2019-07

Root-Hadamard transforms and complementary sequences

Medina, Luis A.; Parker, Matthew G.; Riera, Constanza; Stnic, Pantelimon

Springer

Medina, Luis A., et al. "Root-Hadamard transforms and complementary sequences." Cryptography and Communications (2020): 1-15.
http://hdl.handle.net/10945/65339

Cryptography and Communications
https://doi.org/10.1007/s12095-020-00440-4

Root-Hadamard transforms and complementary sequences

Luis A. Medina[1] · **Matthew G. Parker**[2] · **Constanza Riera**[3] · **Pantelimon Stănică**[4]

Received: 22 July 2019 / Accepted: 1 June 2020 / Published online: 22 June 2020

Abstract

In this paper we define a new transform on (generalized) Boolean functions, which generalizes the Walsh-Hadamard, nega-Hadamard, 2^k-Hadamard, consta-Hadamard and all HN-transforms. We describe the behavior of what we call the root-Hadamard transform for a generalized Boolean function f in terms of the binary components of f. Further, we define a notion of complementarity (in the spirit of the Golay sequences) with respect to this transform and furthermore, we describe the complementarity of a generalized Boolean set with respect to the binary components of the elements of that set.

Keywords Golay pairs · Boolean functions · Correlations · Generalized root-transforms · Complementary sets

Mathematics Subject Classification (2010) 06E30 · 31B83 · 94A55 · 94C10

Dedicated to the memory of our friend and co-author, Francis N. Castro.

This article belongs to the Topical Collection: *Boolean Functions and Their Applications IV*
Guest Editors: Lilya Budaghyan and Tor Helleseth

✉ Pantelimon Stănică
pstanica@nps.edu

Luis A. Medina
luis.medina17@upr.edu

Matthew G. Parker
Matthew.Parker@ii.uib.no

Constanza Riera
csr@hvl.no

[1] Department of Mathematics, University of Puerto Rico, San Juan, PR, 00925, USA

[2] Department of Informatics, University of Bergen, Bergen, Norway

[3] Department of Computer Science, Electrical Engineering, Mathematical Sciences, Western Norway University of Applied Sciences, 5020, Bergen, Norway

[4] Department of Applied Mathematics, Naval Postgraduate School, Monterey, CA, 93943–521, USA

1 (Generalized) Boolean functions

Let $\mathbb{F}_2^n$ be the vector space of the n-tuples over $\mathbb{F}_2$, and, for an integer q, let $\mathbb{Z}_q$ be the ring of integers modulo q. By '$+$' and '$-$' we respectively denote addition and subtraction in $\mathbb{F}_2^n$.

A function $F : \mathbb{F}_2^n \to \mathbb{F}_2$, $n > 0$, is called a *Boolean function* in n variables, whose set 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)

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

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*. The (*Hamming*) *weight* of $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$ is denoted by $wt(\mathbf{x})$ and equals $\sum_{i=1}^n x_i$ (the Hamming weight of a function is the weight of its truth table, that is, the weight of its output vector). The cardinality of a set S is denoted by $|S|$.

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).

If $\mathbf{x} = (x_1, \ldots, x_n)$ and $\mathbf{y} = (y_1, \ldots, y_n)$ are two vectors in $\mathbb{F}_2^n$ we define the *scalar* (*or inner*) *product*, by $\mathbf{x} \cdot \mathbf{y} = x_1 y_1 + x_2 y_2 + \cdots + x_n y_n$. The scalar/inner product $\mathbf{x} \odot \mathbf{y}$ in $\mathbb{C} \times \mathbb{C}$ is similar, with the sum over $\mathbb{C}$. The *intersection* of two vectors $\mathbf{x}$ and $\mathbf{y}$ in some vector space under discussion is $\mathbf{x} \star \mathbf{y} = (x_1 y_1, x_2 y_2, \ldots, x_n y_n)$. We write $a = \Re(z)$, $b = \Im(z)$ for the real part, respectively, imaginary part of the complex number $z = a + b\,i \in \mathbb{C}$, where $i^2 = -1$, and $a, b \in \mathbb{R}$. Further, $|z| = \sqrt{a^2 + b^2}$ is the absolute value of z, and $\overline{z} = a - b\,i$ denotes the complex conjugate of z.

