Journal of Combinatorics and Number Theory
Volume 1, Issue 1, pp. 1-??
ISSN 1942-5600

A BOOLEAN FUNCTIONS VIEW ON THE GOLAY-RUDIN-SHAPIRO SEQUENCE

Pantelimon Stănică*

Department of Applied Mathematics
Naval Postgraduate School, Monterey, CA 93943–5216, USA

Received: December 5, 2019; Accepted: December 31, 2019

Abstract

In this paper we give a Boolean functions approach to the classical Golay-Rudin-Shapiro sequence r_n, which is defined by counting the number of occurrences of the pattern '11' in the binary expansion of n. In the same spirit, we investigate Golay-Rudin-Shapiro-like sequences defined by counting occurrences of '00', '01', '10' in the binary expansion of n. We regard a truncation of such sequences as part of the truth table of a Boolean function. For each such function, we find the algebraic normal form and its weight, consequently, showing that some of them are, in fact, perfect nonlinear, that is, bent (and in odd dimension, semibent) Boolean functions, that is, they have flat (or almost flat) Walsh-Hadamard spectrum. With this new approach proofs of some known results are vastly simplified. As a consequence of our method, we find partial sums (for upper bounds of weight ≤ 3) of the classical Golay-Rudin-Shapiro sequence. Further, we show that using these new sequences we can generate Golay complementary pairs, which was the motivation for the original Golay-Rudin-Shapiro sequence definition from 1950.

Keywords: Golay-Rudin-Shapiro sequence, binary expansions, Boolean functions, bent and semibent Boolean functions, weight.
MSC 2010: 11B83, 11K31, 94A55

1. Short primer on Golay-Rudin-Shapiro sequence

For a sequence $\{a_n\}_n$, where $a_n \in \{\pm 1\}$, one could inquire about the values of the Fourier transforms $f_n = \sum_{k=0}^{n-1} a_k e^{2\pi \imath kx}$, in particular about the supremum of its absolute value, that is,

$$s_n(a) := \sup_{x\in[0,1]} \left| \sum_{k=0}^{n-1} a_k e^{2\pi \imath kx} \right|.$$

*E-mail address: pstanica@nps.edu; Website: http://faculty.nps.edu/pstanica/

Certainly, Parseval's identity will quickly give us a lower bound of $\sqrt{n}$ and, trivially, we have an upper bound of n. However, it turns out that [1, Chapter 3], for almost all (in the sense of the Haar measure on $\{-1,+1\}^{\mathbb{N}}$) sequences of ± 1, the bound

$$\sup_{x\in[0,1]}\left|\sum_{k=0}^{n-1} a_k e^{2\pi\imath kx}\right| = O(\sqrt{n\log n})$$

holds, where the Landau symbol O has its usual meaning. Specifically, $f = O(g)$ means $|f(x)| < c|g(x)|$ holds with some constant c, for x sufficiently large. Are there sequences for which the bound can be improved significantly? We we shall see below that there are such sequences, and this was shown by Shapiro [23] and Rudin [20].

We define the *Golay-Rudin-Shapiro sequence* to be $r_n = (-1)^{e_{2;11}(n)}$, where $e_{2;11}(n)$ counts the number of occurrences of the block '11' in the base-2 expansion of n, that is, for $n = \sum_{i=0}^{\ell} e_i 2^i$, $e_i \in \{0,1\}$, then

$$r_n = (-1)^{\sum_{i=0}^{\ell} e_i e_{i+1}}.$$

We give in Table 1 the first few values.

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
r_n	1	1	1	-1	1	1	-1	1	1	1	1	-1	-1	-1	1

Table 1. The Golay-Rudin-Shapiro sequence, $0 \le n \le 14$

Shapiro [23] and Rudin [20] used the sequence r_n, which we will call Golay-Rudin-Shapiro since it also appears in a somewhat disguised form in the works of Golay [14, 15], as well, to show that

$$\sup_{x\in[0,1]}\left|\sum_{k=0}^{n-1} r_k e^{2\pi\imath kx}\right| \le (2+\sqrt{2})\sqrt{n}$$

(the best constant $\sqrt{6}$ was announced by Balister [2]).

The sequence has been investigated a lot throughout the years (see, for example, [1, 6, 8, 9] and the references therein) and much is known about it. For example, the sequence can be defined recursively by

$$\begin{aligned} r_0 &= 1, \\ r_{2n} &= r_n, \\ r_{2n+1} &= (-1)^n r_n, \end{aligned} \tag{1.1}$$

and its sum has the property [1, 8] that

$$p_n = \sum_{k=0}^{n-1} r_k = \sqrt{n}\, G_1\left(\log_4 n\right),$$

for a continuous nowhere differentiable function G_1 of period 1. Also, in the sequence $(p_n)_{n\ge 0}$ it is known [9] that 0 occurs 0 times, 1 occurs once, 2 occurs twice, and in general

n occurs n times. Using (1.1), one can show that the generating function $F(z) = \sum_{n=0}^{\infty} r_n z^n$ satisfies the functional equation $F(z) = F(z^2) + zF(-z^2)$.

