LETTER *Special Section on Signal Design and Its Applications in Communications*

Pairs of Ternary Perfect Sequences with Three-Valued Cross-Correlation*

Chenchen LIU[†a)], **Wenyi ZHANG**[†b)], ***Nonmembers, and*** **Xiaoni DU**[††c)], ***Member***

SUMMARY The calculation of cross-correlation between a sequence with good autocorrelation and its decimated sequence is an interesting problem in the field of sequence design. In this letter, we consider a class of ternary sequences with perfect autocorrelation, proposed by Shedd and Sarwate (IEEE Trans. Inf. Theory, 1979, DOI: 10.1109/TIT.1979.1055998), which is generated based on the cross-correlation between m-sequence and its d-decimation sequence. We calculate the cross-correlation distribution between a certain pair of such ternary perfect sequences and show that the cross-correlation takes three different values.

key words: *cross-correlation, decimation, exponential sum, ternary perfect sequence*

1. Introduction

The problem of designing sequences with low correlation properties has been an interesting topic for a long time. Due to its good correlation properties, such sequences have found wide range of applications in cryptography, spread spectrum communication, radar ranging, Ultra Wide Band (UWB) and other fields [2]–[5].

Research on calculating the distribution of cross-correlation among a class of sequences with good correlation properties, can be dates back to late 1960s. In 1968, Gold analysed the cross-correlation of two different m-sequences of the same period [6]. Due to its important applications in several communication and sensing scenarios, the cross-correlation between a sequence and its decimations plays a very important role. In 1972, Niho first conjectured the distribution of the cross-correlation function for several kinds of decimations of m-sequences [7]. Working in this direction, in 1996, Cusick and Dobbertin [8], and later in 2001, Dobbertin et al. [9] found some results for binary m-sequences which satisfy the conjectures proposed by Niho. In another line of work, in 1968, Golomb conjectured that the cross-correlation between an odd length m-sequence and its $(2^k + 3)$-decimation sequence is three-valued [10]. This was proved by Canteaut et al. [11] in 2000. Considering the decimation d of the form $(2^{2k} - 2^k + 1)$, Kasami [12] proposed a binary sequence set that asymptotically achieved the Welch bound [13]. For the cross-correlation function between an m-sequence and its d-decimation, an overview of known results can be found in [14]–[16]. Besides, further generalizations have been made to study the cross-correlation of an m-sequence and its d-decimated sequence (see [17]–[26] for more details). Recently, in 2023, using complete permutation polynomials, some new results are obtained on the -1 conjecture on cross-correlation of m-sequences [27].

Interestingly, in parallel to the research on analyzing the cross-correlation of m-sequences, many constructions of sequences were proposed, which lead to ternary sequences with perfect autocorrelation properties. Chang proposed ternary sequences with zero correlation in 1967 [28]. In 1979, Ipatov proposed a construction of a ternary perfect sequence [29]. Shedd and Sarwate proposed a construction of ternary perfect sequences based on m-sequences [1]. Recently, Liu *et al.* studied the cross-correlation of the ternary sequences with perfect autocorrelation, proposed by Ipatov [29], and its 2-decimation [30].

Motivated by the works of [9] and [30], in this letter, we study the cross-correlation between the ternary sequences of length $p^m - 1$ with perfect autocorrelation, proposed by Shedd and Sarwate [1], which are generated with different d-decimations, where $d_1 = (\frac{p^k+1}{2})^{-1}$ and $d_2 = p^{2k} - p^k + 1$ or $d_1 = \frac{1}{2}(p^k + 1)$and $d_2 = (p^{2k} - p^k + 1)^{-1}$, p is prime, and $m/\gcd(m, k)$ is odd. Through calculations, it is shown that the cross-correlation takes on three different low values. The distribution of the cross-correlation values is also completely determined.

The rest of this letter is organized as follows. In Sect. 2, we introduce some basic definitions and notations. We also introduce several properties of correlation functions of the sequences. In Sect. 3, we analyze the cross-correlation distribution between ternary perfect sequences generated with various decimations. Finally, we conclude the letter in Sect. 4.

2. Preliminaries

Before we begin, let us fix some notations, which will be used throughout the letter.

