Constructing Binary Sequences with Optimal Peak Sidelobe Level: An Efficient Analytical-Computational Interplay

Arindam Bose, *Student Member, IEEE*, 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 of such binary sequences from 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*, then the PSL of the constructed binary sequence will experience an *optimal 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 between analytical construction and computational search, but also 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 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

The authors are with the Department of Electrical and Computer Engineering, University of Illinois at Chicago, Chicago, IL, 60607 USA.

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—particularly in the aperiodic cases (see Section II for details). In fact, the task of finding sequences with low auto-correlation is known as an infamously 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]–[39]). 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, if the *peak sidelobe level* (PSL) of the sequence sets grow optimally, then the PSL of the constructed binary sequences also grows in an optimal 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., [40]–[50], 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

[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
$\boldsymbol{x}(k)$	the k^{th} entry of the vector $\boldsymbol{x}$
$\boldsymbol{x}^*(k)$	the complex conjugate of the k^{th} entry of the vector $\boldsymbol{x}$
$\|\boldsymbol{x}\|_p$	the l_p-norm of $\boldsymbol{x}$, defined as $\left(\sum_k \|\boldsymbol{x}(k)\|^p\right)^{\frac{1}{p}}$
$\|\boldsymbol{X}\|_F$	Frobenius norm or the l_2-norm of $\boldsymbol{X}$
$\boldsymbol{X}^H$	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 $\boldsymbol{X}$
$\boldsymbol{I}_n$	the identity matrix for order n
$\mathbb{N}$	the set of natural numbers
$\mathbb{C}$	the set of complex numbers
$\ln a$	natural logarithm of a, equivalent to $\log_e a$
$f(n) = \mathcal{O}(g(n))$	$f(n) < cg(n)$ 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 $f(n) = \Omega(g(n))$

of the problem 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 an 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 binary sequences $\boldsymbol{x}_{m_1}$ and $\boldsymbol{x}_{m_2}$ at shift k are given as,

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

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

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 only on the aperiodic case as it has been traditionally considered to be more practically interesting, as well as more difficult, compared with its periodic counterpart (although the formulations can be directly applied in the periodic case with minor modifications). There has been a long-standing interest in the study of design methods capable of finding binary sequence sets whose aperiodic auto-correlations are, in some measurable sense, collectively small. Note that the in-phase lag (i.e. $k = 0$) of both auto-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 $k \neq 0$) auto-correlation lags are required. To formalize this outcome, several measures of "smallness" have been typically employed, including the *peak sidelobe level* (PSL),

$$\text{PSL}(X) \triangleq \tag{3}$$

$$\max(\{|r_{m_1,m_2}(k)|\}_{m_1 \neq m_2;k} \cup \{|r_{m,m}(k)|\}_{m;k\neq 0}),$$

as well as the *integrated sidelobe level* (ISL),

$$\text{ISL}(X) \triangleq \sum_{m_1 \neq m_2;k} |r_{m_1,m_2}(k)|^2 + \sum_{m;k\neq 0} |r_{m,m}(k)|^2, \tag{4}$$

which are the most relevant to our analysis.

B. Earlier Results

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

$$\mathcal{P}_{min} = \min_{\boldsymbol{x}\in\mathcal{X}_N} \text{PSL}(\boldsymbol{x}). \tag{5}$$

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 [51]-[53]. The value of $\mathcal{P}_{min}$ has been computed up to $N = 70$ in the literature:

1) $\mathcal{P}_{min} \leq 2$ for $N \leq 21$ [54], where $\mathcal{P}_{min} = 1$ is essentially achieved for $N = 2, 3, 4, 5, 7, 11, 13$ by *Barker sequences* [36];
2) $\mathcal{P}_{min} \leq 3$ for $N \leq 48$ (see [55] for $N \leq 40$, and [51] for $N \leq 48$);
3) $\mathcal{P}_{min} \leq 4$ for $N \leq 70$ (see [56] for $49 \leq N \leq 61$, and [52]- [53] for $61 \leq N \leq 70$).

