Punctured Bent Function Sequences for Watermarked DS-CDMA

Min Kyu Song, *Student Member, IEEE*, Gangsan Kim, *Student Member, IEEE*, Hong-Yeop Song, *Senior Member, IEEE*, and Ki Won Song, *Member, IEEE*

***Abstract*— In this letter, we investigate the effect of inserting some randomly generated watermarking chips into known spreading sequences in terms of periodic correlations; moreover, we give two design criteria for good watermarked sequences in the sense of: 1) reducing the average correlation value and 2) minimizing the variance of correlations. For $n = 2m$ with even m, we propose a set of 2^{m-1} punctured bent function sequences of length $2^n - 1$ punctured by the Singer difference set. The maximum non-trivial correlation magnitude of the proposed set turns out to be $2^m + 1$, which is asymptotically two times the Welch bound.**

***Index Terms*— DS-CDMA, watermarked sequences, bent function sequences, punctured sequences, periodic correlations.**

I. Introduction

DIRECT sequence code division multiple access (DS-CDMA) have been widely applied for digital communication systems [1] and global positioning navigation systems [2]. In DS-CDMA, a transmitter uses a unique sequence as its signature, which is called a spreading sequence or a signature sequence.

Nowadays, DS-CDMA with watermarked spreading sequences have been considered to provide some security at the physical-layer level. We call this a watermarked DS-CDMA (W-DS-CDMA). Here, the watermarking is done by replacing some chips in a sequence with other chips. The objectives of the watermarking are authentication of signals [3]–[5], steganography [6] and Military GNSS signal with fast acquisition [7]. Here, we note that many of these just focused on how to use the watermarking chips, but not the effect of inserting the watermarking chips to the spreading sequences in terms of their correlations of various kinds. We note that there are some related works which consider such an effect of combining known sequences and unknown watermarking data in terms of its aperiodic correlation [8], [9]. They call this a distributed sequence for frame synchronization, and considers only a single sequence case.

In this letter, we investigate the effect of inserting some randomly generated watermarking chips into known spreading sequences in terms of periodic correlations and we give two design criteria for good watermarked sequences in the sense of (1) reducing the average correlation value and (2) minimizing the variance of correlations. For $n = 2m$ with even m, we propose a set of 2^{m-1} punctured bent function sequences of length $2^n - 1$ punctured by the Singer difference set. The maximum non-trivial correlation magnitude of the proposed set turns out to be $2^m + 1$, which is asymptotically 2 times the Welch bound.

After reviewing some preliminaries in Section II, we investigate correlation properties of watermarked sequences and propose some design criteria for watermarked sequences in Section III. In Section IV, we propose punctured bent function sequences for watermarked DS-CDMA, which satisfy the proposed criteria. The proposed sequence set is based on the bent function sequences due to Olsen, Scholtz, and Welch [10] and the cyclic difference set by Singer. We finish this letter in Section V.

II. Some Preliminaries

Throughout this letter, we fix the following notation:

- $\mathbb{Z}_L$ is the ring of integers modulo L.
- $\mathbb{F}_{2^n}$ is the finite field of size 2^n.
- $\alpha \in \mathbb{F}_{2^n}$ is a primitive element.
- A k-subset is a subset of size k.
- The symbol '$\setminus$' stands for the set difference operation. That is, $X \setminus Y = \{x : x \in X \text{ and } x \notin Y\}$.
- For two subsets X, Y of $\mathbb{Z}_L$ and an element $\tau \in \mathbb{Z}_L$, we define $D_{X,Y}(\tau) = |X \cap (Y + \tau)|$, where $Y + \tau = \{y + \tau : y \in Y\}$. If $X = Y$, then we denote it by $D_X(\tau)$, simply.

