SHORT COMMUNICATIONS

A formula on linear complexity of highest coordinate sequences from maximal periodic sequences over Galois rings*

HU Lei** and SUN Nigang

(State Key Laboratory of Information Security, Graduate School of Chinese Academy of Sciences, Beijing 100049, China)

Received November 2, 2005

Abstract Using a polynomial expression of the highest coordinate map, we deduce an exact formula on the linear complexity of the highest coordinate sequence derived from a maximal periodic sequence over an arbitrary Galois ring of characteristic p^2, where p is a prime. This generalizes the known result of Udaya and Siddiqi for the case that the Galois ring is $\mathbb{Z}_4$.

Keywords: Galois ring, highest coordinate sequence, linear complexity.

Let p be an arbitrary prime, and e, n, and r be any positive integers. Let $R = GR(p^e, r)$ and $R' = GR(p^e, rn)$ denote the Galois rings of characteristic p^e, with sizes p^{er} and p^{ern} respectively. The group R'^* of units of R' is a direct product of two subgroups G_A and G_C, where G_A is an abelian group of order $p^{(e-1)rn}$ with maximal element order p^{e-1}, and G_C is a cyclic group of order $p^{rn}-1$. Let Tr be the trace function from R' to R[1,2]. Associated with each element $a \in R'^*$, $\gamma \in G_A$ of order p^{e-1}, and $\alpha \in G_C$ of order $p^{rn}-1$, we can define an m-sequence over $R\underline{s} = \{s_t\}_{t\geqslant 0}$ as

$$s_t = \mathrm{Tr}(a(\gamma\alpha)^t), \quad \forall\, t \geqslant 0.$$

Its period is $p^{e-1}(p^{rn}-1)$. This is the maximal period that a linear recurring periodic sequence of degree n over R can have. All maximal periodic linear recurring sequences of degree n over R must be expressed as the form mentioned above[3,4].

Let $q = p^r$ and Γ denote the set of Teichmuller representatives of R, namely,

$$\Gamma = \{0, 1, \beta, \beta^2, \cdots, \beta^{q-2}\},$$

where β is an element in R of order $q-1$. Under the natural homomorphism $\pi: R \to R/pR \cong \mathbb{F}_q$ defined by $\pi(a) = a + pR$, Γ is one-to-one corresponding to $\mathbb{F}_q$[1,2].

Any element a in R can be expressed as $a = a_0 + pa_1 + \cdots + p^{e-1}a_{e-1}$ with $a_0, a_1, \cdots, a_{e-1} \in \Gamma$. For any $t \geqslant 0$, s_t is expressed as

$$s_t = s_{t,0} + ps_{t,1} + \cdots + p^{e-1}s_{t,e-1},$$

where $s_{t,0}, s_{t,1}, \cdots, s_{t,e-1} \in \Gamma$. Then $\{\pi(s_{t,e-1})\}_{t\geqslant 0}$ is a sequence over $\mathbb{F}_q$ and is called the highest coordinate sequence of $\underline{s}$.

The highest coordinate sequences derived from Galois rings were a research focus in the last decade. The sequences have nice correlation properties and are used significantly in cryptography, coding and communication applications. Some results on the linear complexities (LC) of the highest coordinate sequences have been achieved[5-9]. In Refs. [5,6], lower and upper bounds on the LC of the highest coordinate sequences $\{\pi(s_{t,e-1})\}_{t\geqslant 0}$ are given for the case that $q=2$. Kumar and Helleseth gave an upper and a lower bounds on the LC of the highest coordinate sequence derived from the trace sequence over Galois ring $\mathbb{Z}_{2^e}$ in Ref. [7], and in Ref. [8] Sun and Hu extended Kumar and Helleseth's work to the case of general Galois rings. An exact formula on the LC of the highest coordinate sequence $\{\pi(s_{t,1})\}_{t\geqslant 0}$ for the case that $q = e = 2$ is given by Udaya and Siddiqi in Ref. [9], where they used the fact that $2s_{t,1} = s_t - s_t^2$ to deduce the formula.

In this paper, we assume $e=2$ and p and r are

* Supported by National Natural Science Foundation of China (Grant Nos. 60373041 and 90104034)

** To whom correspondence should be addressed. E-mail: hu@is.ac.cn respectively any prime and positive integer. Utilizing the relation that $ps_{t,1} = s_t - s_t^q$, we deduce an exact formula on the LC of the highest coordinate sequence $\{\pi(s_{t,1})\}_{t\geqslant 0}$.

