УДК 512.6, 519.165, 519.725

С.С. Титов, А.В. Торгашова

Генерация неприводимых многочленов, связанных степенной зависимостью корней

Рассмотрен имеющий приложение в криптографии и теории кодирования метод получения новых неприводимых многочленов из данного неприводимого многочлена той же степени при условии, что корни этих многочленов связаны степенной зависимостью. Приведены формулы для генерации таких многочленов.

Ключевые слова: неприводимый многочлен, кодирование, сравнимость по модулю, степень многочлена, генерация многочленов, порождаемый многочлен, алгоритм, коэффициент.

Введение

Генерация неприводимых многочленов является актуальной и сложной прикладной задачей, широко востребованной в криптографических приложениях [1–6] (генерация открытых и закрытых ключей) и теории кодирования (построение кодов полиномиального кодирования и БЧХ-кодов [4, 7–10]). Генерация неприводимых многочленов есть порождение (нахождение) неприводимых многочленов с заведомо хорошими свойствами, что позволяет использовать их для генерации ключей (закрытых и открытых) в системах защищенного документооборота, например, в системах интернет-банка и клиент-банка. Ввиду этого актуальными являются исследования по нахождению методов и алгоритмов, с помощью которых разрабатываются наиболее быстрые и эффективные способы генерации неприводимых многочленов. В данной статье один из таких методов – получение новых неприводимых многочленов из данного неприводимого многочлена той же степени при условии, что корни этих многочленов связаны произвольными степенными зависимостями. Рассмотрим подробно переходы $x \to x^3$ и $x \to x^5$.

Пусть многочлен $f(x) = \sum_{i=0} a_i x^i$ неприводим над полем $GF(2)$, его степень $\deg f = N$; $1 = \omega^0, \omega^1, \omega^2, \ldots, \omega^{t-1}$ – корни степени t из единицы, $\omega^t = 1$, $\omega \neq 1$, t нечетно, $\omega^{t-1} + \omega^{t-2} + \ldots + \omega + 1 = 0$. Пусть $z = x^t$, f_t – характеристический многочлен элемента $\beta = \lambda^t$, где $f(\lambda) = 0$, тогда по теореме 3.39 [11] имеем:

$$f_t(x^t) =$$

$$= (-1)^{N(t-1)} \prod_{j=0}^{N} f(\omega^j x) = \sum_{i=0}^{N} a_i x^i \sum_{j=0}^{N} a_j (\omega x)^j \ldots \sum_{k=0}^{N} a_k (\omega x)^k = \sum_{i=0}^{N} \sum_{j=0}^{N} \ldots \sum_{k=0}^{N} a_i a_j \ldots a_k \omega^{0 \cdot i + 1 \cdot j + \ldots + (t-1) \cdot k} x^{i+j+\ldots+k} =$$

$$= \sum_{s=0}^{N \cdot t} x^s \sum_{\substack{i+j+\ldots+k=s \\ 0 \le i,j,\ldots,k \le N}} a_i a_j \ldots a_k \omega^{0 \cdot i + 1 \cdot j + \ldots + (t-1) \cdot k} = \sum_{r=0}^{N} x^{tr} \sum_{\substack{i+j+\ldots+k=tr \\ 0 \le i,j,\ldots,k \le N}} a_i a_j \ldots a_k \omega^{0 \cdot i + 1 \cdot j + \ldots + (t-1) \cdot k},$$ так что

$$f_t(z) = \sum_{r=0}^{N} b_r z^r, \text{ где } b_r = \sum_{\substack{i+j+\ldots+k=tr \\ 0 \le i,j,\ldots,k \le N}} a_i a_j \ldots a_k \omega^{0 \cdot i + 1 \cdot j + \ldots + (t-1) \cdot k}.$$

Общая формула $f_t(x^t) = (-1)^{N(t-1)} \prod_{j=0}^{N} f(\omega^j x)$ справедлива и для любого поля $GF(q)$. Подробное рассмотрение предложенного метода описано для поля $GF(2)$ для изложения комбинаторного подхода и явного вычисления коэффициентов путем приведения подобных [12], поскольку поле $GF(2)$ используется в большинстве алгоритмов шифрования, например RSA, DES, RC4, и эллиптической криптографии [5, 6].

Так как в результирующей формуле для b_r не содержится сомножителя ω, значит, $\omega^{0 \cdot i + 1 \cdot j + \ldots + (t-1) \cdot k} = 1$, что возможно лишь когда $0 \cdot i_0 + 1 \cdot i_1 + \ldots + (t-1) \cdot i_{t-1} \equiv 0 (\mathrm{mod}\, t)$, $b_r \in GF(2)$, и поэтому, приводя подобные, можно записать:

$$b_r = \sum_{\substack{0n_0+1n_1+\ldots+Nn_N=t\cdot r \\ n_0+n_1+\ldots+n_N=t}} a_0^{n_0} a_1^{n_1} \ldots a_N^{n_N} \cdot \varepsilon_{n_0 n_1 \ldots n_N},$$

где $\varepsilon_{n_0 n_1 \ldots n_N} \in GF(2) = \{0,1\}$. Таким образом, осталось только выяснить, каких слагаемых в этой формуле не будет, т.е. для каких индексов $\varepsilon_{n_0 n_1 \ldots n_N} = 0$. Для этого надо рассмотреть процесс приведения подобных членов.

1. Генерация неприводимых многочленов с помощью перехода $x \to x^3$.

Имеем $b_r = \sum_{i_0+i_1+i_2=3\cdot r} a_{i_0} a_{i_1} a_{i_2} \cdot \omega^{0\cdot i_0+1\cdot i_1+2\cdot i_2}$, где $\omega^3 = 1$, $\omega \neq 1$, $\omega^2 + \omega + 1 = 0$. Рассмотрим три случая в зависимости от количества различных элементов во множестве $\{i_0, i_1, i_2\}$.

1) Если $|\{i_0, i_1, i_2\}| = 1$, т.е. $i_0 = i_1 = i_2 = r$ и $0 \cdot i_0 + 1 \cdot i_1 + 2 \cdot i_2 = 3 \cdot r$, так что $\omega^{0\cdot i_0+1\cdot i_1+2\cdot i_2} = \omega^{3r} = 1$, потому что $3 \cdot r \equiv 0 (\mathrm{mod}\, 3)$, и этот случай дает вклад слагаемого a_r^3 в сумму для коэффициента b_r.

