Constructing Binary Sequences With Good Correlation Properties: An Efficient Analytical-Computational Interplay

Arindam Bose, *Student Member, IEEE*, and Mojtaba Soltanalian, *Member, IEEE*

***Abstract*—Binary sequence sets with asymptotically optimal auto/cross correlation peak sidelobe level (PSL) growth have been known in the literature for a long time, and their construction has been studied both analytically and numerically. In contrast, it has been a long-standing problem whether we can construct a family of binary sequences whose auto-correlation PSL grows in an optimal manner. In this paper, we devise a construction method of binary sequences with asymptotically optimal PSL growth from the sequence sets with good correlation properties. A key component of the design follows from the observation that if the PSL of the sequence set grows *optimally* or *nearly optimally*, then the PSL of the constructed binary sequence will experience a similar growth as a consequence. The proposed construction is simple-to-implement, and is shown to be accomplished in polynomial time. With such a construction, we not only bridge the gap between analytical construction and computational search, but also pave the way to settle the long-standing design problem of binary sequences with an optimal growth of the auto-correlation PSL.**

***Index Terms*—Auto-correlation, binary sequences, information embedding, peak sidelobe level, sequence design.**

I. Introduction

BINARY sequences with small auto/cross-correlation also referred to as good correlation properties form an essential component of a large set of information processing systems, ranging from information collection in active sensing, to information embedding and transmission in communication systems. For instance, they are widely used in Code-Division Multiple-Access (CDMA) schemes to distinguish between different users while at the same time enabling the system to synchronize [1], whereas in active sensing applications, usage of such sequences for pulse modulation paves the way to conveniently retrieve the received signal from the range bin of interest by employing a matched filter, and thus suppress inputs from other range bins [2].

Although several families of *sequence sets* with small auto/cross-correlation have been proposed in the past decades, sequences with low auto-correlation have seen little progress in the analytical arena (see Section II for details). In fact, the task of finding sequences with low auto-correlation is infamously known as a difficult computational problem. The complexity of the optimization problems associated with low auto-correlation binary sequences is discussed in [3]–[5]. On the other hand, the rapid increase in computational resources has motivated the researchers to perform exhaustive search of such sequences with larger length compared with what could have been considered before. The literature on this topic is quite extensive (e.g., see [2], [3], [6]–[32]). Nonetheless, we note that an exhaustive search over a set of binary sequences with a cardinality larger than 10^{20} (i.e., approximate sequence lengths of $N \sim 100$ or larger) is still deemed to be impractical[1] using the current standard computational tools. On the contrary, to analytically construct such binary sequences, it requires only a little computational cost. In this paper, we bridge the gap between *exhaustive search*, also referred to as *computational design*, and *analytical constructions* of binary sequences by resorting to a polynomial-time approach that exploits the strengths of both worlds. The proposed method constructs the binary sequences from sequence sets with good correlation properties through a non-convex quadratic program that can be handled in polynomial-time. In particular, we show that if the *peak sidelobe level* (PSL) of the sequence sets grows optimally in the periodic case and nearly optimally in the aperiodic case, the PSL of the constructed binary sequences also grows in a similar manner.

As a cornerstone of our performance analysis, we present several examples of binary sequence design and the obtained PSL values. Besides the usual design examples, we also present some interesting results on the application of the constructed sequences in information embedding applications, where a high degree of both imperceptibility and robustness must be guaranteed (see e.g., [33]–[37], and the references therein). We will use the optimally constructed binary sequences in lieu of sequence families commonly used in practice such as m-sequences, Gold or Kasami sequences in the pre-existing watermarking frameworks to ensure robustness and imperceptibility of the authorized watermark information and enhance the efficiency of information embedding algorithm. While being one from many, the presented example hints at the significant potential of our approach in practical applications.

The rest of this paper is organized as follows. The formulation as well as a useful background review of the problem

Manuscript received April 27, 2017; revised September 5, 2017, November 30, 2017, and January 29, 2018; accepted February 19, 2018. Date of publication March 12, 2018; date of current version April 23, 2018. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Ian Vaughan Clarkson. *(Corresponding author: Arindam Bose.)*

The authors are with the Department of Electrical and Computer Engineering, University of Illinois at Chicago, Chicago, IL 60607 USA (e-mail: arindam.bose.1990@ieee.org; msol@uic.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TSP.2018.2814990

[1] Assuming that a standard PC can handle 5×10^9 simple math operations per second, an exhaustive search over a space of 10^{20} sequences is *guaranteed to take more than 634 years*.

TABLE I
NOTATIONS

Notation	Description
$\boldsymbol{x}_m(k)$	the k^{th} entry of the column vector $\boldsymbol{x}_m$
$\boldsymbol{x}^*_m(k)$	the complex conjugate of the k^{th} entry of the column vector $\boldsymbol{x}_m$
$\lVert\boldsymbol{x}\rVert_p$	the l_p-norm of $\boldsymbol{x}$, defined as $\left(\sum_k \lvert\boldsymbol{x}(k)\rvert^p\right)^{\frac{1}{p}}$
$\lVert\boldsymbol{X}\rVert_F$	Frobenius norm or the l_2-norm of matrix $\boldsymbol{X}$
$\boldsymbol{X}^H$	the complex conjugate of the matrix $\boldsymbol{X}$
$\boldsymbol{X}^T$	the transpose of the matrix $\boldsymbol{X}$
$\boldsymbol{X}^\dagger$	the Moore-Penrose pseudoinverse of the matrix $\boldsymbol{X}$
$\boldsymbol{I}_M$	the identity matrix for order M
$\boldsymbol{O}$	the zero matrix with all elements as zero
$\mathbb{N}$	the set of natural numbers
$\mathbb{C}$	the set of complex numbers
$\boldsymbol{e}_m$	the m^{th} standard basis of $\mathbb{C}^m$
$\ln a$	natural logarithm of a, equivalent to $\log_e a$
$\text{Re}\{z\}$	the real part of complex scalar z
$f(n) = \mathcal{O}(g(n))$	$f(n) < cg(n)$ for at least one $0 < c < \infty$
$f(n) = o(g(n))$	$f(n) < cg(n)$ for all $0 < c < \infty$
$f(n) = \Omega(g(n))$	$g(n) < cf(n)$ for some $0 < c < \infty$
$f(n) = \Theta(g(n))$	$f(n) = \mathcal{O}(g(n))$ and $f(n) = \Omega(g(n))$

is provided in Section II. Our design approach is presented in Section III. Section IV is dedicated to the numerical results, including discussions on the information embedding application. Finally, Section V concludes the paper.

Notation: We use bold lowercase letters for vectors and bold uppercase letters for matrices. Please see Table I for other notations used throughout this paper.

II. PRELIMINARIES

A. Problem Formulation

Let X be a set of M sequences of length N denoted as $\{\boldsymbol{x}_m\}_{m=1}^M$, each having identical energy of $\|\boldsymbol{x}_m\|_2^2 = N$. Let $\boldsymbol{x}_{m_1}$ and $\boldsymbol{x}_{m_2}$ be two generic sequences from the set X. The periodic $\{c_{m_1,m_2}(k)\}$ and aperiodic $\{r_{m_1,m_2}(k)\}$ cross-correlations of the sequences $\boldsymbol{x}_{m_1}$ and $\boldsymbol{x}_{m_2}$ at shift k are given as,

$$c_{m_1,m_2}(k) \triangleq \sum_{n=1}^{N} \boldsymbol{x}_{m_1}(n)\boldsymbol{x}^*_{m_2}(n+k)_{(mod\,N)}, \tag{1}$$

$$r_{m_1,m_2}(k) \triangleq \sum_{n=1}^{N-k} \boldsymbol{x}_{m_1}(n)\boldsymbol{x}^*_{m_2}(n+k) = r^*_{m_1,m_2}(-k), \tag{2}$$

for $0 \leq k \leq (N-1)$. The periodic and aperiodic auto-correlation of any $\boldsymbol{x}_m \in X$ can be obtained from (1) and (2) by using $\boldsymbol{x}_{m_1} = \boldsymbol{x}_{m_2}$. The inner product of $\boldsymbol{x}_{m_1}$ and $\boldsymbol{x}_{m_2}$ is given as $\boldsymbol{x}^H_{m_1}\boldsymbol{x}_{m_2} = c_{m_1,m_2}(0) = r_{m_1,m_2}(0)$.

