Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Локтионова Оксана Геннадьевна
Должность: проректор по учебной работе
Дата подписания: 18.12.2023 14:07:18
Уникальный программный ключ:
0b817ca911e6668abb13a5d426d39e5f1c11eabbf73e943df4a4851fda56d089

МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра вычислительной техники

УТВЕРЖДАЮ
Проректор по учебной работе
_____ О.Г.Локтионова
«5» 10 2023 г.

ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ И СЖАТИЯ ИНФОРМАЦИИ

Методические указания по выполнению самостоятельной работы
для студентов направления подготовки 09.04.01

Курск 2023

УДК 681.5

Составитель С.И. Егоров

Рецензент

Доктор технический наук, профессор кафедры ВТ Юго-Западного государственного университета *В.С.Титов*

Технические средства защиты и сжатия информации: методические указания по выполнению самостоятельной работы /Юго-Зап. гос. ун-т; сост.: С.И. Егоров. Курск, 2023. 18 с.: ил., прилож. 1. - Библиогр.: с. 10 .

Приводятся краткие сведения о темах для самостоятельного изучения по дисциплине «Технические средства защиты и сжатия информации», необходимые для успешного освоения дисциплины. Указывается порядок выполнения самостоятельной работы всех предусмотренных учебным планом видов, приводятся рекомендации по оформлению результатов работы.

Предназначены для студентов направления подготовки 09.04.01 дневной и заочной форм обучения.

Текст печатается в авторской редакции

Подписано в печать . Формат 60×84 1/16.
Усл. печ. л. ___. Уч.-изд. л. ___. Тираж 20 экз. Заказ . Бесплатно.

Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

Содержание

1 Введение

Самостоятельная работа - это индивидуальная или коллективная учебная деятельность, осуществляемая без непосредственного руководства преподавателя, но по его заданиям и под его контролем.

Самостоятельная работа студентов включает:

- изучение лекционного материала по конспекту с использованием рекомендованной литературы;
- отработку изучаемого материала по печатным и электронным источникам, конспектам лекций;
- подготовку к выполнению лабораторных работ;
- выполнение отчетов по лабораторным работам и подготовку к их защите;
- подготовку к выполнению практических заданий;
- выполнение курсового проекта;
- индивидуальные задания (решение задач, подготовка сообщений, докладов, исследовательские работы и т.п.);
- подготовку кратких сообщений, докладов, рефератов, самостоятельное составление задач по изучаемой теме (по указанию преподавателя);
- работу над выполнением наглядных пособий (схем, таблиц и т.п.).

Назначение самостоятельной работы студентов.

- *Овладение знаниями*, что достигается: чтением текста (учебника, первоисточника, дополнительной литературы), составлением плана текста, графическим структурированием текста, конспектированием текста, выписками из текста, работой со словарями и справочниками, ознакомлением с нормативными документами, выполнением учебно-исследовательской работы, поиском информации в сети Интернет и т.п.;

- *Закрепление знаний,* что достигается: работой с конспектом лекций, обработкой текста, повторной работой над учебным материалом, составлением таблиц для систематизации учебного материала, ответами на контрольные вопросы, заполнением рабочей тетради, аналитической обработкой текста (аннотирование, рецензирование, реферирование, конспект-анализ и др), подготовкой мультимедиа сообщений/докладов к выступлению на семинаре (конференции), подготовкой реферата, составлением библиографии и т.п.;

- *Формирование навыков и умений*, что достигается: решением задач и упражнений по образцу, решением вариативных задач, выполнением чертежей, схем, выполнением расчетов (графических работ), решением ситуационных (профессиональных) задач, подготовкой к деловым играм, проектированием и моделированием разных видов и компонентов профессиональной деятельности, опытно экспериментальной работой и т.п.

Самостоятельная работа может осуществляться индивидуально или группами студентов в зависимости от цели, объема, конкретной тематики самостоятельной работы, уровня сложности, уровня умений студентов.