2) Если $|\{i_0, i_1, i_2\}| = 2$, то два индекса из трех равны и отличны от третьего. Обозначим совпадающие индексы через k, а третий – через l, таким образом, исследуем вхождение слагаемого $a_k^2 a_l$, при $i_0 + i_1 + i_2 = 2 \cdot k + l = 3 \cdot r$. Распределение $\{k,l\}$ по индексам $\{i_0, i_1, i_2\}$ возможно лишь из перечня табл. 1.

Таблица 1

Распределение номеров по индексам

i_0	i_1	i_2	$0 \cdot i_0 + 1 \cdot i_1 + 2 \cdot i_2$	$\omega^{0\cdot i_0+1\cdot i_1+2\cdot i_2}$
k	k	l	$k + 2 \cdot l$	$\omega^{k+2l} = \omega^{3k} \cdot \omega^{2(l-k)} = \omega^{2(l-k)}$
k	l	k	$l + 2 \cdot k$	$\omega^{l+2k} = \omega^{3k} \cdot \omega^{(l-k)} = \omega^{(l-k)}$
l	k	k	$3 \cdot k$	$\omega^{3k} = 1$

Из этого перечня получаем следующие слагаемые при приведении подобных для $a_k^2 a_l$:

$$\sum_{\substack{i_0=i_1=k, i_2=l \\ i_0=i_2=k, i_1=l \\ i_1=i_2=k, i_0=l}} a_{i_0} a_{i_1} a_{i_2} \cdot \omega^{0i_0+1i_1+2i_2} = a_k^2 a_l \cdot [\omega^{2(l-k)} + \omega^{(l-k)} + 1].$$

Здесь возможно 2 варианта: когда k сравним с l и когда они не сравнимы.

Первый вариант: $l - k \equiv 0 (\mathrm{mod}\, 3)$. Это значит, что $\omega^{2(l-k)} + \omega^{(l-k)} + 1 = 1 + 1 + 1 = 3 (\mathrm{mod}\, 2) = 1$. Берем по модулю два, так как $\omega \in GF(2)$. Это означает, что слагаемое $a_k^2 a_l$ будет входить в сумму коэффициента b_r при условии $k \equiv l (\mathrm{mod}\, 3)$.

Второй вариант: $l - k \neq 0 (\mathrm{mod}\, 3)$.

Так как любая степень $z = \omega^{(l-k)}$ удовлетворяет уравнению $z^2 + z + 1 = 0$, то и выражение в квадратных скобках будет равно нулю $\omega^{2(l-k)} + \omega^{(l-k)} + 1 = 0$ при $l - k \neq 0 (\mathrm{mod}\, 3)$. Однако их несравнимость невозможна, так как из условия $2k + l = 3r \equiv 0 (\mathrm{mod}\, 3)$ вытекает $l \equiv -2k \equiv k (\mathrm{mod}\, 3)$, потому что $-2 \equiv 1 (\mathrm{mod}\, 3)$. Делаем вывод, что слагаемое $a_k^2 a_l$ не будет входить в сумму коэффициента b_r при условии $l - k \neq 0 (\mathrm{mod}\, 3)$.

В итоге имеем, что слагаемое $a_k^2 a_l$ будет входить в сумму коэффициента b_r только при условиях $l \equiv k (\mathrm{mod}\, 3)$ и $2k + l = 3r$.

3) Если $|\{i_0, i_1, i_2\}| = 3$, то все индексы различны: $i_0 \neq i_1 \neq i_2 \neq i_0$. Пусть $\{i_0, i_1, i_2\} = \{k, l, m\}$, $k + l + m = 3 \cdot r$, так что исследуется вхождение слагаемого $a_k a_l a_m$. Распределение k, l и m по индексам i_0, i_1, i_2 дают 6 перестановок на трех элементах (табл. 2).

Из этого перечня при приведении подобных слагаемых для $a_k a_l a_m$ получаем следующее выражение: $a_k a_l a_m[\omega^{(l-k)+2(m-k)} + \omega^{(m-k)+2(l-k)} + \omega^{2(m-k)} + \omega^{(m-k)} + \omega^{2(l-k)} + \omega^{(l-k)}]$.

Таблица 2

Перестановки номеров индексов

i_0	i_1	i_2	$i_0+i_1+i_2=3\cdot r$	$0\cdot i_0+1\cdot i_1+2\cdot i_2$	$\omega^{0\cdot i_0+1\cdot i_1+2\cdot i_2}$
k	l	m	$k+l+m=3\cdot r$	$l+2m$	$\omega^{l+2m}=\omega^{3k}\omega^{(l-k)+2(m-k)}$
k	m	l	$k+m+l=3\cdot r$	$m+2l$	$\omega^{m+2l}=\omega^{3k}\omega^{(m-k)+2(l-k)}$
l	k	m	$l+k+m=3\cdot r$	$k+2m$	$\omega^{k+2m}=\omega^{3k}\omega^{2(m-k)}$
l	m	k	$l+m+k=3\cdot r$	$m+2k$	$\omega^{m+2k}=\omega^{3k}\omega^{(m-k)}$
m	k	l	$m+k+l=3\cdot r$	$k+2l$	$\omega^{k+2l}=\omega^{3k}\omega^{2(l-k)}$
m	l	k	$m+l+k=3\cdot r$	$l+2k$	$\omega^{l+2k}=\omega^{3k}\omega^{(l-k)}$

Заметим, что условие $k+l+m=3\cdot r\equiv 0(\mathrm{mod}\,3)$ влечет сравнение $(k-k)+(l-k)+(m-k)=(l-k)+(m-k)\equiv 0(\mathrm{mod}\,3)$ и, значит, $(l-k)\equiv -(m-k)(\mathrm{mod}\,3)$ и $(l-k)\equiv 2(m-k)(\mathrm{mod}\,3)$. Поэтому возникает два варианта: когда $(m-k)$ сравнимо с нулем и когда $(m-k)$ не сравнимо с нулем.

