + x^2 + x^3.$$

Искомый порождающий многочлен

$g(x) = M^1(x)M^3(x)=(1 + x + x^3)(1 + x + x^3)=(1 + x + x^2 + x^3 + x^4 + x^5 + x^6)$

Теорема 2.20. Двоичный БЧХ-код, исправляющий t ошибок, имеет порождающий многочлен

$$g(x) = \text{НОК}\{M^1(x), M^3(x), \dots, M^{2t-1}(x)\},$$

где НОК обозначает наименьшее общее кратное минимальных многочленов.

Пример 2.50. БЧХ-код длиной 15, исправляющий трехкратные ошибки, определяется порождающим многочленом

$g(x) = \text{НОК}\{M^1(x), M^3(x), M^5(x)\}$.

Минимальные многочлены элементов поля $GF(2^4)$ выпишем из упражнения 2.11.

$$M^1(x) = x^4 + x + 1,$$

$$M^3(x) = x^4 + x^3 + x^2 + x + 1,$$

$$M^5(x) = x^2 + x + 1.$$

Согласно свойству 1 минимальных многочленов, $M^1(x),\ M^3(x),\ M^5(x)$ – неприводимы. Тогда

$$\text{НОК}\{M^1(x), M^3(x), M^5(x)\} = M^1(x) \cdot M^3(x) \cdot M^5(x);$$

$g(x)=(x^4+x+1)(x^4+x^3+x^2+x+1)(x^2+x+1)=(x^{10}+x^8+x^5+x^4+x^2+x+1)$

Теорема 2.21. Пусть C–циклический $[n, k, d]$-код с порождающим многочленом $g(x)$. Тогда $g(x)$ делит $x^n - 1$ и выполняется сравнение

$$c(x) \equiv 0 \bmod g(x),$$

при этом

$$g(\alpha) = 0,$$

$$g(x) = \prod_{i \in L}(x - \alpha^i), \qquad (2.26)$$

где $L \subseteq \{1, 2, \ldots, n-1\}$, т. е. L и i – это подмножества чисел множества $\{1,2,\ldots,n-1\}$. Множество L образуется объединением циклотомических классов. Кодовое слово $c(x) \in C$ тогда и только тогда, когда

$$c(\alpha^i) = 0 \text{ для всех } i \in L.$$

Определение 2.43. Корни порождающего многочлена называются нулями кода. Нули кода принадлежат множеству $\{\alpha^i : i \in L\}$.

Теорема 2.22. (Граница БЧХ). Пусть C – циклический $[n, k, d]$-код с порождающим многочленом $g(x)$. Если выполняется равенство

$$g(\alpha) = g(\alpha^2) = g(\alpha^3) = \ldots = g(\alpha^{d-1}), \qquad (2.27)$$

тогда кодовое расстояние кода равно d.

Замечание. Теорема 2.22 справедлива только, тогда когда $(d - 1)$ последовательных степеней примитивного элемента α являются нулями кода.

Пример 2.51. Определить параметры циклического БЧХ-кода, исправляющего трехкратные ошибки. Поле $GF(2^4)$ порождается неприводимым над $GF(2)$ многочленом $p(x) = x^4 + x + 1$.

Решение. Величина кратности ошибки $t = 3$ приводит к $d = 7$. По теореме 2.22 получается множество последовательных нулей БЧХ-кода вида

$$\{ \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6 \}.$$

Данное множество является подмножеством множества $L = \{1,2,\ldots,15\}$.

Циклотомическими классами на L, содержащими числа {1, 2, 3, 4, 5, 6}, являются следующие множества:

$$C_1 = \{1, 2, 4, 8\};$$

$$C_3 = \{3, 6, 12, 9\};$$

$$C_5 = \{5, 10\}.$$

Циклу C_1 соответствует минимальный многочлен $M^1(x) = 1 + x + x^4$, C_3 соответствует $M^3(x) = 1 + x + x^2 + x^3 + x^4$, циклотомическому классу C_5 соответствует $M^5(x) = 1 + x + x^2$.

