Abstract

For an odd prime $p$ and $n = 2m$, a new decimation $d = \frac{(p^m-1)^2}{2} + 1$ of Niho type of $m$-sequences is presented. Using generalized Niho’s Theorem, we show that the cross-correlation function between a $p$-ary $m$-sequence of period $p^n - 1$ and its decimated sequence by the above $d$ is at most six-valued and we can easily know that the magnitude of the cross correlation is upper bounded by $4\sqrt{p^n} - 1$.

Index Terms. $p$-ary $m$-sequence, Niho type, cross-correlation.
and $d = s(p^m - 1) + 1$, Niho converted the problem of finding the values of cross-correlation functions into the problem of determining the number of solutions of a system of equations. This result is called Niho’s Theorem. In 2006, Rosendahl [9] generalized Niho’s Theorem to nonbinary sequences. In 2007, Helleseth et al. [4] proved that the cross correlation function between two $m$-sequences that differ by a decimation $d$ of Niho type is at least four-valued.

When $d = 2p^m - 1 \equiv 1 \pmod{p^m - 1}$, the cross correlation function between a $p$-ary $m$-sequence $\{s_t\}$ of period $p^{2m} - 1$ and its decimated sequence $\{s_{dt}\}$ is four-valued, which was originally given by Niho [8] for the case $p = 2$ and by Helleseth [3] for the case $p > 2$. And when $d = 3p^m - 2$, the cross correlation function between two $m$-sequences that differ by $d$ is at most six-valued, especially, for $p = 3$, the cross correlation function is at most five-valued [9].

In this note, we study a new decimation $d = \frac{(p^m - 1)^2}{2} + 1$ of Niho type. Employing generalized Niho’s Theorem, we show that the cross-correlation function between a $p$-ary $m$-sequence and its decimated sequence by $d$ is at most six-valued.

The rest of this note is organized as follows. Section 2 presents some preliminaries and definitions. Using generalized Niho’s Theorem, we give an alternative proof of a result by Helleseth [3] where $d = \frac{(p^m - 1)(p^m + 1)}{2} + 1$ in section 3. A new decimation $d = \frac{(p^m - 1)^2}{2} + 1$ of Niho type is given in section 4. We prove that the cross correlation function between a $p$-ary $m$-sequence and its decimated sequence by $d$ takes at most six values.

2 Preliminaries

We will use the following notation in the rest of this note. Let $p$ be an odd prime, $\text{GF}(p^n)$ the finite field with $p^n$ elements and $\text{GF}(p^n)^* = \text{GF}(p^n) \setminus \{0\}$. The trace function $\text{Tr}_m^n$ from the field $\text{GF}(p^n)$ onto the subfield $\text{GF}(p^m)$ is defined as

$$\text{Tr}_m^n(x) = x + x^{p^m} + x^{p^{2m}} + \cdots + x^{p^{(l-1)m}},$$

where $l = \frac{n}{m}$ is an integer.

We may assume that a $p$-ary $m$-sequence $\{s_t\}$ of period $p^n - 1$ is given by

$$s_t = \text{Tr}_1^n(\alpha^t),$$

where $\alpha$ is a primitive element of the finite field $\text{GF}(p^n)$ and $\text{Tr}_1^n$ is the trace function from $\text{GF}(p^n)$ onto $\text{GF}(p)$. The periodic cross correlation function $C_d(\tau)$ between $\{s_t\}$ and its decimated sequence $\{s_{dt}\}$ is defined as

$$C_d(\tau) = \sum_{t=0}^{p^n-2} \omega^{s_t - s_{dt}},$$

where $\omega$ is a primitive $m$-th root of unity in $\text{GF}(p^m)$. The rest of this note is organized as follows. Section 2 presents some preliminaries and definitions. Using generalized Niho’s Theorem, we give an alternative proof of a result by Helleseth [3] where $d = \frac{(p^m - 1)(p^m + 1)}{2} + 1$ in section 3. A new decimation $d = \frac{(p^m - 1)^2}{2} + 1$ of Niho type is given in section 4. We prove that the cross correlation function between a $p$-ary $m$-sequence and its decimated sequence by $d$ takes at most six values.
where $\omega = e^{\frac{2\pi \sqrt{-1}}{p}}$ and $0 \leq \tau \leq p^n - 2$.

We will always assume that $n = 2m$ is even in this note unless otherwise specified.