Контроль результатов внеаудиторной самостоятельной работы студентов может осуществляться в пределах времени, отведенного на обязательные учебные занятия по дисциплине и внеаудиторную самостоятельную работу студентов по дисциплине, может проходить в письменной, устной или смешанной форме.

Текущий контроль качества выполнения самостоятельной работы может осуществляться с помощью:

- контрольного опроса;
- собеседования;
- автоматизированного программированного контроля (машинного контроля, тестирования с применением ЭВМ).

Контроль выполнения курсового проекта и индивидуальных заданий осуществляется поэтапно в соответствии с разработанным преподавателем графиком.

2 Учебно-методическое обеспечение для самостоятельной работы

Студенты могут при самостоятельном изучении отдельных тем и вопросов дисциплины пользоваться учебно-наглядными пособиями, учебным оборудованием в лабораториях и методическими разработками кафедры вычислительной техники в рабочее время, установленное Правилами внутреннего распорядка работников.

Учебно-методическое обеспечение для самостоятельной работы обучающихся по данной дисциплине организуется:

библиотекой университета:

- библиотечный фонд укомплектован учебной, методической, периодической, справочной литературой в соответствии с УП и данной РПД;
- имеется доступ к основным информационным образовательным ресурсам, информационной базе данных, в том числе библиографической,
- имеется возможность выхода в Интернет.

кафедрой:

- путем обеспечения доступности всего необходимого учебно-методического и справочного материала;
- путем предоставления сведений о наличии учебно-методической литературы, современных программных средств.
- путем разработки:
  - заданий для самостоятельной работы;
  - вопросов к экзаменам и зачетам;
  - методических указаний к выполнению лабораторных и практических работ и т.д.

типографией университета:
– помощь авторам в подготовке и издании научной, учебной и методической литературы;
– удовлетворение потребности в тиражировании научной, учебной и методической литературы

3 Запланированные виды самостоятельной работы по дисциплине

В соответствии с учебным планом, на самостоятельную работу студентов в рамках дисциплины «Технические средства защиты и сжатия информации» отводится 108 часов. Распределение часов самостоятельной работы по темам (видам деятельности) приведено в таблице 1 в соответствии с рабочей программой дисциплины (РПД).

Таблица 1 – Самостоятельная работа студентов

№	Наименование раздела дисциплины	Срок выполнения	Время, затрачива-емое на выполне-ние СРС, час
1	Конечные поля. Аппаратная реализация вычислений в расширенном конечном поле.	1-3 неделя	16
2	Разработка кодека кода Хемминга (КП)	4-6 неделя	24
3	Алгебраические методы исправления ошибок	7-9 неделя	20
4	Разработка кодека кода Рида-Соломона (КП)	10-12 неделя	20
5	Алгоритмы сжатия информации	13-17 неделя	16
6	Подготовка к лабораторным работам	в течение семестра	12
	Итого		108
	Подготовка к экзамену		36

Текущий контроль знаний, основанный на выяснении качества самостоятельной работы студентов при работе с конспектом лекций и учебной литературой, производится в соответствии с Рабочей программой дисциплины (Таблица 4.1.2) и предусматривает контрольный опрос (КО) и собеседования (С).

Рекомендации по выполнению лабораторных работ приведены в соответствующих методических указаниях к лабораторным работам [1], [2], [3]. Методические указания содержат полные требования к видам и объему самостоятельной работы при подготовке, выполнении, оформлении отчетов и защите лабораторных работ.

Рекомендации по выполнению курсового проекта приведены в соответствующих методических указаниях к курсовому проекту [4]. Методические указания содержат полные требования к видам и объему

самостоятельной работы при подготовке, выполнении, оформлении отчета и защите курсового проекта.

Материалы и задания для изучения конечных полей и аппаратной реализации вычислений в расширенном конечном поле приведены в Приложении.