A. Correlation of Sequences

In DS-CDMA, correlation of sequences is a measurement of interference [11]. Especially, even and odd correlations are important metric to achieve low interference level [11]. Let $\boldsymbol{x}$ and $\boldsymbol{y}$ be two real-valued spreading sequences of length L. The even and odd correlations of $\boldsymbol{x}$ and $\boldsymbol{y}$ are defined by

$$\theta_{\boldsymbol{x},\boldsymbol{y}}(\tau) = \sum_{l=0}^{L-1} x[l+\tau]y[l],$$

$$\hat{\theta}_{\boldsymbol{x},\boldsymbol{y}}(\tau) = \sum_{l=0}^{L-\tau-1} x[l+\tau]y[l] - \sum_{l=L-\tau}^{L-1} x[l+\tau]y[l],$$

respectively, where $l + \tau$ is computed modulo L. If $\boldsymbol{y}$ is a cyclic shift of $\boldsymbol{x}$, then $\theta_{\boldsymbol{x},\boldsymbol{y}}(\tau)$ (or $\hat{\theta}_{\boldsymbol{x},\boldsymbol{y}}(\tau)$) is called even (or odd) autocorrelation, and we simply denoted it by $\theta_{\boldsymbol{x}}(\tau)$ (or $\hat{\theta}_{\boldsymbol{x}}(\tau)$), respectively. Otherwise, it is called even (or odd) crosscorrelation.

Let $\mathcal{S}$ be a set of M sequences of length L all of constant energy E, i.e., $\theta_{\boldsymbol{x}}(0) = E$ for $\boldsymbol{x} \in \mathcal{S}$. The maximum non-trivial even correlation magnitude, denoted by $\theta_{\max}(\mathcal{S})$, is defined by

$$\theta_{\max}(\mathcal{S}) = \max\{\theta_a(\mathcal{S}), \theta_c(\mathcal{S})\},$$

Manuscript received April 7, 2019; accepted April 22, 2019. Date of publication May 7, 2019; date of current version July 10, 2019. This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIP) (No. 2017R1A2B4011191). The associate editor coordinating the review of this letter and approving it for publication was S. Majhi. *(Corresponding author: Hong-Yeop Song.)*

M. K. Song, G. Kim, and H.-Y. Song are with the Department of Electrical and Electronic Engineering, Yonsei University, Seoul 03722, South Korea (e-mail: mk.song@yonsei.ac.kr; gs.kim@yonsei.ac.kr; hysong@yonsei.ac.kr).

K. W. Song is with the Agency for Defense Development, Daejeon 34186, South Korea (e-mail: skw6213@add.re.kr).

Digital Object Identifier 10.1109/LCOMM.2019.2915080

1558-2558 © 2019 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.
See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

where

$$\theta_a(\mathcal{S}) = \max\{|\theta_{\boldsymbol{x}}(\tau)| : \boldsymbol{x} \in \mathcal{S}, \quad 1 \le \tau \le L-1\},$$
$$\theta_c(\mathcal{S}) = \max\{|\theta_{\boldsymbol{x},\boldsymbol{y}}(\tau)| : \boldsymbol{x}, \quad \boldsymbol{y} \in \mathcal{S}, \boldsymbol{x} \ne \boldsymbol{y}, \ 0 \le \tau \le L-1\}.$$

Then, the Welch bound [12] yields that

$$\theta_{\max}(\mathcal{S}) \ge E\sqrt{\frac{M-1}{ML-1}}. \tag{1}$$

Note that, RHS of (1) can be approximated as $E/\sqrt{L}$ if $M \gg 1$.

B. Bent Function Sequences

For an integer m, let $f : \mathbb{F}_{2^m} \to \mathbb{F}_2$. The Walsh transform of f at $\eta \in \mathbb{F}_{2^m}$ is given by [1]

$$\hat{f}(\eta) = \sum_{x \in \mathbb{F}_{2^m}} (-1)^{f(x)+\mathrm{tr}_1^m(\eta x)},$$

where $\mathrm{tr}_1^m(x) = \sum_{r=0}^{m-1} x^{2^r}$ is the trace from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$. Then, f is called bent if, for any $\eta \in \mathbb{F}_{2^m}$, $|\hat{f}(\eta)| = 2^{m/2}$. A bent function exists if and only if m is even. For more details on bent functions and their properties, see [13].

