Available online at www.sciencedirect.com

SCIENCE DIRECT®

Finite Fields and Their Applications 11 (2005) 674–683

FINITE FIELDS AND THEIR APPLICATIONS

http://www.elsevier.com/locate/ffa

New pairs of m-sequences with 4-level cross-correlation

Tor Helleseth, Petri Rosendahl*,[1]

Department of Informatics, University of Bergen, Hoyteknologisenteret, N-5020 Bergen, Norway

Received 20 January 2003; revised 10 August 2004

Communicated by Peter Jau-Shyong Shiue

Available online 6 June 2005

Abstract

Let ω be a primitive element of $GF(2^n)$, where $n \equiv 0 (\mathrm{mod}\, 4)$. Let $d = (2^{2k} + 2^{s+1} - 2^{k+1} - 1)/(2^s - 1)$, where $n = 2k$, and s is such that $2s$ divides k. We prove that the binary m-sequences $s(t) = \mathrm{tr}(\omega^t)$ and $s(dt)$ have a four-level cross-correlation function and give the distribution of the values.

Keywords: Binary m-sequences; Cross-correlation; Finite fields

1. Introduction

For background in m-sequences and sequences in general, we refer to [5,7,8,13]. For applications of m-sequences the reader should see e.g. [5,8].

Recall that the trace function tr_k^n from the field $GF(2^n)$ onto the subfield $GF(2^k)$ is defined by

$$\mathrm{tr}_k^n(x) = x + x^{2^k} + x^{2^{2k}} + \cdots + x^{2^{(t-1)k}},$$

where $t = n/k$. For the properties of the trace function, see [12].

* Corresponding author.

E-mail addresses: torh@ii.uib.no (T. Helleseth), petri@ii.uib.no (P. Rosendahl).

[1] The research of Petri Rosendahl is supported by the Academy of Finland.

1071-5797/$ - see front matter © 2005 Elsevier Inc. All rights reserved.
doi:10.1016/j.ffa.2004.09.001

Let $u(t)$ and $v(t)$ be two binary m-sequences of the same period $\varepsilon = 2^n - 1$. We may assume that $u(t)$ is given by

$$u(t) = \mathrm{tr}_1^n(\omega^t),$$

where ω is a primitive element of the finite field $GF(2^n)$ and tr_1^n is the trace function from $GF(2^n)$ onto $GF(2)$. Furthermore, without loss of generality, we may assume that $v(t)$ is shifted cyclically such that $v(t) = u(dt)$, where $1 \leqslant d \leqslant 2^n - 2$ satisfies $\gcd(d, 2^n - 1) = 1$. The integer d is called a decimation.

The (periodic) cross-correlation function $C_d(\tau)$ between the sequences $u(t)$ and $v(t)$ is defined for $\tau = 0, 1, \ldots, \varepsilon - 1$ by

$$C_d(\tau) = \sum_{t=0}^{\varepsilon-1} (-1)^{u(t+\tau)+v(t)}.$$

A central problem in the theory of m-sequences, and in sequence design in general, is to determine the values and the number of occurrences of each value taken on by the cross-correlation function $C_d(\tau)$. This problem has been completely solved for only a few infinite families of pairs. The reader should consult [8] for an account.

If d is not a power of two, i.e., $u(t)$ and $v(t)$ are cyclically distinct, then the cross-correlation function takes on at least three values [7]. The known three-valued cases are

(i) $d = 2^k + 1$, with $n/\gcd(n, k)$ odd,
(ii) $d = 2^{2k} - 2^k + 1$, with $n/\gcd(n, k)$ odd,
(iii) $d = 2^{n/2} + 2^{(n+2)/4} + 1$, with $n \equiv 2 \pmod 4$,
(iv) $d = 2^{n/2+1} + 3$, with $n \equiv 2 \pmod 4$,
(v) $d = 2^{(n-1)/2} + 3$, with n odd,
(vi) $d = 2^{(n-1)/2} + 2^{(n-1)/4} - 1$, with $n \equiv 1 \pmod 4$, and
(vii) $d = 2^{(n-1)/2} + 2^{(3n-1)/4} - 1$, with $n \equiv 3 \pmod 4$.