4 Рекомендации по выполнению самостоятельной работы

Изучение теоретических основ дисциплин

Изучение теоретической части дисциплин способствует углублению и закреплению знаний, полученных на аудиторных занятиях, а также развивает у студентов творческие навыки, инициативы и умение организовать свое время.

Самостоятельная работа при изучении дисциплины включает:

- работу над конспектом лекций;
- изучение рекомендованной литературы;
- поиск и ознакомление с информацией в сети Интернет;
- подготовку к различным формам контроля (контрольный опрос, собеседование, тесты);
- подготовку и написание рефератов;
- подготовку ответов на вопросы по различным темам дисциплины, в том числе заданным преподавателям по результатам контроля знаний.

Материал, законспектированный в течение лекций, необходимо регулярно прорабатывать и дополнять сведениями из других источников литературы, представленных не только в программе дисциплины, но и в периодических изданиях.

При освоении дисциплины сначала необходимо по каждой теме изучить рекомендованную литературу и составить краткий конспект основных положений, терминов, сведений, требующих запоминания и являющихся основополагающими в этой теме для освоения последующих тем курса. Для расширения знания по дисциплине рекомендуется использовать Интернет-ресурсы; проводить поиски в различных системах и использовать материалы сайтов, рекомендованных преподавателем.

По требованию преподавателя конспект лекций предоставляется ему для проверки. Замеченные недостатки и внесенные замечания и предложения следует отработать в приемлемые сроки.

Лабораторные работы

При подготовке и защите лабораторных работ необходимо обращать особое внимание на полноту и грамотность выполнения отчета по лабораторной работе, наличие в них кратких обоснований принимаемых решений и выводов по результатам работы. При несоответствии отчета этим требованиям преподаватель может возвращать его на доработку. При опросе студентов основное внимание обращается на усвоение ими основных

теоретических положений, на которых базируется данная работа, и понимания того, как эти положения применяются на практике. Для освоения дисциплины в полном объеме студенту необходимо посещать все аудиторные занятия и самостоятельно прорабатывать полученный материал.

Контроль результатов самостоятельной работы студентов осуществляется перед выполнением лабораторной работы, в процессе ее защиты, а так же на зачете и экзамене.

При самостоятельном изучении дисциплины и подготовке к аудиторным занятиям и выполнении домашних заданий студенты должны использовать рекомендованную учебную литературу и учебно-методические указания. Источники информации доступны на сайте кафедры.

Самостоятельная работа осуществляется при подготовке к работе в соответствии с заданными темами, подготовке ответов к вопросам для самоконтроля и контрольным вопросам.

Каждая работа включает пункты «Подготовка к работе» и «Вопросы для самопроверки».

В таблице 2 приводятся вопросы для самопроверки к лабораторным работам.

Таблица 2 – Вопросы для самопроверки

№	Наименование лабораторной работы	Контрольные вопросы
1	Исследование коррекции ошибок в телекоммуникационных каналах с использованием помехоустойчивых кодов Рида-Соломона	1. Как задаются коды Рида-Соломона? 2. Охарактеризуйте исправляющую способность РС-кодов. 3. Дайте математическое обоснование процедуры декодирования РС-кодов. 4. Каким образом вычисляются синдромы РС-кода? 5. Как определяется коэффициенты полинома локаторов ошибок? 6. Как находятся корни степенных уравнений в конечных полях? 7. Как вычисляются значения ошибок? 8. Что такое FER? 9. В чем заключается преимущество мягкого декодирования перед жестким? 10. Как зависит эффективность и сложность мягкого декодирования от величины радиуса декодирования? 11. Изложите основную идею процедуры списочного декодирования. 12. Как используются мягкие решения в процедуре мягкого декодирования кодов Рида-Соломона?
2	Коррекция ошибок с использованием сверточных кодов и	1 Определение и характеристики кода Рида-Соломона. 2 Процедура кодирования кода Рида-Соломона. 3. Процедура декодирования кода Рида-Соломона.