We call a function from $\mathbb{F}_2^n$ to $\mathbb{Z}_q$ ($q \ge 2$) a *generalized Boolean function* on n variables, and denote the set of all generalized Boolean functions by $\mathcal{GB}_n^q$ and, when $q = 2$, by $\mathcal{B}_n$, as previously mentioned. If $q = 2^k$ for some $k \ge 1$, we can associate to any $f \in \mathcal{GB}_n^q$ a unique sequence of Boolean functions $a_i \in \mathcal{B}_n$ ($i = 0, 1, \ldots, k-1$) such that

$$f(\mathbf{x}) = a_0(\mathbf{x}) + 2a_1(\mathbf{x}) + \cdots + 2^{k-1} a_{k-1}(\mathbf{x}), \text{ for all } \mathbf{x} \in \mathbb{F}_2^n.$$

For a Boolean function $f \in \mathcal{B}_n$, we define its sign function $\hat{f}$ by $\hat{f}(\mathbf{x}) = (-1)^{f(\mathbf{x})}$. In general, the sign function of $f \in \mathcal{GB}_n^q$ is $\hat{f}(\mathbf{x}) = \zeta_q^{f(\mathbf{x})}$, where $\zeta_q = e^{\frac{2\pi i}{q}}$ is the q-complex root of 1 (for easy writing, we sometimes use ζ instead of ζ_q, when q is fixed).

For a *generalized Boolean function* $f : \mathbb{F}_2^n \to \mathbb{Z}_q$ we define the (normalized) *generalized Walsh-Hadamard transform* to be the complex valued function

$$\mathcal{H}_f^{(q)}(\mathbf{u}) = 2^{-n/2} \sum_{\mathbf{x} \in \mathbb{F}_2^n} \zeta_q^{f(\mathbf{x})} (-1)^{\mathbf{u} \cdot \mathbf{x}}.$$

(we sometimes use $\mathcal{H}_f$, instead of $\mathcal{H}_f^{(q)}$, when q is fixed.)

For $q = 2$, we obtain the usual *Walsh-Hadamard transform*

$$\mathcal{W}_f(\mathbf{u}) = 2^{-n/2} \sum_{\mathbf{x} \in \mathbb{F}_2^n} (-1)^{f(\mathbf{x}) + \mathbf{u} \cdot \mathbf{x}}.$$

The sum

$$\mathcal{C}_{f,g}(\mathbf{z}) = \sum_{\mathbf{x} \in \mathbb{F}_2^n} \zeta^{f(\mathbf{x}+\mathbf{z}) - g(\mathbf{x})}$$

is the *crosscorrelation* of f and g at $\mathbf{z} \in \mathbb{F}_2^n$. The *autocorrelation* of $f \in \mathcal{GB}_n^q$ at $\mathbf{u} \in \mathbb{F}_2^n$ is $\mathcal{C}_{f,f}(\mathbf{u})$ above, which we denote by $\mathcal{C}_f(\mathbf{u})$.

Given a generalized Boolean function f, the derivative $D_{\mathbf{a}}f$ of f with respect to a vector $\mathbf{a} \in \mathbb{F}_2^n$, is the generalized Boolean function defined by

$$D_{\mathbf{a}}f(\mathbf{x}) = f(\mathbf{x}+\mathbf{a}) - f(\mathbf{x}), \text{ for all } \mathbf{x} \in \mathbb{F}_2^n. \tag{1}$$

A function $f : \mathbb{F}_2^n \to \mathbb{Z}_q$ is called *generalized bent* (*gbent*) if $|\mathcal{H}_f(\mathbf{u})| = 2^{n/2}$ for all $\mathbf{u} \in \mathbb{F}_2^n$. For descriptions of (generalized) bents, the reader can consult [10, 15, 18, 20].