- $N = p^m - 1$ for a positive integer m and a prime p;

Manuscript received February 12, 2023.
Manuscript revised June 5, 2023.
Manuscript publicized August 8, 2023.
[†]The authors are with the Department of Electronic Engineering and Information Science, University of Science and Technology of China, Hefei China.
[††]The author is with the College of Mathematics and Statistics, Northwest Normal University, Lanzhou, China.
[*]The work of X. Du was supported in part by the National Science Foundation of China (NSFC) under Grant 62172337.
a) E-mail: liucc07@mail.ustc.edu.cn
b) E-mail: wenyizha@ustc.edu.cn (Corresponding author)
c) E-mail: ymldxn@126.com
DOI: 10.1587/transfun.2023SDL0003

- F_{p^m} is the finite field with p^m elements, and α is a primitive element of F_{p^m};
- $\mathrm{Tr}_1^m(x) = \sum_{i=0}^{m-1} x^{p^i}$ is the trace function from F_{p^m} to F_p;
- $\mathbf{s} = (s(0), s(1), \cdots, s(N-1))$ is an m-sequence of length $N = p^m - 1$, where $s(i) = \mathrm{Tr}_1^m(\alpha^i)$.
- For any d with $\gcd(d, N) = 1$, $\mathbf{s}_d = (s_d(0), s_d(1), \cdots, s_d(N-1))$, where $s_d(i) = s(di \bmod N)$, is the d-decimation of $\mathbf{s}$.
- Let d^{-1} denote the integer which satisfy $d \cdot d^{-1} \bmod N = 1$, i.e. $d{\cdot}d^{-1} \equiv 1 \pmod N$, where $N = p^m - 1$.

Let $\mathbf{a}$ and $\mathbf{b}$ be two complex-valued sequences of length N, denoted as $\mathbf{a} = (a(0), a(1), \cdots, a(N-1))$ and $\mathbf{b} = (b(0), b(1), \cdots, b(N-1))$, respectively. A sequence is called binary if its elements take values from the set $\{1, -1\}$ and ternary if its elements take values in the set $\{0, 1, -1\}$. The (periodic) cross-correlation between sequences $\mathbf{a}$ and $\mathbf{b}$ at a shift τ is defined by

$$R_{\mathbf{a},\mathbf{b}}(\tau) = \sum_{i=0}^{N-1} a(i) b^*(i+\tau),\ 0 \le \tau \le N-1, \tag{1}$$

where $i+\tau$ is performed modulo N, and x^* denotes the complex conjugate of a complex number x. When $\mathbf{a} = \mathbf{b}$, (1) is called the periodic auto-correlation function, which can be simplified as $R_{\mathbf{a}}(\tau)$. In particular, $\mathbf{a}$ is called *perfect* if $R_{\mathbf{a}}(\tau) = 0$ for all $0 < \tau \le N-1$.

Using the properties of trace function and the definition of correlation function, as well as the results of Dobbertin [9], Helleseth [15] and Trachtenberg [26], we deduce the following lemma.

Lemma 1: Let $R_{\mathbf{s},\mathbf{s}_d}(\tau)$ denote the cross-correlation function between an m-sequence $\mathbf{s}$ and its decimation $\mathbf{s}_d$, then we have

1) $R_{\mathbf{s},\mathbf{s}_d}(\tau)$ is a real number.
2) Let $d \cdot d^{-1} \equiv 1 \pmod{p^m - 1}$, then the values and the number of occurrences of each value of $R_{\mathbf{s},\mathbf{s}_d}(\tau)$ and $R_{\mathbf{s},\mathbf{s}_{d^{-1}}}(\tau)$ are the same as τ ranges from 0 to $p^m - 2$, more specifically, $R_{\mathbf{s},\mathbf{s}_d}(\tau) = R_{\mathbf{s},\mathbf{s}_{d^{-1}}}(-d\tau)$
3) $\sum_{\tau=0}^{p^m-2} R_{\mathbf{s},\mathbf{s}_d}(\tau) = 1.$
4) $R_{\mathbf{s},\mathbf{s}_d}(p^i\tau) = R_{\mathbf{s},\mathbf{s}_d}(\tau)$.