№	Наименование лабораторной работы	Контрольные вопросы
	кодов Рида-Соломона	4. Конструктор кодера кода Рида-Соломона *comm.RSEncoder*. 5 Конструктор декодера кода Рида-Соломона *comm.RSDecoder*. 6 Функции кодера/декодера кодов Рида-Соломона *step*. 7. Понятие сверточного кодирования. 8 Функция кодера сверточного кода *convenc*. 9 Функция декодера сверточного кода *vitdec*.
3	Сжатие изображений по стандарту JPEG	1. Назовите основные требования приложений к алгоритмам компрессии. 2. Почему высокая скорость компрессии, высокое качество изображений и высокая степень компрессии взаимно противоречивы? Покажите противоречивость каждой пары условий. 3. Назовите основные характеристики алгоритмов сжатия изображений. 4. Расскажите о критериях оценки качества сжатия изображений. 5. Дайте общую характеристику алгоритму JPEG. 6. Расскажите об этапах сжатия по алгоритму JPEG. 7. Расскажите о дискретно-косинусном преобразовании. 8. Каким образом осуществляется переход от двумерного ДКП к одномерному? 9. Как работает алгоритм Хоу? 10. Расскажите об использовании распределенной арифметики для реализации ДКП.

Отчет по лабораторной работе выполняется индивидуально или один на бригаду по решению преподавателя.

Отчет должен содержать все предусмотренные методическими указаниями разделы, включая вопросы для самопроверки. Рекомендуется включать в отчет ответы на эти вопросы в *кратком* виде. Поскольку эти ответы являются продуктом самостоятельной работы, совпадение текстов ответов в отчетах разных студентов приводит преподавателя к необходимости формировать дополнительные вопросы по соответствующей теме.

Курсовой проект

Курсовой проект является важным этапом для освоения дисциплины и подготовки к выполнению выпускной квалификационной работы.

По дисциплине "Технические средства защиты и сжатия информации" студенты выполняют курсовой проект по теме «Разработка кодеков кодов Хемминга и Рида-Соломона».

Целью курсового проектирования является:

– формирование навыков проектирование кодеков наиболее популярных блочных помехоустойчивых кодов: а именно кодов Хемминга и Рида-Соломона;

– обобщение, закрепление и углубление знаний по дисциплине "Технические средства защиты и сжатия информации";

– формирование навыков разработки и оформления текстовой и графической технической документации.

Содержанием курсового проекта является проектирование кодеков кодов Хемминга и Рида-Соломона. При этом необходимо построить проверочную и порождающую матрицы кода Хемминга, разработать кодер и декодер кода Хемминга, проверить на примере работоспособность кодека Хемминга. Для кода Рида-Соломона необходимо получить порождающий многочлен кода, разработать кодер и декодер, декодировать слово с ошибками.

Все требования к выполнению курсового проекта излагаются в методических указаниях к рассматриваемому проекту [4], поэтому тщательное их изучение и соблюдение является основой для получения своевременного и качественного результата.

Особое значение при выполнении данного вида работы следует обратить на оформление отчета. Основные требования к оформлению изложены в [5].

5 Библиографический список

1. Коррекция ошибок с использованием сверточных кодов и кодов Рида-Соломона [Электронный ресурс]: методические указания к лабораторной работе по дисциплине "Технические средства защиты и сжатия информации" для студентов, обучающихся по направлению 09.04.01 «Информатика и вычислительная техника» / Юго-Западный государственный университет; сост.: С. И. Егоров, А. В. Кривонос. - Курск, 2017. - 6 с.

2. Исследование коррекции ошибок в телекоммуникационных каналах с использованием помехоустойчивых кодов Рида-Соломона [Электронный ресурс]: методические указания к лабораторной работе по дисциплине "Сети ЭВМ и телекоммуникации" для студентов, обучающихся по направлению 230100.62 «Информатика и вычислительная техника» / Юго-Западный государственный университет; сост.: С. И. Егоров, А. А. Макаревич. - Курск, 2013. - 16 с.

