Cyclic Inequivalence of Cascaded GMW-Sequences

*Solomon W. Golomb, Guang Gong and Zong Duo Dai**

Communication Sciences Institute
University of Southern California
Electrical Engineering-Systems, EEB # 500
Los Angeles, California 90089-2565
Tels. 213 740-7333 and 213 740-7332
Fax. 213 740-8729
E-mails: milly@mizar.usc.edu and guanggon@milly.usc.edu

*Dept. of Math., State Key Lab. of Information Security
Graduate School, Academia Sinica, Beijing 100039-08, China
Email. yangdai@mimi.cnc.ac.cn

Abstract

Cascaded GMW sequences have two-level autocorrelation functions, which have important applications in communications and cryptology. In this paper, we consider the cascaded GMW sequences corresponding to a fixed finite chain of finite fields, and study the problem of how to determine all these different cascaded GMW sequences without repetition, and the problem of whether the different cascaded GMW sequences are cyclically inequivalent. By introducing the so-called restricted integer systems (RISs), it is proved that all the cascaded GMW sequences can be determined by means of the RISs, and the sequences determined by different RISs are different. Moreover, different cascaded GMW sequences are cyclically inequivalent.

Keywords: GMW-sequences, trace functions, cyclic inequivalence.

Cyclic Inequivalence of Cascaded GMW-Sequences

Solomon W. Golomb, Guang Gong and Zong Duo Dai

Abstract

Cascaded GMW sequences have two-level autocorrelation functions, which have important applications in communications and cryptology. In this paper, we consider the cascaded GMW sequences corresponding to a fixed finite chain of finite fields, and study the problem of how to determine all these different cascaded GMW sequences without repetition, and the problem of whether the different cascaded GMW sequences are cyclically inequivalent. By introducing the so-called restricted integer systems (RISs), it is proved that all the cascaded GMW sequences can be determined by means of the RISs, and the sequences determined by different RISs are different. Moreover, different cascaded GMW sequences are cyclically inequivalent.

Keywords: GMW-sequences, trace functions, cyclic inequivalence.

1 Introduction

Pseudo-random sequences have important applications in communications and cryptology. Cascaded GMW sequences, sometimes called generalized GMW sequence, have two-level autocorrelation functions. GMW sequences and generalized GMW sequences have been extensively investigated [8, 1, 5, 2, 3, 7]. The autocorrelations and linear spans of cascaded GMW sequences have been discussed in the literature [5, 2].

Given a finite chain of finite fields, it is known that each of the corresponding cascaded GMW sequences can be determined by a primitive element and an integer system. For sequence design in CDMA communications, stream ciphers and various communications applications [9, 4], guaranteeing that the sequences generated by a specific method and predetermined parameters are cyclically distinct (or cyclically inequivalent) is an important problem. Hence, to determine whether the cascaded GMW sequences generated by different integer systems are cyclically inequivalent is very important in the implementation of cascaded GMW sequences. In the published literature, reference [7] stated a result for a given field chain of characteristic 2 without proof. In this paper, we completely solve this problem for any characteristic and any given field chain. In other words, in this paper we study the problem of how to determine all different cascaded GMW sequences and the problem of whether the different cascaded GMW sequences are cyclically inequivalent. By introducing the so-called restricted integer systems (RISs), we prove that all the cascaded GMW sequences can be determined by means of restricted integer systems (RISs), and that the sequences determined by different restricted integer systems (RISs) are different. Moreover, different cascaded GMW sequences are cyclically inequivalent.

2 $\underline{\mathbf{c}}$-GMW Sequences and $\underline{\mathbf{c}}$-RISs

In this paper, we always assume that p is a prime integer, and c_i $(0 \le i \le r)$ and n_i $(1 \le i \le r)$ are positive integers satisfying

$$c_i = c_{i-1}n_i, n_i > 1, \qquad 0 < i \le r. \tag{1}$$

The corresponding field chain

$$F_0 \subset F_1 \subset \cdots \subset F_r, \qquad F_i = GF(p^{c_i}). \tag{2}$$

will be written simply as $\underline{\mathbf{c}} = (c_0, c_1, \cdots, c_r)$. We call $\underline{\mathbf{e}} = (e_0, e_1, \cdots, e_r)$ a $\underline{\mathbf{c}}-$ integer system if

$$(e_i, p^{c_i} - 1) = 1, \qquad \forall i. \tag{3}$$

Any $\underline{\mathbf{c}}-$integer system $\underline{\mathbf{e}} = (e_0, e_1, \cdots, e_r)$ can determine recursively a function $f_{(e_0,e_1,\cdots,e_r)}(x)$ from F_r onto F_0 by:

$$f_{(e_r)}(x) = x^{e_r}, \qquad f_{(e_i,e_{i+1},\cdots,e_r)}(x) = Tr_{F_i}^{F_{i+1}}(f_{(e_{i+1},\cdots,e_r)}(x))^{e_i}. \tag{4}$$