Let $n = 2m$ be a positive integer with even m and f be a bent function over $\mathbb{F}_{2^m}$. Let $\alpha \in \mathbb{F}_{2^n}$ be a primitive element and $\sigma \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$. For $\mu \in \mathbb{F}_{2^m}$, a bent function sequence $\boldsymbol{b}_\mu$ of length 2^n-1 due to [10] is given by, for $l = 0, 1, \ldots, 2^n-2$, [1, p.360]

$$b_\mu[l] = (-1)^{f\left(\mathrm{tr}_m^n(\alpha^l)\right)+\mathrm{tr}_1^n\left((\mu+\sigma)\alpha^l\right)}. \tag{2}$$

Fact 1 ([1], [10]): For a positive integer $n = 2m$ with even m and a fixed $\sigma \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$, let $\mathcal{B} = \{\boldsymbol{b}_\mu : \mu \in \mathbb{F}_{2^m}\}$ be a set of bent function sequences in which $\boldsymbol{b}_\mu$ is constructed by (2)*. Then,*

$$\theta_{\max}(\mathcal{B}) \le 2^m + 1, \tag{3}$$

and hence, it is optimal in terms of the Welch bound.

C. Cyclic Difference Sets and Their Characteristic Sequences

A k-subset $\mathcal{P}$ of $\mathbb{Z}_L$ is a (L, k, λ) cyclic difference set (CDS) if $D_{\mathcal{P}}(\tau) = \lambda$ for any $\tau \ne 0 \pmod L$. If an (L, k, λ)-CDS exists, then the following is true [1], [14], [15]:

$$k(k-1) = (L-1)\lambda. \tag{4}$$

The set

$$\left\{l \in \mathbb{Z}_{2^n-1} : \mathrm{tr}_1^n(\alpha^l) = 0\right\} \tag{5}$$

is known to be a $(2^n-1, 2^{n-1}-1, 2^{n-2}-1)$-CDS, called the Singer difference set [1], [14], [16], whose characteristic sequence is complement of a binary m-sequence of length 2^n-1. Here, the characteristic sequence $\boldsymbol{p} = \{p[l]\}_{l=0}^{L-1}$ of a subset $\mathcal{P}$ of $\mathbb{Z}_L$ is defined by

$$p[l] = \begin{cases} 1, & \text{if } l \in \mathcal{P}, \\ 0, & \text{otherwise.} \end{cases}$$

A k-subset $\mathcal{P}$ of $\mathbb{Z}_L$ is called an (L, k, λ, t) almost cyclic difference set (ACDS) if, for any $\tau \ne 0 \pmod L$, $D_{\mathcal{P}}(\tau)$ is either λ or $\lambda+1$. In fact, an (L, k, λ, t)-ACDS has the property that, for $\tau = 1, 2, \ldots, L-1$,

$$D_{\mathcal{P}}(\tau) = \begin{cases} \lambda, & t \text{ times}, \\ \lambda+1, & L-1-t \text{ times}. \end{cases}$$

Note that an (L, k, λ, t)-ACDS with $t = L-1$ is just an (L, k, λ)-CDS. If there exists an (L, k, λ, t)-ACDS, then the following is true [17]:

$$k(k-1) = t\lambda + (L-1-t)(\lambda+1). \tag{6}$$

III. Watermarked Spreading Sequence Design

A. System Model

W-DS-CDMA is a variation of DS-CDMA in which each user inserts some watermarks into its original spreading sequences. In the remaining of this letter, we will consider the following watermarking process, which is a variation proposed in [3]:

- **Set up:** Let $\mathcal{U} = \{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_N\}$ be a set of N binary sequences of length L, called *original sequences* corresponding to N users, and $\Psi = \{\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_N\}$ be a set of k-subsets of $\mathbb{Z}_L$, called *puncturing patterns*. A *single pattern scheme* refers to the case where all the puncturing patterns are the same. Otherwise, it is called a *multiple pattern scheme*.
- **Puncturing:** Each user punctures its original sequence according to the assigned puncturing pattern. The *punctured sequence* $\boldsymbol{s}_i$ is given by

$$s_i[l] = \begin{cases} u_i[l], & \text{if } l \notin \mathcal{P}_i \\ 0, & \text{if } l \in \mathcal{P}_i. \end{cases}$$

- **Watermarking:** For each and every transmission of a symbol, each user inserts his/her own watermarking chips into the punctured positions to generate a *watermarked sequence*. How to generate the watermarking chips would be a separate issue depending on some specific application. In this letter, we assume that the watermarking chips is i.i.d. random, i.e., each position will have the value ± 1 equally likely and independently.

