On the PMEPR of binary Golay sequences of length 2^n

Zilong Wang, *Member, IEEE*, Matthew G. Parker, Guang Gong, *Fellow, IEEE* and Gaofei Wu

***Abstract*—In this paper, some questions on the distribution of the PMEPR of standard binary Golay sequences are solved. For n odd, we prove that the PMEPR of each standard binary Golay sequence of length 2^n is exactly 2, and determine the location(s) where peaks occur for each sequence. For n even, we prove that the envelope power of such sequences can never reach 2^{n+1} at time points $t \in \{\frac{v}{2^u} | 0 \leqslant v \leqslant 2^u, v, u \in \mathbb{N}\}$. We further identify 8 sequences of length 2^4 and 8 sequences of length 2^6 that have PMEPR exactly 2, and raise the question whether, asymptotically, it is possible for standard binary Golay sequences to have PMEPR less than $2 - \epsilon$ where $\epsilon > 0$.**

***Index Terms*—Aperiodic autocorrelation, Boolean function, Golay sequences, Littlewood polynomials, peak-to-mean envelope power ratio (PMEPR), Rudin-Shapiro polynomials.**

I. Introduction

MULTICARRIER communications has recently attracted much attention in wireless applications. Orthogonal frequency division multiplexing (OFDM) has been employed in several wireless communication standards. Its popularity is mainly due to its robustness to multipath fading channels and the efficient hardware implementation employing fast Fourier transform (FFT) techniques. However, multicarrier communications have a major drawback of high peak-to-average power ratio (PAPR) of transmitted signals. Please refer to Litsyn's book [10] for a general source on PAPR control.

A coding approach for PAPR control in multicarrier communications is to use Golay complementary sequences [7] for subcarriers, as these sequences provide low peak-to-mean envelope power ratio (PMEPR) of at most 2 for transmitted signals, where the PAPR of the signals is bounded by the PMEPR. Following on from Budišin's recursive construction [4] for Golay sequences of length 2^n, Davis and Jedwab showed that these sequences fill up specific second-order cosets of the generalized first-order Reed-Muller codes [6]. We shall, hereafter, refer to this class of sequences as *standard* Golay sequences. The construction for Golay sequences was further generalized to larger alphabets and code rate was increased by considering near-complementary sequences in [15], [17] [21].

Several lower bounds on the maximum PMEPR, taken over all codewords in a coset of first-order Reed-Muller codes, have been studied in [13], [17], [18], [21], [23], where the approaches were initially proposed by Cammarano and Walker as a result of their summer project [5] in 1999 under the supervision of Davis. In particular, based on the examination of the OFDM signal at time point $t = 0$, it was proved in [5] that the PMEPR of at least one sequence in each standard binary Golay coset of length 2^n for n odd and at least one sequence in each standard quaternary Golay coset of length 2^n for n even is exactly 2. Also, based on the numerical results on the values of OFDM signals at time points $t \in \{\frac{v}{2^u} | 0 \leqslant v \leqslant 2^u, v, u \in \mathbb{N}\}$, several questions on the PMEPR of each standard binary Golay sequence of length 2^n were implicitly raised in Sections 5 and 6 in [5]. Here are three of them, which have remained open until now.

(a) For n odd, the numerical results suggest that the PMEPR might be 2 for every standard binary Golay sequence, but this was only proved for a subset of these sequences by examining the OFDM signal at time $t = 0$. Can additional rules be found to characterize the peak behavior for n odd?
(b) For n even, is the PMEPR of every standard binary Golay sequence always less than 2?
(c) Do the peak positions of the OFDM signal only occur at times $t \in \{\frac{v}{2^u} | 0 \leqslant v < 2^u, v, u \in \mathbb{N}\}$?

In this paper, we develop a method to determine whether the envelope power value of the OFDM signal employing standard binary Golay sequences of length 2^n reaches 2^{n+1} at one or more time points within $t \in \{\frac{v}{2^u} | 0 \leqslant v < 2^u, v, u \in \mathbb{N}\}$. For n odd, we prove that the PMEPR of every standard binary Golay sequence of length 2^n is exactly 2, and that the peak positions occur at times $t \in \{\frac{v}{2^u} | 0 \leqslant v < 2^u, v, u \in \mathbb{N}\}$. Thus we give a positive answer to question (a). For n even, we prove that the envelope power of such sequences can never reach 2^{n+1} at time points $t \in \{\frac{v}{2^u} | 0 \leqslant v < 2^u, v, u \in \mathbb{N}\}$. However, we show that, for both lengths 2^4 and 2^6, the PMEPR of 8 standard binary Golay sequences is exactly 2. Thus we give a negative answer to questions (b) and (c).

The rest of the paper is organized as follows. In Section 2, we introduce some basic definitions and results on peak power control and Golay sequences. In Section 3, we provide two lemmas which play a fundamental role for the proof of the main results. In Section 4, we prove that the PMEPR of

Manuscript received Jan., 2013; revised Sep., 2013. Current version published Jan., 2014. Z. Wang was supported in part by NSFC, No. 11301406, Tian Yuan Foundation, No. 11226074, and Changjiang Scholars and Innovative Research Team in University IRT1078.

Z. Wang is with the State Key Laboratory of Integrated Service Networks, Xidian University, Xi'an, 710071, P.R. China. (e-mail: wzlmath@gmail.com)
M. G. Parker is with the Department of Informatics, University of Bergen, PO Box 7803, N-5020 Bergen, Norway (e-mail: matthew@ii.uib.no)
G. Gong is with Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON. N2L 3G1, Canada. (e-mail: ggong@uwaterloo.ca)
G. Wu is with the State Key Laboratory of Integrated Service Networks, Xidian University, Xi'an, 710071, P.R. China. (e-mail: gaofei_wu@qq.com)
Communicated by K. Yang, Associate Editor for Sequences.

every standard binary Golay sequence of length 2^n for n odd is exactly 2. In Section 5, we first prove that the envelope power of standard binary Golay sequences of length 2^n, n even, can never reach 2^{n+1} at time points $t \in \{\frac{v}{2^u} | 0 \leqslant v < 2^u, v, u \in \mathbb{N}\}$. Then we give a sufficient condition for a self-reciprocal polynomial to have at least one unimodular root. Finally we prove, for both lengths 2^4 and 2^6, that the PMEPR of 8 standard binary Golay sequences is exactly 2. In Section 6, we discuss Rudin-Shapiro polynomials and Littlewood Polynomials, and conclude the paper.

II. Preliminaries

In this section, we introduce some basic concepts and results on peak power control and binary Golay sequences.