a. Пусть $m-k\equiv 0(\mathrm{mod}\,3)$. Отсюда следует, что $m\equiv k(\mathrm{mod}\,3)$, т.е. $(l-k)\equiv 0(\mathrm{mod}\,3)$, откуда $l\equiv k(\mathrm{mod}\,3)$ и, как следствие, $m\equiv k\equiv l(\mathrm{mod}\,3)$. Таким образом, так как все слагаемые равны единице, получаем

$$a_k a_l a_m[\omega^{(l-k)+2(m-k)} + \omega^{(m-k)+2(l-k)} + \omega^{2(m-k)} + \omega^{(m-k)} + \omega^{2(l-k)} + \omega^{(l-k)}] = a\ a\ a\ \cdot 6\equiv 0(\mathrm{mod}\,2).$$

Следовательно, если все три индекса сравнимы между собой по модулю три, $m\equiv k\equiv l(\mathrm{mod}\,3)$, то слагаемое $a_k a_l a_m$ не входит в сумму коэффициента b_r.

b. Пусть $m-k\neq 0(\mathrm{mod}\,3)$. Отсюда $k\neq m(\mathrm{mod}\,3)$ и $k\neq l(\mathrm{mod}\,3)$. Упростим выражения:

$$(l-k)+2(m-k)=2(m-k)+2(m-k)=(m-k)(\mathrm{mod}\,3),$$
$$(m-k)+2(l-k)=(m-k)+(m-k)=(l-k)(\mathrm{mod}\,3).$$

Имеем:

$$a_k a_l a_m[\omega^{(l-k)+2(m-k)} + \omega^{(m-k)+2(l-k)} + \omega^{2(m-k)} + \omega^{(m-k)} + \omega^{2(l-k)} + \omega^{(l-k)}] = a\ a\ a\ [\omega^{2(m-k)} + \omega^{2(l-k)}] =$$
$$= a_k a_l a_m[\omega^{2(l-k)} + \omega^{(l-k)}].$$

Так как любая степень $z=\omega^{(l-k)}$ удовлетворяет тому же уравнению $z^2+z=1$, то и выражение в квадратных скобках равно единице $\omega^{2(l-k)}+\omega^{(l-k)}=1$ при $m-k\neq 0(\mathrm{mod}\,3)$, и это означает, что слагаемое $a_k a_l a_m$ будет входить в сумму при условии $k\neq m(\mathrm{mod}\,3)$.

В итоге имеем, что слагаемое $a_k a_l a_m$ будет входить в сумму b_r только при $k\neq m(\mathrm{mod}\,3)$ и $k\neq l(\mathrm{mod}\,3)$.

В силу сравнения $(l-k)\equiv 2(m-k)(\mathrm{mod}\,3)$ и условий $k\neq m(\mathrm{mod}\,3)$ и $k\neq l(\mathrm{mod}\,3)$ делаем вывод, что и $m\neq l(\mathrm{mod}\,3)$. Потому что, предположив, что $m\equiv l(\mathrm{mod}\,3)$ и заменив m на l в сравнении $(l-k)\equiv 2(m-k)(\mathrm{mod}\,3)$, получим $(m-k)\equiv 2(m-k)(\mathrm{mod}\,3)$, отсюда $m-k\equiv 0(\mathrm{mod}\,3)$ и $m\equiv k(\mathrm{mod}\,3)$, что противоречит условию $k\neq m(\mathrm{mod}\,3)$.

Отсюда получаем:

Утверждение 1: слагаемое $a_k a_l a_m$ будет входить в сумму b_r во всех случаях, кроме $k\neq m\neq l\neq k$, $m\equiv k\equiv l(\mathrm{mod}\,3)$, т.е. кроме случая, когда все индексы k, l и m различны, но сравнимы между собой по модулю три.

Выпишем для примера первые пять слагаемых порождаемого многочлена, найденных согласно утверждению 1:

$$b_0 = {a_0}^3;$$
$$b_1 = {a_0}^2 a_3 + a_0 a_1 a_2 + {a_1}^3;$$
$$b_2 = {a_0}^2 a_6 + a_0 a_1 a_5 + a_0 a_2 a_4 + {a_1}^2 a_4 + a_0 {a_3}^2 + a_1 a_2 a_3 + {a_2}^3;$$
$$b_3 = {a_0}^2 a_9 + a_0 a_1 a_8 + a_0 a_2 a_7 + a_0 a_4 a_5 + {a_1}^2 a_7 + a_1 a_2 a_6 + a_1 a_3 a_5 + a_1 {a_4}^2 + {a_2}^2 a_5 + a_2 a_3 a_4 + {a_3}^3.$$

Заметим, что слагаемого $a_0a_3a_6$ не будет, хотя оно удовлетворяет условию $0\cdot i_0+1\cdot i_1+2\cdot i_2=3\cdot r$, т.е. $1\cdot 0+1\cdot 3+1\cdot 6=3\cdot 3=9$, в силу сравнимости $m\equiv k\equiv l(\mathrm{mod}\,3)$ из утверждения 1.

$$b_4=a_0{}^2a_{12}+a_0a_6{}^2+a_0a_1a_{11}+a_0a_2a_{10}+a_0a_4a_8+a_0a_5a_7+a_1{}^2a_{10}+a_1a_2a_9+a_1a_3a_8+a_1a_5a_6+a_2{}^2a_8+$$
$$+a_2a_3a_7+a_2a_4a_6+a_2a_5{}^2+a_3{}^2a_6+a_3a_4a_5+a_4{}^3.$$

Заметим, что слагаемых $a_0a_3a_9$ и $a_1a_4a_7$ не будет в силу утверждения 1.

Также замечено, что количество слагаемых вида $a_ka_la_m$ в каждом из коэффициентов b_r есть простое число. Мы предполагаем, что и в остальных случаях количество слагаемых всегда будет простым числом. Очевиден факт, что количество слагаемых всегда нечётно.

Переход $x\to x^3$ программно реализован, приведем пример его использования. Возьмем изначальный неприводимый многочлен $x^{127}+x+1$, с помощью программы вычислим порожденные им неприводимые многочлены и несколько первых приведем ниже:

$$x^{127}+x^{85}+x^{43}+x+1,$$
$$x^{127}+x^{113}+x^{15}+x+1,$$
$$x^{127}+x^{113}+x^{80}+x^{38}+x^{15}+x^{10}+x^5+x+1,$$
$$x^{127}+x^{113}+x^{102}+x^{91}+x^{77}+x^{74}+x^{69}+x^{66}+x^{63}+x^{60}+x^{52}+x^{46}+x^{44}+x^{35}+x^{32}+x^{21}+x^{18}+x^{15}+$$
$$+x^{13}+x^{10}+x^5+x^4+x^2+x+1.$$

Дальнейшие многочлены получены, но не приведены здесь ввиду громоздкости.