Case (i) was proved by Gold [4], case (ii) is due to Kasami [10], and cases (iii) and (iv) were proved by Cusick and Dobbertin [2]. Case (v) is the famous Welch conjecture and was proved by Canteaut et al. [1]. Cases (vi) and (vii) were conjectured by Niho [13] and proved by Hollmann and Xiang [6].

There are only three known four-valued cases:

(i) $d = 2^{n/2+1} - 1$, with $n \equiv 0 \pmod 4$,
(ii) $d = (2^{n/2} + 1)(2^{n/4} - 1) + 2$, with $n \equiv 0 \pmod 4$, and
(iii) $d = \sum_{i=0}^{n/2} 2^{im}$, with $n \equiv 0 \pmod 4$, $0 < m < n$, $\gcd(n, m) = 1$.

Cases (i) and (ii) are due to Niho [13]. Case (iii) is due to Dobbertin [3].

The purpose of this paper is to provide a new family of decimations which lead to a four-valued cross-correlation function. The decimations are

$$d = \frac{1}{2^s - 1}(2^{2k} + 2^{s+1} - 2^{k+1} - 1),$$

where it is assumed that $n = 2k$, and that $2s$ divides k.

2. New four-valued cross-correlation functions

For the rest of this paper we will denote $n = 2k$. We begin with a simple lemma. Note that, for a moment, we have modified d a little.

Lemma 1. *Let*

$$d = \frac{2^{k-1}}{2^s - 1}(2^{2k} + 2^{s+1} - 2^{k+1} - 1),$$

where s is such that $2s$ divides k. Then

(i) $\gcd(d, 2^n - 1) = 1$,
(ii) $d \equiv 1 \pmod{2^k - 1}$, *and*
(iii) $d \equiv \frac{2^k - 2^s}{2^s - 1} \pmod{2^k + 1}$.

Proof. Conditions (ii) and (iii) are easy to check directly. Furthermore, (i) can be proved using (ii) and (iii) and the well-known fact that $\gcd(2^i + 1, 2^j - 1) = 1$ if and only if $j/\gcd(i, j)$ is odd; here we need that $2s$ divides k. □

Next we will derive an equation related to the cross-correlation function $C_d(\tau)$. The technique we use is due to Niho [13], and the equation could be derived from Niho's results. However, for reader's convenience, we include the main steps of the proof. Also, there are some details not appearing in [13]. For the theory of characters of finite fields we refer to [12,9].

First we note that every nonzero $x \in GF(2^n)$ can be represented uniquely as $x = \alpha^i \beta^j$, where $0 \leqslant i \leqslant 2^k - 2$, $0 \leqslant j \leqslant 2^k$, α is a primitive element of $GF(2^k)$ and β is a primitive $(2^k + 1)$st root of unity in $GF(2^n)$.

By using the previous remark we get

$$\begin{aligned} C_d(\tau) &= \sum_{t=0}^{2^n-2} (-1)^{\mathrm{tr}_1^n(\omega^{t+\tau} + \omega^{dt})} \\ &= \sum_{x \in GF(2^n)\setminus\{0\}} (-1)^{\mathrm{tr}_1^n(yx + x^d)} \\ &= \sum_{i=0}^{2^k-2} \sum_{j=0}^{2^k} (-1)^{\mathrm{tr}_1^n(y\alpha^i\beta^j + \alpha^{di}\beta^{dj})}. \end{aligned}$$

