Front. Electr. Electron. Eng. China 2009, 4(2): 141–144
DOI 10.1007/s11460-009-0038-6

RESEARCH ARTICLE

Nigang SUN, Lei HU

GMW sequences over Galois rings and their linear complexities

© Higher Education Press and Springer-Verlag 2009

Abstract A new family of GMW sequences over an arbitrary Galois ring was defined by using the trace functions and permutations. This generalizes the concept of GMW sequences over finite fields. Utilizing the Fourier representation, we derived an estimate of the linear complexities of this family of GMW sequences. And the result shows that such sequences have large linear complexities.

Keywords cryptography, GMW sequence, linear complexity, Galois ring

1 Introduction

With good interference-free ability, spread spectrum communications are used significantly in not only military communications but also civil communications. The performance of spread spectrum multiple-access communication systems are greatly influenced by the capabilities of spread sequences. One of the most important capabilities of the spread sequences is the linear complexity. A communication system will have good resistance to analysis if its spread sequences have large linear complexity. Consequently, constructing spread sequences with large linear complexities has become a hot research topic [1].

Utilizing trace functions, Scholtz and Welch [2] first constructed the GMW sequences over finite fields in 1984. Research shows that such sequences not only have two-level autocorrelation functions as m-sequences, but also have larger linear complexities and more cyclically inequivalent classes than m-sequences for the case that they have the same periods. Then the GMW sequences became a hot research focus, and a lot of results on the linear complexities of the GMW sequences have been achieved [3–8]. In 2000, Udaya and Siddiqi [9] extended Scholtz and Welch's work to the case of Galois rings and constructed the GMW sequences over the Galois ring Z_4. The result shows that the GMW sequences over Z_4 have larger linear complexities and more sequence numbers than the GMW sequences over finite fields for the case that these sequences have the same periods. In this paper, we define a new family of GMW sequences over an arbitrary Galois ring, which generalizes the result of Udaya and Siddiqi for the case that the Galois ring is Z_4. We also investigate the upper and lower bounds on the linear complexities of this family of GMW sequences, and the result shows that such sequences have large linear complexities.

Let p be a prime, e, r and u be positive integers. Let R and R' denote the Galois rings of characteristic p^e, with sizes p^{er} and p^{eru}, respectively. The group R^* of units of R is a direct product of two subgroups G_C and G_A, where G_C is a cyclic group of order p^r-1 and G_A is an Abelian group of order $p^{(e-1)r}$ with maximal element order p^{e-1}. Also, we use R'^* to denote the group of units of R'. Any element a in R can be expressed as $a=p^iw$, where $0\leqslant i\leqslant e-1$ and $w\in R^*\cup\{0\}$. Let Tr_r^{ru} denote the trace function from R' to R, and Tr_1^r denote the trace function from R to Z_{p^e}. For the knowledge of Galois rings, please see Refs. [10,11].

2 GMW sequences over Galois rings

Now we define a new family of GMW sequences over Galois ring Z_{p^e}.

2.1 Permutation on R

Let b be an integer with $1\leqslant b\leqslant p^r-1$ and $(b,p)=(b,p^r-1)=1$. For any element $a=p^iw$ in R, where $0\leqslant i\leqslant e-1$ and $w\in R^*\cup\{0\}$, we define the map $\varphi: R\to R$ as

Translated from *Journal on Communications*, 2008, 29(3): 23–26 [译自: 通信学报]

Nigang SUN (✉)
Department of Computer Science and Engineering, East China University of Science and Technology, Shanghai 200237, China
E-mail: nigsun@ecust.edu.cn

Nigang SUN, Lei HU
State Key Laboratory of Information Security, Graduate University of Chinese Academy of Sciences, Beijing 100049, China

$$\varphi(a) = p^i w^b.$$

Lemma 1 The map φ is a permutation on R.