2. Генерация неприводимых многочленов с помощью перехода $x\to x^5$

Имеем $b_r=\sum\limits_{i_0+i_1+i_2+i_3+i_4=5\cdot r} a_{i_0}a_{i_1}a_{i_2}a_{i_3}a_{i_4}\cdot\omega^{0\cdot i_0+1\cdot i_1+2\cdot i_2+3\cdot i_3+4\cdot i_4}$, где $\omega^5=1$, $\omega\neq 1$, $\omega^4+\omega^3+\omega^2+\omega+1=0$.

Рассмотрим пять случаев в зависимости от количества различных элементов в наборе индексов $\{i_0,i_1,i_2,i_3,i_4\}$.

1) Если все индексы одинаковы, $\left|\{i_0,i_1,i_2,i_3,i_4\}\right|=1$, то $i_0=i_1=i_2=i_3=i_4=r$, $0\cdot i_0+1\cdot i_1+2\cdot i_2+3\cdot i_3+4\cdot i_4=(1+2+3+4)\cdot r=10\cdot r\equiv 0(\mathrm{mod}\,5)$, $\omega^{10\cdot r}=1$, так что этот случай дает вклад слагаемого a_r^5 в сумму b_r, так как слагаемое с такими индексами единственное.

2) Если $\left|\{i_0,i_1,i_2,i_3,i_4\}\right|=2$, то либо четыре индекса равны k и отличны от пятого l, либо три индекса равны k и отличны от двух одинаковых l. Отсюда есть два подслучая: в первом (a) мы исследуем вхождение слагаемого $a_k^4a_l$, во втором (b) – вхождение слагаемого $a_k^3a_l{}^2$.

a. Исследуем вхождение слагаемого $a_k^4a_l$. $i_0+i_1+i_2+i_3+i_4=4k+l=5\cdot r\equiv 0(\mathrm{mod}\,5)$, откуда $(4k+l)-5k=(4k-4k)+(l-k)\equiv 0(\mathrm{mod}\,5)$, поэтому $l\equiv k(\mathrm{mod}\,5)$. Значит, $i_0\equiv i_1\equiv i_2\equiv i_3\equiv i_4\equiv k\equiv l(\mathrm{mod}\,5)$ и, следовательно, $0\cdot i_0+1\cdot i_1+2\cdot i_2+3\cdot i_3+4\cdot i_4=$ $=(1+2+3+4)\cdot k=10\cdot k\equiv 0(\mathrm{mod}\,5)$, $\omega^{10\cdot k}=1$. Поскольку числа k и l могут быть распределены по индексам i_0,i_1,i_2,i_3,i_4 пятью способами: $(kkkkl)$, $(kkkkl)$, $(kklkk)$, $(klkkk)$ и $(lkkkk)$, то, приводя подобные слагаемые, получаем $5\cdot a_k^4a_l=a_k^4a_l(\mathrm{mod}\,2)$. Значит, слагаемое $a_k^4a_l$ входит в сумму коэффициента b_r при условии $l\equiv k(\mathrm{mod}\,5)$ и $4k+l=5r$.

b. Исследуем вхождение слагаемого $a_k^3a_l{}^2$. Вычисления дают $i_0+i_1+i_2+i_3+i_4=$ $=3k+2l=5\cdot r\equiv 0(\mathrm{mod}\,5)$, откуда $(3k+2l)-5k=(3k-3k)+(2l-2k)=2l-2k$, т.е. $l\equiv k(\mathrm{mod}\,5)$. Отсюда $i_0\equiv i_1\equiv i_2\equiv i_3\equiv i_4\equiv k\equiv l(\mathrm{mod}\,5)$ и, следовательно, $0\cdot i_0+1\cdot i_1+2\cdot i_2+3\cdot i_3+4\cdot i_4=$ $=(1+2+3+4)\cdot k=10\cdot k\equiv 0(\mathrm{mod}\,5)$, $\omega^{10\cdot k}=1$. Поскольку числа k и l могут быть распределены $C_5^2=10$ способами, то приводя подобные слагаемые, получаем $10\cdot a_k^3a_l{}^2=0$, так как

$10 \equiv 0(\mathrm{mod}\,2)$. Значит, слагаемое $a_k^3 a_l{}^2$ не входит в сумму коэффициента b_r при условии $l \equiv k(\mathrm{mod}\,5)$ и $3k+2l=5r$.

3) Если $|\{i_0,i_1,i_2,i_3,i_4\}|=3$, то, обозначив различные числа через k, l и m, получаем следующие подслучаи, соответствующие значениям $a_k^3 a_l a_m$ и $a_k^2 a_l{}^2 a_m$.

a. Исследуем вхождение слагаемого $a_k^3 a_l a_m$. $i_0+i_1+i_2+i_3+i_4=3k+l+m=5\cdot r$, так что $(3k+l+m)-5k=(3k-3k)+(l-k)+(m-k)\equiv 0(\mathrm{mod}\,5)$, откуда $(l-k)\equiv -(m-k)(\mathrm{mod}\,5)$. Таким образом, имеем два варианта – либо число $(-(m-k))$ сравнимо с нулем, либо не сравнимо (по модулю пять). Распределить числа k, l и m по индексам i_0,i_1,i_2,i_3,i_4 можно $C_5^1\cdot C_4^1=5\cdot 4=20$ способами.

I. Пусть $(-(m-k))\equiv 0(\mathrm{mod}\,5)$, тогда $k-m\equiv 0(\mathrm{mod}\,5)$ и $k\equiv m(\mathrm{mod}\,5)$ и, как следствие, $l-k\equiv 0(\mathrm{mod}\,5)$ и $l\equiv k(\mathrm{mod}\,5)$, т.е. $k\equiv m\equiv l(\mathrm{mod}\,5)$. Получается, при приведении слагаемых будем иметь $20\cdot a_k^3 a_l a_m=0$, так как $20\equiv 0(\mathrm{mod}\,2)$, и **этого слагаемого не будет** в сумме коэффициента b_r при $k\equiv m\equiv l(\mathrm{mod}\,5)$.

II. Пусть $(-(m-k))\neq 0(\mathrm{mod}\,5)$, откуда $m\neq k(\mathrm{mod}\,5)$, тогда составим табл. 3 разностей номеров индексов, отличных от k.