The *nega–Hadamard transform* of $f \in \mathcal{GB}_n^q$ at any vector $\mathbf{u} \in \mathbb{F}_2^n$ is the complex valued function:

$$\mathcal{N}_f^{(q)}(\mathbf{u}) = 2^{-\frac{n}{2}} \sum_{\mathbf{x}\in\mathbb{F}_2^n} \zeta^{f(\mathbf{x})}(-1)^{\mathbf{u}\cdot\mathbf{x}}\iota^{wt(\mathbf{x})}.$$

As customary, we may drop (some of) the superscripts in all of our notations, if convenient. In [13], some of us considered generalized bent criteria for Boolean functions by analyzing Boolean functions which have flat spectrum with respect to one or more transforms chosen from a set of unitary transforms. The transforms chosen are n-fold tensor products of the identity mapping $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, the Walsh–Hadamard transformation $\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, and the nega–Hadamard transform $\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & \iota \\ 1 & -\iota \end{pmatrix}$, where $\iota^2 = -1$. That choice is motivated by local unitary transforms that play an important role in the structural analysis of pure n-qubit stabilizer quantum states.

A function $f : \mathbb{F}_2^n \to \mathbb{Z}_q$ is said to be (generalized) *negabent* if the nega–Hadamard transform is flat in absolute value, namely $|\mathcal{N}_f^{(q)}(\mathbf{u})| = 1$ for all $\mathbf{u} \in \mathbb{F}_2^n$. The sum

$$\mathcal{C}_{f,g}^n(\mathbf{z}) = \sum_{\mathbf{x}\in\mathbb{F}_2^n} \zeta^{f(\mathbf{x}+\mathbf{z})-g(\mathbf{x})}(-1)^{\mathbf{x}\cdot\mathbf{z}}$$

is the *nega–crosscorrelation* of f and g at z. We define the *nega–autocorrelation* of f at $\mathbf{u} \in \mathbb{F}_2^n$ by

$$\mathcal{C}_f^n(\mathbf{u}) = \sum_{\mathbf{x}\in\mathbb{F}_2^n} \zeta^{f(\mathbf{x}+\mathbf{z})-f(\mathbf{x})}(-1)^{\mathbf{x}\cdot\mathbf{z}}.$$

For more on (generalized) Boolean functions, the reader can consult [2, 3, 10, 14, 18, 20] and the references therein.

2 The root-Hadamard transform

Walsh-Hadamard, nega-Hadamard transforms, as well as, 2^k-Hadamard [17], consta-Hadamard [11] and HN-transforms [13], can be generalized (thus, unifying under the same umbrella all of these transforms) into what we will call the *root-Hadamard transform*.

Definition 1 Let $f \in \mathcal{GB}_n^{2^k}$, ζ_{2^k} a 2^k-complex root of 1 (when convenient we drop the index), $A = \{\alpha_1, \ldots, \alpha_r\}$ a set of roots of unity $\alpha_j = e^{\frac{2\pi i}{k_j}}$, $K = \{k_j\}_{1\le j\le r}$ and $L = \{R_s\}_{s\in K}$ be a partition of the index set $\{0, \ldots, n-1\} = \bigsqcup_{s\in K} R_s$, $|L| = r$ (for convenience,

we index the partition by the elements of K). For $L = \{R_s\}_{s\in K}$, we let $\mathbf{x}_{R_s} = (x_j)_{j\in R_s}$ and $\lambda_L(\mathbf{x}) = \prod_{s\in K} \alpha_s^{wt(\mathbf{x}_{R_s})}$, where $wt(\mathbf{x}_{R_s}) = \sum_{j\in R_s} x_j \in \mathbb{N}$(observe that $\lambda_L(\mathbf{0}) = 1$, for any partition L). We define the *root-Hadamard transform* of f at any vector $\mathbf{u} \in \mathbb{F}_2^n$ as the complex valued function:

$$\mathcal{U}^{(2^k)}_{L,A,f}(\mathbf{u}) = 2^{-\frac{n}{2}} \sum_{\mathbf{x}\in\mathbb{F}_2^n} \zeta^{f(\mathbf{x})}(-1)^{\mathbf{u}\cdot\mathbf{x}}\,\lambda_L(\mathbf{x}).$$