In the sequel, we focus on the aperiodic case as well as the periodic case. The periodic correlations are generally considered to be easier to study than their aperiodic counterparts. Often the study of sequences with good aperiodic correlations concerns with obtaining sequences with good periodic correlation properties and then examine their aperiodic correlations. There has been a long-standing interest in the study of design methods capable of finding binary sequence sets whose periodic and aperiodic correlations are, in some measurable sense, collectively small. Note that the in-phase lag (i.e., $k = 0$) of both correlations represents the energy component of the sequence. The problem of sequence design for good correlation properties usually arises when small out-of-phase (i.e., with $k \neq 0$) correlation lags are required. To formalize this outcome, several measures of "smallness" have been typically employed, including the *peak sidelobe level* (PSL), for the aperiodic case

$$\begin{aligned}&\text{PSL}^{\mathcal{AP}}(X) \triangleq \\ &\max(\{|r_{m_1,m_2}(k)|\}_{m_1\neq m_2;k} \cup \{|r_{m,m}(k)|\}_{m;k\neq 0}),\end{aligned} \tag{3}$$

as well as for the periodic case,

$$\begin{aligned}&\text{PSL}^{\mathcal{P}}(X) \triangleq \\ &\max(\{|c_{m_1,m_2}(k)|\}_{m_1\neq m_2;k} \cup \{|c_{m,m}(k)|\}_{m;k\neq 0}),\end{aligned} \tag{4}$$

which are the most relevant to our analysis. Likewise, the periodic and aperiodic PSL of a binary sequence $\boldsymbol{x}$ can be formulated from its auto-correlations as follows,

$$\text{PSL}^{\mathcal{AP}}(\boldsymbol{x}) \triangleq \max(|r_{m,m}(k)|_{m;k\neq 0}), \tag{5}$$

$$\text{PSL}^{\mathcal{P}}(\boldsymbol{x}) \triangleq \max(|c_{m,m}(k)|_{m;k\neq 0}).$$

B. Earlier Results

1) Periodic Auto-Correlations of Binary Sequences: In an ideal setup, a binary sequence with all its out-of-phase periodic auto-correlations equal to zero, is called a *perfect* sequence [38]. A necessary condition required for a perfect sequence to exist is given in the following lemma.

Lemma 1 ([38]): All periodic auto-correlations of a binary sequence $\boldsymbol{x}$ of length N are compatible with $N \mod 4$.

$$\text{PSL}^{\mathcal{P}}(\boldsymbol{x}) \geq \begin{cases} 0 & \text{for } N \equiv 0 \mod 4 \\ 1 & \text{for } N \equiv 1 \text{ or } 3 \mod 4 \\ 2 & \text{for } N \equiv 2 \mod 4 \end{cases} \tag{6}$$

It can be concluded from Lemma 1 that the perfect binary sequence can only exist when the length N is divisible by 4. However, the corollary given in [39] states that there is no perfect binary sequence of length N for $4 < N < 548\,964\,900$. Moreover, a binary sequence is called *optimal* in the sense that the equality holds in (6). Sequence families such as Legendre, Sidelnikov and Galois sequences are good examples of optimal sequences with respect to their periodic auto-correlations [38]. Moreover, considering sequence sets instead of a single sequence, it is indeed possible to generate binary sequence sets with periodic PSL asymptotically bounded as $\mathcal{O}(\sqrt{N})$. For example, [40] states that Kasami family includes sets of binary sequences of length $n = 2^N - 1$ and cardinality $m = 2^{N/2}$ where N is an even natural number. The periodic PSL value of a Kasami set is given by $1 + 2^{N/2}$. In addition, for odd N, Gold binary sequence sets can be constructed for $(m, n) = (2^N + 1, 2^N - 1)$ that have a periodic PSL value of $1 + \sqrt{2^{N+1} - 2}$. The Weil family consists of sequence sets with $n = N$ and $m = (N-1)/2$, where N is prime, that possess a periodic PSL value of $5 + 2\sqrt{N}$.

2) Aperiodic Auto-Correlations of Binary Sequences: On a slightly relaxed note, the *Barker sequences* have the ideal property of all out-of-phase aperiodic autocorrelations are either 0 or 1 in magnitude. According to [38], there is no Barker sequence of odd length greater than 13, furthermore if a Barker sequence of even length N exists, then every odd prime divisor of N is consistent with $3 \mod 4$. In response to the supposedly nonexistence of long Barker sequence, several researchers have studied the asymptotic behavior of collective smallness of the aperiodic auto-correlations of the sequences. Let $\mathcal{X}_N$ denote the set of all binary sequences of length N. The ultimate goal is to optimally compute and understand the asymptotic behavior, i.e., as $N \to \infty$, of

$$\mathcal{P}_{\min} \triangleq \min_{\boldsymbol{x} \in \mathcal{X}_N} \mathrm{PSL}^{\mathcal{AP}}(\boldsymbol{x}). \tag{7}$$

Note that to calculate $\mathcal{P}_{\min}$ numerically for a given sequence length N, even in the most ingenious way, it requires testing an exponential number of combinations. The exponential term of the complexity can be reduced from $\mathcal{O}(2^N)$ to roughly $\mathcal{O}(1.4^N)$ by using more sophisticated and efficient algorithms [41]–[43]. The value of $\mathcal{P}_{\min}$ has been computed up to $N = 105$ in the literature [43]–[45] using exhaustive search.

1) $\mathcal{P}_{\min} \leq 1$ for $N \leq 5$ [38];
2) $\mathcal{P}_{\min} \leq 2$ for $N \leq 21$ [44], where $\mathcal{P}_{\min} = 1$ is essentially achieved for $N = 2, 3, 4, 5, 7, 11, 13$ by *Barker sequences* [46];
3) $\mathcal{P}_{\min} \leq 3$ for $N \leq 48$ (see [45] for $N \leq 40$, and [41] for $N \leq 48$);
4) $\mathcal{P}_{\min} \leq 4$ for $N \leq 82$ (see [47] for $49 \leq N \leq 61$, and [42], [43] for $61 \leq N \leq 70$);
5) $\mathcal{P}_{\min} \leq 5$ for $N \leq 105$ [38].

Ein-Dor *et al.* [48] used a heuristic argument to obtain an "educated guess" about the growth of $\mathcal{P}_{\min}$ and conjectured that, as $N \to \infty$, we have $\dfrac{\mathcal{P}_{\min}}{\sqrt{N}} \to d$, where $d = 0.435...$ Historically, Moon and Moser [27] first studied the asymptotic behavior, as $N \to \infty$, of $\mathcal{P}_{\min}$ for the binary sequences as early as 1968.

Theorem 1: ([27]) If $\mathcal{K}(N)$ is any function of N such that $\mathcal{K}(N) = o(\sqrt{N})$, then the proportion of sequences $\boldsymbol{x} \in \mathcal{X}_N$ which have $\mathrm{PSL}^{\mathcal{AP}}(\boldsymbol{x}) > \mathcal{K}(N)$ approaches 1, as N approaches ∞.

Theorem 2: ([27]) For any fixed $\epsilon > 0$, the proportion of sequences $\boldsymbol{x} \in \mathcal{X}_N$ which have $\mathrm{PSL}^{\mathcal{AP}}(\boldsymbol{x}) \leq (2 + \epsilon)\sqrt{N \ln N}$ approaches 1, as N approaches ∞.

It can be concluded from Theorem 1 and 2 that, as $N \to \infty$, for almost all sequences $\mathcal{K}(N) < \mathrm{PSL}^{\mathcal{AP}}(\boldsymbol{x}) \leq (2 + \epsilon)\sqrt{N \ln N}$ for any $\epsilon > 0$. Mercer [49] further improved the upper bound by showing that for any fixed $\epsilon > 0$, $\mathcal{P}_{\min} \leq (\sqrt{2} + \epsilon)\sqrt{N \ln N}$ when N is sufficiently large. Dmitriev and Jedwab [50] postulated that the typical PSL growth behaves as $\Theta(\sqrt{N \ln N})$ and provided experimental evidence for the same.

We note that there are sequence families (i.e., families of *single* sequences) for which the aperiodic PSL grows faster than $\Theta(\sqrt{N \ln N})$. An example is the sequence family $\mathcal{F} = \{\boldsymbol{\psi}_N : N \in \mathbb{N}\}$ such that each of the N elements of $\boldsymbol{\psi}_N$ is 1. However, the literature does not currently suggest whether there exists any sequence family whose aperiodic PSL grows like the lower bound $o(\sqrt{N})$, nor even like $\Theta(\sqrt{N})$. It has been shown in [9] that the mean value of the PSL of m-sequences of length $N = 2^m - 1$ seems to grow like $\Omega(\sqrt{N})$ and like $\mathcal{O}(\sqrt{N \ln N})$. But, the claim that the PSL of m-sequences grows like $\mathcal{O}(\sqrt{N})$, which appears frequently in the radar literature, *"is concluded to be unproven and not currently supported by data"* [9]. However, aperiodic correlations of families of unimodular sequences, namely Frank and Chu sequences show optimal nature in asymptotic sense. In particular, [38] shows that there exists an infinite family of unimodular sequences of length N whose aperiodic peak sidelobe level grows like a constant times $\sqrt{N}$.