Из формулы (2.26) получаем порождающую матрицу минимального кода

$$g(x) = \prod_{i \in L}(x - \alpha^i) = M^1(x)M^3(x)M^5(x) = 1 + x + x^2 + x^4 + x^5 + x^8 + x^{10}.$$

Число проверочных символов кода определяет deg $g(x)$ = 10 или сумма длин каждого циклотомического класса. Число информационных символов k = 15 – 10 = 5.

Упражнение 2.12. Показать, что порождающий многочлен БЧХ-кода, исправляющего две ошибки длиной n = 15,

$$g(x) = (1 + x^4 + x^6 + x^7 + x^8).$$

2.5.5. Коды Рида – Соломона

Коды Рида – Соломона (РС-коды) относятся к подклассу циклических БЧХ-кодов. Для заданных n и k они имеют наибольшее кодовое расстояние

$$d = n - k + 1 \qquad (2.28)$$

и удовлетворяют границе Синглтона (см. (2.8)).

Определение 2.44. Код Рида – Соломона над полем $GF(q)$ – это БЧХ-код длиной $n = q - 1$.

Длина РС-кода равна числу ненулевых элементов в поле Галуа $GF(q)$. Ранее был определен БЧХ-код в поле $GF(q^m)$ разложения многочлена

$$x^{q^m - 1} - 1 = \prod_{\beta \in F}(x - \beta), \beta \in GF(q^m).$$

РС-код определяется в поле $GF(q)$, т. е. в поле разложения многочлена

$$x^{q-1} - 1 = \prod_{\beta \in F}(x - \beta), \beta \in GF(q).$$

Замечание. В качестве q для построения РС-кода часто выбирают $q = p^m$, где p – простое число, $m \geq 1$.

Согласно теореме 2.10, степень порождающего многочлена циклического кода deg $g(x)=n–k=r$ учетом границы Синглтона (r=2t), для исправления ошибок кратностью t порождающий многочлен будет иметь степень

$$\deg g(x) = r = 2t.$$

Если $M(x) = (x - \beta)$ – минимальный многочлен элемента β поля $GF(q)$, а $\beta_i = \alpha^i$, то порождающий многочлен РС-кода равен

$$g(x) = \prod_{i=1}^{2t} M^{\beta_i}(x) = \prod_{i=1}^{2t}(x - \beta_i) = \prod_{i=1}^{2t}(x - \alpha^i) = (x - \alpha)(x - \alpha)..(x - \alpha^{2t}).$$

Так как $2t = d - 1$, можно определить

$$g(x) = \prod_{i=1}^{d-1}(x - \alpha^i) = \prod_{i=1}^{d-1}(x - \alpha)(x - \alpha^2)\ldots(x - \alpha^{d-1}). \qquad (2.29)$$

Утверждение 2.3. Размерность РС-кода равна $k = (q - 1 - 2t)$, для $k = (q - 1 - 2t)$ существует $[q - 1, q - 1 - 2t, n - k + 1]$-код Рида – Соломона над полем $GF(q)$.

Пример 2.52. Записать порождающий многочлен РС-кода над полем $GF(5)$ длиной $n = q - 1 = 4$ и кодовым расстоянием $d = 3$. Определить параметры кода.

Решение. В качестве примитивного элемента $GF(5)$ возьмём элемент α = 2 (пример 2.37). Порождающий многочлен (2.29)

$g(x) = (x - \alpha)(x - \alpha^2) = (x - 2)(x - 4) = (x + 3)(x + 1) = (x^2 + x + 3x + 3) = x^2 + 4x + 3.$

Находим параметры $[n, k, d]$ РС-кода. Из формулы (2.28)

$$k = n - d + 1 = 2.$$

Пусть информационный полином $f(x) = 1 + x$. Кодовое слово РС-кода $c(x)=f(x)g(x)=(1+x)(x^2+4x+3)=x^2+4x+3+x^3+4x^2+3x=x^3+5x^2+7x+3=x^3+2x+3$.

Полиному $c(x)$ соответствует вектор над $GF(5)$ – (3 2 0 1).