1 Some lemmas

Let $\mathbb{Z}_+$ denote the set of all nonnegative integers. For any $z \in \mathbb{Z} \setminus \{0\}$, define $v_p(z)$ as the index of the largest power of p that divides z, and for any n-tuple $\underline{v} \in \mathbb{Z}_+^n \setminus \{(0, 0, \cdots, 0)\}$, define $v_p(\underline{v})$ as the index of the largest power of p that divides each nonzero component of $\underline{v}$. For any positive integers x and y, set

$$E_{x,y} = \{\underline{v} = (v_0, v_1, \cdots, v_{y-1}) \in \mathbb{Z}_+^y \mid v_0 + v_1 + \cdots + v_{y-1} = x\}$$

and set $l_{x,y} = |E_{x,y}|$.

Lemma 1.

$$l_{x,y} = \binom{y+x-1}{x}.$$

Proof. We prove this lemma by induction on y. Trivially, we have $l_{x,1} = 1 = \binom{1+x-1}{x}$. Assume that for any $1 \leqslant j \leqslant y-1$, $l_{x,j} = \binom{j+x-1}{x}$. Taking a value in $\{0, 1, \cdots, x\}$ for v_j, we have $l_{x,j+1} = \sum_{i=0}^{x} l_{x-i,j}$. So,

$$l_{x,j+1} = \sum_{i=0}^{x} \binom{j+x-i-1}{x-i} = \binom{j+x}{x}.$$

Set

$$E_{p,n}^* = \{\underline{v} \in E_{p,n} \mid v_p(\underline{v}) = 0\}.$$

It is obvious that $|E_{p,n}^*| = \binom{n+p-1}{p} - n$, since

$$E_{p,n}^* = E_{p,n} \setminus \{(p;0,\cdots,0), (0,p,0,\cdots,0), \cdots, (0,\cdots,0,p)\}.$$

Set

$$E_{q,n}^* = \left\{\underline{v} = (v_0, v_1, \cdots, v_{n-1}) \in E_{q,n} \mid v_p\left(\binom{q}{v_0 \cdots v_{n-1}}\right) = 1\right\}$$

and set $l_{q,n}^* = |E_{q,n}^*|$.

Lemma 2. (i) Each vector in $E_{q,n}^*$ can be written as a form $(p^{r-1}v_0', \cdots, p^{r-1}v_{n-1}')$ with $(v_0', v_1', \cdots, v_{n-1}') \in E_{p,n}^*$; and

(ii) $l_{q,n}^* = \binom{n+p-1}{p} - n$.

Proof. For any $\underline{v} = (v_0, v_1, \cdots, v_{n-1}) \in E_{q,n}$, by Lemma 6.39 in Ref. [10], we know that

$$v_p\left(\binom{q}{v_0 \cdots v_{n-1}}\right) \geqslant r - v_p(\underline{v}).$$

So, we have

$$v_p\left(\binom{q}{v_0 \cdots v_{n-1}}\right) = 1 \text{ if and only if } v_p(\underline{v}) = r - 1. \tag{1}$$

For any $\underline{v} \in E_{q,n}^*$, let $\underline{v} = (p^{r-1}v_0', \cdots, p^{r-1}v_{n-1}')$. Then $\underline{v}' = (v_0', v_1', \cdots, v_{n-1}') \in E_{p,n}^*$. This proves the lemma.

2 Linear complexity of highest coordinate sequences

We assume that

$$a = (1 + pb)\alpha^k, \quad \gamma = 1 + p\delta, \tag{2}$$

where $b, \delta \in \{0\} \cup G_C$ and $0 \leqslant k \leqslant q^n - 2$. Then

$$\begin{aligned} s_t &= \mathrm{Tr}(a(\gamma\alpha)^t) \\ &= \sum_{j=0}^{n-1} \alpha^{kq^j}(1 + pb^{q^j})(1 + p\delta^{q^j})^t \alpha^{tq^j} \\ &= \sum_{j=0}^{n-1} (1 + pb^{q^j} + pt\delta^{q^j})\alpha^{(t+k)q^j}. \end{aligned}$$