Sequence sets with 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 PSL has a similar behavior to that of the well-known Welch PSL bound [57]. 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], [58], both analytically and computationally. In particular, such sequence can be conveniently designed via numerical tools such as fast CAN algorithms (see, e.g., [2], [8], [59]). A similar task, however, appears to be more difficult when we are concerned with a single binary sequence as in (5). In support of this claim, we present some theoretical bounds on the asymptotic behaviour of $\mathcal{P}_{min}$ that were identified as early as 1968 [35]:

Theorem 1. *(Moon and Moser [35]) 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 PSL$(\boldsymbol{x}) > \mathcal{K}(N)$ approaches 1, as N approaches ∞.*

Theorem 2. *(Moon and Moser [35]) For any fixed $\epsilon > 0$, the proportion of sequences $\boldsymbol{x} \in \mathcal{X}_N$ which have PSL$(\boldsymbol{x}) \leq (2+\epsilon)\sqrt{N \ln N}$ approaches 1, as N approaches ∞.*

It can be concluded from Theorem 1 and 2 that, as $N \to \infty$, for almost all sequences $\mathcal{K}(N) <$ PSL$(\boldsymbol{x}) \leq (2+\epsilon)\sqrt{N \ln N}$ for any $\epsilon > 0$. Mercer [60] 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 [61] 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 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 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].

In the following, we propose a construction algorithm of sequence families whose PSL grows closely like $\mathcal{O}(\sqrt{N})$. This task will be accomplished by tapping into the potential of sequence sets in achieving

an asymptotically optimal PSL growth.

III. The Proposed Construction

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 $X = \{\boldsymbol{x}_1, \boldsymbol{x}_2, \cdots, \boldsymbol{x}_M\}$ be such a subset of sequences of length N having good correlation properties; namely, X is constructed to achieve

$$\begin{aligned}\text{ISL}(X) = &\sum_{m=1}^{M} \sum_{0<|k|<(N-1)} |r_{m,m}(k)|^2 \\ &+ \sum_{m_1=1}^{M} \sum_{m_2 \neq m_1} \sum_{k=-(N-1)}^{N-1} |r_{m_1,m_2}(k)|^2\end{aligned} \tag{6}$$

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 ISL metric in (6) is given by [59]

$$B_{\text{ISL}}(X) \triangleq N^2 M(M-1). \tag{7}$$

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

$$B_{\text{PSL}}(X) \triangleq N\sqrt{\frac{M-1}{2NM-M-1}}. \tag{8}$$

Interestingly, it was shown in [59] that the above lower bounds for the 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

$$\text{PSL}(X) \sim \sqrt{\frac{M-1}{2M}}\ \sqrt{N} \tag{9}$$

as $N \to \infty$, which implies

$$\text{PSL}(X) \lesssim \frac{1}{\sqrt{2}}\ \sqrt{N}. \tag{10}$$

Now let $\boldsymbol{b}$ be a binary sequence obtained by a linear combination of the sequences $\{\boldsymbol{x}_m\}$, viz.

$$\boldsymbol{b} = w_1\boldsymbol{x}_1 + w_2\boldsymbol{x}_2 + \cdots + w_M\boldsymbol{x}_M = \boldsymbol{X}\boldsymbol{w} \tag{11}$$

where

$$\boldsymbol{X} = \begin{bmatrix}\boldsymbol{x}_1 & \boldsymbol{x}_2 & \cdots & \boldsymbol{x}_M\end{bmatrix}, \text{ and} \tag{12}$$

$$\boldsymbol{w} = \begin{bmatrix}w_1 & w_2 & \cdots & w_M\end{bmatrix}^T \in \mathbb{C}^M, \tag{13}$$

and note that the aperiodic correlation lags of $\boldsymbol{b}$ are given by

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

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

$$\begin{aligned}|\widetilde{r}(k)| &\le \sum_{m_1=1}^{M}\sum_{m_2=1}^{M}|w_{m_1}||w_{m_2}||r_{m_1,m_2}(k)| \\ &\le \max_{m_1,m_2}\{|r_{m_1,m_2}(k)|\}\left(\sum_{m_1=1}^{M}\sum_{m_2=1}^{M}|w_{m_1}||w_{m_2}|\right) \\ &\le \text{PSL}(X)\ \|\boldsymbol{w}\|_1^2.\end{aligned} \tag{15}$$