Sequence sets with aperiodic PSL values behaving like $\mathcal{O}(\sqrt{N})$ as $N \to \infty$ are usually referred to as *asymptotically optimal* owing to the fact that their aperiodic PSL growth has a similar behavior to that of the well-known Welch PSL bound [51]. We refer the interested reader to [9] for further details on this aspect. Note that finding sequence sets with such a behavior is an achievable goal [1], [40] at least computationally. In particular, such sequence can be conveniently designed via numerical tools such as fast CAN algorithms (see, e.g., [2], [8], [52]).

By tapping into the potential of sequence sets in achieving an asymptotically optimal aperiodic PSL growth, in the following, we propose a construction algorithm of binary sequences whose aperiodic PSL grows like $\mathcal{O}(\sqrt{N})$.

III. The Proposed Construction

In this section, we show that sets of sequences with good correlation properties can be used as bases for binary sequences with good auto-correlation. Observe that, for any subset of the sequence sets the PSL growth optimality result holds, as considering a subset only can decrease the PSL. Let $X = \{\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_M\}$ be such a subset of sequences of length N with $\|\boldsymbol{x}_m\|_2^2 = N, \forall m$, having good correlation properties; namely, X is constructed to achieve

$$\begin{aligned} \mathrm{ISL}^{\mathcal{AP}}(X) \triangleq & \sum_{m=1}^{M} \sum_{0<|k|<(N-1)} |r_{m,m}(k)|^2 \\ & + \sum_{m_1=1}^{M} \sum_{m_2 \neq m_1} \sum_{k=-(N-1)}^{N-1} |r_{m_1,m_2}(k)|^2 \end{aligned} \tag{8}$$

that is as small as possible. We assume that $2 \leq M \ll N$, and particularly that M behaves as $\mathcal{O}(1)$ with respect to sequence length N. The lower bound of the aperiodic ISL metric in (8) is given by [52]

$$B_{\mathrm{ISL}^{\mathcal{AP}}}(X) \triangleq N^2 M(M-1). \tag{9}$$

Also note that, using the above lower bound one can achieve the well-known Welch lower bound on $\mathrm{PSL}^{\mathcal{AP}}(X)$:

$$B_{\mathrm{PSL}^{\mathcal{AP}}}(X) \triangleq N \sqrt{\frac{M-1}{2NM - M - 1}}. \tag{10}$$

Interestingly, it was shown in [52] that the above lower bounds for the aperiodic ISL and PSL metrics can be approached conveniently via computational design algorithms such as the fast CAN algorithm in [2]. With this in mind, we further observe that

$$\mathrm{PSL}^{\mathcal{AP}}(X) \sim \sqrt{\frac{M-1}{2M}}\,\sqrt{N} \tag{11}$$

as $N \to \infty$, which implies

$$\mathrm{PSL}^{\mathcal{AP}}(X) \lesssim \frac{1}{\sqrt{2}}\,\sqrt{N}. \tag{12}$$

A. Approaching the Optimal PSL Growth

Let $\boldsymbol{b}$ be a binary sequence (with ± 1 entries) obtained by a linear combination of the sequences $\{\boldsymbol{x}_m\}$, viz.

$$\boldsymbol{b} = w_1 \boldsymbol{x}_1 + w_2 \boldsymbol{x}_2 + \cdots + w_M \boldsymbol{x}_M = \boldsymbol{X}\boldsymbol{w} \tag{13}$$

where

$$\begin{aligned} \boldsymbol{X} &= [\boldsymbol{x}_1 \ \ \boldsymbol{x}_2 \ \ \cdots \ \ \boldsymbol{x}_M], \text{ and} \\ \boldsymbol{w} &= [w_1 \ \ w_2 \ \ \cdots \ \ w_M]^T \in \mathbb{C}^M. \end{aligned}$$

Note that although $\boldsymbol{X}$ and $\boldsymbol{w}$ can be complex vectors, their product $\boldsymbol{X}\boldsymbol{w}$ is not necessarily complex-valued.

Theorem 3: Let $\boldsymbol{X}$ be a set of M sequences each of length N, whose aperiodic PSL is asymptotically upper bounded as in (12). In such a case, the aperiodic PSL of the binary sequence $\boldsymbol{b} = \boldsymbol{X}\boldsymbol{w}$ of (13) will be asymptotically upper bounded by $\frac{\mu^2}{\sqrt{2}}\sqrt{N}$ where $\mu = \|\boldsymbol{w}\|_1 = \sum_{m=1}^{M} |w_m|$.

The significance of Theorem 3 stems from the fact that the asymptotic growth of the aperiodic PSL of the generated binary sequence behaves similarly as that of the original sequence set. The proof of the Theorem 3 goes as follows. The aperiodic auto-correlation lags of $\boldsymbol{b}$ are given by

$$\begin{aligned} r_{\boldsymbol{b}}(k) &= \sum_{l=1}^{N-k} \boldsymbol{b}(l)\boldsymbol{b}^*(l+k) \qquad\qquad (14) \\ &= \sum_{l=1}^{N-k} \left(\sum_{m_1=1}^{M} w_{m_1} \boldsymbol{x}_{m_1}(l) \right) \left(\sum_{m_2=1}^{M} w_{m_2}^* \boldsymbol{x}_{m_2}^*(l+k) \right) \\ &= \sum_{m_1=1}^{M} \sum_{m_2=1}^{M} \left(w_{m_1} w_{m_2}^* \sum_{l=1}^{N-k} \boldsymbol{x}_{m_1}(l) \boldsymbol{x}_{m_2}^*(l+k) \right) \\ &= \boldsymbol{w}^H \boldsymbol{R}_k \boldsymbol{w} \end{aligned}$$

where $[\boldsymbol{R}_k]_{m_1,m_2} = r_{m_1,m_2}(k)$. It follows from (14) that

$$\begin{aligned} |r_{\boldsymbol{b}}(k)| &\leq \sum_{m_1=1}^{M} \sum_{m_2=1}^{M} |w_{m_1}||w_{m_2}||r_{m_1,m_2}(k)| \qquad\qquad (15) \\ &\leq \max_{m_1,m_2} \{|r_{m_1,m_2}(k)|\} \left(\sum_{m_1=1}^{M} \sum_{m_2=1}^{M} |w_{m_1}||w_{m_2}| \right) \\ &\leq \text{PSL}^{\mathcal{AP}}(X)\, \|\boldsymbol{w}\|_1^2. \end{aligned}$$

As a result, using (12) we have that

$$\text{PSL}^{\mathcal{AP}}(\boldsymbol{b}) \lesssim \frac{\mu^2}{\sqrt{2}} \sqrt{N}. \tag{16}$$

In order to determine the growth rate of μ, observe that

$$\begin{aligned} &\left[\boldsymbol{X}^H \boldsymbol{X}\right]_{m,n} = \begin{cases} N & m = n, \\ \alpha_{m,n} & m \neq n, \end{cases} \\ &m, n \in \{1, 2, \ldots, M\}, \end{aligned} \tag{17}$$

where according to (10),

$$|\alpha_{m,n}| \leq N \sqrt{\frac{M-1}{2NM - M - 1}}.$$

Let $\boldsymbol{X} = \boldsymbol{U}\boldsymbol{\Sigma}\boldsymbol{V}^H$ represent the Singular Value Decomposition (SVD) of $\boldsymbol{X}$, where $\boldsymbol{U}$ and $\boldsymbol{V}$ are complex unitary matrices of size $N \times N$ and $M \times M$, respectively, and $\boldsymbol{\Sigma}$ is an $N \times M$ diagonal matrix. Note that $\boldsymbol{X}^H \boldsymbol{X} = \boldsymbol{V}\boldsymbol{\Sigma}^2 \boldsymbol{V}^H$, where

$$\boldsymbol{\Sigma}^2 = \begin{bmatrix} |\sigma_1|^2 & & \boldsymbol{O} \\ & \ddots & \\ \boldsymbol{O} & & |\sigma_M|^2 \end{bmatrix} \tag{18}$$

with $\{\sigma_m\}_{m=1}^{M}$ being the singular values of $\boldsymbol{X}$.