Example 1: For $L = 7$, let $\mathcal{P}_1 = \{0, 1, 3\} \in \mathbb{Z}_7$ and the original sequence be given by

$$\boldsymbol{u}_1 = (1, -1, 1, 1, -1, -1, -1).$$

Then, the punctured sequence by $\mathcal{P}_1$ becomes

$$\boldsymbol{s}_1 = (0, 0, 1, 0, -1, -1, -1).$$

To transmit e-th data symbol, the first user generates three watermarking chips $w_{1,e}[0]$, $w_{1,e}[1]$, $w_{1,e}[3]$ and produces a watermarked sequence

$$\boldsymbol{c}_{1,e} = (w_{1,e}[0], w_{1,e}[1], 1, w_{1,e}[3], -1, -1, -1).$$

A watermarked sequence must be considered to have two different parts: one is a periodically repeated punctured sequence while the other is a non-periodic watermarking chip sequence. This is shown in Fig. 1. For example, $\boldsymbol{c}_{1,e}$ in the above example has periodically repeating punctured sequence $\boldsymbol{s}_1$ and non-periodic watermarking chip sequence

$$\boldsymbol{w}_{1,e} = (w_{1,e}[0], w_{1,e}[1], 0, w_{1,e}[3], 0, 0, 0).$$

Note that two watermarking chip sequences $\boldsymbol{w}_{i,e_1}$ and $\boldsymbol{w}_{j,e_2}$ are assumed to be statistically independent if $(i, e_1) \ne (j, e_2)$.

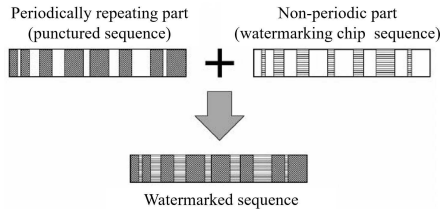

Fig. 1. Two parts of watermarked sequences.

B. Watermarked Sequence Design

When a W-DS-CDMA receiver is not able to generate any watermarking chip, it can acquire and despread a desired W-DS-CDMA signal by using only the periodically repeating punctured sequence. Therefore, the matched filter output can be described by correlation of a punctured sequence and a (received) watermarked sequence. The even correlation of $\boldsymbol{c}_{i,e}$ and $\boldsymbol{s}_j$ becomes

$$\theta_{\boldsymbol{c}_{i,e},\boldsymbol{s}_j}(\tau) = \theta_{\boldsymbol{s}_i,\ \boldsymbol{s}_j}(\tau) + \theta_{\boldsymbol{w}_{i,e},\boldsymbol{s}_j}(\tau). \tag{7}$$

We are interested in characterizing its mean and variance. Note that $w_{i,e}[l+\tau]$ is non-zero only for $l \in \mathcal{P}_i - \tau$ and $s_j[l]$ is non-zero only for $l \in \mathbb{Z}_L \setminus \mathcal{P}_j$. Therefore, $w_{i,e}[l+\tau]s_j[l]$ is non-zero only for

$$l \in (\mathcal{P}_i - \tau) \cap (\mathbb{Z}_L \setminus \mathcal{P}_j) = (\mathcal{P}_i - \tau) \setminus \mathcal{P}_j,$$

and hence, we have

$$\theta_{\boldsymbol{w}_{i,e},\boldsymbol{s}_j}(\tau) = \sum_{l \in (\mathcal{P}_i - \tau) \setminus \mathcal{P}_j} w_{i,e}[l+\tau]s_j[l].$$