As a result, using (10) we have that

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

in which $\mu = \|\boldsymbol{w}\|_1 = \sum_{m=1}^{M}|w_m|$. In order to determine the growth rate of μ, let $\{\sigma_1, \cdots, \sigma_M\}$ denote the singular values of $\boldsymbol{X}$. We note that

$$\|\boldsymbol{X}\|_F^2 = \sum_{m=1}^{M}\sigma_m^2 = MN \tag{17}$$

while, on the other hand,

$$\left\|\boldsymbol{X}^\dagger\right\|_F^2 = \sum_{m=1}^{M}\frac{1}{\sigma_m^2}. \tag{18}$$

Note that, according to the fixed sum in (17), the summation in (18) will be maximized only if $\left\{\sigma_m^2\right\}$ are identical:

$$\sigma_m^2 = N, \qquad \forall\ m \in \{1, 2, \cdots, M\}, \tag{19}$$

which implies

$$\left\|\boldsymbol{X}^\dagger\right\|_F^2 \le \frac{M}{N}. \tag{20}$$

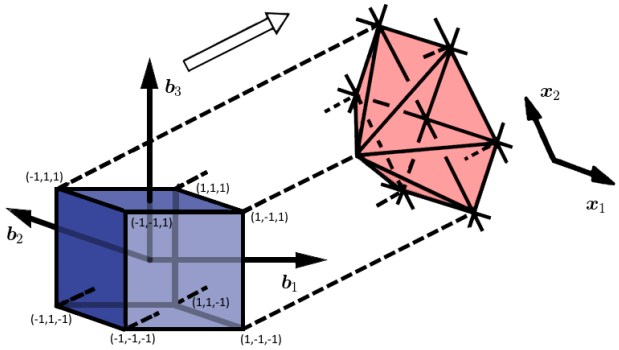


Fig. 1. An illustration of the simplified geometry of construction from the linear combination of sequence sets, and the binary sequence with good correlation in three-dimensional case.

Now, as $\boldsymbol{X}^\dagger \boldsymbol{X} = \boldsymbol{I}$ we have that $\boldsymbol{w} = \boldsymbol{X}^\dagger \boldsymbol{b}$, and as a result,

$$\begin{aligned} \|\boldsymbol{w}\|_2^2 &\leq \left\|\boldsymbol{X}^\dagger\right\|_F^2 \|\boldsymbol{b}\|_2^2 \\ &\leq \left(\frac{M}{N}\right) N = M. \end{aligned} \tag{21}$$

Note that, due to the Cauchy-Schwarz inequality:

$$\left(\sum_{m=1}^{M} |w_m|\right)^2 \leq \left(\sum_{m=1}^{M} |w_m|^2\right)\left(\sum_{m=1}^{M} 1\right) \leq M^2 \tag{22}$$

It follows from the above that

$$\mu = \|\boldsymbol{w}\|_1 = \sum_{m=1}^{M} |w_m| \leq M, \tag{23}$$

showing that μ behaves as $\mathcal{O}(1)$ with respect to the sequence length N. Finally, from (16) and (23) one can observe that PSL($\boldsymbol{b}$) behaves like $\mathcal{O}(\sqrt{N})$.

Remark 1: It is interesting to observe that (19) 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 maximality condition in (19) is nearly met, which should lead to an μ strictly smaller than M. ■

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

$$\min_{\boldsymbol{w},\boldsymbol{b}} \ \|\boldsymbol{X}\boldsymbol{w} - \boldsymbol{b}\|_2^2 \tag{24}$$

As a result, a possible approach to deal with constructing such binary sequences is to apply a cyclic minimization of (24); namely, for fixed $\boldsymbol{b}$ the minimizer $\boldsymbol{w}$ of (24) is given by

$$\boldsymbol{w} = \boldsymbol{X}^{\dagger}\boldsymbol{b}. \tag{25}$$

Moreover, for fixed $\boldsymbol{w}$ the minimizer $\boldsymbol{b}$ of (24) can be obtained as

$$\boldsymbol{b} = \mathrm{sgn}(\boldsymbol{X}\boldsymbol{w}). \tag{26}$$

Fig. 1 illustrates the simplified geometry of construction from a linear combination of sequences, and the binary sequences in their *neighborhood* for the three-dimensional case. Interestingly, the global optimization of (24) 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 (24), it boils down to the following minimization problem:

$$\min_{\boldsymbol{b}} \ \left\| \boldsymbol{X}\boldsymbol{X}^{\dagger}\boldsymbol{b} - \boldsymbol{b} \right\|_2^2 \tag{27}$$

