В.Н. Цыпышев, Ю.С. Виноградова

КРИТЕРИЙ МАКСИМАЛЬНОСТИ ПЕРИОДА ТРЕХЧЛЕНА НАД СОБСТВЕННЫМ КОЛЬЦОМ ГАЛУА НЕЧЕТНОЙ ХАРАКТЕРИСТИКИ

Мы приводим критерий максимальности периода трехчлена над собственным кольцом Галуа нечетной характеристики в терминах коэффициентов этого трехчлена.

Авторы признательны А.С. Кузьмину за помощь и внимание к работе.

Ключевые слова: линейные рекуррентные последовательности, кольцо Галуа, многочлены Галуа, трехчлены, максимальность периода.

Введение

Пусть $R = GR\left(q^n, p^n\right)$ – кольцо Галуа[1], $F(x) \in R[x]$ – реверсивный унитарный многочлен.

Периодом $T(F)$ многочлена $F(x)$ называется наименьшее t со свойством:

$$F(x) \mid x^t - e\,.$$

Через $\overline{F}(x)$ будем обозначать образ $F(x)$ при естественном эпиморфизме:

$$R[x] \to R[x] / pR[x].$$

Напомним[2], что имеет место соотношение:

$$T\left(\overline{F(x)}\right) \mid T\left(F(x)\right) \mid T\left(\overline{F}(x)\right) \cdot p^{n-1}.$$

Многочлен $F(x)$ называется отмеченным, если

$$T(F) = T\left(\overline{F}\right),$$

и называется многочленом полного периода, если

$$T(F) = T\left(\overline{F}\right) \cdot p^{n-1}.$$

Если при этом $T\left(\overline{F}\right) = q^m - 1$, то $F(x)$ называется многочленом максимального периода (МП-многочленом)[3].

Унитарный и реверсивный одновременно многочлен над кольцом R называется регулярным.

Кольцо Галуа называется собственным при $n > 1, p^2 \mid q$, т. е. когда R не совпадает ни с полем, ни с кольцом вычетов[4].

А.А. Нечаевым были сформулированы просто проверяемые достаточные условия максимальности периода многочлена над кольцом вычетов по модулю 2^n в терминах коэффициентов этого многочлена[5]. В работах А.С. Кузьмина[6] тематика этих исследований была продолжена для случая примарных колец вычетов $Z/p^n, p \geq 3$. Ниже мы, основываясь на результатах работ[7], рассмотрим критерий полноты периода трехчленов над собственным кольцом Галуа R, а также многочленов, степени которых ограничены сверху значением $q = |R/pR|$.

Напомним[8], что $F(x)$ – МП-многочлен над кольцом Галуа R нечетной характеристики в том и только в том случае, когда образ $\widetilde{F}(x)$ по модулю $p^2R[x]$ – МП-многочлен над кольцом Галуа $\tilde{R} = R/p^2R = GR\left(q^2, p^2\right)$.

Для удобства ссылок при последующих рассуждениях сформулируем:

Утверждение 1.1[9].

Пусть $F(x) \in R[x], R = GR\left(q^n, p^n\right), n > 1, p \geq 3, p^2 \mid q$.

Если многочлен $F(x)$ представить в виде:

$$F(x) = \sum_{t=0}^{q-1} x^t a_t\left(x^q\right) \qquad (1.1),$$

где

$$a_t(x)=\sum_{s=0}^{u_t} a_{i(s,t)}x^{i(s,t)},$$

то регулярный многочлен Галуа $F(x)$ будет многочленом полного периода в том и только в том случае, когда

$$F\left(x^q\right)\neq\sum_{t=0}^{q-1}x^{qt}\sum_{(c(0,t),\ldots,c(u_t,t)\in\Omega(t))}\frac{p!}{\prod_{s=0}^{u_t}c(s,t)}\prod_{s=0}^{u_t}\left(a_{i(s,t)}x^{qi(s,t)}\right)^{c(s,t)p^{r-1}}\rightarrow$$

$$\rightarrow \bmod p^2R \qquad (1.2),$$

где множества $\Omega(t), t=\overline{0,q-1}$ имеют вид:

$$\Omega(t)=\left\{\left(c(0,t),\ldots,c(u_t,t)\right): c(s,t)\in\overline{0,p}, s=\overline{0,u_t}, \sum_{s=0}^{u_t}c(s,t)=p\right\}.$$

Критерий максимальности периода трехчленов Галуа

Всюду ниже имеется в виду сравнение по модулю q.