Since all the watermarking chips are assumed to be i.i.d. random, $\theta_{\boldsymbol{w}_{i,e},\boldsymbol{s}_j}(\tau)$ is a random variable with mean zero and variance given by

$$|(\mathcal{P}_i - \tau) \setminus \mathcal{P}_j| = |\mathcal{P}_i \setminus (\mathcal{P}_j + \tau)| = k - D_{\mathcal{P}_i,\mathcal{P}_j}(\tau).$$

Thus, $\theta_{\boldsymbol{c}_{i,e},\boldsymbol{s}_j}(\tau)$ in (7) is a random variable with mean $\theta_{\boldsymbol{s}_i,\boldsymbol{s}_j}(\tau)$ and variance $k - D_{\mathcal{P}_i,\mathcal{P}_j}(\tau)$. Similarly, the odd correlation $\hat{\theta}_{\boldsymbol{c}_{i,e},\boldsymbol{s}_j}(\tau)$ of $\boldsymbol{c}_{i,e}$ and $\boldsymbol{s}_j$ becomes a random variable with mean $\hat{\theta}_{\boldsymbol{s}_i,\boldsymbol{s}_j}(\tau)$ and the same variance $k - D_{\mathcal{P}_i,\mathcal{P}_j}(\tau)$. Denote $D_{\min}(\Psi) = \min\{D_a(\Psi), D_c(\Psi)\}$ where

$$D_a(\Psi) = \min\left\{|D_{\mathcal{P}_i}(\tau)| : 0 \le i \le N, 1 \le \tau \le L-1\right\},$$
$$D_c(\Psi) = \min\left\{|D_{\mathcal{P}_i,\mathcal{P}_j}(\tau)| : 0 \le i < j \le N, 0 \le \tau \le L-1\right\}.$$

Now, it becomes obvious that one should maximize the value $D_{\mathcal{P}_i,\mathcal{P}_j}(\tau)$ for multiple patterns case and $D_{\mathcal{P}_i}(\tau)$ for single pattern case in order to minimize the variance of both even and odd correlations. In order to minimize the average correlation value, one must reduce $\theta_{\boldsymbol{s}_i,\boldsymbol{s}_j}(\tau)$ and/or $\hat{\theta}_{\boldsymbol{s}_i,\boldsymbol{s}_j}(\tau)$ as much as possible. This gives the following two criteria of designing the watermarked sequences:

C1:(puncturing pattern design)

$D_{\min}(\Psi)$ should be as large as possible.

C2:(punctured sequence design)

The maximum non-trivial even/odd correlation magnitude of punctured sequences $\boldsymbol{s}_i, \boldsymbol{s}_j$ for all i, j should be as low as possible.

Remark 1: The above design criteria will be the same when the receiver has the complete information on all the watermarking chips and thus makes use of them in acquisition and/or despreading stages. In that case, for some e_1, e_2, we should consider $\theta_{\boldsymbol{c}_{i,e_1},\boldsymbol{c}_{j,e_2}}(\tau)$ instead of (7). It can be shown that $\theta_{\boldsymbol{c}_{i,e_1},\boldsymbol{c}_{j,e_2}}(\tau)$ becomes a random variable with mean $\theta_{\boldsymbol{s}_i,\boldsymbol{s}_j}(\tau)$ and variance $L - D_{\mathcal{P}_i,\mathcal{P}_j}(\tau)$, except for the case when $\tau = 0 \pmod L$ with both $i = j$ and $e_1 = e_2$. For the case of odd correlation, we can obtain similar result.

To find good watermarked sequences, we first consider the first criterion **C1** for finding good puncturing patterns.

Lemma 1: Let $\Psi = \{\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_N\}$ be a set of k-subsets of $\mathbb{Z}_L$. Then,

$$D_{\min}(\Psi) \le \left\lfloor \frac{k^2 - k}{L-1} \right\rfloor. \tag{8}$$

Proof: Consider $D_{\mathcal{P}_i,\mathcal{P}_j}(\tau)$ for all τ from 0 to $L-1$ with $i \ne j$. As τ runs from 0 to $L-1$, each member of $\mathcal{P}_i$ coincides with some member of $\mathcal{P}_j + \tau$ exactly once. Therefore, $\sum_{0 \le \tau \le L-1} D_{\mathcal{P}_i,\mathcal{P}_j}(\tau) = k^2$, and hence,

$$\min_{0 \le \tau \le L-1} D_{\mathcal{P}_i,\mathcal{P}_j}(\tau) \le \left\lfloor \frac{k^2}{L} \right\rfloor. \tag{9}$$