We now give a brief overview of Golay complementary pairs (CP) (see, for example, [12, 13, 16] or the reader's preferred reference on CP). Let $\mathbf{a} = \{a_i\}_{i=0}^{N}$ be a sequence of ± 1 (bipolar) and let the *autocorrelation* of $\mathbf{a}$ at k be defined by $C_{\mathbf{a}}(k) = \sum_{i=0}^{N-k-1} a_i a_{i+k}$, $0 \leq k \leq N-1$. Two bipolar sequences $\mathbf{a}, \mathbf{b}$ form a *Golay complementary pair* if

$$C_{\mathbf{a}}(k) + C_{\mathbf{b}}(k) = 0, \text{ for } k \neq 0.$$

We associate a polynomial A with the sequence $\mathbf{a}$ by $A(x) = a_0 + a_1 x + \cdots + a_{N-1} x^{N-1}$. It is rather straightforward to show that two sequences $\mathbf{a}, \mathbf{b}$ (with corresponding polynomials A, B) form a Golay complementary pair if and only if

$$A(x)A(x^{-1}) + B(x)B(x^{-1}) = 2N. \tag{1.2}$$

Of course, not all lengths N are allowable: for example, if $N > 1$, then N must be even; also, N is not divisible by a prime $\equiv 3 \pmod 4$ (see [4]). There is a large body of literature on these sequences (see Schmidt's thesis [22] and the references therein) since they have applications in coding theory.

In this note we will point out that the Golay-Rudin-Shapiro sequence (and several like it) can be regarded as partial strings of Boolean functions. We will find their algebraic normal forms, and show that the classical Golay-Rudin-Shapiro sequence is made up by concatenating two quadratic (semi)bent functions. With this new approach proofs of some known results are vastly simplified. For example, we find several partial sums (of length weight ≤ 3) of the Golay-Rudin-Shapiro sequence, consequently extending some previously published results. We shall answer the same questions for other sequences constructed in the same manner. Furthermore, we also show that each of these sequences generate Golay complementary pairs (perhaps, as expected).

2. Short primer on Boolean functions

Let $\mathbb{F}_2$ be the finite field with two elements and $\mathbb{Z}$ be the ring of integers. For any $n \in \mathbb{Z}^+$, the set of positive integers, let $[n] = \{1, \ldots, n\}$. The Cartesian product of n copies of $\mathbb{F}_2$ is $\mathbb{F}_2^n = \{\mathbf{x} = (x_1, \ldots, x_n) : x_i \in \mathbb{F}_2, i \in [n]\}$ which is an n-dimensional vector space over $\mathbb{F}_2$, which we will denote by $\mathbb{V}_n$. We will denote by $\oplus$, respectively, $+$, the additions on $\mathbb{F}_2^n$, respectively, $\mathbb{Z}$. For any $n \in \mathbb{Z}^+$, a function $F : \mathbb{V}_n \to \mathbb{F}_2$ is said to be a *Boolean function* in n variables. The set of all Boolean functions will be denoted by $\mathcal{B}_n$. A Boolean function can be regarded as a multivariate polynomial over $\mathbb{F}_2$, called the *algebraic normal form* (ANF)

$$f(x_1, \ldots, x_n) = a_0 \oplus \sum_{1 \leq i \leq n} a_i x_i \oplus \sum_{1 \leq i < j \leq n} a_{ij} x_i x_j \oplus \cdots \oplus a_{12\ldots n} x_1 x_2 \ldots x_n,$$

where the coefficients $a_0, a_{ij}, \ldots, a_{12\ldots n} \in \mathbb{F}_2$. The maximum number of variables in a monomial is called the (*algebraic*) *degree*.

For a Boolean function $f \in \mathcal{B}_n$, we define its sign function $\hat{f}$ by $\hat{f}(\mathbf{x}) = (-1)^{f(\mathbf{x})}$. For $\mathbf{u} = (u_1, \ldots, u_n)$, $\mathbf{x} = (x_1, \ldots, x_n)$, we let $\mathbf{u} \cdot \mathbf{x} = \sum_{i=1}^{n} u_i x_i$ be the regular scalar (inner) product on $\mathbb{V}_n$. For a binary string ß, we let $\bar{ß}$ denote the binary complement of ß. The (Hamming) weight of a binary string ß, denoted by $\mathrm{wt}(ß)$ is the number of nonzero bits in ß.

We order $\mathbb{F}_2^n$ lexicographically, and denote $\mathbf{v}_0 = (0, \ldots, 0, 0)$, $\mathbf{v}_1 = (0, \ldots, 0, 1)$, $\mathbf{v}_{2^n-1} = (1, \ldots, 1, 1)$. The *truth table* of a Boolean function $f \in \mathcal{B}_n$ is the binary string of length 2^n, $[f(\mathbf{v}_0), f(\mathbf{v}_1), \ldots, f(\mathbf{v}_{2^n-1})]$ (we will often disregard the commas). We give an example of the 3-variable Boolean function $f(x_1, x_2, x_3) = x_1 \oplus x_2 x_3$ in Table 2.

x_1	x_2	x_3	f
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	1
1	0	1	1
1	1	0	1
1	1	1	0

Table 2. Truth table of a 3-variable Boolean function

We define the *Walsh-Hadamard transform* of f by

$$\mathcal{W}_f(\mathbf{u}) = \sum_{\mathbf{x} \in \mathbb{V}_n} (-1)^{f(\mathbf{x})} (-1)^{\mathbf{u} \cdot \mathbf{x}}.$$

A function f for which $|\mathcal{W}_f(\mathbf{u})| = 2^{n/2}$ for all $\mathbf{u} \in \mathbb{V}_n$ is called a *bent* function [19]. Further recall that $f \in \mathcal{B}_n$ is called *plateaued* if $|\mathcal{W}_f(\mathbf{u})| \in \{0, 2^{(n+s)/2}\}$ for all $\mathbf{u} \in \mathbb{V}_n$ for a fixed integer s depending on f (we also call f then *s-plateaued*). If $s = 1$ (n must then be odd), or $s = 2$ (n must then be even), we call f semibent. For more on Boolean functions, the reader can consult [10, 11] and the references therein.