Here we have denoted $y = \omega^\tau$. Lemma 1 implies together with the transitivity and linearity of the trace function

$$\begin{aligned}
C_d(\tau) &= \sum_{i=0}^{2^k-2}\sum_{j=0}^{2^k}(-1)^{\mathrm{tr}_1^n(y\alpha^i\beta^j+\alpha^i\beta^{\frac{2^k-2^s}{2^s-1}j})} \\
&= \sum_{i=0}^{2^k-2}\sum_{j=0}^{2^k}(-1)^{\mathrm{tr}_1^n(\alpha^i(y\beta^j+\beta^{\frac{2^k-2^s}{2^s-1}j}))} \\
&= \sum_{i=0}^{2^k-2}\sum_{j=0}^{2^k}(-1)^{\mathrm{tr}_1^k(\alpha^i(y\beta^j+\beta^{\frac{2^k-2^s}{2^s-1}j}+y^{2^k}\beta^{-j}+\beta^{-\frac{2^k-2^s}{2^s-1}j}))} \\
&= -1-2^k+\sum_{j=0}^{2^k}\sum_{z\in GF(2^k)}(-1)^{\mathrm{tr}_1^k(z(y\beta^j+\beta^{\frac{2^k-2^s}{2^s-1}j}+y^{2^k}\beta^{-j}+\beta^{-\frac{2^k-2^s}{2^s-1}j}))} \\
&= -1+2^k(N(y)-1), \qquad (1)
\end{aligned}$$

where $N(y)$ is the number of common solutions to

$$yx + x^{\frac{2^k-2^s}{2^s-1}} + y^{2^k}x^{-1} + x^{-\frac{2^k-2^s}{2^s-1}} = 0$$

and

$$x^{2^k+1} = 1.$$

Since $x \mapsto x^{2^s-1}$ permutes the (2^k+1)st roots of unity we may equivalently find the number of common solutions to

$$yx^{2^s-1} + x^{-1-2^s} + y^{2^k}x^{1-2^s} + x^{2^s+1} = 0$$

and

$$x^{2^k+1} = 1.$$

Now, multiply the first equation by x^{2^s+1} and take the square root to get the equations

$$x^{2^s+1} + y^{2^{2k-1}}x^{2^s} + y^{2^{k-1}}x + 1 = 0$$

and

$$x^{2^k+1} = 1.$$

Here we can replace $y^{2^{k-1}}$ by y. Furthermore, from now on we will denote $\overline{y} = y^{2^k}$. Hence, the equations reduce to (2) and (3) in the next theorem. Before stating the theorem we give a lemma.

Lemma 2. *Let $\alpha \in GF(2^k) \setminus \{0\}$. Then the equation*

$$x^{2^s-1} = \alpha$$

has either no solutions or it has exactly $2^{\gcd(k,s)} - 1$ solutions in the field $GF(2^k)$.

We omit the simple proof.

Theorem 3. *Let $y \in GF(2^n) \setminus \{0\}$. The equations*

$$x^{2^s+1} + yx^{2^s} + \overline{y}x + 1 = 0 \tag{2}$$

and

$$x^{2^k+1} = 1, \tag{3}$$

have either 0, 1, 2 or $2^{\gcd(s,k)} + 1$ common solutions $x \in GF(2^n)$.

Proof. Let $S = \{x \in GF(2^n) | x^{2^k+1} = 1\}$. The set $S \setminus \{1\}$ can be parametrized as

$$x = \frac{z+u}{\overline{z}+u}, \tag{4}$$

where $z \in GF(2^n) \setminus GF(2^k)$ is fixed and u runs through the subfield $GF(2^k)$. This follows from the fact that every x of this form satisfies $\overline{x} = x^{-1}$ and the fact that these elements are all distinct. Previously, this parametrization has been used in a different context in [11].

We apply this parametrization to Eq. (2), which multiplied by $(\overline{z}+u)^{2^s+1}$ takes the form

$$\begin{aligned}(y+\overline{y})u^{2^s+1} &+ (z+\overline{z}+y\overline{z}+z\overline{y})u^{2^s} \\ &+ (z^{2^s}+\overline{z}^{2^s}+yz^{2^s}+\overline{yz}^{2^s})u \\ &+ (z^{2^s+1}+\overline{z}^{2^s+1}+yz^{2^s}\overline{z}+\overline{y}z\overline{z}^{2^s}) = 0.\end{aligned} \tag{5}$$

Note that the coefficients of (5) are in the subfield $GF(2^k)$ and we should now find the solutions in $GF(2^k)$.