A. Peak Power Control in OFDM

Let $\mathbf{a} = (a_0, a_1, \cdots, a_{N-1})$ be a binary sequence of length N where $a_i \in \{0, 1\}$ for $0 \leqslant i < N$.

In an OFDM system with N subcarriers, the transmitted signal by employing sequence $\mathbf{a}$ can be modeled as the real part of

$$s_{\mathbf{a}}(t) = \sum_{i=0}^{N-1} (-1)^{a_i} e^{2\pi\sqrt{-1}(f_0 + i\triangle f)t}, \ t \in [0, \frac{1}{\triangle f}),$$

where $\triangle f$ is the frequency separation between adjacent subcarrier pairs and f_0 is the base frequency.

The sequence $\mathbf{a}$ can be associated with the polynomial

$$A(z) = \sum_{i=0}^{N-1} (-1)^{a_i} z^i$$

in indeterminate z. The relationship between the transmitted signal $s_{\mathbf{a}}(t)$ and the polynomial $A(z)$ can be obtained by restricting z to lie on the unit circle in the complex plane, i.e.,

$$s_{\mathbf{a}}(t) = e^{2\pi\sqrt{-1}f_0 t} A(e^{2\pi\sqrt{-1}\triangle f t}).$$

Then

$$|s_{\mathbf{a}}(t)| = |A(e^{2\pi\sqrt{-1}\triangle f t})|.$$

Instead of $s_{\mathbf{a}}(t)$, we usually study polynomial $A(z)$ by setting $|z| = 1$, i.e., $z = e^{2\pi t\sqrt{-1}}$ for *time points* $t \in [0, 1)$. Then the *instantaneous envelope power* of the transmitted signal is determined by $|A(z)|^2$, and the *peak-to-mean envelope power ratio* (PMEPR) is determined by

$$\text{PMEPR}(\mathbf{a}) = \frac{1}{N} \sup_{|z|=1} |A(z)|^2. \tag{1}$$

For polynomial $A(z)$, straightforward manipulation shows that

$$A(z)A(z^{-1}) = N + \sum_{\tau=1}^{N-1} C_{\mathbf{a}}(\tau)(z^{\tau} + z^{-\tau}) \tag{2}$$

where the *aperiodic autocorrelation* $C_{\mathbf{a}}(\tau)$ of sequence $\mathbf{a}$ is defined by

$$C_{\mathbf{a}}(\tau) = \sum_{i=0}^{N-1-\tau} (-1)^{a_i - a_{i+\tau}}, \ 0 \leqslant \tau < N. \tag{3}$$

A pair of sequences $(\mathbf{a}, \mathbf{b})$ of length N is called a *Golay complementary pair* if

$$C_{\mathbf{a}}(\tau) + C_{\mathbf{b}}(\tau) = 0, \ 0 < \tau < N.$$

Each sequence of such a complementary pair is called a *Golay complementary sequence*, or *Golay sequence* in honor of Golay who first introduced this condition in 1951 [7]. For a brief overview to Golay sequences, see [16].

An upper bound on the PMEPR of signals employing Golay sequences was obtained by Popović [19]. If $(\mathbf{a}, \mathbf{b})$ form a Golay complementary pair of length N, then their associated polynomials $(A(z), B(z))$ satisfy

$$A(z)A(z^{-1}) + B(z)B(z^{-1}) = 2N.$$

By restricting z to lie on the unit circle, we obtain $|A(z)|^2 = A(z)A(z^{-1})$ and

$$|A(z)|^2 + |B(z)|^2 = 2N, \quad |z| = 1. \tag{4}$$

According to (1) and (4), the PMEPR of every Golay sequence is upper bounded by 2.

The basic idea of this paper is derived from an observation on equation (4). If the equation $B(z) = 0$ has at least one unimodular root, then the maximum of $|A(z)|^2$ for $|z| = 1$ equals $2N$ and we have $\text{PMEPR}(\mathbf{a}) = 2$. Otherwise $\text{PMEPR}(\mathbf{a})$ is strictly less than 2. Therefore, this paper is concerned with the unimodular roots of the polynomials associated with Golay sequences.

B. Standard Golay Sequences

Sequence

$$\mathbf{f} = (f_0, f_1, \cdots, f_{2^n-1})$$

of length 2^n can be described by a Boolean function $f(x_1, x_2, \cdots, x_n)$ with an algebraic normal form in n variables where

$$f_i = f(i_1, i_2, \cdots, i_n), \quad i = \sum_{k=1}^{n} i_k 2^{k-1}.$$

Thus the i-th term of the sequence $\mathbf{f}$ is obtained by evaluating the Boolean function $f(x_1, x_2, \cdots, x_n)$ at the 2-adic decomposition of i. The r-th order binary *Reed-Muller code* of length 2^n is the set of all sequences $\mathbf{f}$, where $f(x_1, x_2, \cdots, x_n)$ is a Boolean function of degree at most r.

Golay first gave a direct construction for Golay complementary pairs of length $N = 2^n$ [8]. In 1999, Davis and Jedwab identified a large set of Golay sequences occurring as a subset of the 2nd order binary Reed-Muller code.

Theorem 1: ([6]) For $n \geqslant 2$, let $a(x_1, x_2, \cdots, x_n)$ and $b(x_1, x_2, \cdots, x_n)$ be Boolean functions defined by

$$a(x_1, x_2, \cdots, x_n) = \sum_{i=1}^{n-1} x_{\pi(i)} x_{\pi(i+1)} + \sum_{i=1}^{n} c_i x_i + c_0, \tag{5}$$

$$b(x_1, x_2, \cdots, x_n) = a(x_1, x_2, \cdots, x_n) + x_{\pi(n)}, \tag{6}$$

where π is a permutation of symbols $\{1, 2, \cdots, n\}$ and $c_i \in \{0, 1\}$, $0 \leqslant i \leqslant n$. Then the sequences described

by $a(x_1, x_2, \cdots, x_n)$ and $b(x_1, x_2, \cdots, x_n)$ form a Golay complementary pair.

The above construction gives a set of $n!2^n$ distinct Golay sequences of length 2^n. We call Golay sequences of the form in (5) *standard*. To the best of our knowledge, these are the only known binary Golay sequences of length 2^n.

Note that references [6] and [17] provide more details on the generalized Boolean functions from $\mathbb{Z}_2^n$ to $\mathbb{Z}_H$ and the constructions of H-ary Golay sequences for H even. However, we are only concerned with binary Golay sequences in this paper.