The function $f_{(e_0,e_1,\cdots,e_r)}(x)$ will be called $\underline{\mathbf{c}}-$GMW function, which together with a primitive element α in F_r determines a cascaded GMW sequence. In other words, a $\underline{\mathbf{c}}-$GMW sequence is defined by

$$A(e_0, e_1, \cdots, e_r; \alpha) = \{a_i\}_0^\infty, \qquad a_i = f_{(e_0,e_1,\cdots,e_r)}(\alpha^i). \tag{5}$$

We note that if $\beta = \alpha^k$ is another primitive element, then

$$A(e_0, e_1, \cdots, e_r; \beta) = A(e_0, e_1, \cdots, ke_r; \alpha).$$

Hence, in order to determine all the $\underline{\mathbf{c}}-$sequences, it is enough to use only one primitive element. In the sequel, we fix a primitive element α, and write simply

$$A(e_0, e_1, \cdots, e_r) = A(e_0, e_1, \cdots, e_r; \alpha). \tag{6}$$

We note also that

$$A(e_0, p^{b_1}e_1, \cdots, p^{b_i}e_i, \cdots, p^{b_r}e_r) = A(p^{b_1+b_2+\cdots+b_r}e_0, e_1, \cdots, e_i, \cdots, e_r). \tag{7}$$

Therefore, in order to reduce this kind of redundancy in determining $\underline{\mathbf{c}}-$GMW sequences, we introduce a concept called $\underline{\mathbf{c}}-$restricted integer systems (RIS). There is a $\underline{\mathbf{c}}-$integer system $\underline{\mathbf{e}} = (e_0, e_1, \cdots, e_r)$ with the properties that $0 \le e_0 < p^{c_0} - 1$ and e_i is a $p-$coset leader modulo $p^{c_i} - 1$ for each $i : 1 \le i \le r$. Here, by saying an integer e is a $p-$coset leader modulo $p^c - 1$ we mean

$$e = \min\{t | 0 \le t < p^c - 1,\ t \equiv p^i e \pmod{p^c - 1},\ 0 \le i < c\}. \tag{8}$$

Based on equation (7), it is easy to see the following theorem

Theorem 1 *Each $\underline{\mathbf{c}}-$GMW sequence can be determined by a $\underline{\mathbf{c}}-$RIS.*

3 RISs and Cyclic Inequivalence

Two periodic sequences $A = \{a_i\}_0^\infty$ and $B = \{b_i\}_0^\infty$ are called *cyclically equivalent* if there exists an integer k such that

$$a_i = b_{i+k}, \forall i \geq 0 \tag{9}$$

and in this case we write $A = L^k(B)$, or simply $A \sim B$.

The main result of this paper is

Theorem 2 *Different* $\underline{\mathbf{c}}-$*RISs determine different* $\underline{\mathbf{c}}-$*GMW sequences; moreover, all the different* $\underline{\mathbf{c}}-$*GMW sequences are cyclically inequivalent.*

Note that

$$A(\underline{\mathbf{e}}) = L^k A(\underline{\mathbf{d}})$$

if and only if

$$f_{(\underline{\mathbf{e}})}(\alpha^i) = f_{(\underline{\mathbf{d}})}(\alpha^{k+i}),\ \forall i \geq 0,$$

where the latter is equivalent to

$$f_{(\underline{\mathbf{e}})}(x) = f_{(\underline{\mathbf{d}})}(\alpha^k x).$$

Hence, to prove Theorem 2, it is enough to prove the following theorem:

Theorem 3 *Let* $\underline{\mathbf{e}} = (e_1, e_2, \cdots, e_r)$ *and* $\underline{\mathbf{d}} = (d_1, d_2, \cdots, d_r)$ *be two* $\underline{\mathbf{c}}-$*RISs, and* $0 \neq \theta \in F_r$*. If*

$$f_{(\underline{\mathbf{e}})}(\theta x) = f_{(\underline{\mathbf{d}})}(x), \qquad \forall x \in F_r$$

then

$$\underline{\mathbf{e}} = \underline{\mathbf{d}}, \quad \theta = \mathbf{1}.$$

We will prove Theorem 3 in the next section. As an easy consequence of Theorem 2, we get

Corollary 1 *The total number of different* $\underline{\mathbf{c}}-$*GMW sequences is*

$$\varphi(p^{c_0} - 1) \prod_{1 \leq i \leq r} \frac{\varphi(p^{c_i} - 1)}{c_i}.$$

4 Proof of Theorem 3

It is well known that a function $f(x)$ from a finite field $GF(q)$ to itself can be uniquely represented by a polynomial of the form

$$f(x) = \sum_{0 \leq i < q} f_i x^i, \quad f_i \in GF(q).$$

The number of nonzero coefficients in the above expression will be called the *weight* of f, written $W(f)$. For an integer e, if $e = \sum_{0\leq i} e_i p^i, 0 \leq e_i < p$, the $p-$*weight* of e, denoted by $W_p(e)$, is defined as

$$W_p(e) = \sum_{0\leq i} e_i. \tag{10}$$

We list the following lemma whose proofs for characteristic $p = 2$ and $p > 2$ can be found in [8, 6], respectively.