3 An alternative proof of a known result

For $p = 2$, Niho \cite{8} presented Niho’s Theorem about decimations of Niho type of $m$-sequences. Rosendahl \cite{9} generalized this result as follows.

Lemma 1 (generalized Niho’s Theorem) \cite{9} Let $p$, $n$, and $m$ be defined as in section 2. Assume that $d \equiv 1 \pmod{p^m - 1}$, and denote $s = \frac{d - 1}{p^m - 1}$. Then when $y = \alpha^\tau$ runs through the nonzero elements of the field $GF(p^n)$, $C_d(\tau)$ assumes exactly the values

$$-1 + (N(y) - 1) \cdot p^m,$$

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

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

$$x^{p^{m+1}} = 1.$$

In 1976, Helleseth \cite{3} proved the following result. Here, using the generalized Niho’s Theorem, we give a simple proof.

Theorem 1 \cite{3} Let the symbols be defined as in section 2, $p$ be an odd prime and $d = \frac{p^n - 1}{2} + 1$. Then $C_d(\tau) \in \{-1 - p^m, -1, -1 + p^m, -1 + \frac{p^{m+1} - 1}{2} p^m, -1 + \frac{p^{m+1} - 1}{2} p^m\}$.

Proof of Theorem 1. Since $d = \frac{p^n - 1}{2} + 1 = \frac{p^{m+1}}{2} (p^m - 1) + 1$, we get $s = \frac{d - 1}{p^m - 1} = \frac{p^{m+1}}{2}$. By Lemma 1, we have

$$C_d(\tau) = -1 + (N(y) - 1) \cdot p^m,$$

where $y = \alpha^\tau$, $0 \leq \tau \leq p^n - 2$, and $N(y)$ is the number of common solutions of

$$x^{(p^m+1)-1} + y^p x^{\frac{p^{m+1}}{2}} + yx^{\frac{p^{m+1}}{2}-1} + 1 = 0,$$

$$x^{p^{m+1}} = 1. \quad (1)$$

Note that Eq. (2) implies

$$x^{\frac{p^{m+1}}{2}} = 1 \quad (3)$$
or
\[ x^{\frac{p^m+1}{2}} = -1. \] (4)

Substituting (3) and (4) into (1) respectively, we get
\[ C_d(\tau) = -1 + (N_1(y) + N_{-1}(y) - 1) \cdot p^m, \]
where \( N_1(y) \) is the number of the common solutions of
\[ (3.1.1) \left\{ \begin{array}{l} (y^{p^m} + 1)x + (y + 1) = 0, \\
 x^{\frac{p^m+1}{2}} = 1, \end{array} \right. \]
and \( N_{-1}(y) \) is the number of solutions of
\[ (3.1.2) \left\{ \begin{array}{l} (y^{p^m} - 1)x + (y - 1) = 0, \\
 x^{\frac{p^m+1}{2}} = -1. \end{array} \right. \]

Obviously, for \( y \neq \pm 1, 0 \leq N_1(y) + N_{-1}(y) \leq 2. \)

Let \( y = 1. \) First, it is straightforward to get \( N_{-1}(1) = \frac{p^m+1}{2}. \) Second, we see that \( x = -1 \) is the only solution of (3.1.1) for \( p^m + 1 \equiv 0 \mod 4 \) and \( N_1(1) = 0 \) for \( p^m + 1 \equiv 2 \mod 4. \) Hence, we have
\[ N_1(1) + N_{-1}(1) = \begin{cases} 1 + \frac{p^m+1}{2}, & \text{if } p^m + 1 \equiv 0 \mod 4, \\
\frac{p^m+1}{2}, & \text{if } p^m + 1 \equiv 2 \mod 4. \end{cases} \]

Similarly, for \( y = -1, \) we have
\[ N_1(-1) + N_{-1}(-1) = \begin{cases} \frac{p^m+1}{2}, & \text{if } p^m + 1 \equiv 0 \mod 4, \\
1 + \frac{p^m+1}{2}, & \text{if } p^m + 1 \equiv 2 \mod 4. \end{cases} \]

The result follows. \( \square \)

In Theorem 1, the value \( s \) of Niho type decimation \( d \) is equal to \( \frac{p^m+1}{2} \) corresponding to Lemma 1.