III. Results on Boolean Functions and Polynomials

In this section, we find some relationships between the Boolean functions and the polynomials associated with sequences, which play an important role in the proof of the main results.

The first lemma is a well-known result on the balancedness of Boolean functions.

Lemma 1: (pp.372 in [12]) Let $f'(x_1, x_2, \cdots, x_{n-1})$ be an arbitrary Boolean function of $n-1$ variables. Then Boolean function $f(x_1, x_2, \cdots, x_n) = f'(x_1, x_2, \cdots, x_{n-1}) + x_n$ is balanced. Alternatively, polynomial $F(z)$ associated with sequence $\mathbf{f}$ described by $f(x_1, x_2, \cdots, x_n)$ has a root at 1, or $(z-1)|F(z)$.

Corollary 1 below follows from Lemma 1 by observing that an invertible linear transformation of the input variables of a Boolean function preserves balancedness.

Corollary 1: Let $h_i(x_1, x_2, \cdots, x_n)(1 \leqslant i \leqslant n)$ be linear functions of variables $x_1, x_2, \cdots, x_n$ where $h_1, h_2, \cdots, h_n$ are linearly independent, and $f'(x_1, x_2, \cdots, x_{n-1})$ an arbitrary Boolean function of $n-1$ variables. Then Boolean function

$$\begin{aligned} f(x_1, \cdots, x_n) =& f'(h_1(x_1, \cdots, x_n), \cdots, h_{n-1}(x_1, \cdots, x_n)) \\ &+ h_n(x_1, \cdots, x_n) \end{aligned}$$

is balanced. Alternatively, polynomial $F(z)$ associated with sequence $\mathbf{f}$ has a root at 1, or $(z-1)|F(z)$.

By using Lemma 1 and Corollary 1, we can determine the instantaneous envelope power of the signals employing some Golay sequences at the point $z = 1$, which yields the main results for binary Golay sequences in [5]. To study the polynomial $F(z)$ at the points $z = e^{2\pi t\sqrt{-1}}$ where $t \in \{\frac{v}{2^u} | 0 \leqslant v < 2^u, v, u \in \mathbb{N}\}$, we need the following lemma.

Lemma 2: Let $f(x_1, x_2, \cdots, x_n)$ and $g(x_1, x_2, \cdots, x_n)$ be two Boolean functions satisfying

$$g(x_1, x_2, \cdots, x_n) = f(x_1, x_2, \cdots, x_n) + x_k,$$

for fixed k $(1 \leqslant k \leqslant n)$, and let polynomials $F(z)$ and $G(z)$ be associated with sequences $\mathbf{f}$ and $\mathbf{g}$, respectively. Then we have

$$(z^{2^{k-1}} - 1)|F(z) \Longleftrightarrow (z^{2^{k-1}} + 1)|G(z).$$

Proof: We set the sequences described by Boolean functions $f(x_1, x_2, \cdots, x_n)$ and $g(x_1, x_2, \cdots, x_n)$ as

$$\begin{aligned} \mathbf{f} &= (a_0, a_1, \cdots a_{2^n-1}), \\ \mathbf{g} &= (b_0, b_1, \cdots b_{2^n-1}). \end{aligned}$$

Then the polynomials associated with Boolean functions $f(x_1, x_2, \cdots, x_n)$ and $g(x_1, x_2, \cdots, x_n)$ are given by

$$F(z) = \sum_{i=0}^{2^n-1} (-1)^{a_i} z^i$$

and

$$G(z) = \sum_{i=0}^{2^n-1} (-1)^{b_i} z^i,$$

respectively.

If $k = 1$, we have

$$(z-1)|F(z) \Longleftrightarrow \sum_{i=0}^{2^n-1} (-1)^{a_i} = 0$$

and

$$(z+1)|G(z) \Longleftrightarrow \sum_{i=0}^{2^n-1} (-1)^{b_i} (-1)^i = 0.$$

Since $g(x_1, x_2, \cdots, x_n) = f(x_1, x_2, \cdots, x_n) + x_1$, we have $b_i = a_i$ for i even, and $b_i = a_i + 1$ for i odd, i.e.,

$$(-1)^{a_i} = (-1)^{b_i} (-1)^i.$$

Then it is clear that

$$(z-1)|F(z) \Longleftrightarrow (z+1)|G(z).$$

For general k, the sequence described by Boolean function x_k is

$$(\underbrace{0, \cdots, 0}_{2^{k-1}\ 0s}, \underbrace{1, \cdots, 1}_{2^{k-1}\ 1s}, \underbrace{0, \cdots, 0}_{2^{k-1}\ 0s}, \cdots, \underbrace{1, \cdots, 1}_{2^{k-1}\ 1s}).$$

Then we have $b_i = a_i$ for $\lfloor \frac{i}{2^{k-1}} \rfloor$ even, and $b_i = a_i + 1$ for $\lfloor \frac{i}{2^{k-1}} \rfloor$ odd.

Let ϕ_1 be the natural homomorphism from polynomial ring $\mathbb{C}[z]$ to quotient ring $\mathbb{C}[z]/ < z^{2^{k-1}} - 1 >$. Then we have

$$(z^{2^{k-1}} - 1)|F(z) \Longleftrightarrow \phi_1(F(z)) = 0,$$

where

$$\begin{aligned} \phi_1(F(z)) &= \phi_1\left(\sum_{i=0}^{2^n-1} (-1)^{a_i} z^i\right) \\ &= \sum_{i=0}^{2^n-1} (-1)^{a_i} \phi_1(z^i) \\ &= \sum_{t=0}^{2^{n-k+1}-1} \sum_{s=0}^{2^{k-1}-1} (-1)^{a_{2^{k-1}\times t+s}} \phi_1(z^{2^{k-1}\times t+s}) \\ &= \sum_{s=0}^{2^{k-1}-1} \phi_1(z^s) \sum_{t=0}^{2^{n-k+1}-1} (-1)^{a_{2^{k-1}\times t+s}}. \end{aligned}$$

Note that $\{\phi_1(1), \phi_1(z), \phi_1(z^2), \cdots, \phi_1(z^{2^{k-1}-1})\}$ is a basis for $\mathbb{C}[z]/ < z^{2^{k-1}} - 1 >$ over complex field $\mathbb{C}$. We obtain that the condition $(z^{2^{k-1}} - 1)|F(z)$ is equivalent to

$$\sum_{t=0}^{2^{n-k+1}-1} (-1)^{a_{2^{k-1}\times t+s}} = 0, \text{ for } 0 \leqslant s \leqslant 2^{k-1} - 1. \quad (7)$$