3. Boolean functions approach on the Golay-Rudin-Shapiro sequence

One might wonder what is the connection between the Golay-Rudin-Shapiro sequence and Boolean functions. It is the purpose of this note to show that the Golay-Rudin-Shapiro sequence and several of its modifications are in reality the sign function of truncations of quadratic bent functions.

We shall be using below the simple observation that if b is a bit then $(-1)^b = 1 - 2b$, which is equivalent to $b = (1 - (-1)^b)/2$.

Theorem 3.1. *Let $N \geq 1$ be an arbitrary positive integer and let $n \geq 2$ be the positive integer such that $2^{n-1} < N \leq 2^n$. Let $b_i = (1 - r_i)/2$ (that is, r_i is the sign of the bit b_i) and $b(N) = (b_i)_{i=0}^{N-1}$. Then $b(N)$ are the first N bits of truth table (with $\mathbb{F}_2^n$ ordered lexicographically) of the Boolean function $f_n(x_1, \ldots, x_n) = x_1 x_2 \oplus x_2 x_3 \oplus \cdots \oplus x_{n-1} x_n$, which is bent, for even n, and semibent for odd n. Moreover, the weight of f_n is $2^{n-1} - 2^{\lfloor (n-1)/2 \rfloor}$. The companion sequence (defined below) has algebraic normal form*

$g_n(x_1, \ldots, x_n) = x_1 \oplus x_1x_2 \oplus x_2x_3 \oplus \cdots \oplus x_{n-1}x_n$ *is also bent, for even* n*, and semibent for odd* n*, and has weight* $\mathrm{wt}(g_{2k}) = 2^{2k-1} - 2^{k-1}$, $\mathrm{wt}(g_{2k+1}) = 2^{2k}$.

Proof. f_n be the Boolean function on n variables whose truth table are 2^n consecutive bits b_i, $0 \leq i \leq 2^n - 1$. Using equation (1.1), we immediately see that the function f_n along with a companion function g_n (defined below) satisfy the recurrences (using the customary notation '|' to denote concatenation of strings)

$$\begin{aligned} f_0 &= 0, & g_0 &= 0 \\ f_{n+1} &= f_n|g_n, & g_{n+1} &= f_n|\bar{g}_n. \end{aligned}$$

We let ß $:= s_0s_1 \ldots s_{2^{n-1}} = (-1)^{g_n}$. We will show by induction, concurrently, that the algebraic normal forms of f_n, g_n are $f_n(x_1, \ldots, x_n) = x_1x_2 \oplus x_2x_3 \oplus \cdots \oplus x_{n-1}x_n$, respectively, $g_n(x_1, \ldots, x_n) = x_1 \oplus x_1x_2 \oplus x_2x_3 \oplus \cdots \oplus x_{n-1}x_n$, as well as, we will show that the Hamming weights, $\mathrm{wt}(f_n) = 2^{n-1} - 2^{\lfloor (n-1)/2 \rfloor}$, $\mathrm{wt}(g_{2k}) = 2^{2k-1} - 2^{k-1}$, $\mathrm{wt}(g_{2k+1}) = 2^{2k}$ (thus, balanced). Certainly, one can easily check that our claim is true for $n = 2$.

Using the above obtained recurrences, we infer that

$$\begin{aligned} f_{n+1}(x_1, \ldots, x_{n+1}) &= (1 \oplus x_1)f_n(x_2, \ldots, x_{n+1}) \oplus x_1g_n(x_2, \ldots, x_{n+1}) \\ g_{n+1}(x_1, \ldots, x_{n+1}) &= (1 \oplus x_1)f_n(x_2, \ldots, x_{n+1}) \oplus x_1\bar{g}_n(x_2, \ldots, x_{n+1}), \end{aligned}$$

and using the induction step we get $f_{n+1}(x_1, \ldots, x_{n+1}) = (1 \oplus x_1)(x_2x_3 \oplus \cdots \oplus x_nx_{n+1}) \oplus x_1(x_2 \oplus x_2x_3 \oplus \cdots \oplus x_nx_{n+1}) = x_1x_2 \oplus x_2x_3 \oplus \cdots \oplus x_nx_{n+1}$, and $g_{n+1}(x_1, \ldots, x_{n+1}) = (1 \oplus x_1)(x_2x_3 \oplus \cdots \oplus x_nx_{n+1}) \oplus x_1(1 \oplus x_2 \oplus x_2x_3 \oplus \cdots \oplus x_nx_{n+1}) = x_1 \oplus x_1x_2 \oplus x_2x_3 \oplus \cdots \oplus x_nx_{n+1}$.