Пример 2.53. Найти порождающий полином РС-кода над $GF(4) = \{0, 1, \alpha, \beta = \alpha^2\}$ с кодовым расстоянием $d = 2$. Примитивный элемент поля $\alpha \in GF(4)$ – корень уравнения $(1 + \alpha + \alpha^2) = 0$. Необходимо записать кодовые слова кода.

Решение. Для РС-кодов над $GF(4)$ длиной $n = q - 1 = 3$ с расстоянием $d = 2$ из формулы (2.29) следует выражение

$$g(x) = (x - \alpha).$$

Число информационных символов $k = 2$ вычисляется из выражения (2.28).

Получаем [3, 2, 2] РС-код. Чтобы представить слова кода, необходимо иметь q-ичные значения информационных векторов.

q-ичная запись информационных векторов и соответствующих им полиномов приведена в табл. 2.26 и 2.27.

Таблица 2.26

00	10	α0	β0
01	11	α1	β1
0α	1α	αα	βα
0β	1β	αβ	ββ

Таблица 2.27

0	1	α	β
x	1+ x	α + x	β + x
α x	1+ α x	α +α x	β + α x
β x	1+ β x	α +β x	β + β x

Множество кодовых слов $\{c(x)\}$ РС-кода над полем $GF(4)$ определяется на основе операций сложения и умножения, задаваемых таблицами Кэли (табл. 2.28 и 2.29).

Таблица 2.28

+	0	1	α	β
0	0	1	α	β
1	1	0	β	α
α	α	β	0	1
β	β	α	1	0

Таблица 2.29

×	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α	β	1
β	0	β	1	α

Ненулевые кодовые слова запишем в двух формах: в виде многочленов, коэффициентами которых являются элементы поля $GF(q)$ и векторов.

$$c(x) = f(x)g(x),$$
$$c(x) = \gamma_0 + \gamma_1 x^1 + \gamma_2 x^2,$$
$$c = (\gamma_0\ \gamma_1\ \gamma_2),$$

где $f(x)$ – информационный полином, $\gamma_j \in GF(4)$.

$$c_1(x) = f_1(x)q(x) = 1(x - \alpha) = (x - \alpha); \qquad c_1 = \alpha\ 1\ 0.$$

$$c_2(x) = f_2(x)q(x) = \alpha(x - \alpha) = (\alpha x - \alpha^2) = (\alpha x - \beta); \qquad c_2 = \beta\ \alpha\ 0.$$

$c_3(x) = f_3(x)q(x) = \beta(x-\alpha) = (\beta x - \beta\alpha) = (\beta x - 1);$ $c_3 = 1\ \beta\ 0.$

$c_4(x) = f_4(x)q(x) = x(x-\alpha) = (x^2 - \alpha x);$ $c_4 = 0\ \alpha\ 1.$

$c_5(x) = f_5(x)q(x) = \alpha x(x-\alpha) = (\alpha x^2 - \alpha^2 x);$ $c_5 = 0\ \beta\ \alpha.$

……

$c_{10}(x) = f_{10}(x)q(x) = (\alpha + x)(x-\alpha) = (\alpha x - \alpha^2 + x^2 - \alpha x) = (\beta + x^2);$

$c_{10} = \beta\ \ 0\ 1.$

……

$c_{15}(x) = f_{15}(x)q(x) = (\beta + \beta x)(x-\alpha) = (\beta x - \beta\alpha + \beta x^2 - \beta\alpha x) =$

$(1 + (\beta - \beta\alpha)x + \beta x^2) = (1 + (\beta - 1)x\ + \beta x^2) = (1 + \alpha x\ + \beta x^2;$

$c_{15} = 1\ \alpha\ \beta.$

3. КОНТРОЛЬНЫЕ ВОПРОСЫ И ЗАДАЧИ

3.1. Пусть $A = \{1,2,3,4,5,6,7\},\ B = \{4,5,6,7,8,9,10\}, C = \{2,4,6,8,10\}.$ Определите следующие множества:

а) $A \cup C;$ *б)* $A \cap B;$ *в)* $A \cap (B \cup C);$ *г)* $(A \cap B) \cup C.$

3.2. Пусть $A = \{1,2,3,4,5,6,7\},\ B = \{4,5,6,7,8,9,10\}, C = \{2,4,6,8,10\},$ Определите следующие множества:

а) $A \cup C;$ *б)* $A \cap B;$ в) $A \Delta B;$ г) $A–B.$

3.3. Пусть $A = \{1,2\}, B = \{x,y\}.$ Выписать все элементы декартова произведения $A \times A$ и $B \times A.$

3.4. Пусть $A = \{1,2,3\}, B = \{x,y\}.$ Выписать все элементы декартова произведения $A \times B$ и $B \times A.$

3.5. Пусть A = {1, 2, 3}. Установите, является ли каждое из приведенных отношений на A отношением эквивалентности. Для отношения эквивалентности постройте классы эквивалентности:

а) R_1 = {(2, 2), (1, 1), (3, 3)};

б) R_2 = {(1, 1), (2, 2), (3, 3), (1, 2), (2, 1), (3, 2), (2, 1)}.

3.6. Пусть A = {1, 2, 3}. Установите, является ли каждое из приведенных отношений на A отношением эквивалентности. Для отношения эквивалентности постройте классы эквивалентности:

а) R_1 = {(2, 2), (1, 1)};

б) R_2 = {(1, 1), (2, 2), (3, 3), (1, 2), (2, 1), (3, 1), (1, 3)}.

3.7. Показать, что группа G = < {0,1, 2, 3, 4, 5}; +; 0> содержит подгруппы порядков: 1, 2, 3 и 6.

3.8. Задана мультипликативная абелева группа G = <{1, 2, 3, 4};•;1>.

Построить возможные циклические группы. Определить число примитивных элементов.

3.9. Задано множество целых чисел G = {1, 2, 3, 4, 5, 6, 7}. Найти функцию Эйлера $\varphi(8)$.

3.10. Множество $\{0, 1, 2\}$ принадлежит подмножеству целых чисел Z. Группа G задается таблицей Кэли

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Показать, является ли G подгруппой группы $< Z; + >$.

3.11. Показать, что множество комплексных чисел $\{(1, W, W^2)\}$, где $W = \exp(-j\frac{2\pi}{3})$, образует мультипликативную группу.

3.12. Показать, что алгебраическая система <{0, 1, 2, …,13}; +; ·; 0; 1> – это кольцо целых чисел по модулю $M = 14$.

3.13. Задана G = < {0, 1, 2, 3}; +; 0> – группа порядка 4, задаваемая таблицей Кэли

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Определить подгруппу H группы G.

3.14. Докажите, что числа, кратные 3, образуют подгруппу целых чисел с операцией сложения. Постройте смежные классы этой подгруппы.

3.15. Постройте поле Галуа $GF(4)$, если задано множество элементов G = {0, 1, a, b}.

3.16. Постройте поле Галуа $GF(4)$ с помощью арифметических таблиц.

3.17. Постройте поле Галуа $GF(4)$ для числового множества G = {0, 1, 2, 3}.

3.18 Постройте таблицы Кэли операций деления и вычитания в поле Галуа $GF(5)$.

3.19. Вычислите в поле Галуа $GF(5)$: $((\sqrt{3} \cdot [(2+4) \cdot 3^4]))$.

3.20. Решите в поле Галуа $GF(4)$ систему уравнений

$$2x + y = 3,$$
$$x + 2y = 3.$$

3.21. Поясните принцип построения таблицы смежных классов.

3.22. Определите кратность исправляемых или обнаруживаемых ошибок следующими кодами: [7, 3, 4], [6,1, 6], [7, 6, 2], [5, 2, 3].

3.23. Определите расстояние Хэмминга пар векторов: (100101, 011100), (101110, 111001), (010111, 110010).

3.24. Определите кодовое расстояние кода: 100101, 010111, 001011, 110010, 101110, 011100, 111001.