Similarly, let ϕ_2 be the natural homomorphism from $\mathbb{C}[z]$ to quotient ring $\mathbb{C}[z]/ < z^{2^{k-1}} + 1 >$. Then we have

$$(z^{2^{k-1}} + 1)|G(z) \Longleftrightarrow \phi_2(G(z)) = 0,$$

where

$$\begin{aligned}\phi_2(G(z)) &= \phi_2\left(\sum_{i=0}^{2^n-1}(-1)^{b_i}z^i\right)\\ &= \sum_{t=0}^{2^{n-k+1}-1}\sum_{s=0}^{2^{k-1}-1}(-1)^{b_{2^{k-1}\times t+s}}\phi_2(z^{2^{k-1}\times t+s})\\ &= \sum_{s=0}^{2^{k-1}-1}\phi_2(z^s)\sum_{t=0}^{2^{n-k+1}-1}(-1)^{b_{2^{k-1}\times t+s}}(-1)^t.\end{aligned}$$

Note that $\{\phi_2(1), \phi_2(z), \phi_2(z^2), \cdots, \phi_2(z^{2^{k-1}-1})\}$ is a basis for $\mathbb{C}[z]/ < z^{2^{k-1}} + 1 >$ over $\mathbb{C}$. We obtain that the condition $(z^{2^{k-1}} + 1)|G(z)$ is equivalent to

$$\sum_{t=0}^{2^{n-k+1}-1}(-1)^{b_{2^{k-1}\times t+s}}(-1)^t = 0, \text{ for } 0 \leqslant s \leqslant 2^{k-1} - 1. \tag{8}$$

Recall that $a_{2^{k-1}\times t+s} = b_{2^{k-1}\times t+s}$ for t even, and $a_{2^{k-1}\times t+s} = b_{2^{k-1}\times t+s} + 1$ for t odd, i.e.,

$$(-1)^{a_{2^{k-1}\times t+s}} = (-1)^{b_{2^{k-1}\times t+s}}(-1)^t,$$

which makes the conditions in (7) and (8) equivalent. Therefore, $(z^{2^{k-1}} - 1)|F(z) \Longleftrightarrow (z^{2^{k-1}} + 1)|G(z)$. □

IV. PMEPR of Standard Binary Golay Sequences of Length 2^{2m-1}

In this section, we set $n = 2m - 1$, and prove that the PMEPR of all standard binary Golay sequences of length 2^{2m-1} equals 2. The Boolean functions with the form in (5), describing all the standard binary Golay sequences of length 2^{2m-1}, can be re-expressed as

$$\begin{aligned}&f(x_1, x_2, \cdots, x_{2m-1})\\ &= \sum_{i=1}^{m-1} x_{\pi(2i)}(x_{\pi(2i-1)} + x_{\pi(2i+1)}) + \sum_{i=1}^{2m-1} c_i x_i + c_0,\end{aligned} \tag{9}$$

where π is a permutation of symbols $\{1, 2, \cdots, 2m-1\}$, and $c_i \in \{0, 1\}$ for $0 \leqslant i \leqslant 2m - 1$.

Definition 1: For a given permutation π of symbols $\{1, 2, \cdots, 2m-1\}$, define $\lambda = \lambda(\pi)$ as the smallest positive integer which is not in the set $\{\pi(2i)|1 \leqslant i \leqslant m-1\}$, and define the linear transformation

$$\begin{cases} h_{2i}(x_1, x_2, \cdots, x_{2m-1}) &= x_{\pi(2i)},\\ h_{2i-1}(x_1, x_2, \cdots, x_{2m-1}) &= x_{\pi(2i-1)} + x_{\pi(2i+1)},\\ h_{2m-1}(x_1, x_2, \cdots, x_{2m-1}) &= x_\lambda, \end{cases} \tag{10}$$

where $1 \leqslant i \leqslant m-1$.

Remark 1: From the above definition, we have $h_{\pi^{-1}(k)} = x_k$ for $1 \leqslant k \leqslant \lambda - 1$.

It is not hard to check that the transformation in (10) is an invertible linear transformation of variables $x_1, x_2, \cdots, x_{2m-1}$. So $h_1, h_2, \cdots, h_{2m-1}$ are linearly independent. Then the Boolean function in (9) can be written in the form

$$\begin{aligned}&f(x_1, x_2, \cdots, x_{2m-1})\\ &= \left(\sum_{i=1}^{m-1} h_{2i}h_{2i-1} + \sum_{i=1}^{2m-2} d_i h_i\right) + d_{2m-1}h_{2m-1} + d_0,\end{aligned} \tag{11}$$

where $d_i \in \{0, 1\}$ for $0 \leqslant i \leqslant 2m - 1$. Let

$$f' = \sum_{i=1}^{m-1} h_{2i}h_{2i-1} + \sum_{i=1}^{2m-2} d_i h_i.$$

Then f' is a bent function [20] of $2m - 2$ variables $h_1, h_2, \cdots, h_{2m-2}$, and $f = f' + d_{2m-1}h_{2m-1} + d_0$. Since a bent function is known to be unbalanced, the Boolean function f in (11) must be unbalanced if the coefficient $d_{2m-1} = 0$. If $d_{2m-1} = 1$, then f is balanced according to Corollary 1.

Lemma 3: Let $f(x_1, x_2, \cdots, x_{2m-1})$ be a Boolean function of the form in (11). Then f is balanced if and only if $d_{2m-1} = 1$.

For each polynomial associated with a standard binary Golay sequence of length 2^{2m-1}, we show that there exists at least one unimodular root by the following theorem.

Theorem 2: Let π be a permutation of $(1, 2, \cdots, 2m-1)$, $\lambda = \lambda(\pi)$ given in Definition 1, $f(x_1, \cdots, x_{2m-1})$ a Boolean function of the form in (5), and $F(z)$ the polynomial associated with sequence $\mathbf{f}$. Then $F(z) = 0$ has one unimodular root θ satisfying $\theta^{2^\lambda} = 1$. Moreover,
(1) If f is a balanced function, we have $(z^{2^{\lambda-1}} - 1)|F(z)$.
(2) If f is an unbalanced function, we have $(z^{2^{\lambda-1}} + 1)|F(z)$.

Proof: Write the Boolean function $f(x_1, \cdots, x_{2m-1})$ in the form in (11). We have $h_{2m-1} = x_\lambda$ and $h_{\pi^{-1}(k)} = x_k$ for $1 \leqslant k \leqslant \lambda - 1$ by Definition 1 and Remark 1. Note that f is balanced if and only if $d_{2m-1} = 1$ by Lemma 3.