Теорема 2.1. Пусть $G(x)$ – многочлен над кольцом Галуа $R=GR\left(q^n,p^n\right), q=p^r, r\geq 2, p\geq 3, n\geq 2$, такой, что $G(x)=x^m+ax^k+b, T\left(\overline{G}\right)=q^m-1$.

Тогда многочлен $G(x)$ является многочленом максимального периода над кольцом R в том и только в том случае, если выполнено одно из следующих условий:

(I) $m\neq_q k, k\equiv 0$;

(II) $m\neq_q k, m\neq_q 0, k\neq_q 0$, и, дополнительно, $\gamma_1(a)\neq 0$ или $\gamma_1(b)\neq 0$;

(III) $m\neq_q k, m\equiv 0$;

(IV) $m\neq_q 0, k\equiv 0$.

Доказательство. Для установления максимальности периода многочлена $G(x)$ мы воспользуемся соотношением (1.2).

Рассмотрим классы вычетов по модулю q степеней ненулевых мономов многочлена $G(x)$. Возможны следующие случаи:

(a) $m \equiv k \equiv 0$;

(b) $m \neq_q k, k \equiv 0$;

(c) $m \neq_q k, m \neq_q 0, k \neq_q 0$;

(d) $m \neq_q k, m \equiv 0$;

(e) $m \neq_q 0, k \equiv 0$.

Случай (a). Так как $\overline{G}(x)$ – МП-многочлен, то, согласно[10], числа m и k взаимно просты. Поэтому в условиях Утверждения данный случай не может иметь места.

Случай (b). Пусть $m = t + qi$, $k = qj$. Тогда правая часть соотношения (1.2) имеет вид

$$x^{q^2 t} x^{qi} + \sum_{\substack{c(0),c(1)\in\overline{0,p} \\ c(0)+c(1)=p}} \frac{p!}{c(0)!c(1)!} b^{c(0)p^{r-1}} a^{c(1)p^{r-1}} x^{qjc(1)p^{r-1}} =$$

$$= x^{qm} + a^q x^{qk} + b^q + \sum_{\substack{c(0),c(1)\in\overline{1,p-1} \\ c(0)+c(1)=p}} \frac{p!}{c(0)!c(1)!} b^{c(0)p^{r-1}} a^{c(1)p^{r-1}} x^{qjc(1)p^{r-1}} \quad (2.1)$$

Для всех $c(1), c(1) \in \overline{1, p-1}$, $c(1) \neq c'(1)$, имеют место соотношения: $kc(1)p^{r-1} \neq kc'(1)p^{r-1}$ и $0 < kc(1)p^{r-1}, kc'(1)p^{r-1} < kq < mq$.

Таким образом, все члены суммы (2.1) ненулевые по модулю $p^2 R$ и имеют различные степени. Следовательно, имеет место (1.2), т. е. все многочлены $G(x)$, удовлетворяющие условиям Утверждения и случая (b), являются МП-многочленами.

Случай (c). Правая часть соотношения (1.2) имеет вид:

$$x^{mq} + a^q x^{kq} + b^q \equiv x^{mq} + g_0(a) x^{kq} + g_0(b) \left(\mathrm{mod}\, p^2 R[x]\right).$$

Следовательно, (1.2) имеет место в том и только в том случае, когда

$$\gamma_1(a) \neq 0 \text{ или } \gamma_1(b) \neq 0 .$$

Случай (d). Пусть $m = t + qi$, $k = t + qj$. Тогда правая часть соотношения (1.2) равна

$$b^q + x^{qt} \sum_{\substack{c(0),c(1)\in\overline{0,p-1}: \\ c(0)+c(1)=p}} \frac{p!}{c(0)!c(1)!} a^{c(0)p^{r-1}} x^{c(0)p^{r-1}qj} x^{c(1)p^{r-1}qi} =$$

$$= b^q c + a^q x^{kq} + x^{mq} + x^{qt} \cdot \sum_{\substack{c(0),c(1)\in\overline{1,p-1}: \\ c(0)+c(1)=p}} \frac{p!}{c(0)!c(1)!} a^{c(0)p^{r-1}} x^{p^{r-1}q(c(0)j+c(1)i)} \qquad (2.2).$$

Все члены суммы (2.2) – ненулевые по модулю $p^2 R$. Кроме того, так как

$$qt = c(0)\, p^{r-1} t + c(1)\, p^{r-1} t ,$$

то

$$qt + c(0)\, p^{r-1} qj + c(1)\, p^{r-1} qi = c(0)\, p^{r-1} k + c(1)\, p^{r-1} m.$$

