Criterion of maximal period of a trinomial over nontrivial Galois ring of odd characteristic

V.N.Tsypyschev and Ju.S.Vinogradova *

Russian State Social University, 4,W.Pik Str., Moscow, Russia

Abstract

In earlier eighties of XX century A.A.Nechaev has obtained the criterion of full period of a Galois polynomial over primary residue ring $\mathbb{Z}_{2^n}$. Also he has obtained necessary conditions of maximal period of the Galois polynomial over $\mathbb{Z}_{2^n}$ in terms of coefficients of this polynomial.

Further A.S.Kuzmin has obtained analogous results for the case of Galois polynomial over primary residue ring of odd characteristic .

Later the first author of this article has carried the criterion of full period of the Galois polynomial over primary residue ring of odd characteristic obtained by A.S.Kuzmin to the case of Galois polynomial over nontrivial Galois ring of odd characteristic.

Using this criterion as a basis we have obtained criterion calling attention to. This result is an example how to apply results of the previous work of V.N.Tsypyschev in order to construct polynomials of maximal period over nontrivial Galois ring of odd characteristic. During this it is assumed that period of polynomial modulo prime ideal is known and maximal .

Keywords: Secret-key cryptography, Stream ciphers, Pseudo-randomness, Implementation

MSC[2010] 12, 13

*Corresponding author: Vadim N.Tsypyschev, e-mail address: tsypyschev@yandex.ru.

1 Introduction

Let $R = GR(p^n, r)$ be a Galois ring [8, 9], $q = p^r$, $F(x) \in R[x]$ be a reversible unitary polynomial .

Let $\mathrm{T}(F)$ denote a *period* of polynomial $F(x)$, i.e. minimal t with property: $F(x) \mid x^\lambda(x^t - e)$ for some $\lambda \geq 0$.

Let $\bar{F}(x)$ be an image of $F(x)$ under canonical epimorphism $R[x] \to R[x]/pR[x]$.

Let remind [6], that :

$$\mathrm{T}(\bar{F}(x)) \,|\mathrm{T}(F(x))|\, \mathrm{T}(\bar{F}(x)) \cdot p^{n-1}.$$

Polynomial $F(x)$ is called *distinguished ,* if

$$\mathrm{T}(F) = \mathrm{T}(\bar{F}),$$

and is called *polynomial of full period ,* if

$$\mathrm{T}(F) = \mathrm{T}(\bar{F}) \cdot p^{n-1}.$$

Under additional condition $\mathrm{T}(\bar{F}) = q^m - 1$, polynomial $F(x)$ is called *polynomial of maximal period (MP-polynomial)* . Unitary and reversible polynomial we call *regular*.

Galois ring $R = GR(p^n, r)$ is called *nontrivial* iff $n > 1$, $r \geq 2$, i.e. iff R is neither field nor residue ring of integers .

It is also well-known that the arbitrary element $s \in R$ may be uniquely represented in the form

$$s = \sum_{i=0}^{n-1} \gamma_i(s) p^i, \;\; \gamma_i(s) \in \Gamma(R), \;\; i = \overline{0, n-1}, \tag{1.1}$$

where $\Gamma(R) = \{x \in R \mid x^q = x\}$ is a *p-adic coordinate set of the ring R (Teichmueller's representatives system).*

The set $\Gamma(R)$ with operations $\oplus : x \oplus y = (x + y)^{q^{n-1}}$ and $\otimes : \; x \otimes y = xy$ is a Galois field $GF(q)$.

It is well-known [2] that for the synthesis of algebraic shift registers over finite fields, rings or modules in most cases are necessary to construct polynomials with high periodic properties.

It is very important to understand, that the task of evaluation of period of polynomial over residue ring and Galois ring R is divided into two different

independent tasks. Namely, the first task is to evaluate the period of image of investigating polynomial under canonical epimorphism $R \to pR$, i.e. the evaluation of period of polynomial over finite field. This task is well-known, too difficult and the introduction to this area can be found in [4]. The second task is to evaluate period of polynomial over R under condition that the period of its image over $\bar{R}$ is already known. In this article we investigate exactly the second task. And we don't concern the first task at all in any way.