Now observe that,

$$\begin{aligned} \boldsymbol{V}\boldsymbol{\Sigma}^2\boldsymbol{V}^H &= \boldsymbol{X}^H \boldsymbol{X} \\ &\triangleq N\boldsymbol{I}_M + \boldsymbol{Q}, \end{aligned} \tag{19}$$

where,

$$\|\boldsymbol{Q}\|_F \leq N \sqrt{(M^2 - M)\left(\frac{M-1}{2NM - M - 1}\right)}. \tag{20}$$

As a result,

$$|\sigma_m|^2 = \boldsymbol{e}_m^T \boldsymbol{\Sigma}^2 \boldsymbol{e}_m = N + \boldsymbol{e}_m^T \boldsymbol{V}^H \boldsymbol{Q} \boldsymbol{V} \boldsymbol{e}_m. \tag{21}$$

The bound in (20) implies that

$$|\boldsymbol{e}_m^T \boldsymbol{V}^H \boldsymbol{Q} \boldsymbol{V} \boldsymbol{e}_m| \leq N \sqrt{(M^2 - M)\left(\frac{M-1}{2NM - M - 1}\right)}.$$

Consequently, one can easily verify that

$$|\sigma_m|^2 \geq N - N \sqrt{(M^2 - M)\left(\frac{M-1}{2NM - M - 1}\right)}. \tag{22}$$

Further note that,

$$\begin{aligned} \|\boldsymbol{X}^\dagger\|_F^2 &= \sum_{m=1}^{M} \frac{1}{|\sigma_m|^2} \\ &\leq \frac{M}{N - N\sqrt{(M^2 - M)\left(\frac{M-1}{2NM - M - 1}\right)}}. \end{aligned} \tag{23}$$

Moreover as $\boldsymbol{X}^\dagger \boldsymbol{X} = \boldsymbol{I}_M$, we conclude that $\boldsymbol{w} = \boldsymbol{X}^\dagger \boldsymbol{b}$, and therefore,

$$\begin{aligned} \|\boldsymbol{w}\|_2^2 &\leq \|\boldsymbol{X}^\dagger\|_F^2 \|\boldsymbol{b}\|_2^2 \\ &\leq \frac{M}{1 - \sqrt{(M^2 - M)\left(\frac{M-1}{2NM - M - 1}\right)}}. \end{aligned} \tag{24}$$

Note that, due to the Cauchy-Schwarz inequality,

$$\left(\sum_{m=1}^{M} |w_m| \right)^2 \leq \left(\sum_{m=1}^{M} |w_m|^2 \right) \left(\sum_{m=1}^{M} 1 \right). \tag{25}$$

It follows from the above that

$$\begin{aligned}\mu &= \|\boldsymbol{w}\|_1\\ &\le M\sqrt{\frac{1}{1-\sqrt{\frac{M(M-1)^2}{2NM-M-1}}}}\\ &\triangleq f(M,N), \end{aligned}\tag{26}$$

where

$$\lim_{N\to\infty} f(M,N) = M, \tag{27}$$

showing that μ behaves as $\mathcal{O}(1)$ with respect to the sequence length N, as N grows large. Finally, from (16) and (27) one can observe that $\mathrm{PSL}^{\mathcal{AP}}(\boldsymbol{b})$ behaves like $\mathcal{O}(\sqrt{N})$. This conclusion is summarized in Theorem 4. Note that, a similar asymptotic behavior of the periodic PSL of a binary sequence can also be drawn from the above formulations, with minor modifications. A detailed discussion on this observation, however, is omitted here in for the sake of brevity.

Theorem 4: Let $\boldsymbol{X}$ be a set of M sequences each of length N, whose aperiodic PSL grows like $\mathcal{O}(\sqrt{N})$. A binary sequence created as $\boldsymbol{b} = \boldsymbol{X}\boldsymbol{w}$ with $\boldsymbol{w} \in \mathbb{C}^M$ will similarly have an asymptotic aperiodic PSL growth bounded as $\mathcal{O}(\sqrt{N})$.

Remark 1: It is interesting to observe that $|\sigma_m|^2 = N$ occurs if and only if all the sequences included in $\boldsymbol{X}$ are *orthogonal*, which will follow in a zero cross-correlation case. However, in a usual case where the sequences only have a *low* cross-correlation, the orthogonality condition is nearly met, which would lead to a μ that is upper bounded at a value larger than M. ■

B. The Optimal Construction

In the sequel, we investigate an optimal approach to constructing $\boldsymbol{b}$ through considering $\boldsymbol{X}$ as a *basis*—namely, we can construct the binary vectors $\boldsymbol{b}$ using the optimization problem

$$\min_{\boldsymbol{w},\boldsymbol{b}} \|\boldsymbol{X}\boldsymbol{w} - \boldsymbol{b}\|_2^2 \tag{28}$$

A possible approach to deal with constructing such binary sequences is to apply a cyclic minimization of (28); namely, for fixed $\boldsymbol{b}$ the minimizer $\boldsymbol{w}$ of (28) is given by

$$\boldsymbol{w} = \boldsymbol{X}^{\dagger}\boldsymbol{b}. \tag{29}$$

Moreover, for fixed $\boldsymbol{w}$ the minimizer $\boldsymbol{b}$ of (28) can be obtained as

$$\boldsymbol{b} = \mathrm{sgn}\,(\Re\boldsymbol{X}\boldsymbol{w}). \tag{30}$$

Fig. 1 illustrates the simplified geometry of such a construction from a linear combination of sequences, and the binary sequences in their *neighborhood* for the three-dimensional case.

Remark 2: The careful reader may argue that the above approach, while optimal, does not guarantee finding a binary vector in the subspace spanned by the sequence sets—particularly as $M \ll N$. This is a valid observation, and pertains to situations where $\left\|\tilde{\boldsymbol{b}} - \boldsymbol{X}\boldsymbol{w}\right\|_2$ is non-zero at the optimum $\tilde{\boldsymbol{b}}$. Hence, we will have a non-zero fitting error vector $\boldsymbol{\epsilon} \triangleq \tilde{\boldsymbol{b}} - \boldsymbol{X}\boldsymbol{w}$, whose ℓ_2-norm is being minimized in our construction. Consequently, the auto-correlation sequence in this case can be rewritten as

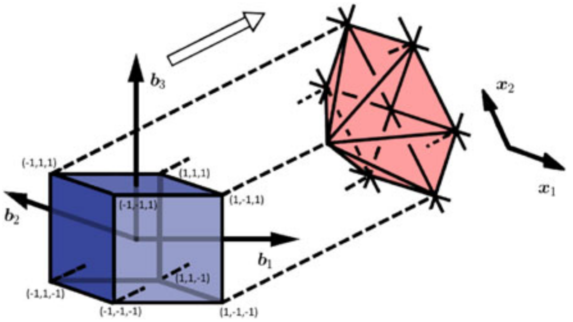


Fig. 1. An illustration of the simplified geometry of construction from the linear combination of sequence sets, and the binary sequence with good correlation in three-dimensional case.

$$\begin{aligned} r_{\tilde{\boldsymbol{b}}}(k) &= \sum_{l=1}^{N-k} \tilde{\boldsymbol{b}}(l)\tilde{\boldsymbol{b}}^*(l+k)\\ &= \sum_{l=1}^{N-k}\left(\sum_{m_1=1}^{M} w_{m_1}\boldsymbol{x}_{m_1}(l) + \boldsymbol{\epsilon}(l)\right)\\ &\qquad \left(\sum_{m_2=1}^{M} w_{m_2}^*\boldsymbol{x}_{m_2}^*(l+k) + \boldsymbol{\epsilon}^*(l+k)\right)\\ &= \sum_{m_1=1}^{M}\sum_{m_2=1}^{M}\left(w_{m_1}w_{m_2}^*\sum_{l=1}^{N-k}\boldsymbol{x}_{m_1}(l)\boldsymbol{x}_{m_2}^*(l+k)\right)\\ &\qquad + \sum_{l=1}^{N-k}\epsilon(l)\epsilon^*(l+k)\\ &\qquad + \left[\sum_{m_1=1}^{M}\left(w_{m_1}\sum_{l=1}^{N-k}\boldsymbol{x}_{m_1}(l)\epsilon^*(l+k)\right)\right.\\ &\qquad \left. + \sum_{m_2=1}^{M}\left(w_{m_2}^*\sum_{l=1}^{N-k}\boldsymbol{x}_{m_2}^*(l+k)\epsilon(l)\right)\right]\\ &= r_{\boldsymbol{b}}(k) + r_{\boldsymbol{\epsilon}}(k) + 2\Re r_{\boldsymbol{b\epsilon}}(k), \end{aligned}\tag{31}$$

