О СВОЙСТВАХ ПОЛИКВАДРАТИЧНЫХ РАСШИРЕНИЙ БИНАРНЫХ ПОЛЕЙ

Геут (Глуско) Кр.Л., Титов С.С.
e-mail: gluskokrl@rtural.ru

В связи с потребностями кодирования и криптографии в настоящее время активно развиваются прикладные аспекты теории конечных полей. Особенность вычислений в конечном поле состоит в необходимости выбора представления элементов. Практически используются в основном два: представление в стандартном и нормальном базисе, а также производные от них.

Элементы нормального базиса $(\alpha, \alpha^2, \alpha^4, ..., \alpha^{2^{n-1}})$ являются корнями одного и того же многочлена степени n, это связано с тем, что операция возведения в квадрат является автоморфизмом поля. Поэтому можно вести речь о нахождении многочленов, корни которого образуют базис для решения конкретных задач в конечных полях, в частности нахождения корней квадратных уравнений [1, 2]. С точки зрения компьютерной реализации имеют значение многочлены двоичных степеней, т.е. 2^n.

Возьмем уравнение $x^2+x=z$, где $z-$корень неприводимого многочлена $f(x)$ и $f(z)=0$. Если x не лежит в этом же поле $GF(2^m)$, а лежит в расширении этого поля $GF(2^{2m})$, то x – корень неприводимого многочлена $F(x)=0$ и F получается из f посредством операции A, т.е.

$$F(t)=f(t^2+t).$$

Многочлен F степени $\deg F=2m$ неприводим, а его период равен единице, т.е. $F(t+1)=F(t)$. При этом $Tr(f)=1$.

Если же x лежит в том же поле $GF(2^m)$, то многочлен, полученный с помощью операции A из многочлена f приводим: $F'(t)=p(t)q(t), Tr(f)=0$, а $\deg\, p=\deg\, q=m$; — и x — корень одного из двух неприводимых многочленов той же степени m, связанных соотношением сдвига: $p(t+1)=q(t)$.

Если $m=2^k$ и $Tr(x)=1$, то при поэтапном применении операции A получается полное бинарное дерево, ветви которого будут символизировать применение операции A, а вершинами соответственно будут многочлены, полученные с помощью этой операции (это дерево

частично представленно на рис. 1). 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. Причем, 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 [3].

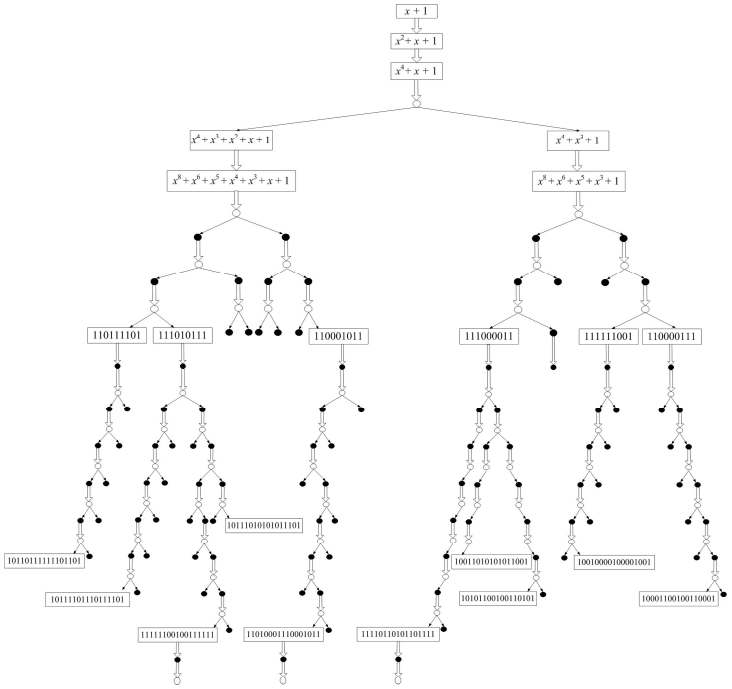

Рис. 1: Дерево неприводимых многочленов степени 2^n

Многочлены степени 2^{n+1} со значением $Tr = 1$ всегда лежат в нижнем уровне, т.к. после применения операции A они дают неприводимый многочлен степени 2^n, на остальных уровнях лежат многочлены со значением $Tr = 0$.

Симметричные многочлены степени 2^{n+1} со значениями $Tr = Tr^{-1} = 0$ получаются из многочленов степени 2^n со значениями

$Tr = 0, Tr^{-1} = 1$, а многочлены 2^{n+1} со значениями $Tr = Tr^{-1} = 1$ из аналогичных многочленов степени 2^n со значениями $Tr = Tr^{-1} = 1$ ровно через 2^n шагов, причем в одной ветви может встретиться только один симметричный многочлен одной степени.

На основании вышеизложенного можно сформулировать

Утверждение 1. *Если $h(z) = x$, $deg\ z = 2n$, $deg\ x = n$, то $Tr(z) = Tr(x)$, где $h(z) = (z + z^{-1})$ – относительный след элемента z.*

Утверждение 2. *Если z – корень симметричного многочлена $f(z)$, то y – корень периодического многочлена $g(y)$, где $y = \frac{1}{z+1}$. И наоборот, если $g(y)$ – периодический, то $f(z)$ – симметричный, где $z = \frac{1}{y+1}$.*

Таким образом, в статье рассмотрен способ получения всех неприводимых многочленов степени 2^n посредством операции A. Свойства такого поликваратичного расширения значительно упрощают процедуру генерации многочленов и дают возможность избежать полного перебора при поиске многочленов больших степеней.

Литература

[1] *Болотов А.А., Гашков С.Б., Фролов А.Б.* Элементарное введение в эллиптическую криптографию: Протоколы криптографии на эллиптических кривых. – М.: КомКнига, 2006. 280 с.

[2] *Лидл Р.,Нидеррайтер Г.* Конечные поля. – В 2 т. Т. 1. Пер. с англ. – М.: Мир, 1988. 430 с.

[3] *Глуско К.Л., Титов С.С.* Нормальные базисы и дерево квадратичных расширений бинарных полей // Некоторые актуальные проблемы современной математики и математического образования: Материалы научной конференции «Герценовские чтения – 2012». С. 221–226. — СПб.: БАН.