Таблица 3

Разности номеров индексов

$m-k$	0	1	2	3	4
0	0	1	2	3	4
1	4	0	1	2	3
2	3	4	0	1	2
3	2	3	4	0	1
4	1	2	3	4	0

В таблице не учитываются нули по диагонали, потому что $m\neq k(\mathrm{mod}\,5)$. Таким образом, видно, что сомножителей в первой степени $(\omega^{(m-k)})^1$ будет пять (они выделены в таблице), также по пять будет сомножителей второй, третьей и четвертой степеней, откуда имеем:

$$a_k^3 a_l a_m\cdot[5\cdot(\omega^{(m-k)})^4+5\cdot(\omega^{(m-k)})^3+5\cdot(\omega^{(m-k)})^2+5\cdot(\omega^{(m-k)})^1].$$

Так как любая степень $z=\omega^{(m-k)}$ удовлетворяет тому же уравнению $z^4+z^3+z^2+z=1$, то и выражение в квадратных скобках равно единице. Это означает, что слагаемое $a_k^3 a_l a_m$ будет входить в сумму коэффициента b_r при условии $l\neq m\neq k\neq l$.

b. Исследуем вхождение одночлена $a_k^2 a_l{}^2 a_m$. Имеем $i_0+i_1+i_2+i_3+i_4=2k+2l+m=5\cdot r$, так что $(2k+2l+m)-5m=2(k-m)+2(l-m)+(m-m)\equiv 0(\mathrm{mod}\,5)$, откуда $(k-m)\equiv -(l-m)(\mathrm{mod}\,5)$. Распределить числа k, l и m по индексам i_0,i_1,i_2,i_3,i_4 можно $C_5^2\cdot C_3^2=10\cdot 3=30$ способами.

I. Пусть $(-(l-m))\equiv 0(\mathrm{mod}\,5)$, тогда $m-l\equiv 0(\mathrm{mod}\,5)$ и $m\equiv l(\mathrm{mod}\,5)$ и, как следствие, $k-m\equiv 0(\mathrm{mod}\,5)$ и $k\equiv m(\mathrm{mod}\,5)$, т.е. $k\equiv m\equiv l(\mathrm{mod}\,5)$. Получается, при приведении слагаемых будем иметь $30\cdot a_k^2 a_l{}^2 a_m=0(\mathrm{mod}\,2)$ и слагаемого $a_k^2 a_l{}^2 a_m$ не будет в сумме коэффициента b_r при $k\equiv m\equiv l(\mathrm{mod}\,5)$.

II. Пусть $(-(l-m))\neq 0(\mathrm{mod}\,5)$, тогда необходимо понять, сколько слагаемых $(\omega^{(k-l)})$ будет не сравнимо с нулем. Для этого обозначим номера индексов следующим образом: $i_u=k$, $i_v=k$, $i_p=l$, $i_q=l$, $i_w=m$. Пусть $\{u,v,p,q,w\}=\{0,1,2,3,4\}$, $\{u,v\}\cap\{p,q\}=\varnothing$ и $u+v+p+q+w\equiv 0(\mathrm{mod}\,5)$, так что $(0i_0+1i_1+2i_2+3i_3+4i_4)-10l=0(i_0-l)+1(i_1-l)+2(i_2-l)+$ $+3(i_3-l)+4(i_4-l)=u(k-l)+v(k-l)+p(l-l)+q(l-l)+w(m-l)=v(u+v)\cdot(k-l)+w(m-l)=(u+v)\cdot(k-l)+$ $+3w\cdot(k-l)=(k-l)\cdot((u+v)+3w)$ потому что $2k+2l+m=5r$; вычтя из этого выражения $5l$, получим: $2(k-l)+2(l-l)+(m-l)=2(k-l)+(m-l)$, откуда имеем сравнение $(m-l)\equiv -2(k-l)\equiv 3(k-l)(\mathrm{mod}\,5)$. Поэтому нужно вычислить выражение $((u+v)+3w)$, результаты приведены в табл. 4.

Получили 30 слагаемых, соответствующих различным степеням элемента $\omega^{(k-l)}$, из которых нулевой степени – 10 (по количеству нулей в таблице), а первой, второй, третьей и четвертой степеней – по 5. Отсюда можно записать следующее равенство:

$$a_k^2 a_l{}^2 a_m\cdot[10\cdot(\omega^{(k-l)})^0+5\cdot(\omega^{(k-l)})^1+5\cdot(\omega^{(k-l)})^2+5\cdot(\omega^{(k-l)})^3+5\cdot(\omega_k^{(k-l)}{}_l)_m^4]=a^2a^2a\quad\cdot 1.$$

Таблица 4

Суммы номеров индексов по модулю пять

w	u	v	$((u+v)+3w)$	w	u	v	$((u+v)+3w)$	w	u	v	$((u+v)+3w)$
0	1	2	3	1	2	4	4	3	0	4	3
0	1	3	4	1	3	4	0	3	1	2	2
0	1	4	0	2	0	1	2	3	1	4	4
0	2	3	0	2	0	3	4	3	2	4	0
0	2	4	1	2	0	4	0	4	0	1	3
0	3	4	2	2	1	3	0	4	0	2	4
1	0	2	0	2	1	4	1	4	0	3	0
1	0	3	1	2	3	4	3	4	1	2	0
1	0	4	2	3	0	1	0	4	1	3	1
1	2	3	3	3	0	2	1	4	2	3	2

Так как любая степень $z=\omega^{(k-l)}$ удовлетворяет уравнению $z^4+z^3+z^2+z=1$, а $10\cdot(\omega^{(k-l)})^0=0$, то выражение в квадратных скобках равно единице. Это означает, что слагаемое $a_k^2 a_l{}^2 a_m$ будет входить в сумму коэффициента b_r при условии $l\neq m\neq k\neq l(\mathrm{mod}\,5)$.

