И. А. Мартынова, И. Г. Машин, В. Н. Фомченко

ВВЕДЕНИЕ В ТЕОРИЮ ПОЛЯ И ЕЕ ПРИЛОЖЕНИЯ

ЭЛЕКТРОННАЯ БИБЛИОТЕКА ФИЗИЧЕСКОГО ФАКУЛЬТЕТА МГУ

ФГУП «Российский федеральный ядерный центр –
Всероссийский научно-исследовательский институт
экспериментальной физики»

И. А. Мартынова, И. Г. Машин, В. Н. Фомченко

ВВЕДЕНИЕ В ТЕОРИЮ ПОЛЯ И ЕЕ ПРИЛОЖЕНИЯ

Монография

Саров
2014

УДК 512.623
ББК 22.14
М29

Одобрено научно-методическим советом
Саровского физико-технического института
Национального исследовательского ядерного университета «МИФИ»
и ученым советом ФГМУ «Институт информатизации
образования» Российской академии образования

Рецензент: проректор по научной работе Нижегородского государственного технического университета им. Р. Е. Алексеева кандидат технических наук, доцент Н. Ю. Бабанов

Мартынова, И. А., Машин, И. Г., Фомченко, В. Н.
Введение в теорию поля и ее приложения: Монография. – Саров: ФГУП «РФЯЦ-ВНИИЭФ», 2014. – 108 с. : ил.

ISBN 978-5-9515-0262-9

Рассмотрены аксиоматический метод познания, краткая история развития алгебры и основные понятия теории множеств. Приведены определения алгебраических структур, групп, колец, полей. Рассмотрены многочлены над полем, вычисления и преобразования в поля Галуа, цифровое устройство, его математическая модель и возможные варианты их применения.

Изложенные материалы предназначены для аспирантов технических специальностей первого года обучения для приведения в систему ранее полученных знаний и могут быть полезны для широкого круга инженерно-технических работников, связанных с разработкой информационных технологий и защитой информации, а также студентов соответствующих специальностей. Приведенные материалы могут быть использованы студентами соответствующих специальностей и школьниками старших классов в качестве дополнительного учебного пособия при первоначальном ознакомлении с введением в теорию поля и подготовке к профильным предметным олимпиадам.

УДК 512.623
ББК 22.14

ISBN 978-5-9515-0262-9

ŋqqþɐʎ þɇ dəþɇƃʎɜə p ɐcɐpcɐ Ɉqqþʎqɐè

Содержание

Такой код единственным образом задается кодовой (n, T)-матрицей, строки которой составляют базис соответствующего векторного пространства.

Если пространство является циклическим, то в качестве такой матрицы выступает любая из базисных матриц, а код, определяемый базисной матрицей, называется циклическим (T, n)-кодом над полем $GF(p)$.

Вес $W(v)$ вектора v равен числу ненулевых компонент v.

Расстоянием $D(\nu_1, \nu_2)$ между векторами ν_1 и ν_2 называется число компонент, которым отличаются эти векторы. Наименьший ненулевой вес векторов кода и наименьшее расстояние между кодовыми векторами называются соответственно минимальным весом и минимальным расстоянием кода.

При необходимости более глубокого изучения данного направления можно обратиться к работам [8, 13], которые являются основой материала данного раздела. В них подробно рассмотрены кодирующие устройства для циклических кодов, вопросы обнаружения ошибок в циклических кодах, обобщенный код Хэмминга и циклические коды максимального периода.

Модель системы связи, приведенная на рис. 8.1, очень похожа на модель криптографической системы предложенной Шенноном и приведенной в работах [8, 12, 15], если в ней кодер и декодер заменить на шифратор и дешифратор, а шум – на криптоаналитика противника.

8.4. Генерация последовательностей псевдослучайных чисел

Последовательности максимального периода можно рассматривать как некоторое множество случайных тестов и использовать их в качестве последовательностей псевдослучай-

ных чисел. Такие последовательности с успехом применяются при расчетах с помощью метода Монте-Карло и в ряде вероятностных экспериментов, в которых для воздействия на различные системы необходимо иметь стандартные случайные последовательности, обладающие свойством многократной повторяемости. Данные последовательности широко применяются и в криптографии [8, 12, 15–17].

8.5. Повышение точности радиолокационных станций

Автокорреляционные свойства последовательностей максимального периода открывают широкие возможности использования таких последовательностей для повышения точности действия радиолокационных станций, которые принимают сигналы с высоким уровнем шума. Эти последовательности применяются для модуляции выходных сигналов радиолокаторов, способствуя сокращению длительности импульсов с целью повышения разрешающей способности станции. Подробное исследование этого вопроса можно найти в работе [18].

8.6. Шифрование сообщений

Один из способов шифрования сообщений, представленных в виде цифровых групп с одинаковым числом знаков, состоит в следующем: перед передачей сообщения к каждой группе добавляется «ключевое слово». Восстановить переданное сообщение можно, только зная ключевое слово, вычитая его из каждой группы. Этот метод шифрования и дешифрования легко реализуется с помощью ЦУ, которое периодически вводит в сообщение или исключает из него ключевое слово. Существует множество и других способов шифрова-

ния. При необходимости с ними можно ознакомиться в работах [13, 14].