where $\{r_{\boldsymbol{b}}(k)\}$ is the *desired* auto-correlation of the binary sequence, and the extra terms $\{r_{\boldsymbol{\epsilon}}(k)\}$ and $\{r_{\boldsymbol{b\epsilon}}(k)\}$ represent the auto-correlation lags of $\boldsymbol{\epsilon}$ and the cross-correlation lags between the *desired* binary sequence $\boldsymbol{b}$ and $\boldsymbol{\epsilon}$, respectively. Interestingly, one can expect that both extra terms $\{r_{\boldsymbol{\epsilon}}(k)\}$ and $\{r_{\boldsymbol{b\epsilon}}(k)\}$ to be small, even if $\boldsymbol{\epsilon}$ is non-zero. This is due to the fact that the optimality of $\tilde{\boldsymbol{b}}$ leads to an $\boldsymbol{\epsilon}$ that has noise-like properties, including a low auto-correlation, as well a low cross-correlation with the binary vector of interest [53]. Therefore, the proposed algorithm works well even if $\|\boldsymbol{b} - \boldsymbol{X}\boldsymbol{w}\| \neq 0$, as is also evident by the numerical results presented in section IV. ■

Interestingly, the global optimization of (28) for finding the *optimal* binary sequences with good auto-correlation can be accomplished in polynomial-time. To see how this goal can be achieved in practice, note that by substituting the minimizer $\boldsymbol{w}$ in (28), the design problem boils down to the following minimization problem:

$$\min_{\boldsymbol{b}} \left\|\boldsymbol{X}\boldsymbol{X}^{\dagger}\boldsymbol{b}-\boldsymbol{b}\right\|_2^2 \tag{32}$$

Now considering that $\boldsymbol{X}\boldsymbol{X}^{\dagger}$ is Hermitian, the objective function of the above minimization problem can be rewritten as

$$\begin{aligned} &\left\|\boldsymbol{X}\boldsymbol{X}^{\dagger}\boldsymbol{b}-\boldsymbol{b}\right\|_2^2 \qquad\qquad (33)\\ &= \left(\boldsymbol{X}\boldsymbol{X}^{\dagger}\boldsymbol{b}-\boldsymbol{b}\right)^H\left(\boldsymbol{X}\boldsymbol{X}^{\dagger}\boldsymbol{b}-\boldsymbol{b}\right)\\ &= \boldsymbol{b}^H\boldsymbol{X}\boldsymbol{X}^{\dagger}\boldsymbol{X}\boldsymbol{X}^{\dagger}\boldsymbol{b}-2\boldsymbol{b}^H\boldsymbol{X}\boldsymbol{X}^{\dagger}\boldsymbol{b}+\boldsymbol{b}^H\boldsymbol{b}\\ &= -\boldsymbol{b}^H\boldsymbol{X}\boldsymbol{X}^{\dagger}\boldsymbol{b}+N. \end{aligned}$$

Therefore, (32) is equivalent to the computation of the binary vector that maximizes the quadratic form $\boldsymbol{b}^H\boldsymbol{X}\boldsymbol{X}^{\dagger}\boldsymbol{b}$; more precisely,

$$\boldsymbol{b}_{opt} \triangleq \arg\max_{\boldsymbol{b}} \boldsymbol{b}^H\boldsymbol{X}\boldsymbol{X}^{\dagger}\boldsymbol{b} \tag{34}$$

in which $\text{rank}(\boldsymbol{X}\boldsymbol{X}^{\dagger}) = M$, that specifically behaves as $\mathcal{O}(1)$ with respect to the problem dimension N. The maximization of a positive (semi-)definite complex quadratic form over a binary vector set is an $\mathcal{NP}$-hard problem in general and can be tackled by exhaustive search when the quadratic form is full-rank. However, as the quadratic form in the above is rank-deficient, the optimum can be found with polynomial complexity in the sequence length N [56], [57]. In particular, [56] proposes an $\mathcal{O}(N^{2M})$ cost algorithm that constructs a set of candidates with cardinality $\mathcal{O}(N^{2M-1})$ including the global optimum of (34) and reduces the size of the feasible set from exponential to polynomial. This is due to the fact that the number of local optima for rank-deficient quadratic forms such as (34) enjoys a polynomial growth, whereas that of a full-rank quadratic form grows exponentially with the sequence length N. Note that the approach presented above can easily be extended to the design of Q-phase (also known as Q-ary) sequences. To this end, one only needs to perform the maximization of the quadratic form in (34) over the set of Q-phase vectors in lieu of binary vectors; which can be completed with polynomial complexity similar to the binary case (see [57] for details).

Finally, the algorithm for construction of the desired binary sequences from the sequence sets with good correlation is summarized in Table II.

Remark 3: We note that norms other than ℓ_2 can also be easily used if one resorts to a cyclic/local optimization of the non-convex problem in (28). But the above discussion reaffirms the key motivation behind using the ℓ_2-norm for our optimization approach: by using ℓ_2-norm, one can formulate the original design problem as a *rank-deficient* quadratic optimization problem. This particular formulation, used along with the computational approach of [56], guarantees not only to (i) find the global optimum sequence of (28), but also to (ii) achieve this goal with a polynomial-time computation cost. These guarantee are central to the promise of the paper, namely finding binary sequences with desirable correlation properties in polynomial-time. Such critical guarantees are not available when using other metrics such as ℓ_1 or ℓ_∞ norms. ■

IV. Numerical Results

In this section, several numerical examples will be presented to examine the performance of our construction in approaching an optimal growth of the PSL metrics. We also show that our optimally constructed sequences are effective in information embedding applications in the sense that they outperform the traditionally employed sequences.

TABLE II
Algorithm for Construction of Binary Sequence Families With Optimal PSL Growth

Step 0: Set N to the lowest feasible sequence length and form $\boldsymbol{X}$ from a well-known family of sequence sets with good correlation properties such as Gold, Kasami, Legendre, Weil families or sequence sets generated by a numerical approach such as the CAN algorithm [2].

Step 1: Find $\boldsymbol{b}$ using (30).

Step 2: Find $\boldsymbol{b}_{opt}$ using (34) following the efficient approach proposed in [57].

Step 3: Increase N to the next available value for which the sequence sets can be generated.

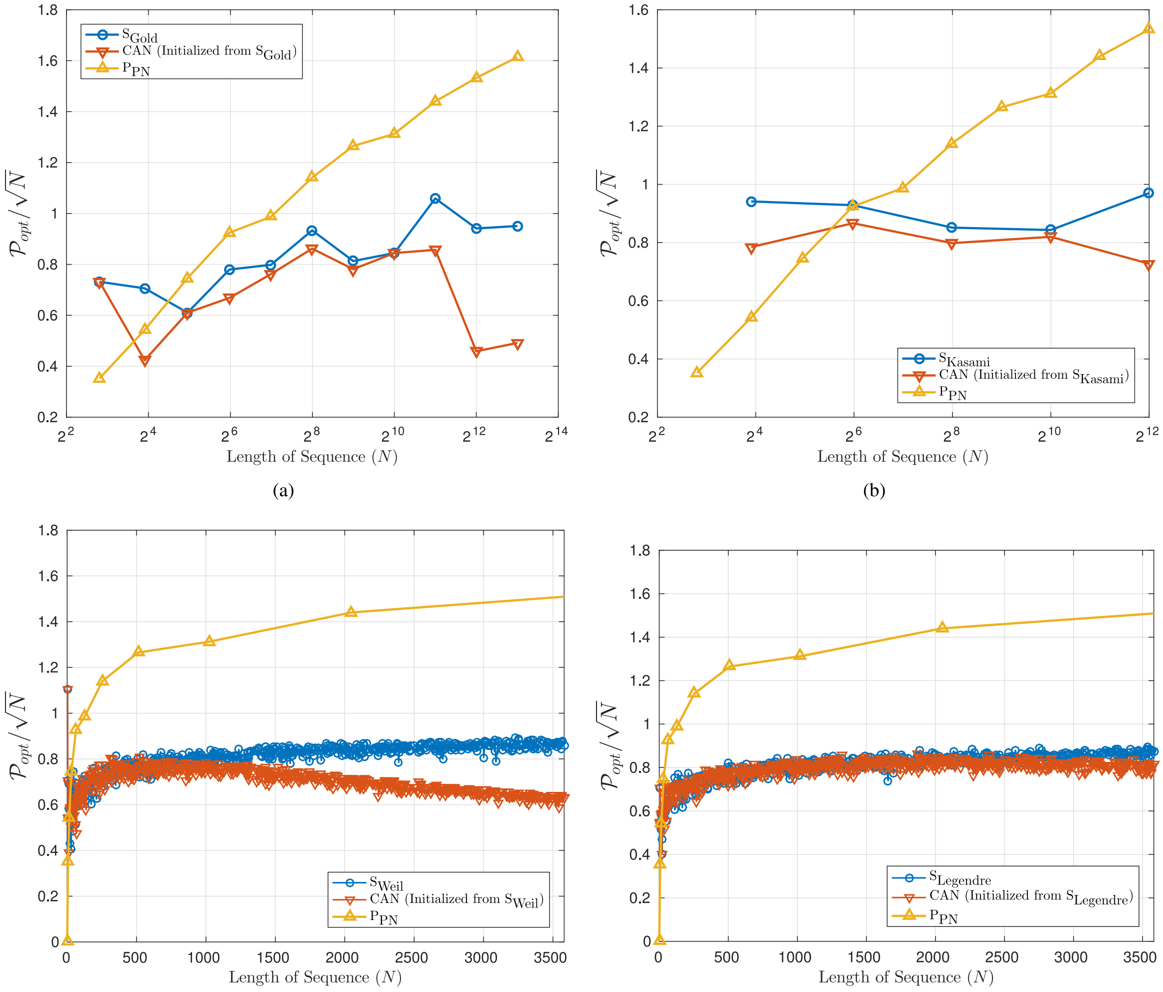
Step 4: Repeat Steps 0–3.