4) Если $\left|\{i_0,i_1,i_2,i_3,i_4\}\right|=4$, то, обозначив различные четыре числа через k, l, m, n, получим (без ограничения общности) единственный одночлен $a_k^2 a_l a_m a_n$, для которого имеем $2k+l+m+n=5r$, вычтя из этого равенства $5k$, мы получаем $(2k-2k)+(l-k)+$ $+(m-k)+(n-k)\equiv 0(\mathrm{mod}\,5)$, откуда $(l-k)+(m-k)+(n-k)\equiv 0(\mathrm{mod}\,5)$ и $(n-k)=-(l-k)-(m-k)$. Обозначим номера индексов следующим образом: $i_u=l$, $i_v=m$, $i_w=n$, так что

$$(0i_0+1i_1+2i_2+3i_3+4i_4)-10k=0(i_0-k)+1(i_1-k)+2(i_2-k)+3(i_3-k)+4(i_4-k)=$$
$$=u(l-k)+v(m-k)+w(n-k)=(u-w)\cdot(l-k)+(v-w)\cdot(m-k)(\mathrm{mod}\,5).$$

a. Обозначим $l-k\equiv\alpha(\mathrm{mod}\,5)$, $m-k\equiv\beta(\mathrm{mod}\,5)$, и тогда $n-k\equiv-(\alpha+\beta)\equiv\gamma(\mathrm{mod}\,5)$. Если не все вычеты α, β, γ различны, то при α=β=γ имеем сравнимость всех этих трёх индексов k,l,m, и такое слагаемое не входит, очевидно, в искомую сумму, а при α=β≠γ получаем степень элемента ω, равную $(u+v-2w)\alpha$. Осуществляя транспозицию u-го и v-го элемента, получаем слагаемое с той же степенью элемента ω, так что эти слагаемые взаимно уничтожатся. Следовательно, если $l\equiv m$, $l\equiv n$ или $n\equiv m$, то такого слагаемого **не будет** в сумме для коэффициента b_r. Если же все вычеты α,β,γ различны и не равны нулю, то мы имеем все ненулевые вычеты: $\{\alpha,\beta,\gamma,\delta\}=\{1,2,3,4\}$. Сумма всех четырех разных ненулевых вычетов по модулю пять равна десяти и сравнима с нулем: $\alpha+\beta+\gamma+\delta=1+2+3+4=10\equiv 0(\mathrm{mod}\,5)$. Отсюда $\alpha+\beta+\gamma=-\delta(\mathrm{mod}\,5)$, и так как $\alpha+\beta+\gamma\equiv 0(\mathrm{mod}\,5)$, то $-\delta\equiv 0(\mathrm{mod}\,5)$ и $\delta\equiv 0(\mathrm{mod}\,5)$, что неверно, потому что δ – это ненулевой вычет. Следовательно, среди вычетов α, β, γ есть один нулевой, обозначим его через $\gamma=0$. Тогда получаем $\alpha+\beta\equiv 0(\mathrm{mod}\,5)$ и $0i_0+1i_1+2i_2+3i_3+4i_4=u(l-k)+v(m-k)+0=u\cdot\alpha+v\cdot\beta(\mathrm{mod}\,5)$, так как $\gamma=n-k=0$ и $w(n-k)=0$. При этом возможно 2 варианта: когда $\beta\equiv 0(\mathrm{mod}\,5)$ и когда $\beta\neq 0(\mathrm{mod}\,5)$.

b. Исследуем вариант, когда $\beta\equiv 0(\mathrm{mod}\,5)$. Если $\beta\equiv 0(\mathrm{mod}\,5)$, то и $\alpha\equiv 0(\mathrm{mod}\,5)$, тогда $0i_0+1i_1+2i_2+3i_3+4i_4\equiv 0(\mathrm{mod}\,5)$, значит $\omega^0=1$. Распределить числа k, l, m и n по индексам i_0,i_1,i_2,i_3,i_4 можно $5\cdot 4\cdot 3=60$ способами. Получается шестьдесят равных единице слагаемых, т.е. нуль в поле $GF(2)$. Таким образом, если $l\equiv m\equiv k\equiv l(\mathrm{mod}\,5)$ и $2k+l+m+n=5r$, то одночлен $a_k^2 a_l a_m a_n$ не входит в сумму для коэффициента b_r.

c. Исследуем вариант, когда $\beta\neq 0(\mathrm{mod}\,5)$. Тогда $\alpha\equiv-\beta\neq 0(\mathrm{mod}\,5)$ и при каждых $u\neq v$ имеется 3 слагаемых (соответствующих выбору w из оставшихся номеров индексов), поэтому получаем $60/3=20$ слагаемых для подобных членов вида

$$a_k^2 a_l a_m a_n\sum_{u\neq v}\omega^{u\cdot\alpha+v\cdot\beta}=a_k^2 a_l a_m a_n\sum_{u=0}^{4}\omega^{u\cdot\alpha}\sum_{v\in\{u+1,u+2,u+3,u+4\}}\omega^{v\cdot\beta}.$$

Поскольку $\sum_{v=0}^{4}(\omega^\beta)^v=0$, $\omega^0=1$, то $\sum_{u\neq v(\mathrm{mod}\,5)}(\omega^\beta)^v=\omega^{\beta\cdot u}$, так что получаем

$$a_k^2 a_l a_m a_n \sum_{u \neq v} \omega^{u\cdot\alpha+u\cdot\beta} = a_k^2 a_l a_m a_n \sum_{u=0}^{4} \omega^{u\cdot(\alpha+\beta)} = 5\cdot a_k^2 a_l a_m a_n .$$

В силу нечетности числа 5 приходим к выводу, что если $2k+l+m+n=5r$, причем $l \neq k(\mathrm{mod}5)$, либо $m \neq k(\mathrm{mod}5)$, либо $n \neq k(\mathrm{mod}5)$, то одночлен $a_k^2 a_l a_m a_n$ будет входить в сумму коэффициента b_r.

