

ЛИТЕРАТУРА

1. Rinott Y. and Rotar V. A multivariate CLT for local dependence with $n^{-1/2} \log n$ rate and applications to multivariate graph related statistics // J. Multivariate Analysis. 1996. V. 56. P. 333–350.

УДК 512.62

О ПОЛИКВАДРАТИЧНОМ РАСШИРЕНИИ БИНАРНЫХ ПОЛЕЙ

Кр. Л. Геут, С. С. Титов

Работа посвящена генерации неприводимых многочленов степени 2^n посредством поликватратичного расширения поля над $\text{GF}(2)$. Построено полное бинарное дерево неприводимых многочленов, рассмотрены свойства этого расширения.

Ключевые слова: неприводимый многочлен, поликватратичное расширение, след многочлена.

Неприводимые многочлены активно применяются при передаче информации по каналам связи в виде битовых строк, помехоустойчивом кодировании, работе конечных автоматов, стандартах защиты информации [1]. Использование свойств неприводимых многочленов позволяет максимизировать эффективность компьютерной реализации арифметики в конечных полях.

Рассмотрим уравнение $x^2 + x = z$ в поле $\text{GF}(2^m)$, где z — корень неприводимого многочлена f над $\text{GF}(2)$ степени m . Если x не лежит в этом же поле $\text{GF}(2^m)$, а лежит в расширении $\text{GF}(2^{2m})$ этого поля, то след $\text{Tr}(f) = 1$ [2] и x — корень неприводимого многочлена F степени $2m$ [3–5]. Многочлен F получается из f посредством так называемой операции A [6]: $F(X) = f(X^2 + X)$. Многочлен F неприводимый и периодический (с периодом равным единице), т. е. $F(X + 1) = F(X)$.

Если же x лежит в том же поле $\text{GF}(2^m)$, то многочлен, полученный с помощью операции A из многочлена f , приводим, $F(X) = p(X)q(X)$, $\text{Tr}(f) = 0$, $\deg p = \deg q = m$, и x — корень одного из этих двух неприводимых многочленов p, q , связанных соотношением сдвига: $p(X + 1) = q(X)$ [6].

Если $m = 2^k$ и $\text{Tr}(x) = 1$, то после поэтапного применения операции A можно построить полное бинарное дерево, ветви которого символизируют применение операции A , а вершины — многочлены, полученные с помощью этой операции [6]. Если представить шаг (т. е. применение операции A) как уровень, то можно заметить, что вершина с неприводимым многочленом степени 2^{n+1} появляется только после прохождения всех уровней с неприводимыми многочленами степени 2^n , причём число этих уровней-шагов равно 2^{n-1} . Приводимость многочлена, полученного с помощью операции A , зависит от следа многочлена, к которому была применена эта операция.

Многочлены степени 2^n со значением следа $\text{Tr} = 1$ всегда лежат на нижнем уровне, так как после применения операции A они дают неприводимый периодический многочлен степени 2^{n+1} , а на остальных уровнях лежат многочлены с нулевым значением следа $\text{Tr} = 0$.

Симметричные (самовозвратные) многочлены (т. е. многочлены, у которых коэффициенты симметричны относительно центрального бита) степени 2^{n+1} с нулевыми значениями следа и антиследа ($\text{Tr} = \text{Tr}^{-1} = 0$) получаются из многочленов степени 2^n со значениями $\text{Tr} = 0$, $\text{Tr}^{-1} = 1$, а многочлены степени 2^{n+1} со значениями $\text{Tr} = \text{Tr}^{-1} = 1$ — из аналогичных многочленов степени 2^n со значениями $\text{Tr} = \text{Tr}^{-1} = 1$,

причём в одной ветви может встретиться только один симметричный многочлен одной степени.

В результате исследования поликвадратичного расширения полей посредством операции A получены следующие свойства этого расширения.

1. Посредством поликвадратичного расширения можно вычислять характеристический многочлен элемента не только из расширенного поля, но и из расширяемого, т. е. движение по дереву возможно как вверх, так и вниз. Для того чтобы «опуститься» по дереву вниз, необходимо применить операцию A , а чтобы «подняться» по дереву вверх — выполнить обратную операцию $\Lambda = A^{-1}$.

2. Для вычисления расширений необходимо вычислить относительный след корня и записать уравнение, задающееся неприводимым многочленом, коэффициенты которого вычисляются в явном виде [3, 4].

Теорема 1. Если $h(x) = z$, $\deg f = n$, $f(z) = 0$, $\deg g = 2n$, $g(z) = 0$, то $\text{Tr}(z) = \text{Tr}(x)$, где $h(x) = x + x^{-1}$ равен относительному следу элемента x .

Теорема 2. Если в поле $\text{GF}(2^m)$, $m > 1$, z — корень симметричного многочлена f , то однозначно определён периодический многочлен g , где $y = 1/(z + 1)$ — его корень. И наоборот, если g — периодический, то f — симметричный, где $z = 1/y + 1$.

Таким образом, с помощью операции A построено полное бинарное дерево неприводимых многочленов степени 2^n . Изученные в работе свойства такого поликвадратичного расширения значительно упрощают процедуру генерации многочленов и дают возможность избежать полного перебора при поиске многочленов больших степеней, что имеет особое значение для криптографии и теории кодирования.

ЛИТЕРАТУРА

1. Информационные технологии и безопасность алгоритмы разделения секрета. Предварительный государственный стандарт республики Беларусь СТБ П 34.101.44. Минск: Госстандарт, 2011.
2. Глуско Кр. Л., Титов С. С. Арифметический алгоритм решения квадратных уравнений в конечных полях характеристики два // Доклады ТУСУРа. 2012. №1(25). Ч. 2. С. 148–152.
3. Болотов А. А., Гашков С. Б., Фролов А. Б. Элементарное введение в эллиптическую криптографию: алгебраические и алгоритмические основы. М.: КомКнига, 2006.
4. Болотов А. А., Гашков С. Б., Фролов А. Б. Элементарное введение в эллиптическую криптографию: Протоколы криптографии на эллиптических кривых. М.: КомКнига, 2006.
5. Лидл Р., Нидеррайтер Г. Конечные поля. М.: Мир, 1988.
6. Геут Кр. Л., Титов С. С. О свойствах поликвадратичных расширений бинарных полей // Проблемы теоретической и прикладной математики: Труды 44-й Всерос. молодежной конф. Екатеринбург: УрО РАН, 2013. С. 17–19.

УДК 512.55

КЛАССЫ ПОЛИНОМИАЛЬНЫХ И ВАРИАЦИОННО-КООРДИНАТНО ПОЛИНОМИАЛЬНЫХ ФУНКЦИЙ НАД КОЛЬЦОМ ГАЛУА

М. В. Заец

Рассматривается новый класс функций над кольцом Галуа $R = \text{GR}(q^m, p^m)$, получивший название класса функций с вариационно-координатной полиномиальностью (ВКП-функций). Рассматривается соотношение между данным классом и