By the facts that $v_p\left(\binom{q}{v_0 \cdots v_{n-1}}\right) \geqslant 2$ for $v_p(\underline{v}) \leqslant r - 2$ and that $p^2 = 0 \in R$ and Formula (1), we have

$$\begin{aligned} s_t^q &= \left(\sum_{j=0}^{n-1} (1 + pb^{q^j} + pt\delta^{q^j})\alpha^{(t+k)q^j}\right)^q \\ &= \sum_{j=0}^{n-1} (1 + pb^{q^j} + pt\delta^{q^j})^q \alpha^{(t+k)q^{j+1}} \\ &\quad + \sum_{\underline{v} \in E_{q,n}^*} \binom{q}{v_0 \cdots v_{n-1}} \prod_{j=0}^{n-1} (1 + pb^{q^j} + pt\delta^{q^j})^{v_j} \\ &\quad \cdot \alpha^{(t+k)(v_0 + qv_1 + \cdots + q^{n-1}v_{n-1})} \\ &= \sum_{j=0}^{n-1} \alpha^{(t+k)q^j} + \sum_{\underline{v} \in E_{q,n}^*} \binom{q}{v_0 \cdots v_{n-1}} \\ &\quad \cdot \alpha^{(t+k)(v_0 + qv_1 + \cdots + q^{n-1}v_{n-1})}. \end{aligned}$$

The last equality holds since $(1 + pc)^p = 1$ and $p(1 + pc) = p$ for any $c \in R$. For any $t \geqslant 0$, let $g_t \in \Gamma$ such that $pg_t = s_t - s_t^q$. Then

$$g_t \equiv \sum_{j=0}^{n-1} (b^{q^j} + t\delta^{q^j})\alpha^{(t+k)q^j} - \sum_{\underline{v} \in E_{q,n}^*} c_{\underline{v}} \alpha^{(t+k)\sum_{i=0}^{n-1} q^i v_i} \pmod{p}, \tag{3}$$

where $c_{\underline{v}} = \frac{1}{p}\binom{q}{v_0 \cdots v_{n-1}} \not\equiv 0 (\bmod\ p)$ for $\underline{v} \in E^*_{q,n}$.

Lemma 3. Define a sequence $\underline{a} = \{a_t\}_{t \geq 0}$ over $\mathbb{F}_q$ as

$$a_t = \sum_{j=0}^{n-1} (\zeta^{q^j} + t\eta^{q^j})\alpha^{(t+k)q^j},$$

where $\zeta, \eta \in \mathbb{F}_{q^n}$, $0 \leqslant k \leqslant q^n - 2$ and α is a primitive element of $\mathbb{F}_{q^n}$. Let $h(x) = (x-\alpha)(x-\alpha^q)\cdots(x-\alpha^{q^{n-1}})$ and $m(x)$ be the minimal polynomial of $\underline{a}$. Then

$$m(x) = \begin{cases} 1 & \eta = 0 = \zeta \\ h(x) & \eta = 0 \neq \zeta \\ h(x)^2 & \eta \neq 0 \end{cases}$$

and the linear complexity of $\underline{a}$ is

$$LC(\underline{a}) = \begin{cases} 0 & \eta = 0 = \zeta \\ n & \eta = 0 \neq \zeta \\ 2n & \eta \neq 0. \end{cases}$$

Proof. When $\eta = \zeta = 0$, $\underline{a} = \underline{0}$; when $\zeta \neq 0 = \eta$, $\underline{a}$ is an m-sequence over $\mathbb{F}q$ and $m(x) = h(x)$. Assume $\eta \neq 0$. For any $0 \leqslant j \leqslant n-1$, define a sequence over $\mathbb{F}_{q^n}$ as $\underline{c}^{(j)} = \{c_t^{(j)}\}_{t \geq 0}$, where

$$c_t^{(j)} = t\eta^{q^j}\alpha^{(t+k)q^j}.$$

Define $\underline{c} = \sum_{j=0}^{n-1} \underline{c}^{(j)}$. For any $0 \leqslant j \leqslant n-1$, since

$$c_{t+2}^{(j)} - 2\alpha^{q^j}c_{t+1}^{(j)} + \alpha^{2q^j}c_t^{(j)} = 0,$$

that is, $(x - \alpha^{q^j})^2$ vanishingly acts on $\underline{c}^{(j)}$, and so, we know $h(x)^2$ also vanishingly acts on $\underline{c}^{(j)}$ and on $\underline{c}$ and $\underline{a}$[5,11]. Since $h(x)$ is irreducible and $\underline{a} \neq \underline{0}$, $m(x) = h(x)$ or $h(x)^2$. If $m(x) = h(x)$, then $\underline{a}$ is an m-sequence and the period of $\underline{a}$ is $q^n - 1$. From $a_{t+q^n-1} = a_t$ for any $t \geqslant 0$, we have

$$\mathrm{Tr}(\eta\alpha^{t+k}) = \sum_{j=0}^{n-1} (\eta\alpha^{t+k})^{q^j} = 0,$$

which implies that $\eta = 0$ and is a contradiction. So $m(x) = h(x)^2$ and $LC(\underline{a}) = 2n$.