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

$$\begin{aligned} & \left\| \boldsymbol{X}\boldsymbol{X}^{\dagger}\boldsymbol{b} - \boldsymbol{b} \right\|_2^2 \\ &= \left(\boldsymbol{X}\boldsymbol{X}^{\dagger}\boldsymbol{b} - \boldsymbol{b} \right)^H \left(\boldsymbol{X}\boldsymbol{X}^{\dagger}\boldsymbol{b} - \boldsymbol{b} \right) \\ &= \boldsymbol{b}^H \boldsymbol{X}\boldsymbol{X}^{\dagger}\boldsymbol{X}\boldsymbol{X}^{\dagger}\boldsymbol{b} - 2\boldsymbol{b}^H \boldsymbol{X}\boldsymbol{X}^{\dagger}\boldsymbol{b} + \boldsymbol{b}^H\boldsymbol{b} \\ &= -\boldsymbol{b}^H \boldsymbol{X}\boldsymbol{X}^{\dagger}\boldsymbol{b} + N. \end{aligned} \tag{28}$$

Therefore, (27) 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,

$$\boldsymbol{b}_{opt} \triangleq \arg\max_{\boldsymbol{b}} \ \boldsymbol{b}^H \boldsymbol{X}\boldsymbol{X}^{\dagger}\boldsymbol{b} \tag{29}$$

in which $\mathrm{rank}(\boldsymbol{X}\boldsymbol{X}^{\dagger}) = M$, 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 [62], [63]. In particular, [62] proposes an $\mathcal{O}(N^{2M})$ algorithm that constructs a set of candidates with cardinality $\mathcal{O}(N^{2M-1})$ including the global optimum of (29) 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 form in (29) enjoys a polynomial growth, whereas that of a full-rank quadratic form grows exponentially with the sequence length N.

TABLE II

NOTATION AND NUMBER OF SEQUENCES

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

Remark 2: The approach presented above can be easily 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 (29) 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 [63] for details). ■

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 metric. We also show that our optimally constructed sequences are effective in information embedding applications in the sense that they outperform the traditionally employed sequences.

A. Construction of the sequences

We construct new families of binary sequences by leveraging sequences drawn from well-known sequence sets including Gold [65], Kasami [66], Weil [67] and Legendre sets [68], [69]. We compare the growth of the obtained 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 are not very effective in finding binary sequence with low PSL, they can