Lemma 2 ([15], [31]): Let $\mathbf{s}$ be an m-sequence with length $p^m - 1$, and d be a positive integer. We have

1) If $\gcd(d,\ p^m - 1) = 1$, then the sequence $\mathbf{s}_d$ is an m-sequence which is either equivalent to the cyclic shift of $\mathbf{s}$, or a new m-sequence of the same length.
2) If $d = p^i$, the sequence $\mathbf{s}_d$ is equivalent to the cyclic shift of $\mathbf{s}$.
3) If $\gcd(d_1,\ p^m - 1) = 1$, $\gcd(d_2,\ p^m - 1) = 1$, then a necessary and sufficient condition for the sequence $\mathbf{s}_{d_1}$ to be equivalent to the translation sequence of $\mathbf{s}_{d_2}$ is the existence of a positive integer i such that $d_2 = p^i d_1$.
4) When $\tau = 0, 1, \cdots, p^m - 2$, the cross-correlation distribution between $\mathbf{s}$ and $\mathbf{s}_d$ is at least three-valued if and only if $d \notin \{1, p, \cdots, p^{m-1}\}$.

In the following, we will discuss the autocorrelation of m-sequences and some other properties. It is well known that

$$R_{\mathbf{s}}(\tau) = \begin{cases} N, & \tau = 0 \\ -1, & 0 < \tau \le N-1. \end{cases} \tag{2}$$

By [1], we note that (1) satisfies

$$R_{\mathbf{a},\mathbf{b}}(\tau) = R_{\mathbf{a},\mathbf{b}}(\tau + N), \tag{3}$$

$$R_{\mathbf{a},\mathbf{b}}(-\tau) = R^*_{\mathbf{b},\mathbf{a}}(\tau), \tag{4}$$

$$\sum_{i=0}^{N-1} R_{\mathbf{a},\mathbf{b}}(i) = \left(\sum_{i=0}^{N-1} a(i)\right)\left(\sum_{i=0}^{N-1} b^*(i)\right). \tag{5}$$

The results of this letter are based on the following identity from [1] which relates the cross-correlation functions for the sequences $\mathbf{a}$, $\mathbf{x}$, $\mathbf{y}$ and $\mathbf{b}$ of period N:

$$\sum_{i=0}^{N-1} R_{\mathbf{a},\mathbf{y}}(i) R^*_{\mathbf{x},\mathbf{b}}(i+\tau) = \sum_{i=0}^{N-1} R_{\mathbf{a},\mathbf{x}}(i) R^*_{\mathbf{y},\mathbf{b}}(i+\tau). \tag{6}$$

3. Pairs of Ternary Perfect Sequences with Three-Valued Cross-Correlation

Based on the framework developed in [1], when p is a prime, the cross-correlation between $\mathbf{s}$ and $\mathbf{s}_d$ for $d = \frac{1}{2}(p^k + 1)$ or $d = p^{2k} - p^k + 1$ takes on three values:

$$R_{\mathbf{s},\mathbf{s}_d}(\tau) = \begin{cases} -1 + p^{\frac{m+e}{2}}, & \text{occuring } \frac{1}{2}(p^{m-e} + p^{(m-e)/2}) \text{ times} \\ -1, & \text{occuring } p^m - p^{m-e} - 1 \text{ times} \\ -1 - p^{\frac{m+e}{2}}, & \text{occuring } \frac{1}{2}(p^{m-e} - p^{(m-e)/2}) \text{ times} \end{cases} \tag{7}$$

where $e = m/\gcd(m,k)$ is odd. Hence one can obtain a ternary perfect sequence $\mathbf{u}_d$ of length N as follows

$$\mathbf{u}_d(t) = p^{-\frac{m+e}{2}}(1 + R_{\mathbf{s},\mathbf{s}_d}(t)), 0 \le t \le N-1, \tag{8}$$

which is called Shedd-Sawarte sequence.

In the following, the cross-correlation functions of Shedd-Sawarte sequences $\mathbf{u}_d$ for different values of d are given.