3.25. Покажите, что многочлен x^7+1 равен произведению неприводимых над полем $GF(2)$ многочленов: $x^7+1=(x+1)(x^3+x^2+1)(x^3+x+1)$.

3.26. Поле образовано полиномами над полем $GF(2)$ по модулю неприводимого полинома $p(x)=1+x+x^3$. Вычислить: $(101)^{-1}$.

3.27. Поле образовано полиномами над полем $GF(2)$ по модулю неприводимого полинома $p(x)=1+x+x^3$. Вычислить: $\sqrt{1+\alpha^2}$, где α – примитивный элемент поля.

3.28. Найти обратный элемент поля Галуа элементу α^5, если элементы поля порождаются полиномом $p(x)=(1+x^3+x^4)$, неприводимым над полем $GF(2)$.

3.29. Поле образовано полиномами над полем $GF(2)$ по модулю неприводимого полинома $p(x)=1+x+x^3$. Вычислите полином, обратный полиному $B=1+\alpha^2$.

3.30. Постройте все неприводимые полиномы третьей степени над полем $GF(2)$.

3.31. Привести четыре формы представления элементов поля Галуа $GF(2^4)$. Поле образовано многочленами над полем $GF(2)$ по модулю неприводимого многочлена $p(x)=(1+x^3+x^4)$.

3.32. Привести четыре формы представления элементов поля $GF(2^4)$. Поле образовано неприводимым над полем $GF(2)$ полиномом $p(x)=1+x+x^4$.

3.33. Запишите передаточную функцию $P(D)$ многотактной переключательной схемы, изображенной на рис. 3.1.

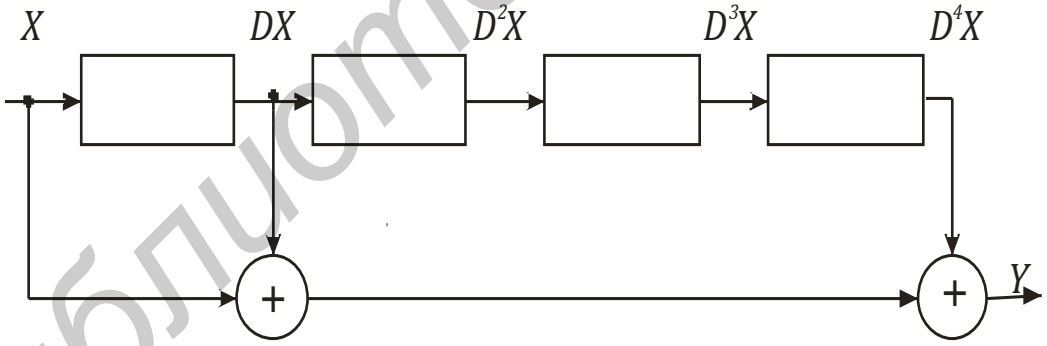

Рис. 3.1

3.34. Постройте М-последовательность длиной 15.

3.35. Изобразите структурную схему генератора М-последовательности длиной 15. Показать смену двоичных состояний ячеек регистра сдвига .

3.36. Постройте проверочную матрицу двоичного [15, 7, 5] БЧХ-кода, исправляющего две ошибки.

3.37. Запишите все кодовые слова РС-кода примера 2.53.

3.38. Запишите порождающий многочлен РС-кода [7, 3, 5] над $GF(8)$. В качестве примитивного элемента поля выбрать α – корень уравнения $1+\alpha+\alpha^3=0$.

3.39. Запишите порождающий многочлен РС-кода над $GF(16)$ длиной 15 с кодовым расстоянием $d = 5$. Поле порождается неприводимым полиномом $p(x) = x^4 + x + 1$. Использовать представление элементов поля $GF(16)$ в виде многочленов и степеней примитивного элемента поля α.

3.40. Запишите все кодовые слова РС-кода над полем $GF(4)$ и расстоянием $d = 2$, α – примитивный элемент $GF(4)$, а $(x^2 + x + 1)$– его минимальный многочлен. Слова представmnt в форме многочленов и векторов.