Case 1: Assume first that $y \in GF(2^k)$. In this case $x = 1$ is a common solution of (2) and (3). Every other solution corresponds to a solution $u \in GF(2^k)$ of

$$(z + \overline{z} + y\overline{z} + z\overline{y})u^{2^s} + (z^{2^s} + \overline{z}^{2^s} + yz^{2^s} + \overline{yz}^{2^s})u = (z^{2^s+1} + \overline{z}^{2^s+1} + yz^{2^s}\overline{z} + \overline{y}z\overline{z}^{2^s}).$$

If $z + \overline{z} + y\overline{z} + yz = 0$, that is $y = 1$, there is nothing to prove. Otherwise we have an affine equation of the form

$$u^{2^s} + \alpha_1 u = \alpha_2, \tag{6}$$

where $\alpha_1, \alpha_2 \in GF(2^k)$. The fact that $\gcd(2^k - 1, 2^s - 1) = 2^{\gcd(k,s)} - 1$ implies that the corresponding linear equation

$$u^{2^s} + \alpha_1 u = 0 \tag{7}$$

has either exactly one root or exactly $2^{\gcd(k,s)}$ roots in $GF(2^k)$. Now, elementary linear algebra (or the theory of linearized polynomials, see [12]) tells that the affine equation (6) has either no solutions or it has the same number of solutions as (7). Hence, in the case $y \in GF(2^k)$, Eqs. (2) and (3) have either 1, 2 or $2^{\gcd(k,s)} + 1$ common solutions.

Case 2: For the rest of the proof, we assume now that $y \in GF(2^n) \setminus GF(2^k)$. If (2) and (3) have no common solution, we are through. Suppose now that β is a common root of (2) and (3). Then $\sqrt{\beta}$ is a solution of

$$x^{2^s+1} + \sqrt{y}x^{2^s} + \sqrt{\overline{y}}x + 1 = 0, \tag{8}$$

as can be easily seen.

In parametrization (4) we choose $z = \sqrt{\beta}$. This can be done since $y \notin GF(2^k)$ implies $\beta \neq 1$. The crux of this choice is that it makes the constant term in (5) vanish. To see this, multiply the constant term by z^{2^s+1} to get an equation which is equivalent to (8).

Now $u = 0$ is a root of (5). The other roots are the roots of the equation

$$(y + \overline{y})u^{2^s} + (z + \overline{z} + y\overline{z} + z\overline{y})u^{2^s-1} + (z^{2^s} + \overline{z}^{2^s} + \overline{yz}^{2^s} + yz^{2^s}) = 0. \tag{9}$$

If the constant term here is zero, then (5) has at most two roots and we are through. Otherwise we can take the reciprocal, which preserves the number of solutions, to get an affine equation of the form

$$u^{2^s} + \alpha_1 u = \alpha_2, \tag{10}$$

where $\alpha_1, \alpha_2 \in GF(2^k)$. Again, since $\gcd(2^k-1, 2^s-1) = 2^{\gcd(k,s)}-1$, the corresponding linear equation has exactly one or exactly $2^{\gcd(k,s)}$ solutions. We may now proceed similarly as in the case $y \in GF(2^k)$ to complete the proof. □

We now normalize (and for convenience still use the same notation) d to

$$d = \frac{1}{2^s-1}(2^{2k} + 2^{s+1} - 2^{k+1} - 1).$$

This does not affect cross-correlation values or their distribution. This simple fact follows from the properties of the trace, and is proven e.g. in [14].

In view of (1), Theorem 3 now implies that for the d in question, $C_d(\tau)$ is indeed four-valued, and that the cross-correlation values are $-1-2^k$, -1, $-1+2^k$, and $-1+2^{k+s}$. In order to find the distribution of the values we will use the following lemma.