Theorem 1: Let $\mathbf{u}_{d_1}$ and $\mathbf{u}_{d_2}$ be two ternary perfect sequences obtained as Eq. (8). Then

$$R_{\mathbf{u}_{d_1},\mathbf{u}_{d_2}}(\tau) = p^{-e}(1 + R_{\mathbf{s}_{d_2},\mathbf{s}_{d_1}}(-\tau)). \tag{9}$$

Proof: Starting from the definition of cross-correlation function and using Lemma 1 and (2), (6), we can obtain

$$
\begin{aligned}
&R_{\mathbf{u}_{d_1},\mathbf{u}_{d_2}}(\tau)\\
&=\sum_{i=0}^{N-1}\mathbf{u}_{d_1}(i)\mathbf{u}^*_{d_2}(i+\tau)\\
&=p^{-(m+e)}\sum_{i=0}^{N-1}\left(1+R_{\mathbf{s},\mathbf{s}_{d_1}}(i)\right)\left(1+R^*_{\mathbf{s},\mathbf{s}_{d_2}}(i+\tau)\right)\\
&=p^{-(m+e)}\Bigg[p^m-1+\sum_{i=0}^{N-1}R_{\mathbf{s},\mathbf{s}_{d_1}}(i)\\
&\quad+\sum_{i=0}^{N-1}R^*_{\mathbf{s},\mathbf{s}_{d_2}}(i+\tau)+\sum_{i=0}^{N-1}R_{\mathbf{s},\mathbf{s}_{d_1}}(i)R^*_{\mathbf{s},\mathbf{s}_{d_2}}(i+\tau)\Bigg]\\
&=p^{-(m+e)}\Bigg[p^m-1+\left(\sum_{i=0}^{N-1}\mathbf{s}(i)\right)\left(\sum_{i=0}^{N-1}\mathbf{s}^*_{d_1}(i)\right)\\
&\quad+\left(\sum_{i=0}^{N-1}\mathbf{s}^*(i+\tau)\right)\left(\sum_{i=0}^{N-1}\mathbf{s}_{d_2}(i+\tau)\right)\\
&\quad+\sum_{i=0}^{N-1}R_{\mathbf{s}}(i)R^*_{\mathbf{s}_{d_1},\mathbf{s}_{d_2}}(i+\tau)\Bigg]\\
&=p^{-(m+e)}\Bigg[p^m+1+\sum_{i=0}^{N-1}R_{\mathbf{s}}(i)R^*_{\mathbf{s}_{d_1},\mathbf{s}_{d_2}}(i+\tau)\Bigg]\\
&=p^{-(m+e)}\Bigg[p^m+1+p^m\cdot R^*_{\mathbf{s}_{d_1},\mathbf{s}_{d_2}}(\tau)\\
&\qquad-\sum_{i=0}^{N-1}R^*_{\mathbf{s}_{d_1},\mathbf{s}_{d_2}}(i+\tau)\Bigg]\\
&=p^{-e}(1+R^*_{\mathbf{s}_{d_1},\mathbf{s}_{d_2}}(\tau))
\end{aligned}
$$

Therefore, we find the relationship between the two decimation factors. Using Theorem 1, we have the following theorem.

Theorem 2: Let k be an integer with $\gcd(m,k)=e$ and m/e be odd. Let p be a prime, $d_1=(\frac{p^k+1}{2})^{-1}$ and $d_2=p^{2k}-p^k+1$. Then

$$
R_{\mathbf{u}_{d_1},\mathbf{u}_{d_2}}(\tau)=
\begin{cases}
0, & \text{occuring } p^m-p^{m-f}-1 \text{ times}\\
p^{(m-f)/2}, & \text{occuring } \frac{1}{2}(p^{m-f}+p^{(m-f)/2}) \text{ times}\\
-p^{(m-f)/2}, & \text{occuring } \frac{1}{2}(p^{m-f}-p^{(m-f)/2}) \text{ times}
\end{cases}
\tag{10}
$$

where $f=m/\gcd(m,3k)$.