3.41. Найдите циклотомические классы целых чисел по модулю $(q^m - 1)$ над $GF(q)$:

а) $2^5 - 1$;

б) $2^6 - 1$.

3.42. Определить параметры БЧХ-кода, исправляющего трехкратные ошибки. Поле порождается неприводимым над $GF(2)$ многочленом $p(x) = x^4 + x^3 + 1$.

ЛИТЕРАТУРА

1. Теория прикладного кодирования : учеб. пособие. В 2 ч. / В. К. Конопелько [и др.]; под ред. проф. В. К. Конопелько. – Минск : БГУИР, 2004.

2. Лосев, В. В. Микропроцессорные устройства обработки информации. Алгоритмы цифровой обработки : учеб. пособие / В. В. Лосев. – Минск : Выш. шк., 1990.

3. Дискретная математика и комбинаторика / Дж. А. Андерсон; пер. с англ. – М. : Вильямс, 2004.

4. Лидл, Р. Конечные поля . В 2 т. / Р. Лидл, Г. Нидеррайдер. – М. : Мир, 1988.

5. Вернер, М. Основы кодирования : учебник для вузов / М. Вернер. – М. : Техносфера, 2006.

6. Морелос-Сарагоса, Р. Искусство помехоустойчивого кодирования. Методы алгоритмы, применение : учеб. пособие / Р. Морелос-Сарагоса. – М. : Техносфера, 2005.

7. Мак-Вильямс, Ф. Дж. Теория кодов, исправляющих ошибки / Ф. Дж. Мак-Вильямс, Н. Дж. Слоэн. – М. : Связь, 1979.

8. Кларк, Дж. Кодирование с исправлением ошибок в системах цифровой связи / Дж. Кларк, Дж. Кейн; пер. с англ. – М. : Радио и связь, 1987.

9. Блейхут, Р. Теория и практика кодов, контролирующих ошибки / Р. Блейхут; пер. с англ. М. : Мир, 1986.

10. Муттер, В. М. Основы помехоустойчивой телепередачи информации / В. М. Муттер. – Л. : Энергоатомиздат. Ленингр. отд-ние, 1990.

11. Габидулин, Э. М. Кодирование в радиоэлектронике / Э. М. Габидулин, В. Б. Афанасьев. – М. : Радио и связь, 1986.

12. Теория кодирования / Т. Касами [и др.]; пер. с яп. – М. : Мир, 1978.

13. Макклеллан, Дж. К. Применение теории чисел в цифровой обработке сигналов / Дж. К. Макклеллан, Ч. М. Рейдер. – М. : Радио и связь, 1983.

14. Хаггарти, Р. Дискретная математика для программистов / Р. Хаггарти. – М. : Техносфера, 2005.

15. Питерсон, У. Коды, исправляющие ошибки / У. Питерсон, Э. Уэлдон; пер. с англ. – М. : Мир, 1976.

Учебное издание

Митюхин Анатолий Иванович
Пачинин Виталий Иванович

ЭЛЕМЕНТЫ АЛГЕБРАИЧЕСКИХ СТРУКТУР ТЕОРИИ КОДИРОВАНИЯ

Методическое пособие по курсам
«Теория кодирования»
и «Специальные математические методы и функции»
для студентов специальностей «Промышленная электроника»,
«Программное обеспечение информационных технологий», «Радиосвязь,
радиовещание и телевидение» вечерней и заочной форм обучения

Редактор Т. Н. Крюкова
Корректор Е. Н. Батурчик
Компьютерная верстка Ю. Ч. Клочкевич

Подписано в печать 19.12.2011. Формат 60x84 1/16. Бумага офсетная.
Гарнитура «Таймс». Отпечатано на ризографе. Усл. печ. л. 3,84.
Уч.-изд. л. 3,2. Тираж 50 экз. Заказ 38.

Издатель и полиграфическое исполнение: учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники»
ЛИ №02330/0494371 от 16.03.2009. ЛП №02330/0494175 от 03.04.2009.
220013, Минск, П. Бровки, 6