5) Если $\left|\{i_0,i_1,i_2,i_3,i_4\}\right|=5$, то пусть $\{i_0,i_1,i_2,i_3,i_4\}=\{j,k,l,m,n\}$. Имеем $j+k+l+m+n=5r\equiv 0(\mathrm{mod}5)$, и эти разные числа можно распределить по индексам i_0,i_1,i_2,i_3,i_4 соответственно всем 5!=120 подстановкам на пяти элементах. Приведем эти числа по модулю пять: $j=\bar{j}(\mathrm{mod}5)$, $k=\bar{k}(\mathrm{mod}5)$, $l=\bar{l}(\mathrm{mod}5)$, $m=\overline{m}(\mathrm{mod}5)$, $n=\overline{n}(\mathrm{mod}5)$. Получается набор по мощности множества: $\{\bar{j},\bar{k},\bar{l},\overline{m},\overline{n}\}=\{\overline{i_0},\overline{i_1},\overline{i_2},\overline{i_3},\overline{i_4}\}$.

a. Если эта мощность меньше пяти, например, $k\equiv l(\mathrm{mod}5)$ (т.е. $\bar{k}=\bar{l}$), то, так как наборы $\{j,k,l,m,n\}$ и $\{k,j,l,m,n\}$ считаем разными, они дают одинаковую степень для ω, что в итоге приводит к сумме четного количества слагаемых, а это – нуль над полем из двух элементов. Таким образом, при наличии каких-либо сравнимостей между индексами слагаемое $a_j a_k a_l a_m a_n$ не входит в сумму для коэффициента b_r.

b. Если же мощность равна пяти, т.е. все числа j, k, l, m и n не сравнимы по модулю пять, $\{j,k,l,m,n\}\equiv\{0,1,2,3,4\}(\mathrm{mod}5)$, то все подстановки индексов распадаются на орбиты из пяти элементов $j\to j+1(\mathrm{mod}5)$, $k\to k+1(\mathrm{mod}5)$ и т.д., на которых степени ω инвариантны. В табл. 5 приведены все степени (S=0j+1k+2l+3m+4n) такие, что $i_0=4$.

Таблица 5

Вычисление степеней корня из единицы

j	k	l	m	n			j	k	l	m	n		
0	1	2	3	4	S	S (mod 5)	0	1	2	3	4	S	S (mod 5)
4	0	1	2	3	20	0	4	1	2	0	3	17	2
4	0	1	3	2	19	4	4	1	3	0	2	15	0
4	0	2	1	3	19	4	4	2	1	0	3	16	1
4	0	2	3	1	17	2	4	2	3	0	1	12	2
4	0	3	1	2	17	2	4	3	1	0	2	13	3
4	0	3	2	1	16	1	4	3	2	0	1	11	1
4	1	0	2	3	19	4	4	1	2	3	0	14	4
4	1	0	3	2	18	3	4	1	3	2	0	13	3
4	2	0	1	3	17	2	4	2	1	3	0	13	3
4	2	0	3	1	15	0	4	2	3	1	0	11	1
4	3	0	1	2	14	4	4	3	1	2	0	11	1
4	3	0	2	1	13	3	4	3	2	1	0	10	0

Таким образом, получили четыре значения нулевой степени и по пять значений ненулевых степеней. Следовательно, получаем сумму:

$$4\omega^0+5\omega^1+5\omega^2+5\omega^3+5\omega^4=\omega+\omega^2+\omega^3+\omega^4=1 \text{ в поле } GF(2).$$

Итак, одночлен $a_j a_k a_l a_m a_n$ входит в сумму для коэффициента b_r при отсутствии сравнимостей между индексами по модулю пять.

Получаем

Утверждение 2: Одночлен $a_j a_k a_l a_m a_n$ входит в сумму для коэффициента b_r тогда и только тогда, когда:

1) либо когда $j=k=l=m=n=r$, и тогда одночлен имеет вид a_r^5;

2) либо когда $l\neq k$, $l\equiv k(\mathrm{mod}5)$ и $4k+l=5r$, и тогда одночлен имеет вид $a_k^4 a_l$;

3) либо когда $l\neq m\neq k\neq l$, $l\neq m\neq k\neq l(\mathrm{mod}5)$, и тогда одночлен имеет вид $a_k^2 a_l{}^2 a_m$ (при $2k+2l+m=5r$) или $a_k^3 a_l a_m$ (при $3k+l+m=5r$);

4) либо когда все четыре индекса различны, и либо $l \neq k(\mathrm{mod}5)$, либо $m \neq k(\mathrm{mod}5)$, либо $n \neq k(\mathrm{mod}5)$, причём $2k+l+m+n=5r$, $l \neq m \neq n \neq l(\mathrm{mod}5)$, тогда одночлен имеет вид $a_k^2 a_l a_m a_n$;

5) либо когда все индексы не равны и не сравнимы между собой по модулю пять, и тогда одночлен имеет вид $a_j a_k a_l a_m a_n$, причём $j+k+l+m+n=5r$.

Выпишем для примера первые три коэффициента порождаемого многочлена, найденные согласно утверждению 2:

$$c_0 = {a_0}^5;$$

$$c_1 = {a_0}^4 a_5 + {a_0}^3 a_1 a_4 + {a_0}^3 a_2 a_3 + {a_1}^3 a_2 a_0 + {a_0}^2 {a_2}^2 a_1 + {a_0}^2 {a_1}^2 a_3 + {a_1}^5;$$

$$c_2 = {a_0}^4 a_{10} + a_9 a_1 {a_0}^3 + a_8 a_2 {a_0}^3 + a_8 {a_1}^2 {a_0}^2 + a_7 a_3 {a_0}^3 + a_7 {a_1}^3 a_0 + a_6 a_4 {a_0}^3 + {a_2}^2 {a_0}^2 a_6 + a_6 a_2 {a_1}^2 a_0 +$$
$$+ a_6 {a_1}^4 + a_5 a_4 a_1 {a_0}^2 + a_5 a_3 a_2 {a_0}^2 + a_5 a_2 {a_1}^3 + a_4 {a_3}^2 {a_0}^2 + a_4 a_3 a_2 a_1 a_0 + a_4 a_3 {a_1}^3 + {a_4}^2 a_2 {a_0}^2 +$$
$$+ {a_4}^2 a_0 {a_1}^2 + a_4 a_0 {a_2}^3 + a_4 {a_1}^2 {a_2}^2 + a_0 {a_2}^2 {a_3}^2 + a_2 {a_3}^2 {a_1}^2 + {a_3}^3 a_1 a_0 + a_3 a_1 {a_2}^3 + {a_2}^5.$$

Отметим, что согласно вышеприведённому анализу в последней сумме опущены слагаемые: ${a_5}^2 {a_0}^3$, $a_7 a_2 a_1 {a_0}^2$, $a_6 a_1 a_3 {a_0}^2$, $a_5 a_3 a_0 {a_1}^2$, $a_5 a_0 a_1 {a_2}^2$.

Во многих алгоритмах шифрования используется генератор псевдослучайных последовательностей. На основании преобразований, изложенных выше в виде Утверждения 1, в работе [13] был предложен генератор ПСП, который при его анализе показал высокие результаты тестирования [14, 15].