If f is balanced, we prove that the statement $(z^{2^{k-1}} - 1)|F(z)$ holds by mathematical induction for $1 \leqslant k \leqslant \lambda$. For the base case $k = 1$, since f is a balanced function, we have $(z-1)|F(z)$. For all balanced Boolean functions f with the form in (11) and specified value λ, suppose the statement $(z^{2^{k-1}} - 1)|F(z)$ holds for some value of k $(1 \leqslant k \leqslant \lambda - 1)$. Consider a pair of Boolean functions and their associated polynomials

$$\begin{cases} f, \\ f_k = f + x_k, \end{cases} \text{and} \quad \begin{cases} F(z), \\ F_k(z). \end{cases}$$

Since f is balanced and $x_k = h_{\pi^{-1}(k)}$, f_k is also balanced by Lemma 3. Then $(z^{2^{k-1}} - 1)$ divides both $F(z)$ and $F_k(z)$ by inductive assumption. According to Lemma 2, we have that $(z^{2^{k-1}} + 1)$ divides both $F(z)$ and $F_k(z)$. Since $\gcd(z^{2^{k-1}} - 1, z^{2^{k-1}} + 1) = 1$ where the abbreviation gcd stands for greatest common divisor, we obtain

$$(z^{2^k} - 1)|F(z).$$

By mathematical induction, $(z^{2^{\lambda-1}} - 1)|F(z)$ follows.

TABLE I
UNIMODULAR ROOTS OF POLYNOMIALS ASSOCIATED WITH BINARY GOLAY SEQUENCES OF LENGTH 8

Boolean Function	h_1, h_2, h_3	λ	Sequence	Balance	Unimodular roots
$x_1x_2 + x_2x_3$	$x_1 + x_3, x_2, x_1$	1	00010010	N	-1
$x_1x_2 + x_2x_3 + x_2$	$x_1 + x_3, x_2, x_1$	1	00100001	N	-1
$x_1x_2 + x_2x_3 + x_3$	$x_1 + x_3, x_2, x_1$	1	00011101	Y	1
$x_1x_2 + x_2x_3 + x_2 + x_3$	$x_1 + x_3, x_2, x_1$	1	00101110	Y	1
$x_2x_1 + x_1x_3$	$x_2 + x_3, x_1, x_2$	2	00010100	N	$\pm\sqrt{-1}$
$x_2x_1 + x_1x_3 + x_2$	$x_2 + x_3, x_1, x_2$	2	00100111	Y	± 1
$x_2x_1 + x_1x_3 + x_3$	$x_2 + x_3, x_1, x_2$	2	00011011	Y	± 1
$x_2x_1 + x_1x_3 + x_2 + x_3$	$x_2 + x_3, x_1, x_2$	2	00101000	N	$\pm\sqrt{-1}$
$x_1x_3 + x_3x_2$	$x_1 + x_2, x_3, x_1$	1	00000110	N	-1
$x_1x_3 + x_3x_2 + x_2$	$x_1 + x_2, x_3, x_1$	1	00110101	Y	1
$x_1x_3 + x_3x_2 + x_3$	$x_1 + x_2, x_3, x_1$	1	00001001	N	-1
$x_1x_3 + x_3x_2 + x_2 + x_3$	$x_1 + x_2, x_3, x_1$	1	00111010	Y	1

If f is unbalanced, consider a pair of Boolean functions and their associated polynomials

$$\begin{cases} f, \\ f_\lambda = f + x_\lambda, \end{cases} \text{and} \quad \begin{cases} F(z), \\ F_\lambda(z). \end{cases}$$

Since $x_\lambda = h_{2m-1}$, f_λ is balanced by Lemma 3. We have $(z^{2^{\lambda-1}} - 1)|F_\lambda(z)$ from the discussions above on balanced functions. $(z^{2^{\lambda-1}} + 1)|F(z)$ then follows from Lemma 2. □

Now we can prove one of the main results.

Theorem 3: The PMEPR of every standard binary Golay sequence of length 2^{2m-1} is exactly 2.

Proof: Let $a(x_1, \cdots, x_{2m-1})$ be a Boolean function with the form in (5), and define $b(x_1, \cdots, x_{2m-1}) = a(x_1, \cdots, x_{2m-1}) + x_{\pi(2m-1)}$. Then the sequences $(\mathbf{a}, \mathbf{b})$ described by these Boolean functions form a Golay complementary pair, and their associated polynomials satisfy $A(z)A(z^{-1}) + B(z)B(z^{-1}) = 2N$ where $N = 2^{2m-1}$. According to Theorem 2, there exists θ on the unit circle such that $B(\theta) = 0$, which yields

$$|A(\theta)|^2 = 2N.$$

Then the assertion follows immediately. □

Remark 2: If f is balanced, the unimodular roots of $F(z)$, as determined in Theorem 2, are located at $z = e^{2\pi t\sqrt{-1}}$ where $t \in \{\frac{v}{2^{\lambda-1}} | 0 \leqslant v < 2^{\lambda-1}, v \in \mathbb{N}\}$. If f is unbalanced, the unimodular roots of $F(z)$, as determined in Theorem 2, are located at $z = e^{2\pi t\sqrt{-1}}$ where $t \in \{\frac{v}{2^\lambda} | 0 \leqslant v < 2^\lambda, v \in \mathbb{N}, v \text{ odd}\}$. Moreover, for a root of the unity ω, $F(\omega) = 0$ if and only if ω satisfies the condition in Theorem 2, which will be shown in a separate paper, since it is outside the scope of this paper.

Example 1: An example of Theorem 2 for $m = 2$, $2^{2m-1} = 8$, is given in Table 1. We do not consider the term $+x_1$, because this term only changes the signs of the roots.

V. PMEPR OF STANDARD BINARY GOLAY SEQUENCES OF LENGTH 2^{2m}

In this section, we set $n = 2m$, and discuss the PMEPR of standard binary Golay sequences of length 2^{2m}. Boolean functions with the form in (5) describing all standard binary Golay sequences of length 2^{2m} can be re-expressed as

$$\begin{aligned} f(x_1, x_2, \cdots, x_{2m}) = &\sum_{i=1}^{m-1} x_{\pi(2i+1)}(x_{\pi(2i)} + x_{\pi(2i+2)}) \\ &+ x_{\pi(1)}x_{\pi(2)} + \sum_{i=1}^{2m} c_i x_i + c_0, \end{aligned} \tag{12}$$

where π is a permutation of symbols $\{1, 2, \cdots, 2m\}$, and $c_i \in \{0, 1\}$ for $0 \leqslant i \leqslant 2m$.