Lemma 1 *Let $q = p^c$, $n \geq 1$, and $e = \sum_{i\geq 0} e_i p^i, 0 \leq e_i < p$, and $(t, q^n) = 1$, and $0 \neq \theta \in GF(p^n)$. Then*

$$W((Tr_{GF(q)}^{GF(q^n)}(\theta x^t))^e) = \prod_{0\leq i<c} \left(\begin{array}{c} n-1+e_i \\ n-1 \end{array} \right).$$

In particular, when $n > 1$, then $W((Tr_{GF(q)}^{GF(q^n)}(\theta x))^e) = n$ if and only if $W_p(e) = 1$.

Lemma 2 *Let $(e_0 p^u, e_1)$ and $(d_0 p^v, d_1)$ be two $(c_0, c_1)-$integer systems, where $0 \leq u < c_0, 0 \leq v < c_0$, let e_0 and d_0 be $p-$coset leaders modulo $p^{c_0} - 1$, and let θ and ρ be elements in F_1. Then*

$$f_{(d_0 p^u, d_1)}(\theta x) = f_{(e_0 p^v, e_1)}(\rho x)$$

if and only if

$$\theta = \rho = 0,$$

or there exists $i, 0 \leq i < n_1$, such that

$$e_0 = d_0, \quad \theta = \rho, \quad d_1 p^u \equiv e_1 p^{v+c_0 i} \pmod{p^{c_1} - 1}.$$

Proof It is enough to prove the "only if". We write

$$e \equiv e_0 d_0^{-1} \pmod{p^{c_0} - 1}, \qquad 0 \leq e < p^{c_0} - 1.$$

From the assumption it is easy to see that

$$f_{(1, d_1 p^u)}(\theta x) = f_{(e, e_1 p^v)}(\rho x) \tag{11}$$

Note that $W(1) = 1$; from Lemma 1 we see

$$n_1 = W(f_{(1,d_1 p^u)}(\theta x)) = W(f_{(e,e_1 p^v)}(\rho x));$$

and then $W(e) = 1$. So there exists j such that $p^j \equiv e \equiv e_0 d_0^{-1} \pmod{p^{c_0} - 1}$. Since both e_0 and d_0 are $p-$leaders modulo $p^{c_0} - 1$, then $j = 0$ and $e = 1$, hence $e_0 = d_0$. Observing the polynomial expressions on the two sides of equation (11), we see that there exists a monomial $(\theta x)^{d_1 p^u}$ on the left side, and that all the monomials on the right side are of the form $(\rho x)^{e_1 p^{v+c_0 j}}, 0 \leq j < n_1$. So there exists $i, 0 \leq i < n_1$, such that

$$d_1 p^u \equiv e_1 p^{v+c_0 i} \pmod{p^{c_1}-1},$$
$$\theta^{d_1 p^u} = \rho^{e_1 p^{v+c_0 i}}$$

which leads to $\theta = \rho$.

$\square$

From Lemma 2 it is easy to obtain the following corollaries.

Corollary 2 *Let K be an extension field of F_1, and both $g(x)$ and $h(x)$ be non-zero functions from K to F_1. Let both $(d_0 p^u, d_1)$ and $(e_0 p^v, e_1)$ be $(c_0, c_1)-$integer systems, both d_0 and e_0 be $p-$coset leaders modulo $p^{c_0}-1$, and $0 \leq u < c_0, 0 \leq v < c_0$. If*

$$f_{(d_0 p^u, d_1)}(g(x)y) = f_{(e_0 p^v, e_1)}(h(x)y), \ \forall y \in F_1, \ x \in K,$$

then there exists $i, 0 \leq i < n_1$, such that

$$d_0 = e_0, \ g(x) = h(x), \ d_1 p^u = e_1 p^{v+c_0 i}.$$

Corollary 3 *Let both (d_0, d_1) and (e_0, e_1) be $(c_0, c_1)-$RISs, and let $\theta \in F_1$. If*

$$f_{(d_0, d_1)}(\theta x) = f_{(e_0, e_1)}(x), \ \forall x \in F_1,$$

then

$$(d_0, d_1) = (e_0, e_1), \ \theta = 1.$$

Proof of Theorem 3.
We will proceed with induction on r. Theorem 3 is true for $r = 1$ by Corollary 3. Now assume that $r > 1$. Set

$$e \equiv e_1 e_2 \cdots e_r \pmod{p^{c_1}-1},$$

$$d \equiv d_1 d_2 \cdots d_r \pmod{p^{c_1}-1},$$

and set

$$g(x) = f_{(e_1, e_2, \cdots, e_r)}(\theta x)^{e^{-1}},$$
$$h(x) = f_{(d_1, d_2, \cdots, d_r)}(x)^{d^{-1}}.$$