If f is a Boolean function, we let $\mathcal{T}_{L,A,f} := \mathcal{U}^{(2)}_{L,A,f}$. A function f on $\mathcal{GB}_n^{2^k}$ is said to be *root-bent* if the root-Hadamard transform is flat in absolute value, namely $|\mathcal{U}_{L,A,f}(\mathbf{u})| = 1$ for all $\mathbf{u} \in \mathbb{F}_2^n$. The sum

$$\mathcal{C}^p_{L,A,f,g}(\mathbf{z}) = \sum_{\mathbf{x}\in\mathbb{F}_2^n} \zeta^{f(\mathbf{x}+\mathbf{z})-g(\mathbf{x})} \prod_{s\in K} \mu_s^{\mathbf{x}_{R_s}\odot\mathbf{z}_{R_s}}$$

is the *root–crosscorrelation* of f and g at z (recall that $\mu_s = \alpha_s^2$). We define the *root–autocorrelation* of f at $\mathbf{u} \in \mathbb{F}_2^n$ by

$$\mathcal{C}^p_{L,A,f}(\mathbf{z}) = \sum_{\mathbf{x}\in\mathbb{F}_2^n} \zeta^{f(\mathbf{x}+\mathbf{z})-f(\mathbf{x})} \prod_{s\in K} \mu_s^{\mathbf{x}_{R_s}\odot\mathbf{z}_{R_s}}.$$

When the sets L, A are understood from the context, to simplify the notation, we may write $\mathcal{U}_f, T_f, \mathcal{C}^p_{f,g}, \mathcal{C}^p_f$ in lieu of $\mathcal{U}^{(2^k)}_{L,A,f}, \mathcal{T}^{(2^k)}_{L,A,f}, \mathcal{C}^p_{L,A,f,g}, \mathcal{C}^p_{L,A,f}$.

Example 2 Consider $A = \left\{e^{\frac{2\pi i}{4}}, e^{\frac{2\pi i}{8}}\right\}$ and $L = \{(0, 2), (1, 3)\}$. The generalized Boolean function

$$f(\mathbf{x}) = x_1x_2 + x_2x_3 + x_2x_4 + x_1x_4 + x_3x_4 + 2\,(x_1x_2 + x_1x_3 + x_3x_4)$$

is root-bent, that is, $|\mathcal{U}_{L,A,f}(\mathbf{u})| = 1$ for all $\mathbf{u} \in \mathbb{F}_2^n$.

This transform is related to (but more general than) the concept of *consta-Hadamard* transform (see [11, 17]). First, we show that it is a proper kernel transform, so we show its invertibility by providing a simple proof of that (the proof also follows from the fact that the matrix corresponding to the root-Hadamard transform is an orthogonal matrix).

Proposition 3 *Let $f \in \mathcal{GB}_n$, A be a set of complex roots of 1 and $\{R_k\}_{k\in K}$ be a partition of $\{0, 1, \ldots, n-1\}$, indexed by the elements in A. Then, for any $\mathbf{y} \in \mathbb{F}_2^n$, we have that*

$$\zeta^{f(\mathbf{y})} = \frac{1}{2^{\frac{n}{2}}\lambda_L(\mathbf{y})} \sum_{\boldsymbol{w}\in\mathbb{F}_2^n} \mathcal{U}_{L,A,f}(\boldsymbol{w})(-1)^{\mathbf{y}\cdot\boldsymbol{w}}.$$

Proof We perform the following computation:

$$\begin{aligned}
&2^{-\frac{n}{2}} \sum_{\mathbf{w}\in\mathbb{F}_2^n} \mathcal{U}_{L,A,f}(\mathbf{w})(-1)^{\mathbf{y}\cdot\mathbf{w}} \\
&= 2^{-n} \sum_{\mathbf{w}\in\mathbb{F}_2^n}\sum_{\mathbf{x}\in\mathbb{F}_2^n} \zeta^{f(\mathbf{x})}(-1)^{\mathbf{w}\cdot\mathbf{x}} \prod_{s\in K} \alpha_s^{wt(\mathbf{x}_{R_s})}(-1)^{\mathbf{y}\cdot\mathbf{w}} \\
&= 2^{-n} \sum_{\mathbf{x}\in\mathbb{F}_2^n} \zeta^{f(\mathbf{x})} \prod_{s\in K} \alpha_s^{wt(\mathbf{x}_{R_s})} \sum_{\mathbf{w}\in\mathbb{F}_2^n} (-1)^{(\mathbf{x}+\mathbf{y})\cdot\mathbf{w}} \\
&= \zeta^{f(\mathbf{y})} \prod_{s\in K} \alpha_s^{wt(\mathbf{y}_{R_s})},
\end{aligned}$$

and the claim follows. □

If α is a complex root of 1, we let $\mu = \alpha^2$ (recall the scalar product $\mathbf{x} \odot \mathbf{z}$ is computed over $\mathbb{C}$). We will make use throughout of the well-known identity on binary vectors (see [9])

$$\mathrm{wt}(\mathbf{x}+\mathbf{y}) = \mathrm{wt}(\mathbf{x}) + \mathrm{wt}(\mathbf{y}) - 2\mathrm{wt}(\mathbf{x} \star \mathbf{y}). \tag{2}$$

The following result is a collection of facts from [18, 19].