$f(x_1, \cdots, x_{2m})$ is a bent function, so is unbalanced, and 1 can not be a root of the polynomial $F(z)$ associated with sequence $\mathbf{f}$. Furthermore, we have the following results.

Theorem 4: Let $f(x_1, x_2 \cdots, x_{2m})$ be a Boolean function of the form in (5), and $F(z)$ the polynomial associated with sequence $\mathbf{f}$. Then $F(z) \neq 0$ for all $z = e^{2\pi t\sqrt{-1}}$ where $t \in \{\frac{v}{2^u} | 0 \leqslant v < 2^u, v, u \in \mathbb{N}\}$.

Proof: Note that the polynomial $z^{2^{k-1}} + 1$ is the 2^kth cyclotomic polynomial, so it is irreducible over the rational field for every positive integer k. Then the condition $(z^{2^{k-1}} + 1) \nmid F(z)$ is equivalent to $\gcd(z^{2^{k-1}} + 1, F(z)) = 1$, where $\gcd(G(z), F(z))$ denotes the greatest common divisor of polynomials $G(z)$ and $F(z)$.

First, since $f(x_1, x_2, \cdots, x_{2m})$ is a bent function, we have $\gcd(z - 1, F(z)) = 1$.

Then we show that $\gcd(z^{2^{k-1}} + 1, F(z)) = 1$ for $1 \leqslant k \leqslant 2m$. Consider a pair of Boolean functions and their associated polynomials

$$\begin{cases} f, \\ f_k = f + x_k, \end{cases} \text{and} \quad \begin{cases} F(z), \\ F_k(z). \end{cases}$$

For $1 \leqslant k \leqslant 2m$, since $\gcd(z - 1, F_k(z)) = 1$, we have $(z^{2^{k-1}} - 1) \nmid F_k(z)$. According to Lemma 2, we obtain $\gcd(z^{2^{k-1}} + 1, F(z)) = 1$ immediately.

Finally, for $k \geqslant 2m$, $\gcd((z^{2^k} + 1), F(z)) = 1$ follows from $\deg(z^{2^k} + 1) > \deg(F(z))$.

For $t = \frac{v}{2^u}$, v odd, $e^{2\pi t\sqrt{-1}}$ is a root of the irreducible polynomial $z^{2^{u-1}} + 1 = 0$. Therefore, $F(z) \neq 0$ for $z = e^{2\pi t\sqrt{-1}}$ where $t \in \{\frac{v}{2^u} | 0 \leqslant v < 2^u, v, u \in \mathbb{N}\}$. □

If one estimates, numerically, the PMEPR of sequences, which is a continuous problem, then the method of oversampling by *fast Fourier transform* (FFT) is usually employed. For the standard binary Golay sequences of length 2^{2m}, if we

estimate the exact PMEPR by FFT (2^u oversampling) on the point $z = e^{2\pi t\sqrt{-1}}$ where $t \in \{\frac{v}{2^u} | 0 \leqslant v < 2^u, v \in \mathbb{N}\}$, the numerical results will always show the PMEPR to be less than 2 according to Theorem 4.

Is the PMEPR of every standard binary Golay sequence of length 2^{2m} strictly less then 2? Based on the following theorem, we can prove, for $m = 2, 3$, that there are some polynomials associated with standard binary Golay sequences of length 2^{2m} that have unimodular roots.

We call a polynomial $F(z)$ of degree d *self-reciprocal* if $F(z) = z^d F(1/z)$. If d is odd then, obviously, -1 is a root of self-reciprocal polynomial $F(z)$. For d even, Konvalina and Matache [9] obtained a sufficient condition for a self-reciprocal polynomial to have at least one unimodular root.

Theorem 5: ([9]) Let $F(z) = a_d z^d + a_{d-1} z^{d-1} + \cdots + a_1 z + a_0 \in \mathbb{R}[z]$ be a self-reciprocal polynomial of degree d even. If there exists $k \in \{0, 1, 2, \cdots, d/2 - 1\}$ such that

$$|a_k| \geqslant |a_{d/2}| \cos\left(\frac{\pi}{[\frac{n/2}{n/2-k}] + 2}\right),$$

then $F(z)$ has at least one unimodular root.

Corollary 2: With the notations of Theorem 5, if $2|a_0| \geqslant |a_{d/2}|$, then $F(z)$ has at least one unimodular root.

Now we look at the case $n = 4$. We find that the polynomial associated with the Golay sequence described by the Boolean function $x_1x_4 + x_4x_2 + x_2x_3 + x_2 + x_4$ is $-(z^5 - z^4 - z - 1)(z^{10} - z^8 + 2z^5 - z^2 + 1)$, and the polynomial associated with the Golay sequence described by the Boolean function $x_1x_4 + x_4x_2 + x_2x_3 + x_2 + x_3 + x_4$ is $(z^5 - z^4 + z + 1)(z^{10} - z^8 - 2z^5 - z^2 + 1)$. Note that both $z^{10} - z^8 + 2z^5 - z^2 + 1$ and $z^{10} - z^8 - 2z^5 - z^2 + 1$ are self-reciprocal polynomials and satisfy the condition in Corollary 2, so there are eight polynomials associated with Boolean functions $x_1x_4 + x_4x_2 + x_2x_3 + x_2 + x_4 + \{0, x_1, x_3, x_1 + x_3\}$, and their negations (adding '+1'), that have unimodular roots, and therefore have PMEPR= 2.

For the case $n = 6$, we find that the polynomials associated with the Golay sequences described by the Boolean functions $x_1x_5 + x_5x_3 + x_3x_6 + x_6x_2 + x_2x_4 + x_2 + x_3 + x_5 + x_6$ and $x_1x_5 + x_5x_3 + x_3x_6 + x_6x_2 + x_2x_4 + x_2 + x_3 + x_4 + x_5 + x_6$ have factors $z^{18} - z^{16} + 2z^9 - z^2 + 1$ and $z^{18} - z^{16} - 2z^9 - z^2 + 1$, respectively, and thereby satisfy the condition in Corollary 2, so there are eight polynomials associated with Boolean functions $x_1x_5 + x_5x_3 + x_3x_6 + x_6x_2 + x_2x_4 + x_2 + x_3 + x_5 + x_6 + \{0, x_1, x_4, x_1 + x_4\}$, and their negations, that have unimodular roots, and therefore have PMEPR= 2.