Поэтому при

$$c(0), c'(0) \in \overline{1, p-1}, c(0) \neq c'(0), c(1) = p - c(0), c'(1) = p - c'(0),$$

имеем:

$$qt + c(0)\, p^{r-1} qj + c(1)\, p^{r-1} qi = qt + c'(0)\, p^{r-1} qj + c'(1)\, p^{r-1} qi \leftrightarrow$$

$$\leftrightarrow c(0)p^{r-1}k + c(1)p^{r-1}m = c'(0)p^{r-1}k + c'(1)p^{r-1}m \leftrightarrow$$

$$\leftrightarrow c(0)k + c(1)m = c'(0)k + c'(1)m \leftrightarrow$$

$$\leftrightarrow k(c(0) - c'(0)) = m(c'(1) - c(1)) \leftrightarrow k = m ,$$

что невозможно. Таким образом, все члены суммы

$$x^{qt} \cdot \sum_{c=1}^{p-1} \frac{p!}{c!(p-c)!} a^{cp^{r-1}} x^{p^{r-1}q(cj+(p-c)i)} \qquad (2.3)$$

имеют различные степени, причем степень каждого слагаемого строго меньше mq. Кроме того, слагаемое $a^q x^{kq}$ в правой части

равенства (2.2) может сократить не более одного из $p-1$ членов суммы (2.3). Это, при условии $p \geq 3$, означает, что имеет место (1.2). Таким образом, все многочлены $G(x)$, удовлетворяющие условиям утверждения и случая (d), имеют максимальный период.

Случай (e). По условию, $m = qi$, $k = t + qj$. Имеем, что правая часть соотношения (1.2) равна

$$\sum_{\substack{c(0),c(1)\in\overline{0,p:}\\ c(0)+c(1)=p}} \frac{p!}{c(0)!c(1)!} b^{c(0)p^{r-1}} x^{c(1)p^{r-1}qi} + a^q x^{kq} =$$

$$= b^q + a^q x^{qk} + x^{mq} + \sum_{\substack{c(0),c(1)\in\overline{1,p-1:}\\ c(0)+c(1)=p}} \frac{p!}{c(0)!c(1)!} b^{c(0)p^{r-1}} x^{c(1)p^{r-1}m} \quad (2.4).$$

Все члены суммы (2.4) – ненулевые по модулю p^2R. При всех $c(1)$, $c'(1) \in \overline{1, p-1}$, $c(1) \neq c'(1)$, имеют место соотношения: $c(1)p^{r-1}m, c'(1)p^{r-1}m < qm$. Кроме того, слагаемое $a^q x^{kq}$ в правой части равенства (2.4) может сократить не более одного из $p-1$ членов суммы

$$\sum_{c=1}^{p-1} \frac{p!}{c!(p-c)!} b^{\varphi^{r-1}} x^{(p-c)p^{r-1}m}.$$

Следовательно, поскольку $p \geq 3$, то имеет место соотношение (1.2). Таким образом, все многочлены $G(x)$, удовлетворяющие условиям утверждения и случая (e), имеют максимальный период.

Следствие 2.2. Пусть $G(x)$ – многочлен над кольцом Галуа $F(x) \in R[x], R = GR(q^n, p^n), n > 1, p \geq 3, p^2 \mid q$, такой, что $G(x) \equiv x^m + ax^k + b \left(\mathrm{mod}\, p^2 R[x]\right), T(\overline{G}) = q^m - 1$.

Тогда многочлен $G(x)$ является многочленом максимального периода над кольцом R, если многочлен $G(x) \equiv x^m + ax^k + b \left(\mathrm{mod}\, p^2 R[x]\right)$ над кольцом $\tilde{R} = R/p^2R = GR(q^2, p^2)$ удовлетворяет условиям Теоремы 2.1.

Утверждение 2.3. Пусть $G(x) = x^{mq} + \sum_{k=0}^{m-1} g_k^q x^{kq}$ – регулярный многочлен Галуа над кольцом Галуа $R = GR(q^n, p^n), q = p^r$, $r \geq 2, p \geq 3, n \geq 2$, степени m, строго меньшей q. Тогда многочлен $G(x)$ является многочленом полного периода в том и только в том случае, когда при некотором $k \in \overline{0, m-1}$ $\gamma_1(g_k) \neq 0$.