TABLE III
Notation and Number of Sequences

Notation	Sequence name	Maximum length of sequences (N)
$\mathrm{P_{PN}}$	PN sequence	$2^{13}-1=8191$
$\mathrm{S_{Gold}}$	Binary sequence constructed from Gold sequence	$2^{13}-1=8191$
$\mathrm{S_{Kasami}}$	Binary sequence constructed from Kasami sequence	$2^{12}-1=4095$
$\mathrm{S_{Weil}}$	Binary sequence constructed from Weil sequence	3581 (first 500 odd prime numbers)
$\mathrm{S_{Legendre}}$	Binary sequence constructed from Legendre sequence	3581 (first 500 odd prime numbers)

A. Construction of the Sequences

We construct new families of binary sequences by leveraging sequences drawn from well-known sequence sets including Gold [58], Kasami [59], Weil [60] and Legendre sets [61], [62]. We compare the growth of the obtained periodic PSL values (denoted by $\mathcal{P}_{opt}$) of the optimally constructed sequences $\boldsymbol{b}_{opt}$ with the function $\sqrt{N}$, where N denotes the sequence length. Our main interest is to test (through numerical investigations) our claim that the PSL of constructed sequences grows like $\mathcal{O}(\sqrt{N})$. Moreover, we show that although CAN algorithms



(a) (b) (c) (d)

Fig. 2. The PSL growth of constructed binary sequences vs. length N obtained from different sequence families: (a) Gold sequence, (b) Kasami sequence, (c) Weil sequence and (d) Legendre sequence.

are not very effective in finding binary sequence with low PSL, they can be effectively used to lower the PSL of the obtained sequences. This is achieved by using the obtained sequences as initialization for the CAN algorithms. The notations used for the sequence families in the forthcoming discussions and length of sequences that are used are given in Table III.

For comparisons, we make use of the PN sequence as it is very easy to generate for virtually any length of power 2 and is frequently used in literature. We calculate the variations of $\mathcal{P}_{opt}$ with the sequence length N and compare the outcome with $\sqrt{N}$ for the constructed sequences from different sequence sets. Fig. 2 provides evidence of an *almost constant* nature of $\mathcal{P}_{opt}/\sqrt{N}$ as N grows large (from which we conclude that the original function must grow as $\mathcal{O}(\sqrt{N})$). Fig. 2 also compares the value $\mathcal{P}_{opt}/\sqrt{N}$ of obtained sequences with that of the sequences from CAN algorithm (CAN-aided) by using the obtained sequence as initialization, and also with that of PN sequences. It can be observed that the CAN algorithm can effectively reduced the PSL of the obtained sequences from our construction. As a result, by our analysis, the *CAN-aided* sequences should also have an optimal PSL growth. The plots also appear to support the claim that the PSL of PN sequences grows as $\mathcal{O}(\sqrt{N \ln N})$.

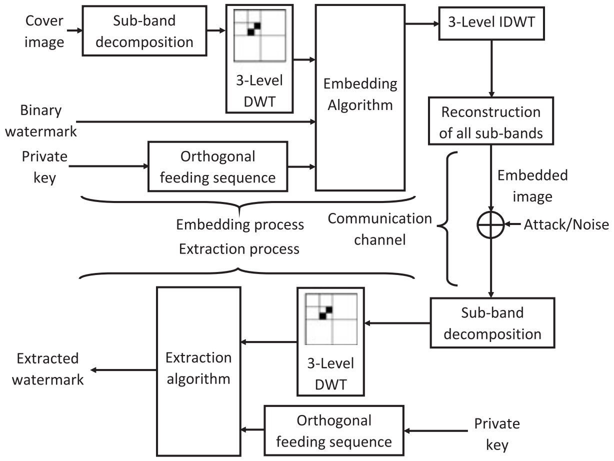
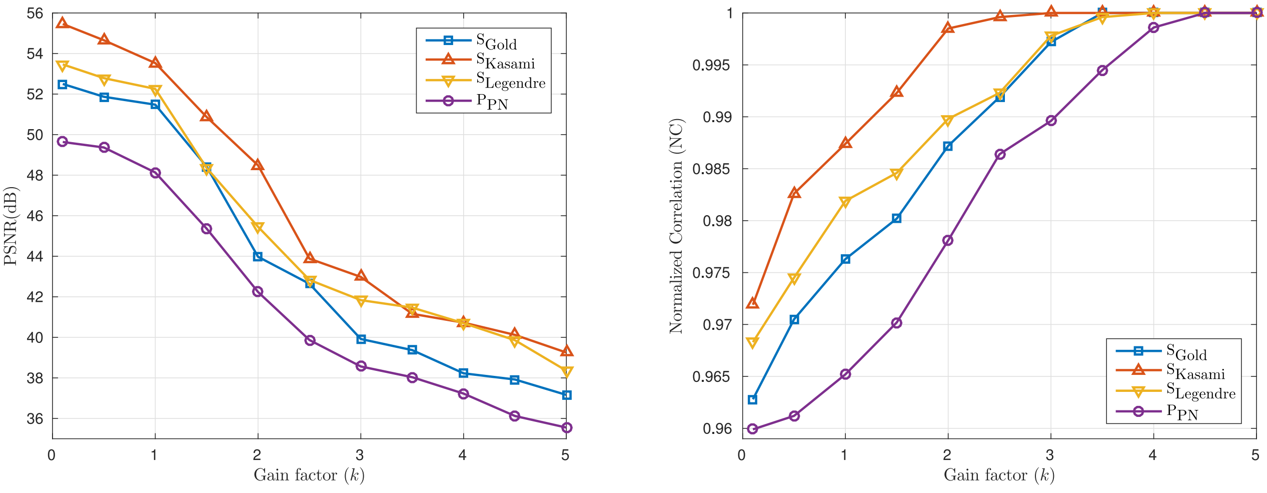


Fig. 3. Block diagram of watermark embedding and extraction algorithm using generated binary sequence.

B. Information Embedding Application

Finally, it is of interest to see the performance of our construction in a practical example. We use our constructed sequences as



(a)

(b)

Fig. 4. The variation of (a) PSNR (dB) and (b) NC with Gain factor (k) for different sequence sets: PN sequence (P_{PN}) and binary sequence constructed from Gold sequence (S_{Gold}), Kasami sequence (S_{Kasami}) and Legendre sequence ($S_{Legendre}$).

orthogonal feeding sequence in a certain digital watermarking algorithm to examine its effectiveness towards imperceptibility and robustness of the watermarked information. The scheme followed in this paper invisibly embeds a binary watermark image into a gray-scale cover image which makes the information about the authentication more secure. The watermarking technique described in [33], [34] employs a Pseudo Noise (PN) sequence as its primary feeding sequence. In this paper, instead of using PN sequences we use our constructed binary sequences for the embedding purpose. The rest of the algorithm closely follows the technique described in [33]. The detailed block diagram of the algorithm is described in Fig. 3.