Our computer search did not find any other standard Golay sequences of length 16 and 64 whose associated polynomials had one or more factors satisfying Corollary 2. Moreover our computer search results suggest strongly that the roots of the other standard binary Golay sequences of length 16 and 64 are not unimodular.

For the case $n = 8$, our computer search results did not find a standard binary Golay sequence whose associated polynomial has a factor satisfying the condition in Corollary 2. However, to within the precision of our computations, we could not be certain that all polynomials associated with standard binary Golay sequences of length 2^8 have no unimodular root. For example, we could not determine whether or not the polynomial associated with $x_7x_3 + x_3x_2 + x_2x_1 + x_1x_5 + x_5x_6 + x_6x_4 + x_4x_8 + x_2 + x_6$ has a unimodular root.

VI. Discussions and Conclusions

A. Rudin-Shapiro Polynomials

In the construction of Theorem 1, set π to be the identity permutation, and $c_i = 0$ for $0 \leqslant i \leqslant n$. Then we obtain Boolean functions

$$\begin{aligned} p(x_1, \cdots, x_n) &= \sum_{i=1}^{n-1} x_i x_{i+1}, \\ q(x_1, \cdots, x_n) &= \sum_{i=1}^{n-1} x_i x_{i+1} + x_n. \end{aligned}$$

The Golay sequences described by these Boolean functions are called Rudin-Shapiro sequences which were introduced by Shapiro [22] and Rudin [14] independently in their study of the magnitude of certain trigonometric sums. The polynomials corresponding to Rudin-Shapiro sequences are called Rudin-Shapiro polynomials which can be obtained recursively by the formulas

$$\begin{aligned} P_{n+1}(z) &= P_n(z) + z^{2^n} Q_n(z), \\ Q_{n+1}(z) &= P_n(z) - z^{2^n} Q_n(z), \end{aligned}$$

where $n \geqslant 0$ and $P_0(z) = Q_0(z) = 1$.

For $n = 2m - 1$, p is an unbalanced Boolean function and q is a balanced Boolean function according to Lemma 3. Thus we have

$$(z+1) | P_{2m-1}(z) \quad \text{and} \quad (z-1) | Q_{2m-1}(z),$$

which imply

$$P_{2m-1}(1) = 2^m \quad \text{and} \quad P_{2m-1}(-1) = 0.$$

The above discussions on the points $z = \pm 1$ of Rudin-Shapiro polynomials provide an alternative proof of Theorem 5 in [1] for $n = 2m - 1$.

Moreover, the roots and cyclotomic properties of the Rudin-Shapiro polynomials were studied in [2] and [3]. In particular, Theorem 4.2 in [3] showed that no root of unity except ± 1 can ever be the root of a Rudin-Shapiro polynomial.

B. Littlewood Polynomials

Polynomial $f(z) = \sum_{i=0}^{N-1} a_i z^i$ is called a *Littlewood polynomial* if all the coefficients $a_i \in \{1, -1\}$. Littlewood conjectured in [11] that there are infinitely many Littlewood polynomials $f_N(z)$, of increasing degree $N - 1$, satisfying

$$C_1\sqrt{N} \leqslant |f_N(z)| \leqslant C_2\sqrt{N},$$

where positive constants C_1 and C_2 are independent of N and $|z| = 1$. The polynomials associated with Golay sequences (including Rudin-Shapiro polynomials) provide a large set of Littlewood polynomials satisfying the upper bound with $C_2 =$

$\sqrt{2}$. However, there are no known Littlewood polynomials that satisfy the lower bound.

We have been motivated to study the unimodular roots of polynomials, not only for PMEPR control, but also because of Littlewood's conjecture. We are interested in whether the polynomials $f_{2^n}(z)$ associated with Golay sequences satisfy

$$\lim_{n\to\infty} \min_{|z|=1} \frac{|f_{2^n}(z)|}{2^n} = 0.$$

Otherwise, there exist infinitely many Golay sequences such that their associated polynomials $f_{2^{n'}}(z)$ satisfy

$$\lim_{n'\to\infty} \min_{|z|=1} \frac{|f_{2^{n'}}(z)|}{2^{n'}} = \epsilon > 0,$$

which would confirm Littlewood's conjecture. From the discussions above, we are particularly interested in the polynomials associated with Golay sequences without unimodular roots, or alternatively, Golay sequences of length 2^{2m} with PMEPR strictly less than 2.

C. Concluding Remarks

This paper has answered three open questions proposed in [5] on the PMEPR of standard binary Golay sequences of length 2^n. It has shown that all such sequences have PMEPR exactly 2 when n is odd, where there always exist peak positions at time(s) $t \in \{\frac{v}{2^u} | 0 \leqslant v < 2^u, v, u \in \mathbb{N}\}$. Conversely, for n even, we have shown that the envelope power of standard binary Golay sequences can never reach 2^{n+1} at such time points.

However, we also show that 8 standard binary Golay sequences of length 2^4 and of length 2^6 have PMEPR exactly 2. We made use here of some previous results in [9] on sufficient conditions for self-reciprocal polynomials to have unimodular roots. Such polynomials occur as factors of the polynomials associated with the above 8 sequences of length 2^4 and of length 2^6. Our computer search results suggest strongly that all other binary Golay sequences of lengths 2^4 and 2^6 have PMEPR strictly less than 2. No self-reciprocal factors were found for any of the polynomials associated with the standard binary Golay sequences of length 2^8, and it is unclear to us whether any of these sequences has PMEPR exactly 2.

Thus the major open problem is to ascertain whether, for n even, $n \geqslant 8$, $\epsilon > 0$, there exist infinitely many standard binary Golay sequences having PMEPR strictly less than $2 - \epsilon$.

ACKNOWLEDGMENT

The authors would like to thank the Associate Editor and anonymous reviewers for their helpful and valuable comments and suggestions.

REFERENCES

[1] J. Brillhart and L. Carlitz, "Note on the Shapiro polynomials,"*Proc. Amer. Math. Soc.*, vol. 25, pp. 114–118, 1970.

[2] J. Brillhart, "On the Shapiro polynomials,"*Duke Mathematical Journal*, vol. 40, no. 2, pp. 114–118, 1973.

[3] J. Brillhart, J. S. Lomont and P. Morton, "Cyclotomic properties of the Rudin-Shapiro polynomials, "*J. Reine Angew. Math.*, vol. 1976, issue 288, pp. 37–65, 1976.

[4] S. Z. Budišin, "New complementary pairs of sequences, "*Electron. Lett.*, vol. 26, pp. 881–883, 1990.

