УДК 512.622

Применение теории многочленов

А.С. Жукабаева
Южно-уральский государственный гуманитарно-педагогический университет, г. Челябинск

Теория многочленов в кодировании

Изучая многочлены от нескольких переменных, наверное, многие зададутся вопросом, как данную тему можно применять на практике.

Человечество живет в мире информации, она окружает нас повсюду. Эту информацию необходимо как-то хранить, обрабатывать или передавать. Как же это сделать, когда вокруг столько информации? За всю свою многовековую историю человечество придумало множество различных способов кодирования информации [3]. Некоторые изобретения мы используем до сих пор, авторы которых известны во всем мире. Коды окружаю нас повсюду, а чтобы разбираться в кодах, нужно иметь представление о многочленах. Именно поэтому тема «Многочлены от нескольких переменных» так актуальна в современном мире.

Примеров кодирования информации, основанной на применении теории многочленов, существует огромное множество. Один из таких−код Адамара, остановимся на нем более подробно.

Код Адамара является кодом коррекции ошибок имени Жака Адамар, который используется для обнаружения и исправления ошибок при передаче сообщений по очень шумным или ненадежным каналам. Благодаря своим уникальным математическим свойствам, данный код используется не только инженерами, но и интенсивно изучается в теории кодирования, математики и теоретической информатики.

Код Адамара состоит из $2m$ кодовых слов, с длиной равной m, любые два из которых отличаются либо ровно в половине позиций (так что соответствующие векторы ортогональны), либо во всех позициях. Код Адамара строится при $m = 2^s$. Для этого позиции в слове будем представлять себе как вершины s −мерного булева куба $\mathbb{B}^s$, а слова− как функции $\mathbb{B}^s \to \mathbb{B}$.Такая функция задаётся своими значениями в $2^s = m$ вершинах, и эти значения образуют слово длины m надо только фиксировать какой-либо порядок на вершинах куба.

В качестве кодовых слов возьмём аффинные функции, то есть функции вида:

$$< x_1, \dots, x_s > \longmapsto a_0 + a_1 x_1 + \cdots + a_s x_s$$

при $a_0, \dots, a_s \in \mathbb{B}$ (умножение и сложение−как в поле из двух элементов). Такая функция задаётся набором своих коэффициентов, и потому имеется $2^{s+1} = 2m$ аффинных функций [4].

Две такие функции либо различаются во всех точках (если отличаются лишь коэффициентом a_0), либо ровно в половине точек (образующих аффинное подпространство размерности 1 над полем $\mathbb{B}$). Код Адамара построен.

Теория многочленов в шифровании

В современном мире одним из наиболее активных направлений развития информационных технологий являются облачные вычисления. Основной причиной такого развития является возможность для компаний и частных лиц снижения расходов на поддержание собственной ИТ-инфраструктуры за счет передачи этой работы провайдеру облачного сервиса. однако в такой ситуации становятся небезопасными хранение и обработка конфиденциальных данных в облачной инфраструктуре, так как у ее провайдера появляется возможность неконтролируемого доступа к обрабатываемым данным. единственным решением этой проблемы может служить шифрование всех приватных данных перед передачей в облако [2].

Существует 3 новые схемы гомоморфного шифрования, в основе которых лежат многочлены от нескольких переменных, остановимся на последней из них.

В основе третьей схемы лежат гомоморфизмы колец полиномов от многих переменных над $\mathbb{Z}_2$. Она применяется для шифрования на уровне отдельных битов. Для шифрования чисел $a_0, b_0 \in \mathbb{Z}_2$ построим полином $a(x_1, \dots, x_n)$ и $b(x_1, \dots, x_n)$, такие, что a_0 и b_0 соответственно являются их свободными членами. Свободные члены многочленов $a(x_1, \dots, x_n) \cdot b(x_1, \dots, x_n)$ и $a(x_1, \dots, x_n) + b(x_1, \dots, x_n)$ будут равны $a_0 b_0$ и $a_0 + b_0$соответственно [2].

Для построения «шифрующего» гомоморфизма используется взаимно однозначная замена переменных:

$$\begin{cases} y_1 = f_1(x_1, \dots, x_n) \\ y_n = f_n(x_1, \dots, x_n) \end{cases}$$

Для построения таких замен переменных можно использовать интерполяционный многочлен Лагранжа или преобразование Кремоны. Взаимная однозначность замены переменных обеспечивает возможность построения обратной замены и расшифровки данных [1].

Таким образом, рассмотренная схема также является полностью гомоморфным шифрованием, поскольку позволяет выполнять операции $+$ и $\times$ над зашифрованными данными. Ее важное свойство — отсутствие роста степени полиномов в силу малой теоремы Ферма.

Библиографический список

1. Биркгоф Г., Барти Т. Современная прикладная алгебра, Мир, 1976.
2. Жиров А. О.,Жиров О. В., Кренделев С. Ф Статья: Безопасные облачные вычисления с помощью гоммофной криптографии.
3. Лидовский В.В. Теория информации, Москва, 2004.
4. Ромащенко А.Е., Румянцев А.Ю., Шень А. Заметки по теории кодирования. 2-е изд., испр. и доп. М.: МЦНМО, 2017.

УДК 512.622

Симметрические многочлены

А.С. Жукабаева, М.А. Дульцева, Л.В. Истомина
Южно-уральский государственный гуманитарно-педагогический университет, г. Челябинск

Фундаментальные знания теории многочленов составляют значительную часть дисциплины алгебра и необходимы в будущей профессиональной деятельности и при прохождении педагогической практики [1]. Теория многочленов служит основой для проведения научно-исследовательских работ бакалавров, применяется в реализации учебных проектов [2-3].

Очень важным разделом в теории многочленов являются специальные многочлены, называемые симметрическими. Они используются при решении некоторых алгебраических уравнений высшего порядка и некоторых систем алгебраических уравнений. Дадим его определение.

Многочлен $f(x_1 \dots x_n)$ называется симметрическим, если для любой подстановки номеров переменных он не изменяется [4].

$$f(x_1 \dots x_n) = f\left(x_{\tau(1)} \dots x_{\tau(n)}\right), \forall \tau$$

Например, многочлен $f(x_1, x_2, x_3) = {x_1}^2 x_2 x_3 + x_1 {x_2}^2 x_3 + x_1 x_2 {x_3}^2$ является симметрическим, а многочлен $g(x_1, x_2, x_3) = {x_1}^2 x_2 x_3 + x_1 {x_2}^2 x_3$ не является симметрическим, т.к $g(x_2, x_3, x_1) = {x_2}^2 x_3 x_1 + x_2 {x_3}^2 x_1 \neq g(x_1, x_2, x_3)$.

Отдельно рассматривают элементарные симметрические многочлены:

$$x_1 + x_2 + \dots + x_n = \sigma_1,$$

$$x_1 x_2 + \dots + x_1 x_n + x_2 x_3 + \dots + x_2 x_n + \dots + x_{n-1} x_n = \sigma_2,$$

$$x_1 x_2 x_3 + \dots + x_{n-2} x_{n-1} x_n = \sigma_3, \text{ и так далее}$$

$$x_1 x_2 x_3 \dots x_n = \sigma_n,$$

$\sigma_k = \sum x_{i_1} \cdots x_{i_k}$(сумма произведений по k переменных без повторений)