В силу утверждений 1 и 2 и на основании доказательств из [16] приведем теорему.

Теорема. Если степень многочлена – число Мерсенна, а его порядок d – простое число Мерсенна, причем p – первообразный корень по модулю d, то получаем все возможные многочлены при переборе вида $x \to x^p$.

Имея подробные описания переходов $x \to x^3$ и $x \to x^5$, появляется возможность осуществлять переход $x \to x^p$ в несколько этапов посредством разложения p на множители 3 и 5. Например, переход $x \to x^{15}$ возможно осуществить в два этапа – сначала сделав преобразование $x \to x^3$, а затем $x \to x^5$.

Заключение

Утверждения 1 и 2 пригодны для программной реализации алгоритма построения неприводимого многочлена $f_p(z)$ по неприводимому многочлену $f(x)$ со степенной связью их корней $z = x^p$. Эти алгоритмы реализованы, апробация показала их эффективность.

Изложенный метод может быть использован для алгоритмизации построения неприводимого многочлена $f_p(z)$ со связью корней $z = x^p$ при таких p, что p – простое число, по модулю которого двойка является первообразным корнем, так что многочлен $F(\omega) = \omega^{t-1} + \omega^{t-2} + \ldots + \omega + 1 = 0$ неприводим над GF(2) и все его корни есть все неединичные корни p-й степени из единицы. Это дает возможность построения общего алгоритма нахождения неприводимых многочленов с общей степенной связью корней $z = x^p$ при таких значениях p, что p – простое число.

Автор благодарит рецензента за конструктивные замечания.

Литература

1. Логарифм Зеха-Якоби в задаче расшифровки / А.В. Торгашова, С.С. Титов, О.М. Баданова, М.А. Ициксон // Проблемы теоретической и прикладной математики: труды 33-й рег. молодежной конф. – Екатеринбург: УрО РАН, 2002. – С. 51–55.

2. Яковлев В.В. Информационная безопасность и защита информации в корпоративных сетях железнодорожного транспорта: учеб. для вузов ж.-д. транспорта / В.В. Яковлев, А.А. Корниенко. – М.: УМК МПС России, 2002. – 328 с.

3. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы и исходные тексты на языке С+. – М.: Триумф, 2002. – 816 с.

4. Логачев О.А. Булевы функции в теории кодирования и криптологии / О.А. Логачев, А.А. Сальников, В.В. Ященко. – М.: МЦНМО, 2004. – 470 с.

5. Элементарное введение в эллиптическую криптографию: Алгебраические и алгоритмические основы / А.А. Болотов, С.Б. Гашков, А.Б. Фролов, А.А. Часовских. – М.: КомКнига, 2006. – 328 с.

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

7. Берлекемп Е. Алгебраическая теория кодирования. – М.: Мир, 1971. – 478 с.

8. Демкина О.Е. Некоторые задачи полиномиального кодирования // Безопасность информационного пространства: матер. рег. конф. – Екатеринбург: ГОУ ВПО УГТУ–УПИ, 2003. – С. 12–13.

9. Торгашова А.В. Рекуррентное вычисление неприводимых многочленов в задачах двоичного кодирования / А.В. Торгашова, С.С. Титов, О.Е. Демкина // Молодые ученые – транспорту: труды IV науч.-техн. конф. – Екатеринбург: УрГУПС, 2003. – С. 391–401.

10. Экстремальные задачи полиномиального кодирования / А.В. Торгашова, С.С. Титов, Л.М. Моклокова и др. // Проблемы теоретической и прикладной математики: труды 35-й рег. молодежной конф. – Екатеринбург: УрО РАН, 2004. – С. 46–50.

11. Лидл Р. Конечные поля / Р. Лидл, Г. Нидеррайтер: В 2 т. – Т. 1. – М.: Мир, 1988. – 820 с.

12. Торгашова А.В. Рекуррентное вычисление коэффициентов степеней экспоненты / А.В. Торгашова, С.С. Титов, О.Е. Демкина // Проблемы теоретической и прикладной математики: труды 34-й рег. молодежной конф. – Екатеринбург: УрО РАН, 2003. – С. 27–30.

13. Усольцев А.В. Проектирование и оценка качества генератора псевдослучайных последовательностей // Проблемы прикладной математики: сб. науч. трудов: в 2 т. / Под общ. ред. д-ра физ.-мат. наук С.Л. Дерябина / УрГУПС (Екатеринбург). – 2006. – № 41(124), т. 2. – С. 24–49.

14. Ткачук С.А. Исследование периода генератора псевдослучайных последовательностей BBS последовательностей // Проблемы прикладной математики: сб. науч. трудов: в 2 т. / Под общ. ред. д-ра физ.-мат. наук С.Л. Дерябина / УрГУПС (Екатеринбург). – 2006. – № 41(124), т. 2. – С. 194–219.

15. Иванов М.А. Теория, применение и оценка качества генераторов псевдослучайных последовательностей / М.А. Иванов, И.В. Чугунков. – М.: КУДИЦ-ОБРАЗ, 2003. – С. 240.

16. Асимметрические криптосистемы на основе алгебры многочленов / О.Е. Демкина, М.А. Ициксон, А.В. Торгашова, С.С. Титов // Проблемы теоретической и прикладной математики: труды 36-й рег. молодежной конф. – Екатеринбург: УрО РАН, 2005. – С. 26–30.

Титов Сергей Сергеевич
Д-р физ.-мат. наук, проф. каф. прикладной математики
Уральского государственного университета путей сообщения (УрГУПС), г. Екатеринбург
Тел.: (343-3) 58-55-50
Эл. почта: sergey.titov@usaaa.ru

Торгашова Александра Викторовна
Аспирант каф. прикладной математики УрГУПС
Тел.: (343-3) 58-55-50
Эл. почта: atorgashova@gmail.com.

Titov S.S., Torgashova A.V.
Generation of irreducible polynomials related by power dependence of the roots

A method, which is intended for obtaining new irreducible polynomials from the given irreducible polynomial of the same degree provided the roots of these polynomials are related by power dependence, is considered. The method is used in cryptography and coding theory. The expressions for generation of such polynomials are given.
Keywords: irreducible polynomial, coding, modulo comparability, polynomial degree, polynomials generation algorithm, coefficient.