Motivated by the above proof, we take \( s \) as the value \( \frac{p^m-1}{2}, \) a new decimation of Niho type will be presented, and cross correlation values will be determined in the following section.

4 A new decimation of Niho type

In this section, we give a new decimation \( d \) of Niho’s type and we show that the cross correlation function between a \( p \)-ary \( m \)-sequence and its decimated sequence by \( d \) is at most six-valued.
Theorem 2 Let the symbols be defined as in section 2. Let \( d = \frac{(p^m - 1)^2}{2} + 1 \). Then \( C_d(\tau) \in \{-1 + (j-1) \cdot p^m | 0 \leq j \leq 5\} \) is at most six-valued.

Proof of Theorem 2. Since \( d = \frac{(p^m - 1)^2}{2} + 1 = \frac{p^m - 1}{2} \cdot (p^m - 1) + 1 \equiv 1 \mod (p^m - 1) \), we know that the value \( s \) corresponding to that in Lemma 1 is \( \frac{m-1}{2} \). By the same argument as in Theorem 1, we get

\[
C_d(\tau) = -1 + (N_1(y) + N_{-1}(y) - 1) \cdot p^m,
\]

where \( N_1(y) \) is the number of solutions of

\[
(4.1.1) \quad \begin{cases} x^3 + yp^m x^2 + yx + 1 = 0, \\ x^{m+1} = 1, \end{cases}
\]

and \( N_{-1}(y) \) is the number of solutions of

\[
(4.1.2) \quad \begin{cases} x^3 - yp^m x^2 - yx + 1 = 0, \\ x^{m+1} = -1. \end{cases}
\]

By the basic algebraic theorem, we know that \( 0 \leq N_1(y) \leq 3 \) and \( 0 \leq N_{-1}(y) \leq 3 \), i.e., \( 0 \leq N_1(y) + N_{-1}(y) \leq 6 \). Further, we will prove \( 0 \leq N_1(y) + N_{-1}(y) \leq 5 \), i.e., we will prove \( N_1(y) + N_{-1}(y) \neq 6 \).

Suppose that \( N_1(y) + N_{-1}(y) = 6 \). Then \( N_1(y) = 3 \) and \( N_{-1}(y) = 3 \), i.e., both (4.1.1) and (4.1.2) have three solutions. Now, for \( i = 1, 2, 3 \), let \( x_i \) and \( x_i^* \) be the solutions of (4.1.1) and (4.1.2), respectively.

Since \( x_i \) satisfies \( x_i^{m+1} = 1 \) and \( x_i^* \) satisfies \( x_i^{m+1} = -1 \), we know that there exists some even integer \( j_i \) satisfying \( x_i = \alpha^{j_i} (p^m - 1) \) and that there exists some odd integer \( j_i^* \) satisfying \( x_i^* = \alpha^{j_i^*} (p^m - 1) \), where \( i = 1, 2, 3 \). Simultaneously, since \( x_i \) and \( x_i^* \) satisfy the first equations of (4.1.1) and (4.1.2) respectively, we have

\[
\prod_{i=1}^{3} x_i = \alpha^{(p^m - 1) \sum_{i=1}^{3} j_i} = -1,
\]

\[
\prod_{i=1}^{3} x_i^* = \alpha^{(p^m - 1) \sum_{i=1}^{3} j_i^*} = -1.
\]

By multiplying the above two equations, we get

\[
\prod_{i=1}^{3} x_i \prod_{i=1}^{3} x_i^* = \alpha^{(p^m - 1)(\sum_{i=1}^{3} j_i + \sum_{i=1}^{3} j_i^*)} = 1,
\]

and induce \( p^m + 1 \) \( \sum_{i=1}^{3} j_i + \sum_{i=1}^{3} j_i^* \). This contradicts to the fact that \( p^m + 1 \) is even but \( \sum_{i=1}^{3} j_i + \sum_{i=1}^{3} j_i^* \) is odd. Therefore, we get \( N_1(y) + N_{-1}(y) \neq 6 \), i.e., \( 0 \leq N_1(y) + N_{-1}(y) \leq 5 \). The result follows. \( \square \)
Remark 1 The decimated sequence \( \{ s_{dt} \} \) in Theorem 2 is not necessarily an \( m \)-sequence. In fact, 
\[
d = \frac{p^m - 1}{2}(p^m - 1) + 1 \equiv \frac{p^m - 1}{2}(-2) + 1 \equiv 3 \mod (p^m + 1).
\]
For \( p \equiv -1 \mod 3 \), \( m \) odd, we know that \( \gcd(d, p^n - 1) = 3 \), \( \{ s_{dt} \} \) is not an \( m \)-sequence. For the other case, \( \gcd(d, p^n - 1) = 1 \), and \( \{ s_{dt} \} \) is an \( m \)-sequence.

