Ермилов И.М.
Произведение линейных рекуррентных последовательностей

Научный руководитель: к.ф-м.н. Богонатов Р.В.

1 Введение

В курсовой работе исследуются ранги произведений линейных рекуррентных последовательностей с одним характеристическим многочленом $f(x)$ над полем $GF(2)$. В работе изучены различные оценки ранга полученной последовательности.

Пусть даны две бесконечные последовательности над произвольным полем $GF(q)$

$$u = (u(1), u(2), u(3), ..., u(n), ...)$$

$$v = (v(1), v(2), v(3), ..., v(n), ...)$$

Пусть S — пространство над полем $GF(q)$, состоящее из всех последовательностей над полем $GF(q)$. И пусть $f_1(x), ..., f_n(x)$ — нормированные многочлены над $GF(q)$, не являющиеся константами и пусть $S(f_1(x)) \cdot ... \cdot S(f_n(x))$ - подпространство пространства S, порожденное всеми произведениями вида:

$$u_1...u_n, u_i \in S(f_i(x)), i = 1, ..., n.$$

Известно [1], что для любого конечного числа произведений семейств линейных рекуррентных последовательностей существует такой многочлен $g(x)$, что

$$S(f_1(x)) \cdot ... \cdot S(f_n(x)) = S(g(x))$$

Далее в работе будет рассмотрен случай

$$f_1(x) = f_2(x) = ... = f_n(x)$$

.

Выберем $u \in S(f(x)$, $t \in \mathbb{N}$ и построим последовательность:

$$w(i) = u(i) \cdot u(i+1) \cdot ... \cdot u(i+t-1), i \geq 0. \quad (1)$$

В 1973 году В.И.Нечаева сформулировал гипотезу, которая заключается в том,, что

$$rang\, w = \binom{m}{1} + \binom{m}{2} + ... + \binom{m}{t} \qquad (2)$$

В 2005 году Богонатов Р.В. в своей работе [2] опровергнул эту гипотезу.

В рамках работы использовался алгоритм Берлекэмпа-Мэсси нахождения минимального многочлена отрезка над полем, с помощью которого были найдены ранги последовательностей w для $t = 4$ для многочленов степени $n \in \overline{4, 11}$ и $t = 5$ для многочленов степени $n \in \overline{4, 9}$. Восстановлена полная таблица примеров, опровергающих гипотезу В.И.Нечаева для $t = 4$, $n \in \overline{4, 11}$ и $t = 5$, $n \in \overline{4, 9}$.

2 Произведение линейных рекуррент

Для того, чтобы описать многочлен $g(x)$ ведем понятие дизъюнкции многочленов.

Определение 1. Пусть $f_1(x), ..., f_n(x)$ - нормированные многочлены над $GF(q)$, не являющиеся константами. Определим $f_1(x) \vee ... \vee f_n(x)$ как нормированный многочлен, корни которого являются различными элементами вида $\alpha_1 ... \alpha_n$, где α_i — корень многочлена $f_i(x)$, $i \in \overline{1, n}$ из поля разложения многочлена $f_1(x)...f_n(x)$ над полем $GF(q)$.

В [1] имеется уточнение теоремы **??**

Теорема 2. *Пусть $f_i(x), i = \overline{1, n}$ — нормированные многочлены над полем $GF(q)$ не имеющие кратных корней и не являющиеся константами. Тогда справедливо следующее равенство:*

$$S(f_1(x))...S(f_n(x)) = S(f_1(x) \vee ... \vee f_n(x)) \qquad (3)$$

Зафиксируем $t \geq 2$ и рассмотрим последовательность w со знаками

$$w(i) = u(i) \cdot u(i + 1) \cdot ... \cdot u(i + t - 1), i \geq 0 \qquad (4)$$

где $u \in S(f(x)) \backslash (0)$ — ЛРП максимального периода над полем $GF(q)$, ранга m. А $f(x) \in GF(q)[x]$ — нормированный, не являющийся константой.

Определим $f(x) \vee ... \vee f(x) (t$ раз), как многочлен равный наименьшему общему кратному многочленов $(x - \alpha_1 \cdot ... \cdot \alpha_t)$, где $\alpha_i, i \in \overline{1, t}$ — корни многочлена $f(x)$ в его поле разложения([1],[7]). Многочлен $f(x) \vee ... \vee f(x)(t$ раз) является характеристическим многочленом последовательности w [7].