3. Сжатие изображений по стандарту JPEG [Электронный ресурс]: методические указания к лабораторной работе по дисциплине "Технические

средства защиты и сжатия информации" для студентов, обучающихся по направлению 09.04.01 «Информатика и вычислительная техника» / Юго-Западный государственный университет; сост.: Е.Г. Анпилогов, С. И. Егоров. - Курск, 2017. - 30 с.

4. Разработка кодеков кодов Хемминга и Рида-Соломона: методические рекомендации по выполнению курсового проекта / Юго-Зап. гос. ун-т;сост. : С.И. Егоров. - Курск, 2017. - 27 с.: ил. 4, табл. 1, прилож. 2. Библиогр.: с. 25.

5. СТУ 04.02.030–2017 СТАНДАРТ УНИВЕРСИТЕТА - Курсовые работы (проекты). Выпускные квалификационные работы. Общие требования к структуре и оформлению.

Приложение

Задание для самостоятельной работы

Изучить :

1) определение и свойства простого конечного поля;
2) определение и свойства расширенного конечного поля;
3) методы реализации операций в конечных полях.

Используя базовые логические элементы спроектировать (разработать) схемы, реализующие основные операции в расширенном конечном поле характеристики 2 (сложение, умножение, возведение в квадрат).

Конечные поля

Конечное поле – множество, состоящее из конечного числа элементов, для которых определены операции сложения и умножения.

Конечные поля называют еще полями Галуа, по имени гениального французского математика Эвариста Галуа, опубликовавшего в 1830 году в возрасте 18 лет статью, заложившую основу общей теории конечных полей. В возрасте 20 лет Галуа бил убит на дуэле.

Число элементов в поле q называется его порядком. Конечное поле обозначается GF(q) (сокращение от Galois field). С точностью до изоморфизма конечное поле полностью определяется его порядком. Порядок q всегда является степенью какого-нибудь простого числа, то есть $q = p^n$, где p — простое число, а n — любое натуральное число. Простое число p называется характеристикой поля.

Поля, для которых порядок поля равен его характеристике $q = p$ ($n = 1$) называются простыми. В противном случае поля называются расширенными ($n > 1$).

Простое поле можно представить следующим образом. Элементами поля будут числа $\{0,1,...,p\text{-}1\}$. Сложение и умножение в поле определены, как обычные операции сложение и умножение натуральных чисел с приведением результата по модулю p.

Самым известным простым полем является двоичное поле с $q = p = 2$, состоящее всего из двух элементов $\{0,1\}$. Операциями в двоичном поле являются сложение и умножение по модулю 2. Эти операции часто называют логическим сложением и логическим умножением. Задаются они с помощью таблиц истинности, приведенных ниже.

+	0	1
0	0	1
1	1	0

×	0	1
0	0	0
1	0	1

В этом поле 1 + 1 = 0.

Элементы конечного поля образуют группу по сложению. Также все элементы конечного поля кроме нулевого образуют группу по умножению.

Свойства группы:

1. Сумма (произведение) двух элементов группы всегда лежит в группе (замкнутость).
2. Выполняется правило ассоциативности: $(a + b) + c = a + (b + c)$ $((a \cdot b) \cdot c = a \cdot (b \cdot c))$.
3. Группа всегда содержит единичный элемент: $a + 0 = a$ $(a \cdot 1 = a)$.

4. Каждый элемент группы обладает обратным, для которого: $a + (-a) = 0$ ($a \cdot a^{-1} = 1$).