Proof: Using the basic definition and properties of cross-correlation functions, the cross-correlation is given as follows

$$
\begin{aligned}
R_{\mathbf{s}_{d_1},\mathbf{s}_{d_2}}(\tau)&=\sum_{i=0}^{N-1}\mathbf{s}_{d_1}(i)\mathbf{s}^*_{d_2}(i+\tau)\\
&=\sum_{i=0}^{N-1}\mathbf{s}(d_1 i)\mathbf{s}^*(d_2(i+\tau))\\
&=\sum_{j=0}^{N-1}\mathbf{s}(j)\mathbf{s}^*(d_2d_1^{-1}(j+d_1\tau)),
\end{aligned}
$$

where $j\equiv d_1 i\ (\ mod\ N)$. If $\tau'=d_1\tau$, then

$$
R_{\mathbf{s}_{d_1},\mathbf{s}_{d_2}}(\tau)=\sum_{j=0}^{N-1}\mathbf{s}(j)\mathbf{s}^*(d_2d_1^{-1}(j+\tau')).\tag{11}
$$

where $d_2d_1^{-1}=(\frac{p^{3k}+1}{2})\ (mod\ N)$. Since $R^*_{\mathbf{s}_{d_1},\mathbf{s}_{d_2}}(\tau)$ and $R_{\mathbf{s},\mathbf{s}_{d_2d_1^{-1}}}(\tau)$ have the same distribution, we will consider the distribution $R_{\mathbf{s},\mathbf{s}_{d_2d_1^{-1}}}(\tau)$. Note that $f=m/\gcd(m,3k)$ is also odd since e is odd and $f|e$, so the result can be derived by Eq. (7). This completes the proof.

Remark 1: Similarly, if $d_1=(\frac{p^k+1}{2})$ and $d_2=(p^{2k}-p^k+1)^{-1}$, the corresponding cross-correlation between them also has three values and has the same distribution as Theorem 2.

Remark 2: Using Theorem 2 and (6), it is easy to show $p^{(f-m)/2}R_{\mathbf{u}_{d_1},\mathbf{u}_{d_2}}(\tau)$ is also a ternary perfect sequence.

4. Conclusion

In this letter, we studied the cross-correlation between a class of ternary perfect sequences proposed by Shedd and Sarwate [1], which is generated with different d-decimations. For a pair of ternary perfect sequence with corresponding decimation values $d_1=(\frac{p^k+1}{2})^{-1}, d_2=p^{2k}-p^k+1$ or $d_1=(\frac{p^k+1}{2})$ and $d_2=(p^{2k}-p^k+1)^{-1}$, its cross-correlation distribution is derived. We found that, interestingly, the cross-correlation function takes only three values and can be used to construct another ternary perfect sequence.

References

[1] D. Shedd and D. Sarwate, "Construction of sequences with good correlation properties," IEEE Trans. Inf. Theory, vol.25, no.1, pp.94–97, 1979.
[2] T. Helleseth, "Sequences with low correlation," Handbook of Coding Theory, pp.1765–1853, North-Holland, 1998.
[3] S.W. Golomb and G. Gong, Signal Design for Good Correlation: For Wireless Communication, Cryptography, and Radar, Cambridge University Press, 2005.
[4] P.Z. Fan and M. Darnell, Sequence Design for Communications Applications, Wiley, New York, NY, USA, 1996.
[5] M.I. Skolnik, Introduction to Radar Systems, McGraw Hill, New York, NY, USA, 1980.
[6] R. Gold, "Maximal recursive sequences with 3-valued recursive cross-correlation functions (corresp.)," IEEE Trans. Inf. Theory, vol.14, no.1, pp.154–156, 1968.
[7] Y. Niho, "Multi-valued cross-correlation functions between two maximal linear recursive sequences," Ph.D. dissertation, Department of Electrical Engineering, University of Southern California (USCEE Rep. 409), 1972.
[8] T.W. Cusick and H. Dobbertin, "Some new three-valued crosscorrelation functions for binary m-sequences," IEEE Trans. Inf. Theory, vol.42, no.4, pp.1238–1240, 1996.
[9] 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,

no.4, pp.1473–1481, 2001.

[10] S.W. Golomb, "Theory of transformation groups of polynomials over $GF(2)$ with applications to linear shift register sequences," Information Sciences, vol.1, no.1, pp.87–109, 1968.