For $i = j$, $\sum_{1 \le \tau \le L-1} D_{\mathcal{P}_i}(\tau) = k^2 - k$, since $D_{\mathcal{P}_i}(0) = k$. Therefore,

$$\min_{1 \le \tau \le L-1} D_{\mathcal{P}_i}(\tau) \le \left\lfloor \frac{k^2 - k}{L-1} \right\rfloor. \tag{10}$$

Note that the RHS of (10) is always smaller than or equal to the RHS of (9). ■

In the remaining of this letter, we call a set of puncturing patterns optimal if it achieves the bound in (8) with equality. The proof of Lemma 1 implies that a single pattern scheme may be enough to achieve the bound in (8) with equality.

Theorem 1: Assume that a single pattern scheme is applied, i.e., $\mathcal{P}_i = \mathcal{P}_j = \mathcal{P}$ for any $\mathcal{P}_i, \mathcal{P}_j \in \Psi$. If $\mathcal{P}$ is an (L, k, λ, t)-ACDS (or, an (L, k, λ)-CDS in special), then Ψ is optimal.

Proof: It is straightforward to check using (6). ■

Remark 2: A pattern from a cyclic (Singer's) difference set was used in [18, Thm. 3] in order to puncture the spectrum of a sequence with zero PACF sidelobes in frequency domain and obtain a constant smallest auto-correlation in time domain.

IV. Punctured Bent Function Sequence Set

Definition 1: Let $n \equiv 0 \pmod 4$ and $m = n/2$. Let Γ be a subset of $\mathbb{F}_{2^m}$ such that, for any $\mu, \nu \in \Gamma$, $\mu + \nu \ne 1$. For a bent function $f : \mathbb{F}_{2^m} \to \mathbb{F}_2$, let $\boldsymbol{b}_\mu$ be a bent sequence of length $2^n - 1$ constructed by (2). For a given Γ, we define a set of punctured bent sequences $\mathcal{S} = \{\boldsymbol{s}_\mu : \mu \in \Gamma\}$ where $\boldsymbol{s}_\mu$ is obtained by puncturing $\boldsymbol{b}_\mu$ by the pattern given in (5), i.e.,

$$s_\mu[l] = \begin{cases} b_\mu[l], & \text{if } \mathrm{tr}_1^n(\alpha^l) = 1, \\ 0, & \text{if } \mathrm{tr}_1^n(\alpha^l) = 0. \end{cases} \tag{11}$$

Theorem 2: Assume all the notation in Def. 1. Then,

$$\theta_{\max}(\mathcal{S}) \le 2^m + 1. \tag{12}$$

Proof: Let $\boldsymbol{s}_1$, $\boldsymbol{s}_2$ be two punctured sequences of length L constructed by puncturing $\boldsymbol{b}_1, \boldsymbol{b}_2$ according to the pattern $\mathcal{P}$.

By using the characteristic sequence $\boldsymbol{p}$ of $\mathcal{P}$, we may rewrite (11) as

$$s_i[l] = \frac{1}{2}\left(1-(-1)^{p[l]+1}\right) b_i[l].$$

Then, the even correlation of $\boldsymbol{s}_1$ and $\boldsymbol{s}_2$ is

$$\begin{aligned}\theta_{\boldsymbol{s}_1,\boldsymbol{s}_2}(\tau) &= \sum_{l=0}^{L-1} s_1[l+\tau]s_2[l] \\ &= \frac{1}{4}\sum_{l=0}^{L-1}\left(1-(-1)^{p[l+\tau]+1}\right) \\ &\quad b_1[l+\tau]\left(1-(-1)^{p[l]+1}\right) b_2[l] \\ &= \frac{1}{4}\left[\theta_{\boldsymbol{b}_1',\boldsymbol{b}_2'}(\tau)+\theta_{\boldsymbol{b}_1,\boldsymbol{b}_2}(\tau)-\theta_{\boldsymbol{b}_1',\boldsymbol{b}_2}(\tau)-\theta_{\boldsymbol{b}_1,\boldsymbol{b}_2'}(\tau)\right].\end{aligned} \tag{13}$$