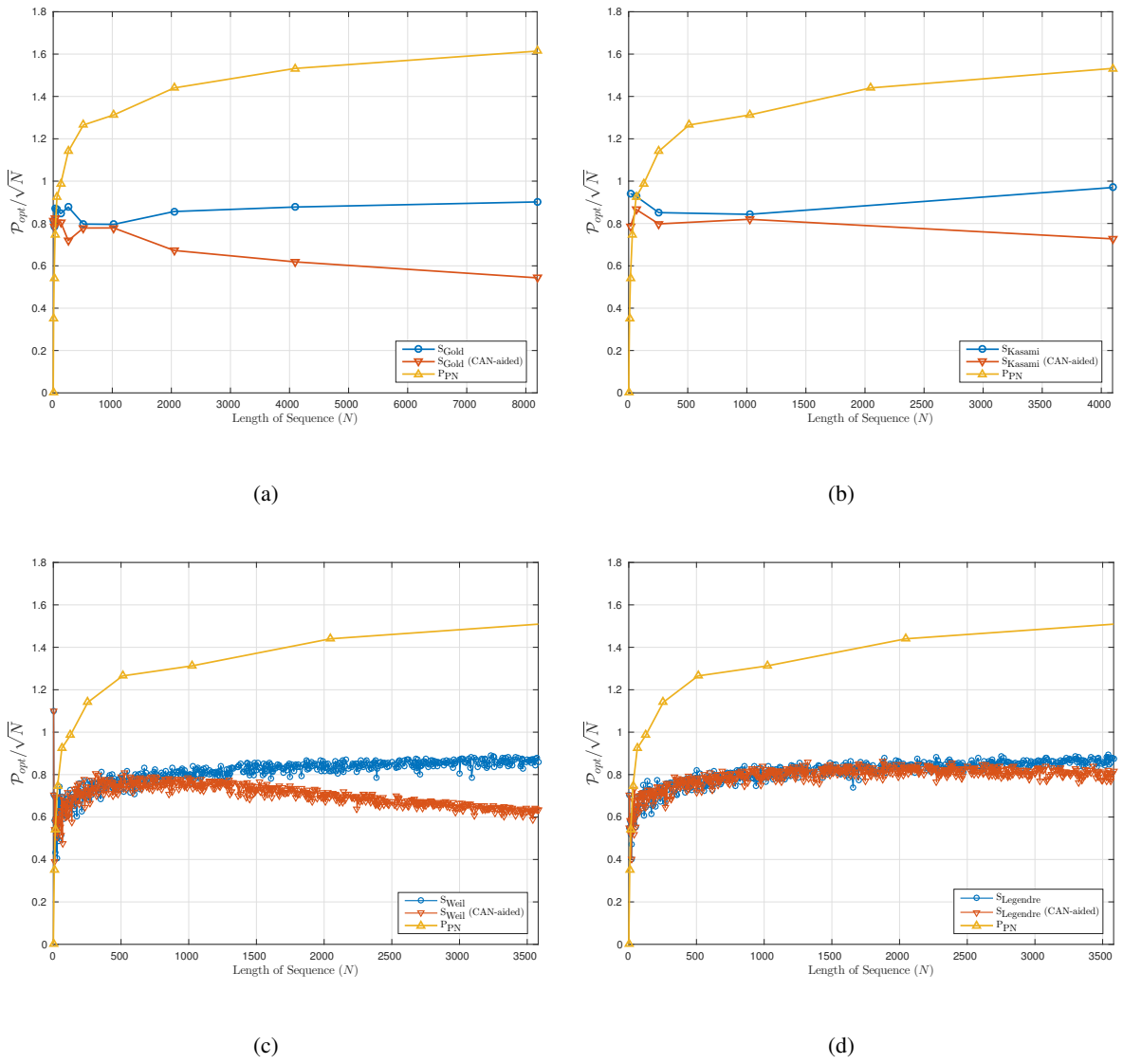


Fig. 2. The PSL growth of constructed binary sequences vs. length N obtained from different sequence families: (a) Gold sequence, (b) Kasami sequence, (c) Weil sequence and (d) Legendre sequence.

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 II.

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

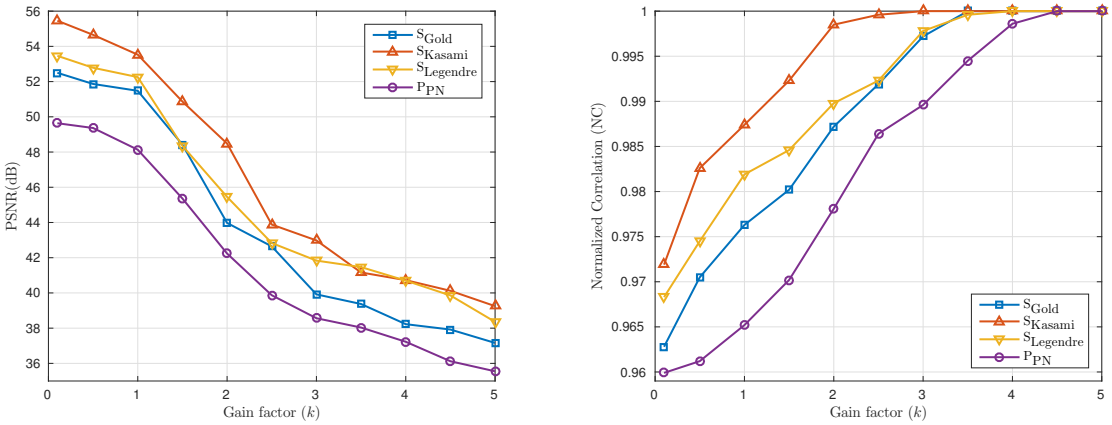
conclude that the original function must grow as $\mathcal{O}(\sqrt{N})$). Fig. 2 also compares the value $\mathcal{P}_{opt}/\sqrt{N}$ of obtained sequences with that of the sequences from CAN algorithm (CAN-aided) by using the obtained sequence as initialization, and also with that of PN sequences. 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 $\mathcal{O}(\sqrt{N \ln N})$.