Все конечные поля обладают следующими свойствами:

1. Результатом умножения или сложения двух элементов поля является третий элемент, лежащий в том же поле.
2. Поле всегда содержит мультипликативную единицу 1 и аддитивную единицу 0. Таким образом, $a + 0 = a$ и $a \cdot 1 =$ а для любого элемента a.
3. Для любого элемента a существует обратный элемент по сложению $(-a)$ и обратный элемент по умножению a^{-1} (если $a \neq 0$), такие что $a+(-a)=0$ и $a \cdot a^{-1} = 1$. Существование этих элементов позволяет использовать обычные обозначения для вычитания и деления.
4. Для операций в поле выполняются обычные правила ассоциативности [$a+(b+c) = (a+b)+c$, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$], коммутативности [$a+b=b+a$, $a \cdot b = b \cdot a$] и дистрибутивности [$a \cdot (b+c) = a \cdot b + a \cdot c$].

Еще один пример простого поля – поле GF(5). Оно содержит 5 элементов: {0, 1, 2, 3, 4}. Таблицы сложения и умножения для этого поля приведены ниже.

+	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

•	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 в конечном поле следует, используя таблицы, найти соответствующий обратный элемент по сложению или умножению, а затем выполнить сложение или умножение обычным образом. Например, для поля GF(5): $3-4 = 3+(-4) = 3+1 = 4$. Аналогично $3/4 = 3 \cdot 4^{-1} = 3 \cdot 4 = 2$.

Если q является степенью простого числа $q = p^m$, то элементами поля являются все многочлены степени $m - 1$ или менее, коэффициенты которых лежат в простом поле GF(p). Такое поле называют расширенным.

Правила умножения и сложения элементов расширенного поля получаются из обычного умножения и сложения многочленов и последующего приведения результата по модулю некоторого специального многочлена $p(x)$ степени m. Этот многочлен обладает тем свойством, что его нельзя разложить на множители, используя только многочлены с коэффициентами из GF(p). Такие многочлены называются неприводимыми. Они аналогичны простым числам. Как и простые числа, неприводимые многочлены обычно находятся методом перебора.

Многочлен $p(x) = x^3 + x + 1$ неприводим над полем GF(2) и поэтому может быть использован для построения поля GF(2^3). Пусть $\beta_1 = x^2 + x + 1$ и $\beta_2 = x^2 + 1$ – два элемента поля GF(2^3). Тогда можно образовать их сумму следующим образом

$\beta_1 + \beta_2 = (x^2 + x + 1) + (x^2 + 1) = (1+1) \cdot x^2 + x + (1+1) \cdot 1 = x$,

а также и их произведение

$\beta_1 \cdot \beta_2 = (x^2 + x + 1) \cdot (x^2 + 1) =$

$= (x^4 + x^3 + x^2 + x^2 + x + 1) \bmod p(x) =$

$= (x^4 + x^3 + x + 1) \bmod (x^3 + x + 1) = x^2 + x.$

Приведение многочлена по модулю $p(x)$ эквивалентно делению на $p(x)$ и взятию остатка. С этим тесно связано понятие сравнимости: $a(x) \equiv b(x) \bmod p(x)$, что читается как "$a(x)$ сравнимо с $b(x)$ по модулю $p(x)$" и означает, что $a(x)$ и $b(x)$ имеют одинаковые остатки при делении на $p(x)$ или что $a(x) - b(x)$ делится на $p(x)$. Все эти понятия имеют смысл и в случае, когда a, b и p являются целыми числами.

Примитивным элементом или генератором в поле GF(q) называется такой элемент α , что все элементы поля, за исключением нулевого элемента, могут быть представлены в виде степени элемента α .

Например, из ранее приведенной таблицы видно, что для поля GF(5) элемент 2 является примитивным элементом, поскольку $2^0 = 1$, $2^1 = 2$, $2^2 = 4$, $2^3 = 3$, $2^4 = 2^0 = 1$.

Все конечные поля обладают тем свойством, что существует по крайней мере один примитивный элемент. Таким образом, в конечных полях, как и для обычных чисел, можно ввести понятие логарифма. И тогда другой способ выполнения умножения элементов поля будет состоять в том, чтобы найти логарифмы элементов, сложить их и найти антилогарифм суммы.