Proof Let i be an integer with $0 \leqslant i \leqslant e-1$. It suffices to show that φ is an injection on $p^i R^*$. Let $p^i w_1$, $p^i w_2$ be any two elements of $p^i R^*$, where $w_1, w_2 \in R^*$. Assume that

$$\varphi(p^i w_1) = p^i w_1^b = \varphi(p^i w_2) = p^i w_2^b,$$

then we have

$$w_1^b = w_2^b + p^{e-i}x, \tag{1}$$

where $x \in R$. Equation (1) implies that $w_1^{bp^{e-1}} = w_2^{bp^{e-1}}$, since the characteristic of R equals p^e. Suppose $w_1 = \alpha_1\beta_1$ and $w_2 = \alpha_2\beta_2$, where $\alpha_1, \alpha_2 \in G_C$, $\beta_1, \beta_2 \in G_A$, and applied to the equation $w_1^{bp^{e-1}} = w_2^{bp^{e-1}}$, we can conclude that $\alpha_1^{bp^{e-1}} = \alpha_2^{bp^{e-1}}$. Note that the orders of α_1 and α_2 are both factors of $p^r - 1$ and $(p^r - 1, bp^{e-1}) = 1$, we obtain that $\alpha_1 = \alpha_2$. Hence, we have $p^i\beta_1^b = p^i\beta_2^b$. It follows that $\beta_1^b = \beta_2^b + p^{e-i}y$, where $y \in R$. From $(b, p^{e-1}) = 1$, we know that there exists an integer c which satisfies that $bc \equiv 1 \pmod{p^{e-1}}$, then

$$\beta_1 = (\beta_1^b)^c = (\beta_2^b + p^{e-i}y)^c = \beta_2 + p^{e-i}y', \tag{2}$$

where $y' \in R$. Multiplying both sides of Eq. (2) by p^i, we have $p^i\beta_1 = p^i\beta_2$. This implies that $p^i w_1 = p^i w_2$. The Lemma follows.

2.2 Construction of GMW sequences

Let α be an element of order $p^{ru} - 1$ in R' and $v \in R'^*$. Associated with the permutation φ, we can define the GMW sequence S^v over Galois ring Z_{p^e} as

$$S^v = \{\mathrm{Tr}_1^r\{\varphi[\mathrm{Tr}_r^{ru}(v\alpha^i)]\}\}_{i \geqslant 0}.$$

We also can define the GMW sequences family GGMW as

$$\mathrm{GGMW} = \{S^v : v \in R'^*\}.$$

Note that φ is a permutation on R, the period of S^v is equal to $p^{ru} - 1$.

3 Linear complexity

We employ the same techniques and notations as in the preceding sections.

Definition 1 We call polynomial $C(x) = 1 + c_1x + c_2x^2 + \cdots + c_mx^m \in Z_{p^e}[x]$ the associated connection polynomial of periodic sequence $S = \{s_i\}_{i \geqslant 0}$ over Z_{p^e}, if the coefficients $c_1, c_2, \ldots, c_m$ satisfy

$$s_j = -\sum_{i=1}^{m} c_i s_{j-i}, \ \forall j \geqslant m.$$

Definition 2 The linear complexity (LC) of periodic sequence $S = \{s_i\}_{i \geqslant 0}$ over Z_{p^e} is equal to $\min\{\deg(C(x))$: $C(x)$ is an associated connection polynomial of $S\}$.

Lemma 2 [12] Suppose $S = \{s_i\}_{i \geqslant 0}$ is a sequence of period L. Let $S(x) = s_0 + s_1x + \cdots + s_{L-1}x^{L-1}$. Then $C(x)$ is an associated connection polynomial of S if and only if $S(x)C(x) = 0 \pmod{x^L - 1}$.