It is known (and rather easy to show) that both of these polynomials are bent functions for n even and semibent for n odd. From the recurrences $f_{n+1} = f_n|g_n$, $g_{n+1} = f_n|\bar{g}_n$ we also obtain the claim for the weights of both f_n, g_n. □

We call the ± 1-sequence determined by the g_n, the *companion Golay-Rudin-Shapiro* sequence, which we will denote by $t_n = (-1)^{g_n}$ (of length 2^n). We give in Table 3 the first few values (see [18] for more details on companion sequences for more such patterns).

t_0	1
t_1	$1, -1$
t_2	$1, 1, -1, 1$
t_3	$1, 1, 1, -1, -1, -1, 1, -1$
t_4	$1, 1, 1, -1, 1, 1, -1, 1, -1, -1, -1, 1, 1, 1, -1, 1$

Table 3. The companion Golay-Rudin-Shapiro sequence

The representation of the Golay-Rudin-Shapiro sequence from our previous theorem has as a consequence several results whose previously published proofs were much more involved. For example, the following theorem is an extension of a result of [3] (we let ß $:= s_0s_1 \ldots s_{2^n-1} = (-1)^{g_n}$ and $s(k) = s_0s_1 \ldots s_{k-1}$, $k \leq 2^n$). We note that alternative approaches for this next theorem can be found in [8], but our proof is rather simple and in line with our Boolean functions approach to warrant inclusion here.

Theorem 3.2. *We have* $p_{2^k} = \sum_{i=0}^{2^k-1} r_j = 2^{\lfloor (k+1)/2 \rfloor}$, *and* $q_{2^k} = \sum_{i=0}^{2^k-1} s_j = 0$, *if* k *is odd and* $q_{2^k} = p_{2^{k-1}} = 2^{k/2}$, *for* k *even. Furthermore, with these values,*

$$p_{2^k+2^{k-1}} = 2^{\lfloor (k+1)/2 \rfloor} + 2^{\lfloor k/2 \rfloor}, p_{2^k+2^{k-2}} = 2^{\lfloor (k+1)/2 \rfloor} + 2^{\lfloor (k-1)/2 \rfloor},$$
in general, $p_{2^k+2^{k-\ell}} = 2^{\lfloor (k+1)/2 \rfloor} + 2^{\lfloor (k-\ell+1)/2 \rfloor}, \ell \leq k$;
$$p_{2^k+2^{k-1}+2^{k-2}} = p_{2^k} + p_{2^{k-1}} - p_{2^{k-2}} = 2^{\lfloor (k+1)/2 \rfloor} + 2^{\lfloor k/2 \rfloor} - 2^{\lfloor (k-1)/2 \rfloor},$$
in general, $p_{2^k+2^{k-1}+2^{k-\ell}} = 2^{\lfloor (k+1)/2 \rfloor} + 2^{\lfloor k/2 \rfloor} - 2^{\lfloor (k-\ell+1)/2 \rfloor}$.

Further, for weight with 3 *indices*

$$p_{2^k+2^{k-j}+2^{k-\ell}} = 2^{\lfloor (k+1)/2 \rfloor} + 2^{\lfloor (k-j+1)/2 \rfloor} + 2^{\lfloor (k-\ell+1)/2 \rfloor}, 1 < j < \ell.$$

Proof. For easy writing, let $b_i = (1 - r_i)/2$ be the bit corresponding to r_i, and $b(n) = (b_i)_{i=0}^{n-1}$ be the binary string corresponding to $r(n) = (r_i)_{i=0}^{n-1}$. Thus, in the previous notation,

$$\begin{aligned} p_n &= \sum_{i=0}^{n-1} r_i \\ &= (\#1\text{'s in } r(n)) - (\#(-1)\text{'s in } r(n)) \\ &= (\#0\text{'s in } b(n)) - (\#1\text{'s in } b(n)) \\ &= n - 2\mathrm{wt}(b(n)). \end{aligned}$$

Since we showed in the previous theorem that the weight of the function in k variables, f_k, corresponding to the sequence $r(2^k)$ is exactly $2^{k-1} - 2^{\lfloor (k+1)/2 \rfloor}$, and using the above displayed identity, we obtain the first claim (similarly, for q_{2^k}).

For the next claim, we write (recall that $f_{k+1} = f_k g_k$, $g_{k+1} = f_k \bar{g}_k$)

$$f_{k+1} = f_k f_{k-1} \bar{g}_{k-1},$$

and so,

$$p_{2^k+2^{k-1}} = p_{2^k} + p_{2^{k-1}} = 2^{\lfloor (k+1)/2 \rfloor} + 2^{\lfloor k/2 \rfloor}.$$

In a similar fashion, we can show that $p_{2^k+2^{k-1}+2^{k-2}} = 2^{\lfloor k/2 \rfloor} + 2^{\lfloor (k-1)/2 \rfloor}$, or the more general, $p_{2^k+2^{k-\ell}} = 2^{\lfloor (k+1)/2 \rfloor} + 2^{\lfloor (k-\ell+1)/2 \rfloor}$, $\ell \leq k$.