Proposition 4 *We have:*

(1) *If $f, g \in \mathcal{GB}_n^q$, then*

$$\begin{aligned}
\sum_{\boldsymbol{u}\in\mathbb{F}_2^n} \mathcal{C}_{f,g}(\boldsymbol{u})(-1)^{\langle \boldsymbol{u},\mathbf{x}\rangle} &= \mathcal{H}_f(\mathbf{x})\overline{\mathcal{H}_g(\mathbf{x})}, \\
\mathcal{C}_{f,g}(\boldsymbol{u}) &= 2^{-n} \sum_{\mathbf{x}\in\mathbb{F}_2^n} \mathcal{H}_f(\mathbf{x})\overline{\mathcal{H}_g(\mathbf{x})}(-1)^{\langle \boldsymbol{u},\mathbf{x}\rangle}.
\end{aligned} \tag{3}$$

In particular, if $f = g$, then $\mathcal{C}_f(\boldsymbol{u}) = 2^{-n} \sum_{\mathbf{x}\in\mathbb{F}_2^n} |\mathcal{H}_f(\mathbf{x})|^2 (-1)^{\langle \boldsymbol{u},\mathbf{x}\rangle}$.

(2) *If $f, g \in \mathcal{B}_n$, then the nega–crosscorrelation equals*

$$\mathcal{C}^n_{f,g}(\mathbf{z}) = \imath^{wt(\mathbf{z})} \sum_{\boldsymbol{u}\in\mathbb{F}_2^n} \mathcal{N}_f(\boldsymbol{u})\overline{\mathcal{N}_g(\boldsymbol{u})}(-1)^{\boldsymbol{u}\cdot\mathbf{z}}.$$

We now prove a result similar to Proposition 4 for this newly defined transform.

Theorem 5 *Let $f, g \in \mathcal{B}_n^{2^k}$, A be a set of complex roots of 1 and $\{R_k\}_{k\in K}$ be a partition of $\{0, 1, \ldots, n-1\}$ as before. The root-crosscorrelation of f, g is*

$$\mathcal{C}^p_{L,f,g}(\mathbf{z}) = \lambda_L(\mathbf{z}) \sum_{\boldsymbol{u}\in\mathbb{F}_2^n} \mathcal{U}_{L,A,f}(\boldsymbol{u})\overline{\mathcal{U}_{L,A,g}(\boldsymbol{u})}(-1)^{\boldsymbol{u}\cdot\mathbf{z}}.$$

Furthermore, the root-Parseval identity holds

$$\sum_{\boldsymbol{u}\in\mathbb{F}_2^n} |\mathcal{U}_{L,A,f}(\boldsymbol{u})|^2 = 2^n.$$

Moreover, f is root-bent if and only if $\mathcal{C}^p_{L,A,f}(\boldsymbol{u}) = 0$, for all $\boldsymbol{u} \neq \mathbf{0}$.