Now return to Formula (3) for the linear complexity of $\{\pi(g_t)\}_{t \geq 0}$. Let

$$u = \begin{cases} 2 & \delta \not\equiv 0 (\bmod\ p) \\ 1 & \delta \equiv 0 (\bmod\ p) \text{ and } b \not\equiv 0\ (\bmod\ p). \\ 0 & \delta \equiv 0 (\bmod\ p) \text{ and } b \equiv 0\ (\bmod\ p) \end{cases}$$

Notice that $0, 1, q, q^2, \cdots, q^{n-1}, v_0 + qv_1 + \cdots + q^{n-1}v_{n-1} (v \in E^*_{q,n})$ are all distinct. By Lemma 3, we have the following

Theorem 1. The linear complexity of $\{\pi(g_t)\}_{t \geq 0}$ is

$$un + l^*_{q,n} = (u-1)n + \binom{n+p-1}{p}. \quad (4)$$

Remark 1. From (4) we know the linear complexity of the highest coordinate sequence $\{\pi(g_t)\}_{t \geq 0}$ is independent of the value of r (compared with the result in Ref. [9] of Udaya and Siddiqi for the case that $q = e = 2$), and that the complexity becomes large for large p and is of magnitude of $n^p/p!$ for large n.

At the end of the paper, we point out that it seems impossible to directly generalize the above method to get an exact formula on the linear complexity of the highest coordinate sequence in the cases of $e \geqslant 3$, since for the case that $e = 2$ we utilize a polynomial (namely $x - x^q$) whose evaluation at an element $a \in R$ exactly represents whole information of the highest coordinate of a, however, such a polynomial does not exist when $e \geqslant 3$, as shown in the following proposition.

Definition 1. A polynomial $f(x) \in R[x]$ is called a highest coordinate polynomial map of R if there is an injection $g(\cdot)$ from Γ to R such that

$$f(a_0 + pa_1 + \cdots + p^{e-1}a_{e-1}) = g(a_{e-1})$$

for any $a_0, a_1, \cdots, a_{e-1} \in \Gamma$.

Proposition 1. There does not exist any highest coordinate polynomial map when $e \geqslant 3$.

Proof. Assume that

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots$$

is the highest coordinate polynomial map of R. Then for any $z \in \Gamma$,

$$g(z) = f(p^{e-1}z) = a_0 + p^{e-1}a_1z,$$

and thus, $a_1 \not\equiv 0 (\bmod\ p)$ since otherwise $g(z) = a_0$ is a constant. On the other hand, we have

$$a_0 = g(0) = f(p^{e-2}) = a_0 + p^{e-2}a_1 + p^{2(e-2)}a_2,$$

and $a_1 \equiv 0 (\bmod\ p)$, which is a contradiction.

References

1 McDonald B. R. Finite Rings with Identity. New York: Marcel Dekker, 1974.

2 Wan Z. X. Finite Fields and Galois Rings. Singapore: World Scientific Publisher, 2003.

3 Zhu Y. F. A criterion for primitive polynomials over Galois rings. Acta Mathematica Sinica (in Chinese), 1996, 39(6): 783—788.

4 Zhu Y. F. Injectiveness of a mapping generating ring derived sequences and a restoring algorithm. Acta Mathematica Sinica (in Chinese), 2001, 44(1): 103—110.

5 Dai Z. D., Beth T. and Gollmann D. Lower bounds for the linear complexity of sequences over residue rings. Advances in Cryptology-EUROCRYPT '90, 1991, 473: 189—195.

6 Dai Z. D. Binary sequences derived from ML-sequences over rings I: periods and minimal polynomials. Journal of Cryptology, 1992, 5: 193—207.

7 Kumar P. V. and Helleseth T. An expansion for the coordinates of the trace function over Galois rings. Applicable Algebra in Engineering, Communication and Computing, 1997, 8(5): 353—361.

8 Sun N. G. and Hu L. Expansion and linear complexity of the coordinate sequences over Galois rings. Journal of Complexity, Academic Press, Inc.

9 Udaya P. and Siddiqi M. U. Optimal biphase sequences with large linear complexity derived from sequences over $\mathbb{Z}_4$. IEEE Trans. Inform. Theory, 1996, 42(1): 206—216.

10 Lidl R. and Niederreiter H. Finite Fields. London: Addison-Wesley, 1983.

11 Wan Z. X. Algebra and Coding Theory (in Chinese). Beijing: Science Press, 1979.