To verify the effectiveness of the proposed watermarking method, a series of experiments are conducted on several random test images. We use a set of gray cover images of standard size for this purpose. For each test image, the results of proposed watermark scheme are compared with the widely used PN sequences. Perceptual quality of watermarked image is measured by calculating the Peak Signal to Noise Ratio (PSNR) between original cover image and watermarked image. At the receiver, the watermark is extracted from the watermarked image by using the orthogonal codes and evaluation of extracted watermark is done by measuring Normalized Cross-correlation (NC) with the original watermark—see [33] for details.

Fig. 4 compares the variation of PSNR (dB) in watermarked image and NC of original and extracted watermarks with varying *watermarking strength* or *gain factor* (k) for the binary sequences constructed from Gold, Kasami and Legendre sequence families with that of PN sequences. The overall PSNR decreases and the NC increases with increasing k. However, in all cases, our constructed sequences outperform the PN sequence. It can also be observed from Fig. 4 that the binary sequence obtained from Kasami sequence set works best in both cases. Also to comment on the robustness of embedding scheme, a number of spatial and geometrical attacks are applied to the watermarked image. The quality of the watermark extracted from the attacked image is checked using NC between original watermark and extracted watermark. Table IV summarizes the results from various attacks for binary sequences constructed as described before in comparison with the PN sequence. Similar to the previous case, the constructed binary sequences appear to outperform the PN sequence, with S_{Kasami} producing the best result.

TABLE IV
COMPARISON OF RESULTS FROM VARIOUS ATTACKED WATERMARKED IMAGE AT GAIN FACTOR $k = 2$

Attack	NC for Sequences			
	P_{PN}	S_{Gold}	$S_{Legendre}$	S_{Kasami}
Lowpass filter	0.9362	0.9563	0.9725	0.9854
Wiener filter	0.9073	0.9234	0.9541	0.9635
Laplacian high pass filter	0.9463	0.9547	0.9623	0.9841
Edge sharpening	0.9236	0.9339	0.99521	0.9751
JPEG compression	0.9523	0.9712	0.9795	0.9911
Histogram equalization	0.9562	0.9743	0.9829	0.9863
Gaussian noise	0.9672	0.9645	0.9861	0.9910
Salt and Pepper noise	0.9503	0.9739	0.9791	0.9938
Speckle noise	0.9629	0.9719	0.9851	0.9884

V. Concluding Remarks

A polynomial-time construction approach for designing binary sequences with optimal PSL growth was proposed. The suggested approach taps into the potential of sequence sets in achieving an asymptotically optimal PSL growth both in periodic and aperiodic sense, and moreover, makes an effective use of efficient algorithms available for (a specific subset of) non-convex quadratic optimization problems. Several numerical examples have been presented to investigate the PSL growth of the constructed sequences, particularly for rather long sequences (with length $N \sim 2^{12}$). Moreover, it was shown that the constructed sequences can outperform the widely used PN sequence in information embedding applications.

Acknowledgment

The authors would like to thank Prof. P. Stoica of Uppsala University for his insightful comments that helped them immensely in improving parts of their analysis.

References

[1] D. V. Sarwate, "Meeting the Welch bound with equality," in *Sequences and Their Applications (SETA)*. New York, NY, USA: Springer, 1999, pp. 79–102.

[2] H. He, P. Stoica, and J. Li, "Designing unimodular sequence sets with good correlations—Including an application to MIMO radar," *IEEE Trans. Signal Process.*, vol. 57, no. 11, pp. 4391–4405, Nov. 2009.

[3] S. Mertens, "Exhaustive search for low-autocorrelation binary sequences," *J. Phys. A, Math. Gen.*, vol. 29, no. 18, pp. L473–L481, 1996.

[4] F.-M. Dittes, "Optimization on rugged landscapes: A new general purpose Monte Carlo approach," *Phys. Rev. Lett.*, vol. 76, pp. 4651–4655, Jun. 1996.

[5] J. Bernasconi, "Low autocorrelation binary sequences: Statistical mechanics and configuration space analysis," *J. Phys. France*, vol. 48, no. 4, pp. 559–567, 1987.

[6] M. J. E. Golay and D. B. Harris, "A new search for skewsymmetric binary sequences with optimal merit factors," *IEEE Trans. Inf. Theory*, vol. 36, no. 5, pp. 1163–1166, Sep. 1990.

[7] M. Soltanalian and P. Stoica, "Computational design of sequences with good correlation properties," *IEEE Trans. Signal Process.*, vol. 60, no. 5, pp. 2180–2193, May 2012.

[8] P. Stoica, H. He, and J. Li, "New algorithms for designing unimodular sequences with good correlation properties," *IEEE Trans. Signal Process.*, vol. 57, no. 4, pp. 1415–1425, Apr. 2009.

[9] J. Jedwab and K. Yoshida, "The peak sidelobe level of families of binary sequences," *IEEE Trans. Inf. Theory*, vol. 52, no. 5, pp. 2247–2254, May 2006.

[10] J. Jedwab, "A survey of the merit factor problem for binary sequences," in *Sequences and Their Applications—SETA 2004*, T. Helleseth, D. Sarwate, H.-Y. Song, and K. Yang, Eds. Berlin, Heidelberg: Springer, 2005, pp. 30–55.

[11] S. W. Golomb and G. Gong, *Signal Design for Good Correlation: For Wireless Communication, Cryptography, and Radar*. Cambridge, U.K.: Cambridge Univ. Press, 2005.

[12] H. He, J. Li, and P. Stoica, *Waveform Design for Active Sensing Systems: A Computational Approach*, Cambridge, U.K.: Cambridge Univ. Press, 2012.

[13] J. Ling, H. He, J. Li, W. Roberts, and P. Stoica, "Covert underwater acoustic communications," *J. Acoust. Soc. Amer.*, vol. 128, no. 5, pp. 2898–2909, Nov. 2010.

[14] P. Stoica, H. He, and J. Li, "On designing sequences with impulse-like periodic correlation," *IEEE Signal Process. Lett.*, vol. 16, no. 8, pp. 703–706, Aug. 2009.

[15] S. Kocabas and A. Atalar, "Binary sequences with low aperiodic autocorrelation for synchronization purposes," *IEEE Commun. Lett.*, vol. 7, no. 1, pp. 36–38, Jan. 2003.

[16] S. M. Tseng and M. Bell, "Asynchronous multicarrier DS-CDMA using mutually orthogonal complementary sets of sequences," *IEEE Trans. Commun.*, vol. 48, no. 1, pp. 53–59, Jan. 2000.

[17] P. Spasojevic and C. Georghiades, "Complementary sequences for ISI channel estimation," *IEEE Trans. Inf. Theory*, vol. 47, no. 3, pp. 1145–1152, Mar. 2001.

[18] Z. Zhang, F. Zeng, and G. Xuan, "Design of complementary sequence sets based on orthogonal matrixes," in *Proc. Int. Conf. Commun. Circuits Syst.*, Jul. 2010, pp. 383–387.

[19] M. J. E. Golay, "Multi-slit spectrometry," *J. Opt. Soc. Amer.*, vol. 39, no. 6, pp. 437–444, Jul. 1949.

[20] M. J. E. Golay, "Complementary series," *IRE Trans. Inf. Theory*, vol. 7, no. 2, pp. 82–87, Apr. 1961.

[21] J. Davis and J. Jedwab, "Peak-to-mean power control in OFDM, Golay complementary sequences, and Reed-Muller codes," *IEEE Trans. Inf. Theory*, vol. 45, no. 7, pp. 2397–2417, Nov. 1999.

[22] R. Turyn, "Ambiguity functions of complementary sequences (corresp.)," *IEEE Trans. Inf. Theory*, vol. 9, no. 1, pp. 46–47, Jan. 1963.

[23] Y. Tanada, "Synthesis of a set of real-valued shift-orthogonal finite-length PN sequences," in *Proc. IEEE 4th Int. Symp. Spread Spectrum Techn. Appl.*, Sep. 1996, vol. 1, pp. 58–62.

[24] M. Soltanalian and P. Stoica, "On prime root-of-unity sequences with perfect periodic correlation," *IEEE Trans. Signal Process.*, vol. 62, no. 20, pp. 5458–5470, Oct. 2014.

[25] M. Parker, "Even length binary sequence families with low negaperiodic autocorrelation," in *Proc. 14th Int. Conf. Appl. Algebra, Algebraic Algorithms Error-Correcting Codes*, 2001, vol. 2227, pp. 200–209.