Proof Using [3, Lemma 2.9] and identity (2), we write

$$\begin{aligned}
&\lambda_L(\mathbf{z}) \sum_{\mathbf{u}\in\mathbb{F}_2^n} \mathcal{U}_{L,A,f}(\mathbf{u})\overline{\mathcal{U}_{L,A,g}(\mathbf{u})}(-1)^{\mathbf{u}\cdot\mathbf{z}} \\
&= 2^{-n} \sum_{\mathbf{x},\mathbf{y}\in\mathbb{F}_2^n} \zeta_{2^k}^{f(\mathbf{x})-g(\mathbf{y})}\lambda_L(\mathbf{x})\overline{\lambda_L(\mathbf{y})}\lambda_L(\mathbf{z}) \sum_{\mathbf{u}\in\mathbb{F}_2^n}(-1)^{\mathbf{u}\cdot(\mathbf{x}+\mathbf{y}+\mathbf{z})} \\
&= 2^{-n} \sum_{\mathbf{x},\mathbf{y}\in\mathbb{F}_2^n} \zeta_{2^k}^{f(\mathbf{x})-g(\mathbf{y})} \prod_{s\in K} \alpha_s^{wt(\mathbf{x}_{R_s})-wt(\mathbf{y}_{R_s})+wt(\mathbf{z}_{R_s})} \sum_{\mathbf{u}\in\mathbb{F}_2^n}(-1)^{\mathbf{u}\cdot(\mathbf{x}+\mathbf{y}+\mathbf{z})} \\
&= \sum_{\mathbf{x},\mathbf{y}\in\mathbb{F}_2^n} \zeta_{2^k}^{f(\mathbf{x})-g(\mathbf{x}+\mathbf{z})} \prod_{s\in K} \alpha_s^{2wt(\mathbf{x}_{R_s}\star\mathbf{z}_{R_s})} \\
&= \sum_{\mathbf{x}\in\mathbb{F}_2^n}(-1)^{f(\mathbf{x})-g(\mathbf{x}+\mathbf{z})} \prod_{s\in K} \mu_s^{\mathbf{x}_{R_s}\odot\mathbf{z}_{R_s}} = \mathcal{C}_{f,g}^p(\mathbf{z}).
\end{aligned}$$

If $f = g$, then we get

$$\begin{aligned}
\mathcal{C}_{L,A,f}^p(\mathbf{z}) &= \sum_{\mathbf{x}\in\mathbb{F}_2^n}(-1)^{f(\mathbf{x})-f(\mathbf{x}+\mathbf{z})} \prod_{s\in K} \mu_s^{\mathbf{x}_{R_s}\odot\mathbf{z}_{R_s}} \\
&= \lambda_L(\mathbf{z}) \sum_{\mathbf{u}\in\mathbb{F}_2^n} \mathcal{U}_{L,A,f}(\mathbf{u})\overline{\mathcal{U}_{L,A,f}(\mathbf{u})}(-1)^{\mathbf{u}\cdot\mathbf{z}},
\end{aligned}$$

and by replacing $\mathbf{z} = \mathbf{0}$, then we get the root-Parseval identity. The last claim is also implied by the previous identity. □

Example 6 The generalized Boolean function $f(\mathbf{x})$ in Example 2 satisfies $\mathcal{C}_{L,A,f}^p(\mathbf{u}) = 0$ for all $\mathbf{u} \neq \mathbf{0}$ (as predicted by Theorem 5).

3 Complementary sequences

We next give a brief overview of Golay complementary pairs (CP) (see, for example, [4–8, 16] or the reader's preferred reference on CP). Let $\mathbf{a} = \{a_i\}_{i=0}^{N-1}$ be a sequence of ± 1 (bipolar) and let the *aperiodic autocorrelation* of $\mathbf{a}$ at k be defined by $\mathcal{A}_\mathbf{a}(k) = \sum_{i=0}^{N-k-1} a_i a_{i+k}$, $0 \leq k \leq N-1$. The *periodic autocorrelation* of $\mathbf{a}$ at $0 \leq k \leq N-1$ is defined by $\mathcal{C}_\mathbf{a}(k) = \sum_{i=0}^{N-1} a_i a_{i+k}$, $0 \leq k \leq N-1$, where we take indices modulo N. The *negaperiodic autocorrelation* is $\mathcal{C}_f^n(\mathbf{u}) = \sum_{i=0}^{2^n-1} a_i a_{i+k}(-1)^{\lfloor (k+i)/2^n \rfloor}$.

Two bipolar sequences $\mathbf{a}$, $\mathbf{b}$ form a (*Golay*) *complementary pair* if

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

We call them a P-complementary pair if

$$\mathcal{C}_\mathbf{a}(k) + \mathcal{C}_\mathbf{b}(k) = 0, \text{ for } k \neq 0,$$

and N-complementary pair if

$$\mathcal{C}_\mathbf{a}^n(k) + \mathcal{C}_\mathbf{b}^n(k) = 0, \text{ for } k \neq 0,$$