The next identity (for weight 3 indexed sums, that is, $p_{2^k+2^{k-1}+2^{k-\ell}}$) will follow from the recurrences

$$\begin{aligned} f_{k+1} &= f_k g_k = f_k f_{k-1} \bar{g}_{k-1} = f_k f_{k-1} \bar{f}_{k-2} g_{k-2}, \text{ and} \\ f_{k+1} &= f_k f_{k-1} \bar{g}_{k-1} = f_k f_{k-2} g_{k-2} \bar{g}_{k-1}. \end{aligned}$$

Finally, the last claimed sum is actually easier than the previous ones, since, if $j > 1$, then the terms from the sum $p_{2^k+2^{k-j}+2^{k-\ell}}$ all will occur within $f_k f_{k-j+1}$ only, and so, $p_{2^k+2^{k-j}+2^{k-\ell}} = p_{2^k} + p_{2^{k-j}+2^{k-\ell}}$, which will imply our claim. □

4. Several Golay-Rudin-Shapiro-like sequences

Certainly, one would wonder if similar results would hold for a counting function for other patterns in the binary expansion of n. In [5, p. 46] pattern sequences for binary patterns other than '11' are studied, and the limit functions for '10', '01', '00' are discussed; moreover, a limit function is derived for all but '10' binary patterns, where the limit functions do not exist in the ordinary sense (see [5, Tables 4 and 5 on pp. 48–50]). In [17], the Rudin-Shapiro-like sequence $i_n = (-1)^{inv_2(n)}$, where $inv_2(n)$ is the number of inversions, that is, the number of occurrences of '10' as a scattered subsequence in the binary expansion of n, was investigated and it was shown that several results similar to the case of the classical Golay-Rudin-Shapiro sequence hold. In particular, $S(n) = \sum_{k=0}^{n} i_k = G(\log_4 n)\sqrt{n}$, for a bounded, continuous, nowhere differentiable, periodic (of period 1) function G. Also, the inequalities $\sqrt{3}/3 \le S(n)/\sqrt{n} \le \sqrt{2}$ hold.

In the spirit of the classical Golay-Rudin-Shapiro sequence, we modify the above definition and let $i_n = (-1)^{e_{2;10}(n)}$, where $n = \sum_{i=0}^{\ell} e_i 2^i$, $e_i \in \{0,1\}$, $e_{2;10}(n) = \sum_{i=0}^{n-1} e_i(e_{i+1} \oplus 1)$. Let $b_k = (1 - i_k)/2$ regarded in $\mathbb{F}_2$ and $b(N) = \{b_k\}_{k=0}^{N}$. This new sequence $\{i_k\}_k$ satisfies the recurrence

$$\begin{aligned} i_{4n} = i_n, i_{4n+1} = -i_{2n}, i_{8n+2} = -i_n, \\ i_{8n+3} = -i_{2n}, i_{8n+6} = a_{2n+1}, i_{8n+7} = a_{2n+1}. \end{aligned} \tag{4.3}$$

Theorem 4.3. *Let $2^{n-1} < N \le 2^n - 1$. The sequence $\{i_k\}_{k=0}^{N}$ is the initial N-bit string of the sign sequence of a Boolean function f_n whose algebraic normal form is $f_n(\mathbf{x}) = \sum_{j-i\ge 2} x_i x_j \oplus \sum_{k=3}^{n} s_k(\mathbf{x})$, where $s_k(\mathbf{x})$ are the elementary symmetric polynomials of degree k. The weight of f_n is $\mathrm{wt}(f_n) = 2^{n-1} - 2^{\lfloor n/2 \rfloor} - 2^{\lfloor (n-1)/2 \rfloor} + 1$, $n \ge 1$. The companion sequence (defined below) has algebraic normal form $g_n(\mathbf{x}) = \sum_{i=2}^{n} x_i \oplus \sum_{i=1}^{n-1} x_i x_{i+1}$, which is bent for n even and semibent for n odd, and its weight is $\mathrm{wt}(g_n) = 2^{n-1} - 2^{\lfloor (n-1)/2 \rfloor}$, $n \ge 1$.*

Furthermore, the first and second halves of the sign sequence of g_n gives rise to a Golay complementary pair.

Proof. From Equations (4.3) (we could avoid using these recurrences, surely, and show the below constructions of f_n, g_n by induction), we see that the sequence $b(N)$, along with a companion sequence $c(N)$ of the same length (where $2^{n-1} < N \le 2^n$) are initial "chunks" of the functions f_n, respectively, g_n (observe below that $c(2^n - 1)$ is the second half of the sequence $b(2^{n+1} - 1)$), which can be constructed by the following recurrence (we use the notation, $g_n = u_n v_n$, for the first and second halves, which are functions in $n-1$ variables)

$$\begin{aligned} f_0 &= 0, & g_0 &= 0, \\ f_1 &= 00, & g_1 &= 00, \\ f_{n+1} &= f_n g_n, & g_{n+1} &= u_n \bar{v}_n u_n v_n. \end{aligned}$$

We first show that, if $n \geq 3$, the algebraic normal form (ANF) of $g_n \in \mathcal{B}_n$ is $g_n(\mathbf{x}) = \sum_{i=2}^{n} x_i \oplus \sum_{i=1}^{n-1} x_i x_{i+1}$ (which is known to be bent for n even and semibent for n odd). This will help us in showing (also by induction) that the ANF of f_n is $f_n(\mathbf{x}) = \sum_{j-i\geq 2} x_i x_j \oplus \sum_{k=3}^{n} s_k(\mathbf{x})$, where $s_k(\mathbf{x})$ are the elementary symmetric polynomials of degree k.