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 *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 [40], [41] 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 [40].

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 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 [40] for details.

Fig. 3 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. 3 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 III summarizes the results from various attacks for binary sequences



(a) (b)

Fig. 3. 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 ($S_{Legendre}$).

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.

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, 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 $N \sim 2^{12}$). Moreover, it was shown that the constructed sequences can outperform the widely used PN sequence in information embedding applications.

References

[1] D. V. Sarwate, "Meeting the welch bound with equality," in *Sequences and their Applications (SETA)*. New York: 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 Transactions on Signal Processing*, vol. 57, no. 11, pp. 4391–4405, November 2009.

[3] S. Mertens, "Exhaustive search for low-autocorrelation binary sequences," *Journal of Physics A: Mathematical and General*, vol. 29, no. 18, p. L473, 1996.

TABLE III

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

[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] Bernasconi, J., "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 Transactions on Information 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 Transactions on Signal Processing*, vol. 60, no. 5, pp. 2180–2193, 2012.

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

[9] J. Jedwab and K. Yoshida, "The peak sidelobe level of families of binary sequences," *IEEE Transactions on Information 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*, ser. Lecture Notes in Computer Science, T. Helleseth, D. Sarwate, H.-Y. Song, and K. Yang, Eds. Springer Berlin / Heidelberg, 2005, vol. 3486, pp. 19–21.

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

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

[13] J. Ling, H. He, J. Li, W. Roberts, and P. Stoica, "Covert underwater acoustic communications," *Journal of the Acoustical*

Society of America, vol. 128, no. 5, pp. 2898–2909, November 2010.

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

[15] H. Luke, "Sequences and arrays with perfect periodic correlation," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 24, no. 3, pp. 287–294, May 1988.

[16] S. Kocabas and A. Atalar, "Binary sequences with low aperiodic autocorrelation for synchronization purposes," *IEEE Communications Letters*, vol. 7, no. 1, pp. 36–38, January 2003.

[17] X. Tang and W. H. Mow, "A new systematic construction of zero correlation zone sequences based on interleaved perfect sequences," *IEEE Transactions on Information Theory*, vol. 54, no. 12, pp. 5729–5734, December 2008.

[18] R. Frank, "Polyphase complementary codes," *IEEE Transactions on Information Theory*, vol. 26, no. 6, pp. 641–647, November 1980.

[19] S. M. Tseng and M. Bell, "Asynchronous multicarrier DS-CDMA using mutually orthogonal complementary sets of sequences," *IEEE Transactions on Communications*, vol. 48, no. 1, pp. 53–59, January 2000.

[20] Q. Liu, C. Khirallah, L. Stankovic, and V. Stankovic, "Image-in-image hiding using complete complementary sequences," in *IEEE International Conference on Multimedia and Expo*, April 2008, pp. 249–252.

[21] P. Cristea, R. Tuduce, and J. Cornelis, "Complementary sequences for coded aperture imaging," in *50th International ELMAR Symposium*, vol. 1, September 2008, pp. 53–56.

[22] P. Spasojevic and C. Georghiades, "Complementary sequences for ISI channel estimation," *IEEE Transactions on Information Theory*, vol. 47, no. 3, pp. 1145–1152, March 2001.

[23] E. Garcia, J. Garcia, J. Urena, M. Perez, and D. Ruiz, "Multilevel complementary sets of sequences and their application in UWB," in *International Conference on Indoor Positioning and Indoor Navigation (IPIN)*, September 2010, pp. 1–5.

[24] Z. Zhang, F. Zeng, and G. Xuan, "Design of complementary sequence sets based on orthogonal matrixes," in *International Conference on Communications, Circuits and Systems (ICCCAS)*, July 2010, pp. 383–387.

[25] M. J. E. Golay, "Multi-slit spectrometry," *Journal of the Optical Society of America*, vol. 39, no. 6, p. 437, 1949.

[26] ——, "Complementary series," *IRE Transactions on Information Theory*, vol. 7, no. 2, pp. 82–87, April 1961.