Remark 2 Theoretically, the number of the values of \( C_d(\tau) \) can not be reduced to less than 6. Following is an example whose cross correlation function between an \( m \)-sequence and its decimated sequence by \( d \) has exactly six values.

Example 1 Let \( p = 3 \), \( n = 6 \), \( m = 3 \) and \( d = \frac{(p^m - 1)^2}{2} + 1 = 339 \). The polynomial \( f(x) = x^6 + x^5 + 2 \) is primitive over GF(3). Let \( \alpha \) be a root of \( f(x) \), then \( s_t = \text{Tr}_1^6(\alpha^t) \), \( s_{dt} = \text{Tr}_1^6(\alpha^{339t}) \). Computer experiment gives the following cross correlation values:

\[
\begin{align*}
-1 - 3^3 & \text{ occurs 246 times,} \\
-1 & \text{ occurs 284 times,} \\
-1 + 3^3 & \text{ occurs 144 times,} \\
-1 + 2 \cdot 3^3 & \text{ occurs 42 times,} \\
-1 + 3 \cdot 3^3 & \text{ occurs 3 times,} \\
-1 + 4 \cdot 3^3 & \text{ occurs 9 times.}
\end{align*}
\]

Conclusion

In this note, using generalized Niho’s Theorem, we give an alternative proof of a known result. By changing the form of the known decimation factor, we give a new decimation \( d = \frac{(p^m - 1)^2}{2} + 1 \) of Niho type. We prove that the cross correlation function between a \( p \)-ary \( m \)-sequence of period \( p^n - 1 \) and its decimated sequence by the value \( d \) is at most six-valued, and we can easily see that the magnitude of the cross correlation values is upper bounded by \( 4\sqrt{p^n - 1} \).

References

[1] S.-T. Choi, J.-S. No, H. Chung, On the cross-correlation of a ternary \( m \)-sequence of period \( 3^{4k+2} - 1 \) and its decimated sequence by \( \frac{(3^{2k+1}+1)^2}{8} \), ISIT 2010, Austin, Texas, U.S.A., June 13-18, 2010.

[2] H. Dobbertin, T. Helleseth, P.V. Kumar, and H. Martinsen, Ternary \( m \)-sequences with three-valued cross-correlation function:new decimations of Welch and Niho type, IEEE Trans. Inf. Theory, vol. 47 (2001), pp. 1473-1481.
[3] T. Helleseth, Some results about the cross-correlation function between two maximal linear sequences. *Discrete Math.*, vol. 16 (1976) pp. 209-232.

[4] T. Helleseth, J. Lahtonen, and P. Rosendahl, On Niho type cross-correlation functions of $m$-sequences, *Finite Field and Their Applications*, vol. 13 (2007) pp. 305-317.

[5] T. Helleseth and P. V. Kumar, Sequences with low correlation, In V. S. Pless and W.C. Huffman (eds.), Handbook of Coding Theory, Elsevier Science (1998), pp. 1765-1853.

[6] Z. Hu, Z. Li, D. Mills, E. N. Müller, W. Sun, W. Willems, Y. Yang, and Z. Zhang, On the cross-correlation of sequences with the decimation factor $d = \frac{p^n+1}{p+1} - \frac{p^n-1}{2}$, *Applicable Algebra in Engineering, Communication and Computing*, vol. 12 (2001) pp. 255-263.

[7] E.N. Müller, On the cross-correlation of sequences over GF$(p)$ with short periods, *IEEE Trans. Inf. Theory*, vol.45 (1999) pp. 289-295.

[8] Y. Niho, Multivalued cross-correlation functions between two maximal linear recursive sequences. PhD Thesis, University of Southern California (1972).

[9] P. Rosendahl, A generalization of Niho’s Theorem, *Des. Codes Cryptogr.*, vol. 38 (2006), pp. 331-336.

[10] H.M. Trachtenberg, On the cross-correlation functions of maximal linear sequences, PhD Thesis, University of Southern California (1970).