where we let, for $i = 1, 2$,

$$\boldsymbol{b}_i' = \left\{b_i[l](-1)^{p[l]+1}\right\}_{l=0}^{L-1}.$$

Observe that, for any $x \in \mathbb{F}_{2^m}$,

$$\begin{aligned} b_x'[l] &= b_x[l](-1)^{\mathrm{tr}_1^n(\alpha^l)} \\ &= (-1)^{f\left(\mathrm{tr}_m^n(\alpha^l)\right)+\mathrm{tr}_1^n\left((x+\sigma)\alpha^l\right)}(-1)^{\mathrm{tr}_1^n(\alpha^l)} \\ &= (-1)^{f\left(\mathrm{tr}_m^n(\alpha^l)\right)+\mathrm{tr}_1^n\left((x+1+\sigma)\alpha^l\right)} = b_{x+1}[l]\end{aligned}$$

Therefore, by using (13) and the triangular inequality, we have

$$\begin{aligned}4\left|\theta_{\boldsymbol{s}_\mu,\boldsymbol{s}_\nu}(\tau)\right| \le \left|\theta_{\boldsymbol{s}_{\mu+1},\boldsymbol{s}_{\nu+1}}(\tau)\right| + \left|\theta_{\boldsymbol{s}_\mu,\boldsymbol{s}_\nu}(\tau)\right| \\ + \left|\theta_{\boldsymbol{s}_{\mu+1},\boldsymbol{s}_\nu}(\tau)\right| + \left|\theta_{\boldsymbol{s}_\mu,\boldsymbol{s}_{\nu+1}}(\tau)\right|\end{aligned} \tag{14}$$

for any $\mu, \nu \in \Gamma$.

Now, assume that $\mu = \nu$. Then, for any $\tau \not\equiv 0 \pmod{2^n-1}$, each term in RHS of (14) is either even autocorrelation of a bent sequence or even crosscorrelation of two bent sequences at some non-zero shift. Therefore, from Fact 1, RHS of (14) is upper-bounded by $4(2^m+1)$. If $\mu \neq \nu$, each term in RHS of (14) is even crosscorrelation of two bent sequences, and hence, RHS of (14) is upper-bounded by $4(2^m+1)$. ■

We describe the properties of $\mathcal{S}$ in Def. 1 as follows:

- The cardinality of $\mathcal{S}$ is $|\Gamma| = 2^{m-1}$. This is because of Γ in which $\mu + \nu \neq 1$.
- Any sequence $\boldsymbol{s} \in \mathcal{S}$ has $E = \theta_{\boldsymbol{s}}(0) = 2^{n-1}$ as its energy, which is about half the energy of the original bent function sequences. There are $2^{n-1}-1$ zeros (punctured positions) in every sequence of $\mathcal{S}$.
- The puncturing pattern is optimal in terms of (8) since the pattern is the Singer difference set given in (5). Therefore, the design is optimized by the criterion **C1**.
- The design $\mathcal{S}$ has the even correlation property given in (12), which is exactly the same as (3). That is, the sidelobe maintains the same level without any degradation. However, note that

$$E/\sqrt{L} = 2^{n-1}/\sqrt{(2^n-1)} \simeq 2^{m-1}$$

as $n = 2m$ becomes larger. Therefore, the proposed punctured bent function sequence set asymptotically achieves 2 times the Welch bound in (1). This gives a main result for watermarked sequences with low average correlation, thus satisfying the criterion **C2**. In summary, the sidelobe level remains the same without any degradation, but the mainlobe decreases by half due to puncturing, and hence the gap appears.

V. Concluding Remarks

The main contribution of this letter is the computation of the maximum magnitude of even correlations of watermarked sequences, constructed by puncturing bent function sequences [10] with the puncturing pattern given by the Singer difference set [1], [14], [16]. It is widely open for the computation of the maximum magnitude of odd correlation of these sequences.