В работе [2] сказано, что при $q = 2$ и $t \leq m$ степень многочлена $(f(x) \vee ... \vee f(x)(t$ раз) равна $\binom{m}{1} + \binom{m}{2} + ... + \binom{m}{t}$.

В 1973 года В.И. Нечаев сформулировал гипотезу о том, что при $t \leq m$ и $q = 2$ ранг последовательности (4) будет в точности равен

$$rang\, w = \binom{m}{1} + \binom{m}{2} + ... + \binom{m}{t} \tag{5}$$

то есть многочлен $f(x) \vee ... \vee f(x)(t$ раз) является ее минимальным многочленом. Также, В.И.Нечаев показал, что для $t = 2, t = 3$ это предположение верно.

А.А.Нечаевым гипотеза была доказана для $t = 2$ и произвольного q. Также им была получена следующая оценка ранга последовательности w при $q = 2^n, t \leq q, t \leq m$, $n \in \mathbb{N}$

$$rang\, w \geq \binom{m}{1} + \binom{m}{t} \tag{6}$$

Затем, В.Л.Куракиным оценка была уточнена

$$rang\, w \geq \binom{m}{1} + (t-1)\binom{m}{2} + \binom{m}{t} \tag{7}$$

В работе [2] Р.В.Богонатова было приведено следующее утверждение для произвольного поля $GF(q)$, $q \leq t$:

Утверждение 3. *Пусть $f(x)$ — многочлен максимального периода над полем $GF(q)$ степени m, $u \neq 0$ — линейная рекуррентная последовательность с характеристическим многочленом $f(x)$, $t \geq 2$, и последовательность w, вида (4). Тогда при условиях $t \leq m$, $t \leq q$*

$$rang\, w \geq \binom{m}{1} + (t-1)\binom{m}{2}$$

Также, в этой статье можно найти несколько примеров, где ранг полученной последовательности w не равен $\binom{m}{1} + \binom{m}{2} + ... + \binom{m}{t}$, что опровергло гипотезу В.И.Нечаева.

3 Алгоритм Берлекэмпа-Мэсси

Определение 4. Пусть дана последовательность u над полем P(не обязательно конечным). Назовем

$$u(\overline{0,n}) = (u(0), u(1), ..., u(n-1))$$

отрезком длины n последовательности u.

Введем понятие минимального многочлена отрезка и свяжем его с минимальным отрезком ЛРП.

Определение 5. Дан отрезок $u(\overline{0,n})$ длины n над полем P. Говорят, что нормированный многочлен $f(x) = x^s - c_{s-1}x^{s-1} - ... - c_1 x - c_0$, $f(x) \in P[x]$ порождает отрезок $u(\overline{0,n})$, если $s \geq n$ или $s < n$ и

$$u(i+s) = c_{s-1}u(i+s-1) + ... + c_1 u(i+1) + c_0 u(i) i \in \overline{0, n-s-1} \quad (8)$$

Нормированный многочлен наименьшей степени, порождающий отрезок, назовем минимальным многочленом, а степень этого многочлена — рангом отрезка. Из определения следует, что ранг отрезка не превосходит его длины. Сумма и умножение на константу определяется аналогично сумме и произведению последовательностей.

Сдвигом отрезка $u(\overline{0,n})$ на s шагов, $s \in \overline{0, n-1}$, будем называть отрезок

$$x^s u(\overline{0,n}) = (u(s), ..., u(l-1))$$

над полем P длины $n - s$.

В работе [3] приведено следующее утверждение

Утверждение 6. *Пусть u — ЛРП порядка m над кольцом K. Унитарный многочлен $f(x) \in R[x]$ является минимальным многочленом ЛРП тогда и только тогда, когда он является минимальным многочленом отрезка $u(\overline{0, 2m-1})$*

Очевидно, данный факт верен и для полей.

Алгоритм 7. *На вход алгоритма поступает отрезок $u_s(\overline{0, n-1})$ длины n над полем P. На выходе алгоритма мы наблюдаем минимальный многочлен $m(x) \in P[x]$ входящего отрезка.*

Пример. Пусть $q = 2$, $f(x) = x^4 + x^2 + 1 \in GF(2)[x]$, начальное заполнение $u(\overline{0,3}) = (0, 1, 1, 0)$ и $d = 8$.