[5] M. W. Cammarano and M. L. Walker, "Integer Maxima in Power Envelopes of Golay Codewords,"1999 [Online]. Available: http://www.mathcs.richmond.edu/~jad/summerwork/final.pdf.

[6] J. A. 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, 1999.

[7] M. J. E. Golay, "Static multislit spectrometry and its application to the panoramic display of infrared spectra,"*J. Optical Soc. America*, vol. 41, pp. 468–472, 1951.

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

[9] J. Konvalina and V. Matache, "Palindrome-polynomials with roots on the unit circle,"*C. R. Math. Acad. Sci. Soc. R. Can.* vol. 26, no. 2, pp. 39–44, 2004.

[10] S. Litsyn, *Peak Power Control in Multi-carrier Communications*, Cambridge University Press, 2007.

[11] J. E. Littlewood, On polynomials $\sum \pm Z^m$, $\sum exp(a_m)z^m$, $z = e^\theta$, *London Math. Soc.*, vol. 41, pp. 367-376, 1966.

[12] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, Amsterdam, The Netherlands: North Holland Mathematical Library, 1977.

[13] K. Manji and B. S. Rajan, "On the PAPR of binary Reed-Muller OFDM codes,"*in Proc. IEEE ISIT*, Chicago, IL, Jun./Jul., pp. 423, 2004.

[14] W. Rudin, "Some theorems on Fourier coefficients,"*Proc. Amer. Math. Soc.* vol. 10, pp. 855–859, 1959.

[15] M. G. Parker, C. Tellambura, "Generalised Rudin-Shapiro Constructions, "in *WCC 2001, Workshop on Coding and Cryptography,* Paris, France, Jan., published in *Electronic Notes in Discrete Mathematics*, vol. 6, pp. 364–374, 2001.

[16] M. G. Parker, K. G. Paterson and C. Tellambura, *Golay Complementary Sequences*, Wiley Encyclopedia of Telecommunications, Editor: J. G. Proakis, Wiley Interscience, 2002.

[17] K. G. Paterson, "Generalized Reed-Muller codes and power control in OFDM modulation,"*IEEE Trans. Inf. Theory*, vol. 46, no. 1, pp. 104–120, 2000.

[18] K. G. Paterson, "Sequences for OFDM and multi-code CDMA: Two problems in algebraic coding theory,"in *Proc. SETA 2001*, ser. Discrete Mathematics and Theoretical Computer Science, Berlin, Germany: Springer-Verlag, pp. 46–71, 2002.

[19] B. M. Popović, "Synthesis of power efficient multitone signals with flat amplitude spectrum,"*IEEE Trans. Commun.*, vol. 39, no. 7, pp. 1031–1033, 1991.

[20] O. S. Rothaus, "On "bent" functions,"*J. Comb. Theory, Series A*, vol. 20, 3, pp. 300–305, May 1976.

[21] K.-U. Schmidt, "On cosets of the generalized first-order Reed-Muller code with low PMEPR,"*IEEE Trans. Inf. Theory*, vol. 52, no. 7, pp. 3220–3232, 2006.

[22] H. S. Shapiro, "Extremal problems for polynomials and power series,"Master's thesis, M.I.T., Cambridge, Mass., 1951.

[23] T. E. Stinchcombe, "Aperiodic autocorrelations of length 2^m sequences, complementarity, and power control for OFDM,"Ph.D. dissertation, Univ. London, U.K., 2000.

Zilong Wang (M'11) received the B.S. degree from Nankai University, China, in 2005, and the Ph.D. degree from Peking University, China, in 2010, both in Mathematics. During 2008-2009, he was a visiting Ph.D. student in the Dept. of Electrical and Computer Engineering, University of Waterloo, Canada.

He received a Postdoctoral Fellowship from University of Waterloo in 2012. Since 2010, Dr. Wang has been an associate professor in the State Key Laboratory of Integrated Service Networks, Xidian University, Xi'an, China. His research interests are in the areas of sequence design, coding theory, applied mathematics and information security.

Matthew G. Parker has been a professor at the Institute for Informatics, University of Bergen, Norway, since 2008, and prior to that a researcher at the same institute since 1998. Before coming to Bergen, he was a researcher with the telecommunications research group at the University of Bradford, UK. He received his PhD from the University of Huddersfield, UK, in 1995. He is research active in the areas of quantum information theory, sequence design, Boolean functions, message-passing algorithms, coding theory, information theory, communications systems, and graph theory.

Guang Gong (M'00-SM'07-F'13) received a B.S. degree in Mathematics in 1981, an M.S. degree in Applied Mathematics in 1985, and a Ph.D. degree in Electrical Engineering in 1990, from Universities in China.

She received a Postdoctoral Fellowship from the Fondazione Ugo Bordoni, in Rome, Italy, and spent the following year there. After returning from Italy, she was promoted to an Associate Professor at the University of Electrical Science and Technology of China. During 1995-1998, Dr. Gong worked with several internationally recognized, outstanding coding experts and cryptographers, including Dr. Solomon W. Golomb, at the University of Southern California. Dr. Gong joined the University of Waterloo, Canada in 1998, as an Associate Professor in the Dept. of Electrical and Computer Engineering in September 2000. She has been a full Professor since 2004. Dr. Gong's research interests are in the areas of sequence design, cryptography, and communication security. She has authored or co-authored more than 200 technical papers and two books, one co-authored with Dr. Golomb, entitled as *Signal Design for Good Correlation for Wireless Communication, Cryptography and Radar*, published by Cambridge Press in 2005, and the other coauthored with Dr. Lidong Chen, *Communication System Security*, published by CRC 2012.

Dr. Gong serves/served as Associate Editors for several journals including Associate Editor for Sequences for *IEEE Transactions on Information Theory*, and served on a number of technical program committees and conferences as co-chairs or committee members. Dr. Gong has received several awards including the Best Paper Award from the Chinese Institute of Electronics in 1984, Outstanding Doctorate Faculty Award of Sichuan Province, China, in 1991, the Premier's Research Excellence Award, Ontario, Canada, in 2001, NSERC Discovery Accelerator Supplement Award, 2009, Canada, and Ontario Research Fund-Research Excellence Award, 2010, Canada, Best Paper Award of IEEE ICC 2012.

Gaofei Wu received his B.S. degree in mathematics from Xidian University, Xi'an, China, in 2009, where he is currently pursuing the Ph.D. degree in information security. He is a visiting PhD student (Sep. 2012- Aug. 2014) in the Department of Informatics, University of Bergen. His research interests include cryptography and sequence design.