Lemma 4. *We have*

(i) $\sum_{\tau=0}^{2^n-2}(C_d(\tau)+1) = 2^n$,
(ii) $\sum_{\tau=0}^{2^n-2}(C_d(\tau)+1)^2 = 2^{2n}$,
(iii) $\sum_{\tau=0}^{2^n-2}(C_d(\tau)+1)^3 = 2^{2n}b$,

where b is the number of solutions $x \in GF(2^n)$ of the equation vspace*-5pt

$$(x+1)^d + x^d = 1.$$

Eqs. (i) and (ii) are well known and proofs can be found, e.g. in [13]. Eq. (iii) is proved in [7].

Lemma 5. *The equation*

$$(x+1)^d = x^d + 1 \tag{11}$$

has exactly 2^k solutions in $GF(2^n)$.

Proof. Every $x \in GF(2^k)$ is a solution of (11) since $d \equiv 2 \pmod{2^k-1}$. We now assume that $x \neq 1$ is a solution of (11).

We raise (11) to the power of 2^s and then divide by $(x+1)^d = x^d + 1$ to get

$$(x+1)^{(2^s-1)d} = \frac{x^{2^s d}+1}{x^d+1},$$

i.e.,

$$(x+1)^{2^{s+1}-2^{k+1}} = \sum_{i=0}^{2^s-1} x^{id}.$$

Thus

$$x^{2^{s+1}}+1=\sum_{i=0}^{2^s-1}x^{id}+x^{2^{k+1}}\sum_{i=0}^{2^s-1}x^{id},$$

which is equivalent to

$$\sum_{i=1}^{2^s-1}x^{id}+x^{2^{k+1}}\sum_{i=0}^{2^s-2}x^{id}=0.$$

This can be written as

$$(x^{2^{k+1}}+x^d)\sum_{i=0}^{2^s-2}x^{id}=0$$

or

$$(x^{2^{k+1}}+x^d)\left(\frac{x^{(2^s-1)d}+1}{x^d+1}\right)=0.$$

Here, the first factor is zero if and only if

$$x^{2^{k+1}}=x^{\frac{1}{2^s-1}(2^{2k}+2^{s+1}-2^{k+1}-1)}.$$

Hence

$$x^{2^{k+1}(2^s-1)}=x^{2^{s+1}-2^{k+1}}$$

and thus also

$$x^{2^{k+s+1}}=x^{2^{s+1}}.$$

Raising this to the power of 2^{-s-1} gives $x\in GF(2^k)$.

The second factor is zero if and only if $x^d\in GF(2^s)$. But since $x\mapsto x^d$ is one to one on $GF(2^n)$ this is equivalent to $x\in GF(2^s)$. Since s divides k, we have $GF(2^s)\subseteq GF(2^k)$. Thus $x\in GF(2^k)$. □

Finally, we give the distribution of the values.

Theorem 6. *Let $n = 2k$, where $2s$ divides k, and let $d = (2^{2k} + 2^{s+1} - 2^{k+1} - 1)/(2^s - 1)$. Then the cross-correlation function $C_d(\tau)$ between two m-sequences takes on the following values:*

$$\begin{aligned} -1 - 2^k \quad & occurs \quad \frac{2^{2k+s-1} - 2^{k+s-1}}{2^s + 1} \quad times, \\ -1 \quad & occurs \quad \frac{2^{2k} - 2^k - 2^s}{2^s} \quad times, \\ -1 + 2^k \quad & occurs \quad \frac{2^{2k+s-1} - 2^{2k} + 2^{k+s-1}}{2^s - 1} \quad times, \\ -1 + 2^{k+s} \quad & occurs \quad \frac{2^{2k} - 2^k}{2^{3s} - 2^s} \quad times. \end{aligned}$$