На выходе алгоритм дает следующие результаты:

$$u(\overline{0,8}) = (0,1,1,0,1,1,0,1)$$

$$m(x) = x^2 + x + 1$$

Проверим данные результаты, согласно алгоритму 7. Для этого составим таблицу Table, указанную в алгоритме. Количество лидирующих нулей будем держать в уме, в виду очевидности.

s	$u_s(\overline{n-s-1})$	$f_s(x)$
1:	0,$\underline{1}$,1,0,1,1,0,1	1
2:	$\underline{1}$,1,0,1,1,0,1	x
3:	$\underline{1}$,0,1,1,0,1	x^2
	0,$\underline{1}$,1,0,1,1	
	0,0,0,0,0,0	

Таким образом, мы видим, что $f_s(x) = m(x) = x^2 + x + 1$.

4 Опровержение гипотезы В.И.Нечаева

Приведем новый пример в доказательство того, что гипотеза В.И.Нечаева не верна.

Пример. Пусть $P = GF(2)$ и $t = 4$(число дизъюнкций многочлена $f(x)$), $f(x) = x^9 + x^7 + x^6 + x^5 + x^4 + x^2 + 1$. В качестве $u \in S(f(x))$ возьмем импульсную последовательность с начальным вектором $u(\overline{0,8}) = (0,0,0,0,0,0,0,0,1)$. Данная линейная рекуррентная последовательность является последовательностью максимального периода $T = 511$.

Минимальный многочлен данной последовательности w равен $m(x) = 1+x+x^2+x^6+x^9+x^{13}+x^{15}+x^{17}+x^{18}+x^{21}+x^{22}+x^{24}+x^{26}+x^{31}+x^{32}+ x^{33}+x^{35}+x^{37}+x^{38}+x^{39}+x^{41}+x^{42}+x^{46}+x^{48}+x^{49}+x^{50}+x^{53}+x^{55}+ x^{58}+x^{61}+x^{62}+x^{66}+x^{68}+x^{69}+x^{70}+x^{73}+x^{74}+x^{75}+x^{76}+x^{77}+x^{79}+ x^{88}+x^{89}+x^{91}+x^{93}+x^{94}+x^{97}+x^{98}+x^{99}+x^{101}+x^{102}+x^{104}+x^{105}+x^{108}+ x^{109}+x^{110}+x^{112}+x^{114}+x^{115}+x^{116}+x^{117}+x^{118}+x^{119}+x^{121}+x^{122}+ x^{123}+x^{124}+x^{125}+x^{126}+x^{127}+x^{128}+x^{129}+x^{131}+x^{133}+x^{134}+x^{135}+x^{141}+ x^{144}+x^{145}+x^{156}+x^{158}+x^{159}+x^{160}+x^{163}+x^{167}+x^{168}+x^{173}+x^{175}+x^{177}+ x^{179}+x^{181}+x^{182}+x^{184}+x^{185}+x^{187}+x^{188}+x^{189}+x^{190}+x^{191}+x^{194}+x^{196}+ x^{199}+x^{200}+x^{201}+x^{202}+x^{203}+x^{204}+x^{206}+x^{210}+x^{213}+x^{215}+x^{216}+x^{221}+ x^{225}+x^{226}+x^{227}+x^{228}+x^{229}+x^{233}+x^{239}+x^{240}+x^{248}+x^{249}+x^{251}+x^{252}$

Согласно гипотезе В.И.Нечаева ранг полученной последовательности w должен быть равен 255. Однако, $rang\, w = 252$, что и является опровержением гипотезы В.И.Нечаева.

Обозначим за $H_n^{(t)}$ — число неприводимых многочленов максимального периода степени n, не удовлетворяющих гипотезе В.И.Нечаева для заданного t и H_n — общее число неприводимых многочленов максимального периода степени n. Теперь приведем таблицу, в которой будет указано число H_n и $H_n^{(t)}$ для $t = 4$, $n \in \overline{5, 11}$ и $t = 5$, $n \in \overline{7, 9}$.

t	n	H_n	$H_n^{(t)}$
4	5	6	0
4	6	6	2
4	7	18	2
4	8	16	2
4	9	45	8
4	10	60	0
4	11	175	2
5	6	6	0
5	7	18	0
5	8	16	6
5	9	45	6

Таким образом, можно сделать вывод, что среди всех неприводимых многочленов максимального периода можно выделить такие многочлены, для которых гипотеза В.И.Нечаева не верна, то есть $rang\, w \geq \binom{m}{1} + \binom{m}{2} + ... + \binom{m}{t}$.