We show both of these claims by induction. Certainly, for $n = 3$, $f_3(x_1, x_2, x_3) = x_1x_3 \oplus x_1x_2x_3$, and $g_3(x_1, x_2, x_3) = x_2 \oplus x_3 \oplus x_1x_2 \oplus x_2x_3$, which fits our claim. We assume the claim for n and we show it for $n + 1$. If $g_n = u_n v_n$, then

$$\begin{aligned} g_n(\mathbf{x}) &= \bar{x}_1 u_n(x_2, \ldots, x_n) \oplus x_1 v_n(x_2, \ldots, x_n) \\ &= x_1(u_n(x_2, \ldots, x_n) \oplus v_n(x_2, \ldots, x_n)) \oplus u_n(x_2, \ldots, x_n) \\ &= \sum_{i=2}^{n} x_i \oplus \sum_{i=1}^{n-1} x_i x_{i+1} \\ &= x_1x_2 \oplus \sum_{i=2}^{n} x_i \oplus \sum_{i=2}^{n-1} x_i x_{i+1}, \end{aligned}$$

which implies that $u_n(x_2, \ldots, x_n) = \sum_{i=2}^{n} x_i \oplus \sum_{i=2}^{n-1} x_i x_{i+1}$ and $v_n(x_2, \ldots, x_n) = u_n(x_2, \ldots, x_n) \oplus x_2 = \sum_{i=3}^{n} x_i \oplus \sum_{i=2}^{n-1} x_i x_{i+1}$. Since $g_{n+1} = u_n \bar{v}_n u_n v_n$, then

$$\begin{aligned} g_{n+1}(\mathbf{x}) &= \bar{x}_1\bar{x}_2 u_n(x_3, \ldots, x_{n+1}) \oplus \bar{x}_1 x_2 \bar{v}_n(x_3, \ldots, x_{n+1}) \\ &\oplus x_1\bar{x}_2 u_n(x_3, \ldots, x_{n+1}) \oplus x_1x_2 v_n(x_3, \ldots, x_{n+1}) \\ &= (1 \oplus x_1 \oplus x_2 \oplus x_1x_2) u_n(x_3, \ldots, x_{n+1}) \\ &\oplus (x_2 \oplus x_1x_2)(u_n(x_3, \ldots, x_{n+1}) \oplus x_3 \oplus 1) \\ &\oplus (x_1 \oplus x_1x_2) u_n(x_3, \ldots, x_{n+1}) \\ &\oplus x_1x_2(u_n(x_3, \ldots, x_{n+1}) \oplus x_3) \\ &= x_2 \oplus x_1x_2 \oplus x_2x_3 \oplus u_n(x_3, \ldots, x_{n+1}) \\ &= \sum_{i=2}^{n+1} x_i \oplus \sum_{i=1}^{n} x_i x_{i+1}. \end{aligned}$$

Now, since $f_{n+1} = f_n g_n$, then, using the induction hypothesis and the expression for g_n, we get

$$\begin{aligned} f_{n+1}(\mathbf{x}) &= \bar{x}_1 f_n(x_2, \ldots, x_{n+1}) \oplus x_1 g_n(x_2, \ldots, x_{n+1}) \\ &= \bar{x}_1 \left(\sum_{i\geq 2, j-i\geq 2} x_i x_j \oplus \sum_{k=3}^{n} s_k(x_2, \ldots, x_{n+1}) \right) \end{aligned}$$

$$\oplus\, x_1 \left(\sum_{i=3}^{n} x_i \oplus \sum_{i=2}^{n} x_i x_{i+1} \right),$$

which by expansion and simplification, renders the claim on the ANF of f_{n+1}.

The fact that g_n is (semi)bent is rather easy to show, observing that one can associate every two terms (except for the last one, if n is odd) and we write $g_n(\mathbf{x}) = x_2(x_1 \oplus x_3) + x_4(x_3 \oplus x_5) \oplus \cdots$, which is obviously affinely equivalent to a Maiorana-McFarland [19] bent Boolean function (the result about the (semi)bentness of g_n should be known, but we could not find a suitable reference, so the previous argument applies). We now show the claim about weights of f_n. A simple computation shows the result about the weight of f_n for $n = 1$. We now assume our claim to be true for n and show it for $n + 1$. Since $f_{n+1} = f_n g_n$, we have the recurrence

$$\mathrm{wt}(f_{n+1}) = \mathrm{wt}(f_n) + \mathrm{wt}(g_n),$$

and by using the induction hypothesis, we get the claim.

We now show the claim about the Golay complementary pair. Let $A_n(x)$, $B_n(x)$ be the polynomials corresponding to the first, respectively, the second half of $(-1)^{g_{n+1}}$. We need to show that

$$A_n(x)A_n(x^{-1}) + B_n(x)B_n(x^{-1}) = 2 \cdot 2^n = 2^{n+1}.$$

We shall use induction on n. Certainly, $A_0(x) = 1, B_0(x) = 1$, and the above identity is satisfied. We take one more example, that is, $A_1(x) = 1 - x, B_1(x) = 1 + x$, and so,

$$\begin{aligned} A_1(x)A_1(x^{-1}) + B_1(x)B_1(x^{-1}) &= (1-x)(1-x^{-1}) + (1+x)(1+x^{-1}) \\ &= 1 - x - x^{-1} + 1 + 1 + x + x^{-1} + 1 = 2^2. \end{aligned}$$