Пример для поля GF(2^3), построенного с помощью неприводимого многочлена $p(x) = x^3 + x + 1$. В данном поле элемент $\alpha = x$ является примитивным. Тогда, с учетом того, что $\alpha^i = x^i \bmod p(x)$, можно определить следующую связь между обычным и логарифмическим представлением элементов поля GF(2^3):

$\alpha^0 = 1$,

$\alpha^1 = x$,

$\alpha^2 = x^2$,

$\alpha^3 = x + 1$,

$\alpha^4 = x^2 + x$,

$\alpha^5 = x^2 + x + 1$,

$\alpha^6 = x^2 + 1$,

$\alpha^7 = 1 = \alpha^0$.

В таком представлении умножение выполняется легко, например

$\beta_1 \cdot \beta_2 = (x^2 + x + 1) \cdot (x^2 + 1) = \alpha^5 \cdot \alpha^6 = \alpha^{11} = \alpha^{11 \bmod 7} = \alpha^4 = x^2 + x.$

Элемент $\alpha = x$ будет примитивным только в случае, если многочлен $p(x)$, с помощью которого было построено поле, является примитивным. Примитивные многочлены являются непустым подмножеством неприводимых многочленов. Можно сказать, что примитивный многочлен представляет собой простой многочлен, корнем которого является примитивный элемент поля.

Существование логарифмов в конечном поле означает, что имеется представление элементов конечного поля, которое оказывается удобным для умножения, и другое представление, которое оказывается удобным для сложения. После того как установлено соответствие между этими представлениями, уже не нужно явно выписывать элементы поля в виде многочленов. Наиболее удобный метод состоит в представлении элемента поля в виде набора коэффициентов многочлена длиной m при выполнении операций в поле, например для $GF(2^3)$:

$$\beta_1 \bullet \beta_2 = (111) \bullet (101) = \alpha^{(\log(111)+\log(101)) \bmod 7} = (110).$$

Таким образом, для программной реализации арифметических операций в поле $GF(2^m)$ потребуется две таблицы размером 2^m: таблица логарифмов ($\log_\alpha x$) и таблица антилогарифмов (α^x).

Практическое значение представляют собой конечные поля $GF(2^m)$, являющиеся расширением поля GF(2). Аппаратная реализация операций в полях $GF(2^m)$ представляет собой достаточно простые комбинационные схемы, состоящие из сумматоров по модулю 2 (XOR) и логических элементов И.

В качестве примера рассмотрим сумматор, выполняющий суммирование двух произвольных элементов $c = a + b$ в уже упоминавшемся поле $GF(2^3)$, построенного с помощью порождающего многочлена $p(x) = x^3 + x + 1$. Данная схема, приведенная на рис. 1, содержит всего лишь 3 сумматора по модулю 2.

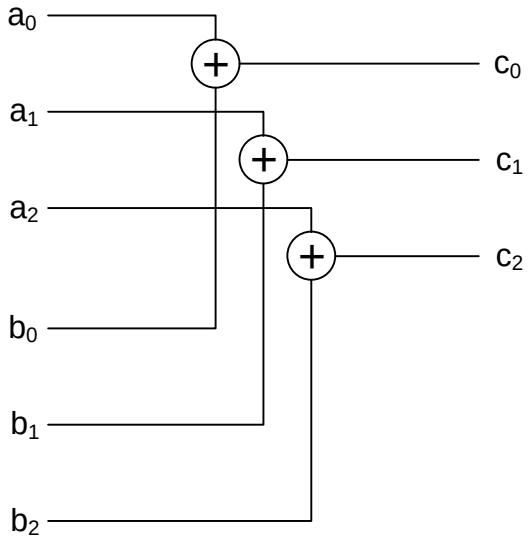

Рис. 1. Сумматор в поле $GF(2^3)$.