The first step in solution of the second task was made by A.A.Nechaev. He had obtained that polynomial $G(x)$ of degree m over Galois ring $R = GR(p^n, r)$ is of maximal period $\mathrm{T}(G) = (p^{rm} - 1)p^{n-1}$ iff period of $\bar{G}(x)$ over R/pR is equal to $p^{rm} - 1$ and the root θ of $G(x)$ in Galois extension $S = GR(p^n, rm)$ has a property: $\gamma_1(\theta) \neq 0$. Because to verify whether $\gamma_1(\theta) \neq 0$ is difficult task, further investigations were concentrated around coefficients of polynomial under investigation.

This way A.A.Nechaev had obtained easily verifiable necessary conditions of maximal period for polynomial over $\mathbb{Z}_{2^n}$ in terms of coefficients of this polynomial [7]. A.S.Kuzmin has carried this research to the case of primary residue ring of integers $\mathbb{Z}_{p^n}$, $p \geq 3$, [7]. What follows is only application of results of [10] for obtaining of criterion of full period for trinomials over nontrivial Galois ring $R = GR(p^n, r)$, $n \geq 2$, $r \geq 2$. Previously this result was published in Russian in the thesis form [11].

Let's remind [7, 5, 10] that $F(x)$ is a MP-polynomial over nontrivial Galois ring R of odd characteristic iff its image $\tilde{F}(x)$ modulo $p^2R[x]$ is a MP-polynomial over Galois ring $\tilde{R} = R/p^2R = GR(p^2, r)$.

For convenience of referring let's remind also that

Statement 1.1 ([10]). *Let $F(x) \in R[x]$, $R = GR(p^n, r)$, $n > 1$, $p \geq 3$, $r \geq 2$.*

If polynomial $F(x)$ is represented in the form

$$F(x) = \sum_{t=0}^{q-1} x^t a_t(x^q), \tag{1.2}$$

for $a_t(x) = \sum_{s=0}^{u_t} a_{i_s(t)} x^{i_s(t)}$, $t = \overline{0, q-1}$, then regular Galois polynomial $F(x)$

is a polynomial of full period if and only if this condition holds:

$$F(x^q) \not\equiv \sum_{t=0}^{q-1} x^{qt} \sum_{(c_{0,t},\ldots,c_{u_t,t})\in\Omega(t)} \frac{p!}{\prod_{s=0}^{u_t} c_{s,t}!} \prod_{s=0}^{u_t} \left(a_{i_s(t)} x^{qi_s(t)}\right)^{c_{s,t}p^{r-1}} \left(\mathrm{mod}\, p^2 R\right), \tag{1.3}$$

where family of sets $\Omega(t)$, $t = \overline{0, q-1}$ *is defined as*

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

2 Criterion of maximal period for trinomials

Theorem 2.1. *Let* $G(x)$ *be a polynomial over Galois ring* $R = GR(p^n, r)$, $q = p^r$, $r \geq 2$, $p \geq 3$, $n \geq 2$, *of the form* $G(x) = x^m + ax^k + b$, *and let* $\mathrm{T}(\bar{G}) = q^m - 1$.

Then $G(x)$ *is a polynomial of maximal period over ring* R *if and only if at least one of following conditions holds:*

(I) $m \not\equiv_q k$, $k \equiv_q 0$;

(II) $m \not\equiv_q k$, $m \not\equiv_q 0$, $k \not\equiv_q 0$, *and additionally* $\gamma_1(a) \neq 0$ *or* $\gamma_1(b) \neq 0$;

(III) $m \equiv_q k$, $m \not\equiv_q 0$;

(IV) $m \equiv_q 0$, $k \not\equiv_q 0$.

Proof. To investigate maximality of period of polynomial $G(x)$ we have to apply the relation (1.3).

Let's consider residue classes modulo q of degrees of non-zero monomials of polynomial $G(x)$.

These cases are possible:

(a) $m \equiv_q k \equiv_q 0$.

(b) $m \not\equiv_q k$, $k \equiv_q 0$.

(c) $m \not\equiv_q k$, $m \not\equiv_q 0$, $k \not\equiv_q 0$.

(d) $m \equiv_q k$, $m \not\equiv_q 0$.

(e) $m \equiv_q 0$, $k \not\equiv_q 0$.

The case (a). Because according to conditions of the Theorem $\bar{G}(x)$ is a MP-polynomial then [1] numbers m and k are co-prime. Thus under conditions of the Theorem the case (a) is impossible.