Assume the claim is true for n and show it for $n + 1$. From the recurrence satisfied by g_n we see that (these identities can be obtained from [7], as well)

$$\begin{aligned} A_{n+1}(x) &= A_n(x) - x^{2^n} B_n(x), \\ B_{n+1}(x) &= A_n(x) + x^{2^n} B_n(x), \end{aligned}$$

which implies (by using the induction hypothesis in the last step),

$$\begin{aligned} &A_{n+1}(x)A_{n+1}(x^{-1}) + B_{n+1}(x)B_{n+1}(x^{-1}) \\ &= (A_n(x) - x^{2^n} B_n(x))(A_n(x^{-1}) - x^{-2^n} B_n(x^{-1})) \\ &+ (A_n(x) + x^{2^n} B_n(x))(A_n(x^{-1}) + x^{-2^n} B_n(x^{-1})) \\ &A_n(x)A_n(x^{-1}) + B_n(x)B_n(x^{-1}) - x^{2^n} A_n(x^{-1})B_n(x) - x^{-2^n} A_n(x)B_n(x^{-1}) \\ &+ A_n(x)A_n(x^{-1}) + B_n(x)B_n(x^{-1}) + x^{2^n} A_n(x^{-1})B_n(x) + x^{-2^n} A_n(x)B_n(x^{-1}) \\ &= 2 \cdot 2^{n+1} = 2^{n+2}, \end{aligned}$$

and the result is shown. □

Remark. Using the previous theorem, we immediately obtain [17, Theorems 7 & 9].

We give below an example. Let $n = 4$, and the Boolean function from our previous theorem,

$$f_4(x_1, x_2, x_3, x_4) = \sum_{j-i\geq 2} x_i x_j \oplus s_3(x_1, \ldots, x_4) \oplus s_4(x_1, \ldots, x_4)$$
$$= x_1x_3 \oplus x_1x_4 \oplus x_2x_4 \oplus x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_3x_4 \oplus x_2x_3x_4 \oplus x_1x_2x_3x_4,$$

whose truth table is 0000010001110100, which is exactly the sequence $b(15)$.

Next, we will introduce yet two more Golay-Rudin-Shapiro-like sequences, state our theorems, but leave their proofs to the interested reader, since, the method of proof is the same as in our Theorems 3.1 and 4.3. Let $\{j_n\}_n$, $\{k_n\}_n$ be the sequences given by $j_n = (-1)^{\sum_{i=0}^{\ell}(e_i\oplus 1)\cdot e_{i+1}}$, respectively, $k_n = (-1)^{\sum_{i=0}^{\ell}(e_i\oplus 1)\cdot(e_{i+1}\oplus 1)}$, which depend upon the number of patterns '01', respectively, '00' in the binary expansion $n = \sum_{i=0}^{\ell} e_i 2^i$.

Similarly to the previous two cases, one can observe (and prove, certainly) that $\{j_n\}_n$ is the sign sequence corresponding to the beginning string of the Boolean functions f_n (with companion g_n) defined by

$$\begin{aligned} f_0 &= 0 & g_0 &= 0, \\ f_{n+1} &= f_n g_n, & g_{n+1} &= \bar{f}_n g_n. \end{aligned}$$

The following theorem holds.

Theorem 4.4. *Let $2^{n-1} < N \leq 2^n - 1$. The sequence $\{j_s\}_{s=0}^{N}$ is the initial N-bit string of the sign sequence of a Boolean function f_n whose algebraic normal form is $f_n(\mathbf{x}) = \sum_{i=1}^{n-1} x_i x_{i+1} \oplus \sum_{i=1}^{n-1} x_i$. The function f_n is bent for n even and semibent for n odd, and its weight is*

$$\mathrm{wt}(f_n) = 2^{n-1} - 2^{(n-1)/2} \sin\left(\frac{(n+1)\pi}{4}\right),\ n \geq 0.$$

The companion sequence g_n has algebraic normal form $g_n(\mathbf{x}) = \sum_{i=1}^{n-1} x_i x_{i+1} \oplus \sum_{i=2}^{n-1} x_i \oplus 1$, which is bent for n even and semibent for n odd, and its weight, for $n \geq 0$, is

$$\mathrm{wt}(g_n) = \sum_{k=0}^{n} \left(2^{k-1} + 2^{(k-1)/2} \sin\left(\frac{(k+1)\pi}{4}\right)\right)$$
$$= \begin{cases} 2^n & \text{if, } n = 4k \\ 2^n + (-1)^{\lfloor n/4 \rfloor} 2^{\lfloor n/2 \rfloor} & \text{otherwise.} \end{cases}$$

Furthermore, the sign sequences of f_n and g_n form a Golay complementary pair.

Next, one can show that the sequence $\{k_n\}_n$ is the sign sequence corresponding to the beginning string of the Boolean functions f_n (with companion g_n) defined by

$$\begin{aligned} f_0 &= 0 & g_0 &= 0, \\ f_1 &= 00 & g_1 &= 00, \end{aligned}$$

$$f_{n+1} = f_n g_n, \qquad\qquad g_{n+1} = \bar{u}_n v_n u_n v_n,$$

and the following theorem holds (the ANF of f_n will be given in terms of a recurrence, as it is rather cumbersome to write a "clean" expression for it).