[26] L. Bomer and M. Antweiler, "Binary and biphase sequences and arrays with low periodic autocorrelation sidelobes," in *Proc. Int. Conf. Acoust., Speech, Signal Process.*, Apr. 1990, vol. 3, pp. 1663–1666.

[27] J. W. Moon and L. Moser, "On the correlation function of random binary sequences," *SIAM J. Appl. Math.*, vol. 16, no. 2, pp. 340–343, 1968.

[28] S. Wang, "Efficient heuristic method of search for binary sequences with good aperiodic autocorrelations," *Electron. Lett.*, vol. 44, no. 12, pp. 731–732, 2008.

[29] J. Song, P. Babu, and D. P. Palomar, "Optimization methods for designing sequences with low autocorrelation sidelobes," *IEEE Trans. Signal Process.*, vol. 63, no. 15, pp. 3998–4009, Aug. 2015.

[30] K. H. Park, H. Y. Song, D. S. Kim, and S. W. Golomb, "Optimal families of perfect polyphase sequences from the array structure of fermat-quotient sequences," *IEEE Trans. Inf. Theory*, vol. 62, no. 2, pp. 1076–1086, Feb. 2016.

[31] A. Bose and M. Soltanalian, "Non-convex shredded signal reconstruction via sparsity enhancement," in *Proc. IEEE Int. Conf. Acoust., Speech, Signal Process.*, Mar. 2017, pp. 4691–4695.

[32] A. Bose, N. Mohammadi, and M. Soltanalian, "Designing signals with good correlation and distribution properties," in *Proc. IEEE Int. Conf. Acoust., Speech, Signal Process.*, Apr. 2018.

[33] S. Maiti, A. Bose, C. Agarwal, S. K. Sarkar, and N. Islam, "An improved method of pre-filter based image watermarking in DWT domain," *Int. J. Comput. Sci. Technol.*, vol. 4, no. 1, pp. 133–140, Jan.–Mar. 2013.

[34] C. Agarwal, A. Bose, S. Maiti, N. Islam, and S. K. Sarkar, "Enhanced data hiding method using DWT based on saliency model," in *Proc. IEEE Int. Conf. Signal Process., Comput. Control* 2013, pp. 1–6.

[35] S. P. Maity and M. K. Kundu, "A blind CDMA image watermarking scheme in wavelet domain," in *Proc. Int. Conf. Image Process.*, Oct. 2004, vol. 4, pp. 2633–2636.

[36] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Trans. Image Process.*, vol. 6, no. 12, pp. 1673–1687, Dec. 1997.

[37] Y. Fang, J. Huang, and Y. Q. Shi, "Image watermarking algorithm applying CDMA," in *Proc. Int. Symp. Circuits Syst.*, May 2003, vol. 2, pp. II–948–II–951.

[38] K.-U. Schmidt, "Sequences with small correlation," *Des., Codes Cryptography*, vol. 78, no. 1, pp. 237–267, Jan. 2016. [Online]. Available: https://doi.org/10.1007/s10623-015-0154-7

[39] K. H. Leung and B. Schmidt, "The field descent method," *Des., Codes Cryptography*, vol. 36, no. 2, pp. 171–188, Aug. 2005.

[40] M. Soltanalian, M. M. Naghsh, and P. Stoica, "On meeting the peak correlation bounds," *IEEE Trans. Signal Process.*, vol. 62, no. 5, pp. 1210–1220, Mar. 2014.

[41] M. N. Cohen, M. R. Fox, and J. M. Baden, "Minimum peak sidelobe pulse compression codes," in *Proc. IEEE Int. Radar Conf.*, 1990, pp. 633–638.

[42] G. E. Coxson, A. Hirschel, and M. N. Cohen, "New results on minimum-PSL binary codes," in *Proc. IEEE Radar Conf.*, 2001, pp. 153–156.

[43] G. Coxson and J. Russo, "Efficient exhaustive search for optimal-peak-sidelobe binary codes," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 41, no. 1, pp. 302–308, Jan. 2005.

[44] R. J. Turyn, "Sequences with small correlation," in *Error Correcting Codes*, H. B. Mann, Ed. New York, NY, USA: Wiley, 1968, pp. 195–228.

[45] J. Lindner, "Binary sequences up to length 40 with best possible autocorrelation function," *Electron. Lett.*, vol. 11, pp. 507–507, 1975.

[46] N. Levanon and E. Mozeson, *Radar Signals*. New York, NY, USA: Wiley, 2004.

[47] H. Elders-Boll, H. Schotten, and A. Busboom, "A comparative study of optimization methods for the synthesis of binary sequences with good correlation properties," in *Proc. IEEE Symp. Commun. Veh. Technol*, 1997, pp. 24–31.

[48] L. Ein-Dor, I. Kanter, and W. Kinzel, "Low autocorrelated multiphase sequences," *Phys. Rev. E*, vol. 65, Jan. 2002, Art. no. 020102.

[49] I. D. Mercer, "Autocorrelations of random binary sequences," *Combinatorics, Probability Comput.*, vol. 15, no. 5, pp. 663–671, 2006.

[50] D. Dmitriev and J. Jedwab, "Bounds on the growth rate of the peak sidelobe level of binary sequences," *Adv. Math. Commun.*, vol. 1, pp. 461–475, 2007.

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

[52] H. He, P. Stoica, and J. Li, "On aperiodic-correlation bounds," *IEEE Signal Process. Lett.*, vol. 17, no. 3, pp. 253–256, Mar. 2010.
[53] A. H. Sayed, *Adaptive Filters*. New York, NY, USA: Wiley, 2008.
[54] M. Soltanalian and P. Stoica, "Design of perfect phase-quantized sequences with low peak-to-average-power ratio," in *Proc. 20th Eur. Signal Process. Conf.*, 2012, pp. 2576–2580.
[55] M. Soltanalian and P. Stoica, "Designing unimodular codes via quadratic optimization," *IEEE Trans. Signal Process.*, vol. 62, no. 5, pp. 1221–1234, Mar. 2014.
[56] G. Karystinos and A. Liavas, "Efficient computation of the binary vector that maximizes a rank-deficient quadratic form," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3581–3593, Jul. 2010.
[57] A. T. Kyrillidis and G. N. Karystinos, "Rank-deficient quadratic-form maximization over m-phase alphabet: Polynomial-complexity solvability and algorithmic developments," in *Proc. IEEE Int. Conf. Acoust., Speech, Signal Process.*, 2011, pp. 3856–3859.
[58] R. Gold, "Optimal binary sequences for spread spectrum multiplexing," *IEEE Trans. Inf. Theory*, vol. 13, no. 4, pp. 619–621, Oct. 1967.
[59] T. Kasami, "Weight distribution formula for some class of cyclic codes," Coordinated Sci. Lab., Univ. Illinois at Urbana-Champaign, Champaign, IL, USA, Tech. Rep. R-285, Apr. 1966.
[60] J. Rushanan, "Weil sequences: A family of binary sequences with good correlation properties," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2006, pp. 1648–1652.
[61] A. Pott, *Finite Geometry and Character Theory*. Berlin, Germany: Springer-Verlag, 1995.
[62] T. Beth, D. Jungnickel, and H. Lenz, *Design Theory* (Series Design Theory). Cambridge, U.K.: Cambridge Univ. Press, 1999.

Arindam Bose (S'15) received the B.Tech. degree in electronics and computer engineering from the West Bengal University of Technology, Kolkata, India, in 2012. He is currently working toward the Ph.D. degree in electrical engineering with applications in signal processing at the Department of Electrical Engineering, University of Illinois at Chicago, Chicago, IL, USA.

His research interests include different aspects of signal designing for active sensing and communications.

Mojtaba Soltanalian (S'08–M'14) received the Ph.D. degree in electrical engineering (with specialization in signal processing) at the Department of Information Technology, Uppsala University, Uppsala, Sweden, in 2014. He is currently with the faculty of the Electrical and Computer Engineering Department, University of Illinois at Chicago (UIC), Chicago, IL, USA.

Before joining UIC, he held research positions at the Interdisciplinary Centre for Security, Reliability and Trust (SnT, University of Luxembourg), and California Institute of Technology (Caltech). His research interests include interplay of signal processing, learning and optimization theory, and specifically different ways the optimization theory can facilitate a better processing and design of signals for collecting information, communication, as well as to form a more profound understanding of data, whether it is in everyday applications or in large-scale, complex scenarios. He serves as a member of the editorial board of *Signal Processing*, and as the Vice Chair of the IEEE Signal Processing Society Chapter in Chicago. He has been a recipient of the 2017 IEEE Signal Processing Society (SPS) Young Author Best Paper Award.