[27] J. Davis and J. Jedwab, "Peak-to-mean power control in OFDM, Golay complementary sequences, and Reed-Muller codes," *IEEE Transactions on Information Theory*, vol. 45, no. 7, pp. 2397–2417, November 1999.

[28] S. Eliahou, M. Kervaire, and B. Saffari, "A new restriction on the lengths of Golay complementary sequences," *Journal of Combinatorial Theory, Series A*, vol. 55, no. 1, pp. 49–59, 1990.

[29] R. Turyn, "Ambiguity functions of complementary sequences (corresp.)," *IEEE Transactions on Information Theory*, vol. 9, no. 1, pp. 46–47, January 1963.

[30] Y. Tanada, "Synthesis of a set of real-valued shift-orthogonal finite-length PN sequences," in *IEEE 4th International Symposium on Spread Spectrum Techniques and Applications Proceedings*, vol. 1, September 1996, pp. 58–62.

[31] M. Soltanalian and P. Stoica, "On prime root-of-unity sequences with perfect periodic correlation," *IEEE Transactions on Signal Processing*, vol. 62, pp. 5458–5470, August 2014.

[32] M. Parker, "Even length binary sequence families with low negaperiodic autocorrelation," in *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, ser. Lecture Notes in Computer Science, S. Boztas and I. Shparlinski, Eds. Springer Berlin / Heidelberg, 2001, vol. 2227, pp. 200–209.

[33] L. Bomer and M. Antweiler, "Binary and biphase sequences and arrays with low periodic autocorrelation sidelobes," in *International Conference on Acoustics, Speech, and Signal Processing (ICASSP)*, vol. 3, April 1990, pp. 1663–1666.

[34] K. Arasu, C. Ding, T. Helleseth, P. Kumar, and H. Martinsen, "Almost difference sets and their sequences with optimal autocorrelation," *IEEE Transactions on Information Theory*, vol. 47, no. 7, pp. 2934–2943, November 2001.

[35] J. W. Moon and L. Moser, "On the correlation function of random binary sequences," *SIAM Journal on Applied Mathematics*, vol. 16, no. 2, pp. 340–343, 1968.

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

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

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

[39] 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 Transactions on Information Theory*, vol. 62, no. 2, pp. 1076–1086, Feb 2016.

[40] S. Maiti, A. Bose, C. Agarwal, S. K. Sarkar, and N. Islam, "An improved method of pre-filter based image watermarking in dwt domain," *International Journal of Computer Science and Technology*, vol. 4, no. 1, pp. 133–140, 2013.

[41] C. Agarwal, A. Bose, S. Maiti, N. Islam, and S. K. Sarkar, "Enhanced data hiding method using dwt based on saliency model," in *International Conference on Signal Processing, Computing and Control (ISPCC), 2013*. IEEE, 2013, pp. 1–6.

[42] S. P. Maity and M. K. Kundu, "A blind CDMA image watermarking scheme in wavelet domain," in *International Conference on Image Processing (ICIP)*, vol. 4. IEEE, 2004, pp. 2633–2636 Vol. 4.

[43] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Transactions on Image Processing*, vol. 6, pp. 1673–1687, 1997.

[44] Y. Fang, J. Huang, and Y. Q. Shi, "Image watermarking algorithm applying CDMA," in *Circuits and Systems, 2003. ISCAS '03. Proceedings of the 2003 International Symposium on*, vol. 2. IEEE, 2003, pp. II–948–II–951 vol.2.

[45] N. Nikolaidis and I. Pitas, "Copyright protection of images using robust digital signatures," in *Acoustics, Speech, and Signal Processing, 1996. ICASSP-96. Conference Proceedings., 1996 IEEE International Conference on*, vol. 4. IEEE, 1996, pp. 2168–2171 vol. 4.

[46] M. K. Samee and J. Gtze, "CDMA based blind and reversible watermarking scheme for images in wavelet domain," in *2012 19th International Conference on Systems, Signals and Image Processing (IWSSIP)*. IEEE, 2012, pp. 154–159.

[47] M.-S. Hsieh, D.-C. Tseng, and Y.-H. Huang, "Hiding digital watermarks using multiresolution wavelet transform," *IEEE Transactions on Industrial Electronics*, vol. 48, pp. 875–882, 2001.