Доказательство. В рассматриваемом нами случае правая часть соотношения (1.2) примет вид:

$$x^{mq} + \sum_{k=0}^{m-1} g_k^q x^{kq} \equiv x^{mq} + \sum_{k=0}^{m-1} g_0(g_k) x^{kq} \left(\mathrm{mod}\, p^2 R[x]\right) \qquad (2.5)$$

Следовательно, соотношение (1.2) выполнено в том и только в том случае, когда имеет место наше Утверждение.

Утверждение 2.4[11]. Пусть $G(x) = x^{mq} + \sum_{k=0}^{m-1} g_k^q x^{kq}$ – многочлен над кольцом Галуа $R = GR(q^n, p^n), q = p^r, r \geq 2, p \geq 3, n \geq 2$. Если $T(\overline{G}) = q^m - 1$ **и** $\gamma_1(g_0) \neq 0$, то $G(x)$ – МП-многочлен.

Примечания

[1] *McDonald C.* Finite rings with identity. N. Y.: Marcel Dekker, 1974; *Radghavendran R.* A class of finite rings // Compositio Mathematica. 1970. Vol. 22. № 1. P. 49–57.

[2] *Нечаев А.А.* Цикловые типы линейных подстановок над конечными коммутативными кольцами // Мат. сб. 1993. Т. 184. № 4. С. 21–56.

[3] *Нечаев А.А.* Линейные рекуррентные последовательности над коммутативными кольцами // Дискретная математика. 1991. Т. 3. № 4. С. 107–121.

[4] *Нечаев А.А., Цыпышев В.Н.* Полилинейные рекурренты над бимодулями // Мат. методы и прил.: Тр. III мат. чтений (24–29 янв. 1995). Тез. докл. М., 1995. С. 95–100; *Они же.* Артинов бимодуль с квазифробениусовым каноническим бимодулем // Междунар. алгебраич. семинар, посвящ. 70-летию науч.-исслед. семинара МГУ по алгебре, основ. О.Ю. Шмидтом в 1930 г. (13–16 нояб. 2000 г.). Тез. докл. М., 2000. С. 39–40; *Цыпышев В.Н.* Матричный линейный конгруэнтный генератор над кольцом Галуа нечетной характеристики // Тез. докл. V междунар. конф. «Алгебра и теория чисел: Современные проблемы и приложения». Тула, 2003. С. 233–237; *Tsypyschev V.N.* Rank estimations of the second coordinate sequence of MP-LRS over nontrivial Galois ring of odd characteristic

(in Russian) // II International Scientific Conference on Problems of Security and Counter-Terrorism Activity (Oct. 25–26, 2006). Moscow, 2007. P. 287–289.

[5] *Kuzmin A.S., Nechaev A.A.* Linear recurrent sequences over Galois rings // Contemporary Mathematics. 1995. Vol. 184. P. 237–254.

[6] *Кузьмин А.С.* Многочлены максимального периода над кольцами вычетов целых чисел // III междунар. конф. по алгебре памяти М.И. Каргополова (Красноярск, 23–28 авг. 1993 г.). Тез. докл. Красноярск, 1993. С. 192; *Он же.* Многочлены максимального периода над кольцами вычетов // Фундамент. и приклад. математика. 1995. Т. 1. № 2. С. 549–551.

[7] *Цыпышев В.Н.* Критерий полноты периода многочлена Галуа над собственным кольцом Галуа нечетной характеристики // Соврем. математика и ее прил. 2004. Т. 14. С. 108–120; *Tsypyschev V.N.* Full periodicity of Galois polynomials over nontrivial Galois rings of odd characteristic // Journal of Mathematical Sciences. 2005. Vol. 131. № 6. P. 6120–6132.

[8] *Kuzmin A.S., Kurakin V.L., Mikhalev A.V., Nechaev A.A.* Linear recurrences over rings and modules // Journal of Mathematical Sciences. 1995. Vol. 76. № 6. P. 2793–2915; *Нечаев А.А.* Код Кердока в циклической форме // Дискрет. математика. 1989. Т. 1. № 4. С. 123–139; *Куракин В.Л.* Первая координатная последовательность линейной рекурренты максимального периода над кольцом Галуа // Там же. 1994. Т. 6. № 2. С. 88–100.

[9] *Tsypyschev V.N.* Full periodicity of Galois polynomials...

[10] *Альберт А.А.* Конечные поля // Кибернет. сб. (нов. сер.). 1966. № 3. С. 7–49.

[11] *Tsypyschev V.N.* Full periodicity of Galois polynomials...; *Цыпышев В.Н.* Матричный линейный конгруэнтный генератор над кольцом Галуа нечетной характеристики // Чебышев. сб. 2003. Т. 4. Вып. 1 (5). С. 112–125.