It is not difficult to see that

$$f_{(e_0, e_1, e_2, \cdots, e_r)}(\theta y x) = f_{(e_0, e)}(y f_{(e_1, e_2, \cdots, e_r)}(\theta x)^{e^{-1}}) = f_{(e_0, e)}(y g(x)), \forall y \in F_1, x \in F_r.$$

Similarly

$$f_{(d_0, d_1, d_2, \cdots, d_r)}(yx) = f_{(d_0, d)}(y h(x)), \forall y \in F_1, x \in F_r.$$

So we have

$$f_{(e_0,e)}(yg(x)) = f_{(e_0,e_1,e_2,\cdots,e_r)}(\theta yx) = f_{(d_0,d_1,d_2,\cdots,d_r)}(yx) = f_{(d_0,d)}(yh(x)), \forall y \in F_1, x \in F_r.$$

Now we write

$$d_0 \equiv a_0 p^u \pmod{p^{c_0} - 1}, \qquad 0 \le u < c_0,$$

and

$$e_0 \equiv b_0 p^v \pmod{p^{c_0} - 1}, \qquad 0 \le v < c_0$$

where both a_0 and b_0 are $p-$coset leaders modulo $p^{c_0} - 1$. Notice that both $f(x)$ and $g(x)$ are nonzero functions. From Corollary 2, there exists $i, 0 \le i_1 < n_1$ such that

$$a_0 = b_0,\ g(x) = h(x),\ dp^u \equiv ep^{v+c_0 i_1} \pmod{p^{c_1} - 1}.$$

Then we have

$$f_{(e_1 p^{v+c_0 i_1}, e_2 \cdots e_r)}(\theta x) = g(x)^{ep^{v+c_0 i_1}} = h(x)^{dp^u} = f_{(d_1 d_2 \cdots d_r)}(x)^{p^u} = f_{(d_1 p^u, d_2 \cdots d_r)}(x).$$

By the inductive assumption we have $\theta = 1$, $(e_2, \cdots, e_r) = (d_2, \cdots, d_r)$ and $d_1 p^u \equiv e_1 p^{v+c_0 i_1} \pmod{p^{c_1} - 1}$. Since both d_1 and e_1 are $p-$coset leaders modulo $p^{c_1} - 1$, we get $e_1 = d_1$ and $u \equiv v + c_0 i_1 \pmod{c_1}$, so that $u = v$. Consequently, $d_0 = a_0 p^u = b_0 p^v = e_0$. $\square$

Acknowledgment: The work of the third author was supported by the Chinese Natural Science Foundation (69473019).

References

[1] M. Antweiler and L. Bőmer, Complex sequences over $GF(p)$ with a two-level autocorrelation function and a large linear span, *IEEE Trans. on Inform. Theory*, vol. IT-38, No. 1, pp. 120-130, January 1992.

[2] G. Gong, On q-ary cascaded GMW sequences, *IEEE Trans. on Inform. Theory*, vol. 42, No. 1, January 1996, pp. 263-267.

[3] G. Gong, A new class of q-ary PN sequences, *IEEE Trans. on Inform. Theory*, May 1997.

[4] S.W. Golomb, *Shift-Register Sequences*, Holden-Day, San Francisco, CA, 1967; Aegean Park Press, Laguna Hills, CA, 1982.

[5] A. Klapper, A.H. Chan, and M. Goresky, Cascaded GMW sequences, *IEEE Trans. on Inform. Theory*, vol. IT-39, No. 1, pp. 177-183, January 1993.

[6] Tor Herlestam, On functions of linear shift register sequences, *Advances in Cryptology-EuroCrypt'85*, Lecture Notes in Computer Science, No. 219, Springer-Verlag, 1985, pp. 119-129.

[7] J. S. No, Generalization of GMW sequences and No sequences, *IEEE Trans. on Inform. Theory*, vol. 42, No. 1, January 1996, pp. 260-262.

[8] R.A. Scholtz and L.R. Welch, GMW sequences, *IEEE Trans. on Inform. Theory*, vol. IT-30, No. 3, pp. 548-553, May 1984.

[9] M.K. Simon, J.K. Omura, R.A. Scholtz and B.K. Levitt, *Spread Spectrum Communications Handbook*, McGraw-Hill, Inc., Revised version, 1994, Computer Science Press, 1985.