[48] R. Safabakhsh, S. Zaboli, and A. Tabibiazar, "Digital watermarking on still images using wavelet transform," in *Information Technology: Coding and Computing, 2004. Proceedings. ITCC 2004. International Conference on*, vol. 1. IEEE, 2004, pp. 671–675 Vol.1.

[49] Y. Fang, J. Huang, and S. Wu, "CDMA-based watermarking resisting to cropping," in *Circuits and Systems, 2004. ISCAS '04. Proceedings of the 2004 International Symposium on*, vol. 2. IEEE, 2004, pp. II–25–8 Vol.2.

[50] R. G. van Schyndel, A. Z. Tirkel, and C. F. Osborne, "A digital watermark," in *Image Processing, 1994. Proceedings. ICIP-94., IEEE International Conference*, vol. 2. IEEE, 1994, pp. 86–90 vol.2.

[51] M. N. Cohen, M. R. Fox, and J. M. Baden, "Minimum peak sidelobe pulse compression codes," in *Radar Conference, 1990., Record of the IEEE 1990 International*. IEEE, 1990, pp. 633–638.

[52] G. E. Coxson, A. Hirschel, and M. N. Cohen, "New results on minimum-psl binary codes," in *Radar Conference, 2001. Proceedings of the 2001 IEEE*. IEEE, 2001, pp. 153–156.

[53] G. Coxson and J. Russo, "Efficient exhaustive search for optimal-peak-sidelobe binary codes," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 41, pp. 302–308, 2005.

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

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

[56] 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 *IEEE Symposium on Communication and Vehicular Technology in the Benelux*. IEEE, 1997, pp. 24–31.

[57] L. Welch, "Lower bounds on the maximum cross correlation of signals," *IEEE Transactions on Information Theory*, vol. 20, no. 3, pp. 397–399, 1974.

[58] M. Soltanalian, M. M. Naghsh, and P. Stoica, "On meeting the peak correlation bounds," *IEEE Transactions on Signal Processing*, vol. 62, no. 5, pp. 1210–1220, 2014.

[59] H. He, P. Stoica, and J. Li, "On aperiodic-correlation bounds," *IEEE Signal Processing Letters*, vol. 17, no. 3, pp. 253–256, March 2010.

[60] I. D. Mercer, "Autocorrelations of random binary sequences," *Combinatorics, Probability and Computing*, vol. 15, no. 05, pp. 663–671, 2006.

[61] D. Dmitriev and J. Jedwab, "Bounds on the growth rate of the peak sidelobe level of binary sequences," *Adv. Math. Commun*, p. 475, 2007.

[62] G. Karystinos and A. Liavas, "Efficient computation of the binary vector that maximizes a rank-deficient quadratic form," *IEEE Transactions on Information Theory*, vol. 56, no. 7, pp. 3581–3593, July 2010.

[63] A. T. Kyrillidis and G. N. Karystinos, "Rank-deficient quadratic-form maximization over m-phase alphabet: Polynomial-complexity solvability and algorithmic developments," in *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE, 2011, pp. 3856–3859.

[64] M. Soltanalian and P. Stoica, "Design of perfect phase-quantized sequences with low peak-to-average-power ratio," in *Proceedings of the 20th European Signal Processing Conference (EUSIPCO)*. IEEE, 2012, pp. 2576–2580.

[65] R. Gold, "Optimal binary sequences for spread spectrum multiplexing," *IEEE Transactions on Information Theory*, vol. 13, no. 4, pp. 619 –621, October 1967.

[66] T. Kasami, "Weight distribution formula for some class of cyclic codes," Coordinated Science Laboratory, University of Illinois, Tech. Rep., April 1966.

[67] J. Rushanan, "Weil sequences: A family of binary sequences with good correlation properties," in *IEEE International Symposium on Information Theory*, Seattle, Washington, USA, July 2006, pp. 1648–1652.

[68] A. Pott, *Finite Geometry and Character Theory*, ser. Lecture Notes in Mathematics. Springer-Verlag Berlin Heidelberg, 1995.

[69] T. Beth, D. Jungnickel, and H. Lenz, *Design Theory*, ser. Design Theory. Cambridge University Press, 1999.