[11] A. Canteaut, P. Charpin, and H. Dobbertin, "Binary m-sequences with three-valued crosscorrelation: A proof of Welch's conjecture," IEEE Trans. Inf. Theory, vol.46, no.1, pp.4–8, 2000.

[12] T. Kasami, "Weight distribution formula for some class of cyclic codes," Coordinated Science Laboratory, University of Illinois, Report 285, 1966.

[13] L. Welch, "Lower bounds on the maximum cross correlation of signals (corresp.)," IEEE Trans. Inf. Theory, vol.20, no.3, pp.397–399, 1974.

[14] T. Helleseth, "Open problems on the cross-correlation of m-sequences," Open Problems in Mathematics and Computational Science, pp.163–179, Springer, 2014.

[15] T. Helleseth, "Some results about the cross-correlation function between two maximal linear sequences," Discrete Math., vol.16, no.3, pp.209–232, 1976.

[16] H. Dobbertin, P. Felke, T. Helleseth, and P. Rosendahl, "Niho type cross-correlation functions via Dickson polynomials and Kloosterman sums," IEEE Trans. Inf. Theory, vol.52, no.2, pp.613–627, 2006.

[17] G.J. Ness and T. Helleseth, "Cross correlation of m-sequences of different lengths," IEEE Trans. Inf. Theory, vol.52, no.4, pp.1637–1648, 2006.

[18] G.J. Ness and T. Helleseth, "A new three-valued cross correlation between m-sequences of different lengths," IEEE Trans. Inf. Theory, vol.52, no.10, pp.4695–4701, 2006.

[19] G.J. Ness and T. Helleseth, "A new family of four-valued cross correlation between m-sequences of different lengths," IEEE Trans. Inf. Theory, vol.53, no.11, pp.4308–4313, 2007.

[20] E.Y. Seo, Y.S. Kim, J.S. No, and D.J. Shin, "Cross-correlation distribution of p-ary m-sequence of period $p^{4k}-1$ and its decimated sequences by $(\frac{p^{2k}+1}{2})^2$," IEEE Trans. Inf. Theory, vol.54, no.7, pp.3140–3149, 2008.

[21] T. Zhang, S. Li, T. Feng, and G. Ge, "Some new results on the cross correlation of m-sequences," IEEE Trans. Inf. Theory, vol.60, no.5, pp.3062–3068, 2014.

[22] G.J. Ness, T. Helleseth, and A. Kholosha, "On the correlation distribution of the Coulter-Matthews decimation," IEEE Trans. Inf. Theory, vol.52, no.5, pp.2241–2247, 2006.

[23] T. Helleseth, "A note on the cross-correlation function between two binary maximal length linear sequences," Discrete Math., vol.23, no.3, pp.301–307, 1978.

[24] T. Helleseth and P. Rosendahl, "New pairs of m-sequences with 4-level cross-correlation," Finite Fields and Their Applications, vol.11, no.4, pp.674–683, 2005.

[25] T. Hoholdt and J. Justesen, "Ternary sequences with perfect periodic autocorrelation (corresp.)," IEEE Trans. Inf. Theory, vol.29, no.4, pp.597–600, 1983.

[26] H.M. Trachtenberg, "On the cross-correlation functions of maximal linear sequences," Ph.D. Dissertation, Univ. of Southern California, 1970.

[27] G.F. Wu, K.Q. Feng, N. Li, and T. Helleseth, "New results on the -1 conjecture on cross-correlation of m-sequences based on complete permutation polynomials," IEEE Trans. Inf. Theory, vol.69, no.6, pp.4035–4044, 2023.

[28] J.A. Chang, "Ternary sequence with zero correlation," Proc. IEEE, vol.55, no.7, pp.1211–1213, 1967.

[29] V.P. Ipatov, "Ternary sequences with ideal periodic autocorrelation properties," Radio Engineering and Electronic Physics, vol.24, pp.75–79, 1979.

[30] C. Liu, W. Zhang, and Y. Yang, "Ternary perfect sequences with three-valued cross-correlation," Adv. Math. Commun., vol.16, no.4, pp.893–901, 2022.

[31] R. Lidl and H. Niederreiter, Finite Fields, Cambridge University Press, 1997.