Proof. Theorem 3 shows that $C_d(\tau)$ is four-valued and gives the values. Furthermore, Lemma 5 gives the number b of Lemma 4. Denote by N_i the number of times (2) and (3) have exactly i common solutions. We have a system of linear equations

$$\begin{aligned} N_0 + N_1 + N_2 + N_{2^s+1} &= 2^{2k} - 1, \\ -2^k N_0 + 2^k N_2 + 2^{k+s} N_{2^s+1} &= 2^{2k}, \\ 2^{2k} N_0 + 2^{2k} N_2 + 2^{2k+2s} N_{2^s+1} &= 2^{4k}, \\ -2^{3k} N_0 + 2^{3k} N_2 + 2^{3k+3s} N_{2^s+1} &= 2^{5k}. \end{aligned}$$

The first of these equations comes from the number of equations of form (2), and the other ones are simple consequences of Lemma 4. Straightforward calculations give the claimed distribution. □

Remark 7. It is easy to see that the case $s = 1$ (resp. $s = k/2$) corresponds to the Niho's four-valued case (i) (*resp.*(ii)) given in the Introduction.

Dobbertin [3] has studied Eq. (2) with the condition $\gcd(s, n) = 1$, and this gives the four-valued case (iii) in the introductory section. Thus our method provides an alternative proof of this case. Note that the result of Lemma 5 holds (this can be proved exactly the same way). Note also that the cross-correlation values in this case do not directly depend on s.

As might be expected, our decimation gives a large family of cross-correlation functions which have -1 as one of the values. This fact is related to an old conjecture by Helleseth, see [7].

Acknowledgments

The authors wish to thank Jyrki Lahtonen for his kind help.

References

[1] A. Canteaut, P. Charpin, H. Dobbertin, Binary *m*-sequences with three-valued cross-correlation: a proof of Welch's conjecture, IEEE Trans. Inform. Theory 46 (2000) 4–8.

[2] T.W. Cusick, H. Dobbertin, Some new three-valued crosscorrelation functions for binary *m*-sequences, IEEE Trans. Inform. Theory 42 (1996) 1238–1240.
[3] H. Dobbertin, One-to-one highly nonlinear power functions on $GF(2^n)$, AAECC Appl. Algebra Eng. Comm. Comput. 9 (1998) 139–152.
[4] R. Gold, Maximal recursive sequences with 3-valued cross-correlation functions, IEEE Trans. Inform. Theory 14 (1967) 154–156.
[5] S.W. Golomb, Shift Register Sequences, Aegean Park Press, Laguna Hills, CA, 1982.
[6] H.D. Hollmann, Q. Xiang, A proof of the Welch and Niho conjectures on cross-correlation of binary *m*-sequences, Finite Fields Appl. 7 (2001) 253–286.
[7] T. Helleseth, Some results about the cross-correlation function between two maximal linear sequences, Discrete Math. 16 (1976) 209–232.
[8] T. Helleseth, P.V. Kumar, Sequences with low correlation, in: V.S. Pless, W.C. Huffman (Eds.), Handbook of Coding Theory, Elsevier Science, Amsterdam, 1998, pp. 1765–1853.
[9] I. Honkala, A. Tietäväinen, Codes and number theory, in: V.S. Pless, W.C. Huffman (Eds.), Handbook of Coding Theory, Elsevier Science, Amsterdam, 1998, pp. 1141–1194.
[10] T. Kasami, The weight enumerators for several classes of subcodes of the second order binary Reed–Muller codes, Inform. Control 18 (1971) 369–394.
[11] J. Lahtonen, On the odd and the aperiodic correlation properties of the Kasami sequences, IEEE Trans. Inform. Theory 41 (1995) 1506–1508.
[12] R. Lidl, H. Niederreiter, Finite Fields, Encyclopedia of Mathematics and its Applications, vol. 20, Addison-Wesley, Reading, MA, 1983.
[13] Y. Niho, Multivalued cross-correlation functions between two maximal linear recursive sequences, Ph.D. Thesis, University of Southern California, 1972.
[14] H.M. Trachtenberg, On the cross-correlation functions of maximal linear sequences, Ph.D. Thesis, University of Southern California, 1970.