8.7. Адресация

Последовательности, генерируемые цифровыми устройствами, могут использоваться для передачи списка адресатов, связанных однородной деятельностью. Такими адресатами могут быть как люди, так и ячейки памяти цифровых вычислительных машин.

Как правило, всем адресам целесообразно приписывать одинаковые по длине подпоследовательности. При этом однородные операции (например, обращение к памяти) могут выполняться в течение равных промежутков времени. Для этой цели могут быть применены k-управляемые ЦУ, рассмотренные в работах [13, 14].

8.8. Генерация тестовых последовательностей

В процессе проверки состояния или ремонта цифровых систем к ним приходится подводить всевозможные последовательности над некоторым множеством символов определенной длины n. Для образования таких последовательностей может быть использовано n-мерное ЦУ максимального периода. В таком случае время, необходимое для проверки системы, будет наименьшим [13, 14].

Сходной областью применения является запись символов последовательности максимального периода вдоль линии или по окружности, например, дорожки магнитного барабана. С помощью последовательности максимального периода возможно осуществить разметку наибольшего количества ячеек при заданном числе цифр.

Список литературы

1. Энциклопедический словарь юного математика / Сост. А. П. Савин. М.: Педагогика, 1989.

2. Математика: Энциклопедия / Под ред. Ю. В. Прохорова. М.: Большая Российская энциклопедия, 2003.

3. Детская энциклопедия для среднего и старшего возраста. Академия педагогических наук РСФСР. Т. 2. Второе издание. М. 1965.

4 Ван Б. Л. дер Варден. Алгебра. М.: Наука. 1976.

5. Яковлев Г. Н. Лекции по математическому анализу. Часть 3: Учебное пособие для вузов. 2-е изд., перераб. и доп. М.: Изд-во физ.-мат. лит., 2004.

6. Чебраков Ю. В. Магические квадраты. Теория чисел, алгебра, комбинаторный анализ. СПб: СПб. гос. техн. ун-т, 1995.

7. Кан Д. Взломщики кодов: Пер. с англ. А. Ключевского. М.: ЗАО Центр-полиграф, 2000.

8. Мартынов А. П., Фомченко В. Н. Криптография и электроника / Под ред. А.И. Астайкина. Саров: ФГУП «РФЯЦ-ВНИИЭФ», 2006.

9. Виленкин Н. Я. Рассказы о множествах. М.: Наука, 1969.

10. Мельников О. В., Ремесленников В. Н., Романьков В. А. и др. Общая алгебра. Т. 1 / Под общей редакцией Л. А. Скорнякова. М.: Наука, 1990.

11. Винберг Э. Б. Курс алгебры. М.: Изд-во «Факториал», 1999.

12. Грибунин В. Г., Мартынов А. П., Николаев Д. Б., Фомченко В. Н. Криптография и безопасность цифровых систем:

Учебное пособие / Под ред. А. И. Астайкина. Саров: ФГУП «РФЯЦ-ВНИИЭФ», 2011.

13. Гилл А. Линейные последовательные машины. Анализ, синтез и применение: Пер. с англ. А. С. Берштейна // Под ред. Я. З. Цыпкина. М.: Наука, 1974.

14. Питерсон У. Коды, исправляющие ошибки: Пер. с англ. Л. Е. Филипповой / Под. ред. Р. Л. Добрушина. М.: Мир, 1964.

15. Мартынова И. А. Методы защиты результатов физических экспериментов / Тезисы докладов VII Международных школьных Харитоновских чтений. Саров: ФГУП «РФЯЦ-ВНИИЭФ». 2007. С. 50–51.

16. Мартынова И. А. Алгоритмы распределения и защиты информации и пример их практического применения // Международная научная конференция школьников. XVIII Сахаровские чтения. Санкт-Петербург. 2008.

17. Мартынова И. А., Бузденкова Ю. М., Немченко И. А. Адаптивная концепция управления как элемент системы информационной безопасности // Сб. докл. 6-й Всероссийской молодежной научно-инновационной школы «Математика и математическое моделирование». Саров: СарФТИ НИЯУ «МИФИ», 2012.

18. Golomb S.W. (ed.), Digital communication with space applications, Prentice-Hall, Inc., Englewood Cliffs, N. J., 1964.

Мартынова Инна Александровна, **Машин** Игорь Геннадьевич,
Фомченко Виктор Николаевич

ВВЕДЕНИЕ В ТЕОРИЮ ПОЛЯ И ЕЕ ПРИЛОЖЕНИЯ

Монография

Редактор *Н. П. Мишкина*
Компьютерная подготовка оригинала-макета *Н. В. Мишкина*

Подписано в печать 01.08.2014. Формат 60×84/16
Печать офсетная. Усл. печ. л. ~6,3 Уч.-изд. л. ~5,0
Тираж 300 экз. Зак. тип. 1422-2014

Отпечатано в Издательско-полиграфическом комплексе
ФГУП «РФЯЦ-ВНИИЭФ»
607188, г. Саров Нижегородской обл., ул. Силкина, 23