It will be an interesting future research topic of trying to puncture some other well-known sequences using some optimum puncturing patterns and compute their correlation magnitudes.

References

[1] S. W. Golomb and G. Gong, *Signal Design for Good Correlation: For Wireless Communication, Cryptography, and Radar*. New York, NY, USA: Cambridge Univ. Press, 2005.

[2] *Global Positioning Systems Directorate Systems Engineering & Integration Interface Specification*, document IS-GPS-200H, Mar. 2014.

[3] G. Caparra and J. T. Curran, "On the achievable equivalent security of GNSS ranging code encryption," in *Proc. IEEE/ION Positions, Location Navigat. Symp. (PLANS)*, Monterey, CA, USA, Apr. 2018, pp. 956–966.

[4] D. Margaria, B. Motella, M. Anghileri, J.-J. Floch, I. Fernandez-Hernandez, and M. Paonni, "Signal structure-based authentication for civil GNSSs: Recent solutions and perspectives," *IEEE Signal Process. Mag.*, vol. 34, no. 5, pp. 27–37, Sep. 2017.

[5] L. Scott, "Anti-spoofing and authenticated signal architectures for civil navigation systems," in *Proc. ION GPS/GNSS*, Portland, OR, USA, Sep. 2003, pp. 1543–1552.

[6] X. Li, C. Yu, M. Hizlan, W.-T. Kim, and S. Park, "Physical layer watermarking of direct sequence spread spectrum signals," in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, Nov. 2013, pp. 476–481.

[7] C. Yang, "FFT acquisition of periodic, aperiodic, puncture, and overlaid code sequences in GPS," in *Proc. ION GPS*, Salt Lake City, UT, USA, Sep. 2001, pp. 137–147.

[8] M. Villanti, M. Iubatti, A. Vanelli-Coralli, and G. E. Corazza, "Design of distributed unique words for enhanced frame synchronization," *IEEE Trans. Commun.*, vol. 57, no. 8, pp. 2430–2440, Aug. 2009.

[9] A. J. D. L. V. Wijngaarden and T. J. Willink, "Frame synchronization using distributed sequences," *IEEE Trans. Commun.*, vol. 48, no. 12, pp. 2127–2138, Dec. 2000.

[10] J. Olsen, R. Scholtz, and L. Welch, "Bent-function sequences," *IEEE Trans. Inf. Theory*, vol. IT-28, no. 6, pp. 858–864, Nov. 1982.

[11] M. B. Pursley and D. Sarwate, "Performance evaluation for phase-coded spread-spectrum multiple-access communication—Part II: Code sequence analysis," *IEEE Trans. Commun.*, vol. 25, no. 8, pp. 800–803, Aug. 1977.

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

[13] S. Mesnager, *Bent Functions: Fundamentals and Results*. New York, NY, USA: Springer-Verlag, 2016.

[14] L. D. Baumert, *Cyclic Difference Sets*. New York, NY, USA: Springer-Verlag, 1972.

[15] J.-H. Kim and H.-Y. Song, "Existence of cyclic Hadamard difference sets and its relation to binary sequences with ideal autocorrelation," *J. Commun. Netw.*, vol. 1, no. 1, pp. 14–18, Mar. 1999.

[16] J. Singer, "A theorem in finite projective geometry and some applications to number theory," *Trans. Amer. Math. Soc.*, vol. 43, no. 3, pp. 377–385, 1938.

[17] K. T. Arasu, C. Ding, T. Helleseth, P. V. Kumar, and H. M. Martinsen, "Almost difference sets and their sequences with optimal autocorrelation," *IEEE Trans. Inf. Theory*, vol. 47, no. 7, pp. 2934–2943, Nov. 2001.

[18] Z. Liu, Y. L. Guan, U. Parampalli, and S. Hu, "Spectrally-constrained sequences: Bounds and constructions," *IEEE Trans. Inf. Theory*, vol. 64, no. 4, pp. 2571–2582, Apr. 2018.