Теперь выпишем в отдельную таблицу все многочлены из множества $H_n^{(t)}$ для $t = 4$, $n \in \overline{6, 11}$ и $t = 5$, $n \in \overline{8, 9}$.

t	$degf(x)$	$f(x)$	$rang\, w$	Предп. ранг
4	6	x^6+x+1	53	56
4	6	x^6+x^5+1	53	56
4	7	$x^7+x^5+x^2+x+1$	91	98
4	7	$x^7+x^6+x^5+x^2+1$	91	98
4	8	$x^8+x^4+x^3+x^2+1$	158	162
4	8	$x^8+x^6+x^5+x^4+1$	158	162
4	9	$x^9+x^6+x^4+x^3+x^2+x+1$	252	255
4	9	$x^9+x^8+x^7+x^6+x^5+x^3+1$	252	255
4	9	$x^9+x^7+x^6+x^3+x^2+x+1$	252	255
4	9	$x^9+x^8+x^7+x^6+x^3+x^2+1$	252	255
4	9	$x^9+x^7+x^6+x^5+x^4+x^2+1$	252	255
4	9	$x^9+x^7+x^5+x^4+x^3+x^2+1$	252	255
4	9	$x^9+x^7+x^5+x+1$	252	255
4	9	$x^9+x^8+x^4+x^2+1$	252	255
4	11	$x^{11}+x^6+x^2+x+1$	550	561
4	11	$x^{11}+x^{10}+x^9+x^5+1$	550	561
5	8	$x^8+x^6+x^5+x+1$	210	218
5	8	$x^8+x^7+x^3+x^2+1$	210	218
5	8	$x^8+x^5+x^3+x+1$	214	218
5	8	$x^8+x^7+x^5+x^3+1$	214	218
5	8	$x^8+x^6+x^3+x^2+1$	216	218
5	8	$x^8+x^6+x^5+x^2+1$	216	218
5	9	$x^9+x^7+x^5+x+1$	378	381
5	9	$x^9+x^8+x^4+x^2+1$	378	381
5	9	$x^9+x^8+x^7+x^6+x^3+x^2+1$	378	381
5	9	$x^9+x^7+x^6+x^3+x^2+x+1$	378	381
5	9	$x^9+x^7+x^2+x+1$	378	381
5	9	$x^9+x^8+x^7+x^2+1$	378	381

Приведем следующее очевидное замечание:

Замечание.

1.Если для многочлена $f(x) \in GF(q)[x]$-унитарный многочлен степени n не выполняется формула (5), то и для многочлена $rev(f(x)) = x^n(1/f(x))$ также (5) будет не верна.

2. Для каждого множества $H_n^{(4)}$, $n \in \overline{4,11}$ понижение ранга одинаковое для всех многочленов из $H_n^{(4)}$.

Список использованных источников и литературы

[1] Лидл Р.Нидеррайтер Г.,*Конечные поля*, (1988), 494Џ554;

[2] Богонатов Р.В., *Гипотеза В.И.Нечаева о произведении линейных рекуррент*, Чебышевский сборник том 6 выпуск 1 (2005), 48-55;

[3] Куракин В.Л., *Алгоритм Берлекэмпа-Мэсси над конечными коммутативными кольцами*, Учебно-методическое пособие (2003),3-5,26-29,41;

[4] Berlekamp E. R. *Algebraic Coding Theory.* Џ New York: McGrow Hill, (1968).
(перевод: Берлекэмп Э. *Алгебраическая теория кодирования.* Џ М.: Мир,1971).

[5] Massey J.L., *Shift Register Synthesis and BCH Decoding*, // IEEE Trans. Inform. Theory. Ч vol. IT-15, no. 1, (1969).

[6] Глухов М.М., Елизаров В.П., Нечаев А.А. *Алгебра в 2-ух томах*, издательство в/ч 33965, том 2.

[7] Zierler N.,Mills W.H., *Product of linear recurring sequences.* J.Algebra(1973) 27, 1, 147-157