Definition 3 [13] Suppose $S = \{s_i\}_{i \geqslant 0}$ is a sequence of period $p^{ru} - 1$ over Z_{p^e}. Let α be any primitive element of R', then the Fourier representation of S is

$$s_i = \sum_{j=0}^{p^{ru}-2} \hat{s}_j \alpha^{ji}, \ 0 \leqslant i < p^{ru} - 1,$$

where

$$\hat{s}_j = n\sum_{i=0}^{p^{ru}-2} s_i \alpha^{-ji}, \ n(p^{ru} - 1) \equiv 1 \bmod p^e, \ 0 \leqslant j < p^{ru} - 1.$$

Theorem 1 Suppose $S = \{s_i\}_{i \geqslant 0}$ is a sequence of period $p^{ru} - 1$ over Z_{p^e}. Then the linear complexity of S is equal to the number of nonzero terms appearing in the Fourier representation of S, i.e.,

$$\mathrm{LC}(S) = |\{\hat{s}_j : \hat{s}_j \neq 0, \ 0 \leqslant j \leqslant p^{ru} - 2\}|.$$

Proof Assume that $j_1, j_2, \ldots, j_m$ are nonzero positions in the Fourier representation of S. This means that $\hat{s}_{j_i} \neq 0$ for $i = 1, 2, \ldots, m$. Note that $\hat{s}_j = nS(\alpha^{-j})$, we have

$$S(\alpha^{-j}) = \begin{cases} 0, \ j \in \{0,1,\ldots,p^{ru} - 2\} \setminus \{j_1, j_2, \ldots, j_m\}, \\ \text{nonzero}, \ j \in \{j_1, j_2, \ldots, j_m\}. \end{cases}$$

Now choose $C(x) = (x - \alpha^{-j_1})(x - \alpha^{-j_2}) \cdots (x - \alpha^{-j_m})$. Then all the roots of $x^{p^{ru}-1} - 1$, i.e., $\alpha^0, \alpha^{-1}, \alpha^{-2}, \ldots, \alpha^{2-p^{ru}}$, are the roots of $S(x)C(x)$. From Lemma 2, $C(x)$ is an associated connection polynomial of S. It implies that $\mathrm{LC}(S) \leqslant m$. If $\mathrm{LC}(S) \neq m$, then there exists another associated connection polynomial $C_0(x)$ of S with degree less than m. Also from Lemma 2, we obtain that the number of nonzero terms appearing in the Fourier representation of S is less than m. It is a contradiction. Thus, $\mathrm{LC}(S) = m$. This completes the proof.

We assume from now on that $b \geqslant e$. For any element $a = p^i w$ with $0 \leqslant i \leqslant e-1$ and $w \in R^* \cup \{0\}$ in R, we define a map $\hat{\varphi} : R \to R$ as

$$\hat{\varphi}(a) = \begin{cases} 0, \ i = 0, \\ p^i w^b, \ i \geqslant 1. \end{cases}$$

For any sequence $S^v = \{s_i\}_{i \geqslant 0}$ of GGMW, where $s_i = \mathrm{Tr}_1^r\{\varphi[\mathrm{Tr}_r^{ru}(v\alpha^i)]\}$, utilizing the map $\hat{\varphi}$, we have

$$s_i = \mathrm{Tr}_1^r\{[\mathrm{Tr}_r^{ru}(v\alpha^i)]^b\} + \mathrm{Tr}_1^r\{\hat{\varphi}[\mathrm{Tr}_r^{ru}(v\alpha^i)]\}.$$

Let

$$S_1^v = \{\mathrm{Tr}_1^r\{[\mathrm{Tr}_r^{ru}(v\alpha^i)]^b\}\}_{i\geqslant 0},$$
$$S_2^v = \{\mathrm{Tr}_1^r\{\hat{\varphi}[\mathrm{Tr}_r^{ru}(v\alpha^i)]\}\}_{i\geqslant 0},$$

then we have

$$S^v = S_1^v + S_2^v. \tag{3}$$

Using the p-adic expansion of b, we can write b in the form

$$b = \sum_{i=1}^{H} b_i p^{j_i},$$

where $1\leqslant b_i\leqslant p-1$, $0\leqslant j_i\leqslant r-1$ and H is the number of nonzero terms appearing in the p-adic expansion of b.