The case (b). Let $m = t+qi, k = qj$. Then right-hand side of the relation (1.3) takes a form

$$\begin{aligned} &x^{qt}x^{q^2i} + \sum_{\substack{c_0,c_1\in\overline{0,p}:\\ c_0+c_1=p}} \frac{p!}{c_0!c_1!} b^{c_0p^{r-1}} a^{c_1p^{r-1}} x^{qjc_1p^{r-1}} = \\ &= x^{qm} + a^q x^{qk} + b^q + \sum_{\substack{c_0,c_1\in\overline{1,p-1}:\\ c_0+c_1=p}} \frac{p!}{c_0!c_1!} b^{c_0p^{r-1}} a^{c_1p^{r-1}} x^{kc_1p^{r-1}}. \end{aligned} \tag{2.1}$$

For any $c_1, c_1' \in \overline{1, p-1}, c_1 \neq c_1'$ these relations take place:

$$kc_1p^{r-1} \neq kc_1'p^{r-1}$$

and

$$0 < kc_1p^{r-1}, kc_1'p^{r-1} < kq < mq.$$

Hence all members of the sum (2.1) are non-zero modulo p^2R and has different degrees. It follows that the relation (1.3) takes place, i.e. all polynomials $G(x)$ which satisfies to conditions of Theorem and of case (b) are polynomials of maximal period.

The case (c). The right-hand side of the relation (1.3) has a form:

$$x^{mq} + a^q x^{kq} + b^q \equiv x^{mq} + \gamma_0(a)x^{kq} + \gamma_0(b) \pmod{p^2R[x]}.$$

Hence the relation (1.3) takes place if and only if either $\gamma_1(a) \neq 0$ or $\gamma_1(b) \neq 0$. So all polynomials $G(x)$ which satisfies to conditions of Theorem and of case (c) are polynomials of maximal period.

The case (d). Let $m = t + qi, k = t + qj$. Then right-hand side of the relation (1.3) is equal

$$\begin{aligned} &b^q + x^{qt} \sum_{\substack{c_0,c_1\in\overline{0,p}:\\ c_0+c_1=p}} \frac{p!}{c_0!c_1!} a^{c_0p^{r-1}} x^{c_0p^{r-1}qj} x^{c_1p^{r-1}qi} = \\ &= b^q + a^q x^{kq} + x^{mq} + x^{qt} \sum_{\substack{c_0,c_1\in\overline{1,p-1}:\\ c_0+c_1=p}} \frac{p!}{c_0!c_1!} a^{c_0p^{r-1}} x^{p^{r-1}q(c_0j+c_1i)}. \end{aligned} \tag{2.2}$$

All members of the sum (2.2) are non-zero modulo p^2R. Besides that,

$$qt = c_0p^{r-1}t + c_1p^{r-1}t.$$

Hence

$$qt + c_0p^{r-1}qj + c_1p^{r-1}qi = c_0p^{r-1}k + c_1p^{r-1}m.$$

It follows that under conditions $c_0, c_0' \in \overline{1, p-1}, c_0 \neq c_0'$ and $c_1 = p - c_0, c_1' = p - c_0'$ these equivalencies hold:

$$qt + c_0 p^{r-1} qj + c_1 p^{r-1} qi = qt + c_0' p^{r-1} qj + c_1' p^{r-1} qi \Leftrightarrow$$
$$\Leftrightarrow c_0 p^{r-1} k + c_1 p^{r-1} m = c_0' p^{r-1} k + c_1' p^{r-1} m \Leftrightarrow$$
$$\Leftrightarrow c_0 k + c_1 m = c_0' k + c_1' m \Leftrightarrow$$
$$\Leftrightarrow k(c_0 - c_0') = m(c_1' - c_1) \Leftrightarrow k = m.$$

Last equality is impossible. Hence all members of the sum

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

are of different degrees strictly less then mq.

Besides that summand $a^q x^{kq}$ in the right-hand side of the equality (2.2) may zeroize no more than one of $p-1$ members of the sum (2.3). Because $p \geq 3$ it means that relation (1.3) holds .

So all polynomials $G(x)$ which satisfies to conditions of the Theorem and of the case (d) are of maximal period.

The case (e). According to conditions of the Theorem , $m = qi, k = t + qj$. So the right-hand side of the relation (1.3) is equal to

$$\begin{aligned} &\sum_{\substack{c_0, c_1 \in \overline{0,p}: \\ c_0 + c_1 = p}} \frac{p!}{c_0! c_1!} b^{c_0 p^{r-1}} x^{c_1 p^{r-1} qi} + a^q x^{kq} = \\ &= b^q + a^q x^{kq} + x^{mq} + \sum_{\substack{c_0, c_1 \in \overline{1,p-1}: \\ c_0 + c_1 = p}} \frac{p!}{c_0! c_1!} b^{c_0 p^{r-1}} x^{c_1 p^{r-1} m}. \end{aligned} \tag{2.4}$$

All members of the sum (2.4) are non-zero modulo $p^2 R$. For all $c_1, c_1' \in \overline{1, p-1}$ such that $c_1 \neq c_1'$ these relations take place: $c_1 p^{r-1} m \neq c_1' p^{r-1} m$ and $c_1 p^{r-1} m < mq$.