Theorem 4.5. *Let $2^{n-1} < N \leq 2^n - 1$. The sequence $\{k_s\}_{s=0}^{N}$ is the initial N-bit string of the sign sequence of a Boolean function f_n whose algebraic normal form (of degree n) is $f_n(\mathbf{x}) = (1 \oplus x_1) f_{n-1}(x_2, \ldots, x_n) \oplus g_{n-1}(x_2, \ldots, x_n)$ (see below the ANF of g_n), of weight $\mathrm{wt}(f_n) = 2^{n-1} - 2^{\lfloor n/2 \rfloor} - 2^{\lfloor (n-1)/2 \rfloor} + 1$. The companion sequence g_n has algebraic normal form $g_n(\mathbf{x}) = \sum_{i=1}^{n-1} x_i x_{i+1} \oplus x_1 \oplus x_n \oplus \epsilon$ (where $\epsilon = 1$ for n even, and $\epsilon = 0$ for n odd), which is bent for n even and semibent for n odd, and its weight is $\mathrm{wt}(g_n) = 2^{n-1} - 2^{\lfloor (n-1)/2 \rfloor}$, for $n \geq 0$.*

Furthermore, the first and second half of the sign sequence of g_n gives rise to a Golay complementary pair.

We note that one can find partial sums of all of these sequences (besides the ones where the length has binary weight 1, since that is derived from the weights we found).

We are certain that there are many other questions on the Golay-Rudin-Shapiro sequence and/or complementary pairs one can investigate where our approach may be applicable to and we therefore invite/challenge the reader to do so.

Acknowledgement. The author would like to thank the referee for comments and the editors for the prompt handling of our paper.

References

[1] J.-P. Allouche, J. Shallit, Automatic sequences. Theory, applications, generalizations, Cambridge University Press, Cambridge, 2003.

[2] P. Balister, *Bounds on Rudin-Shapiro polynomials of arbitrary degree*, available at: https://arxiv.org/abs/1909.08777.

[3] R. Blecksmith, L. W. Purushottam, *Some Exact Number Theory Computations via Probability Mechanisms*, Amer. Math. Monthly **102:10** (1995), 893–903.

[4] P. B. Borwein, R. A. Ferguson, *A complete description of Golay pairs for lengths up to* 100, Math. Comp. **73** (2004), 967–985.

[5] D. W. Boyd, J. Cook, P. Morton, *On sequences ± 1's defined by binary patterns*, Dissertationes Math. **283**, Warszawa, 1989, pp. 1-60.

[6] J. Brillhart, P. Erdös, P. Morton, *On sums of Rudin-Shapiro coefficients* II, Pacific J. Math. **107:1** (1983), 39–69.

[7] J. Brillhart, J. S. Lomont, P. Morton, *Cyclotomic properties of the Rudin-Shapiro polynomials*, J. Reine Angew. Math. **288** (1976), 37–65.

[8] J. Brillhart, P. Morton, *Über summen von Rudin-Shapiroschen Koeffizienten*, Illinois J. Math. **22** (1978), 126–148.

[9] J. Brillhart, P. Morton, *A case study in mathematical research: the Golay-Rudin-Shapiro sequence*, Amer. Math. Monthly **103** (1996), no. 10, 854–869.

[10] C. Carlet, *Boolean Functions for Cryptography and Error Correcting Codes*, Chapter of the volume "Boolean Models and Methods in Mathematics, Computer Science, and Engineering", Cambridge University Press (Eds. Y. Crama, P. Hammer) (2010), 257–397.

[11] T. W. Cusick, P. Stănică, Cryptographic Boolean functions and applications (2nd ed.), Elsevier–Academic Press, 2017.

[12] J. A. Davis, J. Jedwab, *Peak-to-mean power control in OFDM, Golay complementary sequences, and Reed-Muller codes*, IEEE Trans. Inf. Theory **45** (1999), 2397–2417.

[13] F. Fiedler, J. Jedwab, M. G. Parker, *A framework for the construction of Golay sequences*, IEEE Trans. Inf. Theory **54** (2008), 3114–3129.

[14] M. J. E. Golay, *Multislit spectrometry*, J. Optical Soc. Amer. **39** (1949), 437–444.

[15] M. J. E. Golay, *Static multislit spectrometry and its application to the panoramic display of infrared spectra*, J. Optical Soc. Amer. **41** (1951), 468–472.

[16] J. Jedwab, M. G. Parker, *Golay complementary array pairs*, Designs, Codes, & Cryptography **44** (2007), 209–216.

[17] P. Lafrance, N. Rampersad, R. Yee, *Some properties of a Rudin-Shapiro-like sequence*, Adv. Appl. Math. **63** (2015), 19–40.

[18] P. Morton, W. Mourant, *Paper folding, digit patterns and groups of arithmetic fractals*, Proc. London Math. Soc. **3:59** (1989), 253–293.

[19] O. S. Rothaus, *On bent functions*, J. Combin. Theory – Ser. A **20** (1976), 300–305.

[20] W. Rudin, *Some theorems on Fourier coefficients*, Proc. Amer. Math. Soc. **10** (1959), 855–859.

[21] B. Saffari, *Structure algébrique sur les couples de Rudin-Shapiro*, C.R. Acad. Sci. Paris **304** (1987), 127–130.

[22] K.-U. Schmidt, On Spectrally Bounded Codes for Multicarrier Communications, Techn. Univ. Dresden, Dr. Diss., 2007, available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.472.645&rep=rep1&type=pdf.

[23] H. S. Shapiro, Extremal problems for polynomials and power series, Master's thesis, MIT, 1952, available at: http://dspace.mit.edu/handle/1721.1/12198.