Lemma 3 The linear complexity of S^v satisfies

$$\mathrm{LC}(S^v)\geqslant r\prod_{i=1}^{H}\binom{u+b_i-1}{b_i}.$$

Proof It is clear that $p^{e-1}S^v = p^{e-1}S_1^v$ is isomorphic to some p-ary GMW sequence. Utilizing the result given by Zhu and Li (Theorem 2 in Ref. [6]), we obtain that

$$\mathrm{LC}(p^{e-1}S_1^v) = r\prod_{i=1}^{H}\binom{u+b_i-1}{b_i}.$$

Hence, from the Fourier representation of S^v and Theorem 1, we have

$$\mathrm{LC}(S^v)\geqslant \mathrm{LC}(p^{e-1}S^v) = \mathrm{LC}(p^{e-1}S_1^v)$$
$$= r\prod_{i=1}^{H}\binom{u+b_i-1}{b_i}.$$

Lemma 4 The linear complexity of S_1^v satisfies

$$\mathrm{LC}(S_1^v)\leqslant r\binom{eu+b-1}{b}.$$

Proof Let $\Gamma = \{0,1,\alpha,\alpha^2,...,\alpha^{p^{ru}-2}\}$. Then v can be expressed as $v = a_0 + pa_1 + \cdots + p^{e-1}a_{e-1}$, where a_0, $a_1,...,a_{e-1}\in\Gamma$. This implies that v is a linear sum of at most e distinct powers of α. Moreover, each term $\mathrm{Tr}_1^r\{[\mathrm{Tr}_r^{ru}(v\alpha^i)]^b\}$ $(i\geqslant 0)$ of S_1^v can be expressed as a linear sum of at most $r\binom{eu+b-1}{b}$ distinct powers of α. From Theorem 1, we have

$$\mathrm{LC}(S_1^v)\leqslant r\binom{eu+b-1}{b}.$$

Let $T = (p^{ru}-1)/(p^r-1)$. We need the following lemma.

Lemma 5 [6] Let $S=\{\mathrm{Tr}_r^{ru}(\alpha^i)\}_{i\geqslant 0}$ be a field sequence, where α is primitive in GF(p^{ru}). Then every segment of T consecutive elements from S contains exactly $(p^{(u-1)r}-1)/(p^r-1)$ zeros.

Lemma 6 For any $v\in R'^*$, let $\hat{S}^v = \{s_i'\}_{i\geqslant 0}$ be an intermediate sequence over R given by $s_i'=\mathrm{Tr}_r^{ru}(v\alpha^i)$, where α is primitive in R'. Then every segment of T consecutive elements from $\hat{S}^v$ contains exactly $(p^{(u-1)r}-1)/(p^r-1)$ elements from the ideal (p).

Proof Observe that $p^{e-1}\hat{S}^v$ is isomorphic to some sequence defined in Lemma 5. Thus, from Lemma 5, every segment of T consecutive elements in $p^{e-1}\hat{S}^v$ contains exactly $(p^{(u-1)r}-1)/(p^r-1)$ zeros. Since $p^{e-1}s_i'$ is zero if and only if $s_i'\in(p)$, the result follows.

Lemma 7 The linear complexity of S_2^v satisfies

$$\mathrm{LC}(S_2^v)\leqslant Tr.$$

Proof Assume that S_2^v is nonzero and $S_2^v = \{s_i\}_{i\geqslant 0}$. Let $V(x) = v_0 + v_1x + \cdots + v_{p^{ru}-2}x^{p^{ru}-2}$, where $v_i = \hat{\varphi}[\mathrm{Tr}_r^{ru}(v\alpha^i)]$. From the definition of $\hat{\varphi}$ and Lemma 6, $v_0,v_1,...,v_{T-1}$ are not all zeros. Let $v_{i_1},v_{i_2},...,v_{i_t}$ be the nonzero terms in $\{v_0,v_1,...,v_{T-1}\}$. It is obvious that $\mathrm{Tr}_r^{ru}(v\alpha^{i_j})$ $(1\leqslant j\leqslant t)$ are zero divisors of R. From