Besides that the summand $a^q x^{kq}$ in the right-hand side of the equality (2.4) may zeroize no more than one of $p-1$ other members of the sum

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

So because $p \geq 3$ the relation (1.3) takes place.

Hence all polynomials $G(x)$ which satisfies to conditions of the Theorem and of the case (e) has a maximal period . $\square$

Theorem 2.2. *Let $G(x)$ be a polynomial over Galois ring $R = GR(p^n, r)$, $q = p^r$, $r \geq 2$, $p \geq 3$, $n \geq 2$, such that $G(x) \equiv x^m + ax^k + b \pmod{p^2R[x]}$, and $\mathrm{T}(\bar{G}) = q^m - 1$.*

Then polynomial $G(x)$ is a polynomial of maximal period over R if and only if polynomial $G(x) \pmod{p^2R[x]}$ over p^2R satisfies to at least one of conditions (I)–(IV) of the Theorem 2.1

3 Conclusion

Theorem 2.2 provides us by method how to verify in easy way whenever a polynomial of special form over nontrivial Galois ring R has a maximal period. Let's note here once more that we don't concern the task of evaluating period of its image modulo pR. We suggest that its period modulo pR is maximal as a predefined condition. And after that we concern period of investigating polynomial over ring R.

From other side the same Theorem provides an easy way to construct polynomials of maximal period of special form over nontrivial Galois ring R.

4 Acknowledgments

This work was partially supported by Russian State University for the Humanities.

References

[1] Albert A.A. Finite fields // Cybernetic summary (a new series)— 1966— 3—pp 7-49 (in Russian).

[2] Goresky, Mark; Klapper, Andrew // Algebraic shift register sequences, Cambridge: Cambridge University Press (ISBN 978-1-107-01499-2/hbk). xv, 498 p., 2012.

[3] Kuzmin A.S., Kurakin V.L., Mikhalev A.V., Nechaev A.A. Linear recurrences over rings and modules. // J. Math. Science (Contemporary Math. and its Appl., Thematic surveys)—1995—v.76—N6—p.2793-2915

[4] Lidl, Rudolf; Niederreiter, Harald // Finite fields. Paperback reprint of the hardback 2nd edition 1996. (English) Zbl 1139.11053 Encyclopedia of Mathematics and Its Applications 20. Cambridge: Cambridge University Press (ISBN 978-0-521-06567-2/pbk). xiv, 755 p. (2008).

[5] Nechaev, A.A. Linear recurrence sequences over commutative rings. (English; Russian original) Discrete Math. Appl. 2, No.6, 659-683 (1992); translation from Diskretn. Mat. 3, No.4, 105-127 (1991).Zbl 0787.13007

[6] Nechaev A.A. Cyclic types of linear permutations over finite commutative rings // Matemat. sbornik —1993—ò.184—N4—C.21- 56 (in Russian)

[7] Kuzmin A.S., Nechaev A.A. Linear recurrent sequences over Galois rings // II Int.Conf.Dedic.Mem. A.L.Shirshov—Barnaul—Aug.20-25 1991 (Contemporary Math.—v.184—1995—p.237-254)

[8] McDonald C. Finite rings with identity // New York: Marcel Dekker—1974—495p.

[9] Radghavendran R. A class of finite rings // Compositio Math.—1970—v.22—N1—p.49-57

[10] Tsypyschev, V.N. Full periodicity of Galois polynomials over nontrivial Galois rings of odd characteristic. (English. Russian original) Zbl 1195.11160 // J. Math. Sci., New York 131, No. 6, 6120-6132 (2005); translation from Sovrem. Mat. Prilozh. 2004, No. 14, 108-120 (2004)

[11] Tsypyschev V.N., Vinogradova Ju.S. Criterion of period maximality of trinomial over nontrivial Galois ring of odd characteristic // Russian State University for Humanities bulletin—Record management and Archival science, Informatics, Data Protection and Information Security series—**18**—pp.32-43—2015 (in Russian)