Допустим, необходимо синтезировать умножитель, выполняющий следующую операцию в этом же поле $GF(2^3)$: $c = a \bullet b$, где $b = \alpha^3 = \text{const}$. Так как $x = \alpha$, то произвольный элемент поля $GF(2^3)$ a может быть записан в виде $a = a(x) = a_2x^2 + a_1x + a_0 = a_2\alpha^2 + a_1\alpha + a_0$, где коэффициенты многочлена $a(x)$ принадлежат полю GF(2). Тогда

$c = a \bullet \alpha^3 = (a_2\alpha^2 + a_1\alpha + a_0) \bullet \alpha^3 = a_2\alpha^5 + a_1\alpha^4 + a_0\alpha^3$.

Поскольку в указанном поле выполняются следующие соотношения $\alpha^5 = \alpha^2 + \alpha + 1$, $\alpha^4 = \alpha^2 + \alpha$, $\alpha^3 = \alpha + 1$, получаем

$c = a_2\alpha^5 + a_1\alpha^4 + a_0\alpha^3 = a_2 \cdot (\alpha^2 + \alpha + 1) + a_1 \cdot (\alpha^2 + \alpha) + a_0 \cdot (\alpha + 1) =$

$= a_2\alpha^2 + a_2\alpha + a_2 + a_1\alpha^2 + a_1\alpha + a_0\alpha + a_0 =$

$= (a_2+a_1) \cdot \alpha^2 + (a_2+a_1+a_0) \cdot \alpha + (a_2+a_0)$.

Таким образом $c_2 = a_2 + a_1$, $c_1 = a_2 + a_1 + a_0$, а $c_0 = a_1 + a_0$. Схема данного умножителя приведена на рис. 2.

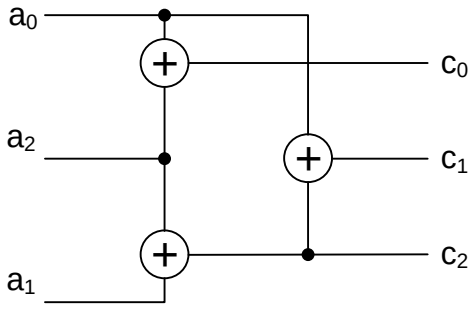

Рис. 2. Умножитель на константу α^3 в поле $GF(2^3)$.

В общем случае умножитель двух произвольных элементов поля $GF(2^3)$ может быть синтезирован на основе следующих преобразований:

$c = a \bullet b = (a_2\alpha^2 + a_1\alpha + a_0) \bullet (b_2\alpha^2 + b_1\alpha + b_0) =$

$= a_2b_2\alpha^4 + a_1b_2\alpha^3 + a_0b_2\alpha^2 + a_2b_1\alpha^3 + a_1b_1\alpha^2 +$

$+ a_0b_1\alpha + a_2b_0\alpha^2 + a_1b_0\alpha + a_0b_0$.

Так как в указанном поле $\alpha^3 = \alpha + 1$, $\alpha^4 = \alpha^2 + \alpha$, то, аналогично предыдущему случаю, получаем

$c_0 = a_0b_0 + a_2b_1 + a_1b_2$,

$c_1 = a_1b_0 + a_0b_1 + a_2b_1 + a_1b_2 + a_2b_2$,

$c_2 = a_2b_0 + a_1b_1 + a_0b_2 + a_2b_2$.

Таким образом, для реализации умножителя двух произвольных элементов рассматриваемого поля $GF(2^3)$ потребуется 9 двухвходовых элементов И (в качестве умножителя коэффициентов в поле GF(2)) и 8 двухвходовых элементов сложения по модулю 2 (в качестве сумматоров в поле GF(2)).

Деление двух элементов поля $GF(2^m)$ в общем случае может быть сведено к возведению в степень и умножению $c = a / b = a \bullet b^{-1} = a \cdot b^{N-1}$, где $N = 2^m - 1$ – число ненулевых элементов поля $GF(2^m)$. Деление является трудоемкой операцией, поэтому в практических приложениях ее стараются

избегать.