$$\mathrm{Tr}_r^{ru}(v\alpha^{mT+i}) = \alpha^{mT}\mathrm{Tr}_r^{ru}(v\alpha^i),\ 0\leqslant m < p^r-1,$$

we can conclude that the nonzero terms in $\{v_0,v_1,...,v_{p^{ru}-2}\}$ follow the T periodicity. Let $\hat{V}(x) = v_{i_1}x^{i_1} + v_{i_2}x^{i_2} + \cdots + v_{i_t}x^{i_t}$, we have

$$\begin{aligned}V(x) &= \sum_{m=0}^{p^r-2}(v_{mT+i_1}x^{mT+i_1} + v_{mT+i_2}x^{mT+i_2} + \cdots + v_{mT+i_t}x^{mT+i_t})\\ &= \sum_{m=0}^{p^r-2}x^{mT}\{\hat{\varphi}[\mathrm{Tr}_r^{ru}(v\alpha^{mT+i_1})]x^{i_1} + \hat{\varphi}[\mathrm{Tr}_r^{ru}(v\alpha^{mT+i_2})]x^{i_2}\\ &\quad + \cdots + \hat{\varphi}[\mathrm{Tr}_r^{ru}(v\alpha^{mT+i_t})]x^{i_t}\}\\ &= \sum_{m=0}^{p^r-2}x^{mT}\alpha^{mTb}\{\hat{\varphi}[\mathrm{Tr}_r^{ru}(v\alpha^{i_1})]x^{i_1} + \hat{\varphi}[\mathrm{Tr}_r^{ru}(v\alpha^{i_2})]x^{i_2}\\ &\quad + \cdots + \hat{\varphi}[\mathrm{Tr}_r^{ru}(v\alpha^{i_t})]x^{i_t}\}\\ &= \sum_{m=0}^{p^r-2}\alpha^{mTb}x^{mT}\,\hat{V}(x).\end{aligned}$$

For any integer j with $0\leqslant j < p^{ru}-1$, $V(\alpha^{-j}) = \delta\sum_{m=0}^{p^r-2}\alpha^{mT(b-j)}$, where $\delta = \hat{V}(\alpha^{-j})$. If $j = b' + n(p^r-1)$, where $b'\neq b$, $0\leqslant n < T$, we have $V(\alpha^{-j}) = \delta\sum_{m=0}^{p^r-2}\alpha^{mT(b-b')} = 0$. If $j = b + n(p^r-1)$, where $0\leqslant n < T$, we have $V(\alpha^{-j}) = (p^r-1)\delta$. Then $V(\alpha^{-j})\neq 0$ if and only if δ is nonzero. Hence, the number of j's in $\{0,1,...,p^{ru}-2\}$ which satisfy that $V(\alpha^{-j})\neq 0$ is at most T.

Now we prove by contradiction that the linear complexity of S_2^v is at most Tr. Assume that the number of j's

in $\{0,1,...,p^{ru}-2\}$ which satisfy that $S(\alpha^{-j})\neq 0$ is greater than Tr. Let $j_0\in\{0,1,\ldots,p^{ru}-2\}$ and satisfy $S(\alpha^{-j_0})=\sum_{i=0}^{p^{ru}-2} s_i\alpha^{-j_0 i}\neq 0$. From the definition of v_i, $s_i=\mathrm{Tr}_1^r(v_i)$. Thus

$$\sum_{i=0}^{p^{ru}-2} s_i\alpha^{-j_0 i}=\sum_{i=0}^{p^{ru}-2}\mathrm{Tr}_1^r(v_i)\alpha^{-j_0 i}=\sum_{i=0}^{p^{ru}-2}\sum_{k=0}^{r-1}\sigma^k(v_i)\alpha^{-j_0 i}$$

$$=\sum_{k=0}^{r-1}\sum_{i=0}^{p^{ru}-2}\sigma^k(v_i\alpha^{-j_0 i p^{ru-k}})=\sum_{k=0}^{r-1}\sigma^k[V(\alpha^{-j_0 p^{ru-k}})],$$

where σ is the Frobenius automorphism of R over Z_{p^e} [11]. From $S(\alpha^{-j_0})=\sum_{i=0}^{p^{ru}-2} s_i\alpha^{-j_0 i}\neq 0$, $\sum_{k=0}^{r-1}\sigma^k[V(\alpha^{-j_0 p^{ru-k}})]\neq 0$. Then there exists $k_0\in\{0,1,\ldots,r-1\}$ satisfying that $\sigma^{k_0}[V(\alpha^{-j_0 p^{ru-k_0}})]\neq 0$. Moreover, we have $V(\alpha^{-j_0 p^{ru-k_0}})\neq 0$. This means that for any j with $S(\alpha^{-j})\neq 0$, there exists one $k\in\{0,1,...,r-1\}$ satisfying that $V(\alpha^{-jp^{ru-k}})\neq 0$. And we also can conclude that for any two distinct $j_1,j_2\in\{0,1,...,p^{ru}-2\}$, if there exists two corresponding k_1, $k_2\in\{0,1,...,r-1\}$ satisfying that $j_1 p^{ru-k_1}\equiv j_2 p^{ru-k_2}$ mod $p^{ru}-1$, then we must have $k_1\neq k_2$. Hence, the number of j's in $\{0,1,...,p^{ru}-2\}$ which satisfy that $V(\alpha^{-j})\neq 0$ is greater than T. It is a contradiction. Then the number of j's in $\{0,1,...,p^{ru}-2\}$ which satisfies that $S(\alpha^{-j})\neq 0$ is at most Tr. From Theorem 1, we obtain that the linear complexity of S_2^v is at most Tr. This completes the proof.

Utilizing Eq. (3), Lemmas 3, 4 and 7, we can finally obtain the following theorem.

Theorem 2 The linear complexities of sequences of GGMW satisfy

$$r\prod_{i=1}^{H}\binom{u+b_i-1}{b_i}\leqslant \mathrm{LC}\leqslant r\binom{eu+b-1}{b}+Tr.$$

References

1. Kumar P V. Frequency-hopping code sequence designs having large linear span. IEEE Transactions on Information Theory, 1988, 34(1): 146–151
2. Scholtz R A, Welch L R. GMW sequences. IEEE Transactions on Information Theory, 1984, 30(3): 548–553
3. Antweiler M, Bömer L. Complex sequences over GF (p^M) with a two-level autocorrelation function and a large linear span. IEEE Transactions on Information Theory, 1992, 38(1): 120–130
4. Klapper A, Chan A H, Goresky M. Cascaded GMW sequences. IEEE Transactions on Information Theory, 1993, 39(1): 177–183
5. Chung H, No J S. Linear span of extended sequences and cascaded GMW sequences. IEEE Transactions on Information Theory, 1999, 45(6): 2060–2065
6. Zhu J K, Li S P. P-ary GMW sequences. Journal of China University of Science and Technology, 1991, 21(4): 433–446 (in Chinese)
7. No J S. Generalization of GMW sequences and No sequences. IEEE Transactions on Information Theory, 1996, 42(1): 260–262
8. Gong G. Q-ary cascaded GMW sequences. IEEE Transactions on Information Theory, 1996, 42(1): 263–267
9. Udaya P, Siddiqi M U. Generalized GMW quadriphase sequences satisfying the Welch bound with equality. Applicable Algebra in Engineering, Communication and Computing, 2000, 10(3): 203–225
10. McDonald B R. Finite Rings With Identity. New York: Marcel Dekker, 1974
11. Wan Z X. Finite Fields and Galois Rings. Singapore: World Scientific Publisher, 2003
12. Wan Z X. Algebra and Coding Theory. Beijing: Science Press, 1976 (in Chinese)
13. Golomb S W, Gong G. Signal Design for Good Correlation: For Wireless Communication, Cryptography and Radar. Cambridge: Cambridge University Press, 2005