We associate a polynomial A to 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

$$A(x)A(x^{-1}) + B(x)B(x^{-1}) = 2N. \tag{4}$$

Similarly, they form a P-complementary pair if

$$A(x)A(x^{-1}) + B(x)B(x^{-1}) \equiv 2N \pmod{x^N - 1} \tag{5}$$

and a N-complementary pair if

$$A(x)A(x^{-1}) + B(x)B(x^{-1}) \equiv 2N \pmod{x^N + 1}. \tag{6}$$

Let U, V be the following $N \times N$ matrices, defined by

$$U = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ldots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & 0 & \cdots & 0 & 0 \end{pmatrix}, \quad V = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ldots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ -1 & 0 & 0 & \cdots & 0 & 0 \end{pmatrix}.$$

We can quickly see that the periodic and negaperiodic autocorrelations satisfy $\mathcal{C}_{\mathbf{a}}(k) = \mathbf{a}\cdot\mathbf{a}U^k$ and $\mathcal{C}^n_{\mathbf{a}}(k) = \mathbf{a}\cdot\mathbf{a}V^k$. It is interesting to note that a pair of sequences is complementary if and only if it is P-complementary and N-complementary, which easily follows from the identities

$$\begin{aligned} \mathcal{P}_{\mathbf{a}}(k) &= \mathcal{A}_{\mathbf{a}}(k) + \mathcal{A}_{\mathbf{a}}(N-k), \\ \mathcal{C}^n_{\mathbf{a}}(k) &= \mathcal{A}_{\mathbf{a}}(k) - \mathcal{A}_{\mathbf{a}}(N-k). \end{aligned}$$

All of the above concepts can be extended to a set of sequences $S = \{\mathbf{a}_i\}_{1\le i\le M}$ by imposing the sum of autocorrelations to be zero at nonzero shift, and we shall such, a *complementary set*) (with respect to some fixed autocorrelation). For example, the set S is P-complementary (respectively, N-complementary) if $\sum_{i=1}^{M} \mathcal{A}_{\mathbf{a}_i}(k) = 0$ (respectively, $\sum_{i=1}^{M} \mathcal{C}_{\mathbf{a}_i}(k) = 0$), for $k \neq 0$. We shall also define the notion of *pairwise complementary set* S, by assuming that any pair within the set is complementary with respect to some autocorrelation (see [21] for a particular case of what we suggest here, and the reference to applications in signal multiplexing of acoustic surface-wave sequences – there are surely more recent references, and we simply added one of the earliest we know on the concept of complementary sets).

The previous concepts take different forms for Boolean functions, since when we add vectors in the input of a function, we lose the circular permutation property (though, it can regarded as negacyclic permutation property). For two functions $f, g \in \mathcal{GB}^q_n$, we let the *periodic/negaperiodic correlation* of f, g to be

$$\begin{aligned} \mathcal{C}_{f,g}(\mathbf{u}) &= \sum_{i=0}^{2^n-1} \zeta^{f(\mathbf{v})-g(\mathbf{v}+\mathbf{u})}, \\ \mathcal{C}^n_{f,g}(\mathbf{u}) &= \sum_{i=0}^{2^n-1} \zeta^{f(\mathbf{v})-g(\mathbf{v}+\mathbf{u})}(-1)^{\mathbf{u}\cdot\mathbf{v}}. \end{aligned}$$

We say that two Boolean functions are *complementary* if and only if they are both P-complementary and N-complementary.

We will now define our new concept of (periodic and aperiodic) complementarity.

Definition 7 We say that two pairs of functions (a_1, a_2), (b_1, b_2) are:

(i) *A-crosscomplementary* if

$$\mathcal{A}_{a_1,a_2}(k) + \mathcal{A}_{b_1,b_2}(k) = 0, \text{ for } k \neq 0.$$

(ii) *P-crosscomplementary* if

$$\mathcal{C}_{a_1,a_2}(k) + \mathcal{C}_{b_1,b_2}(k) = 0, \text{ for } k \neq 0.$$

(iii) *N-crosscomplementary* if

$$\mathcal{C}^n_{a_1,a_2}(k) + \mathcal{C}^n_{b_1,b_2}(k) = 0, \text{ for } k \neq 0.$$

4 Complementary pairs and components of generalized Boolean functions

The following lemma from [10, 18, 20], provides a relationship between the generalized Walsh-Hadamard transform and the classical transform. Recall the "canonical bijection" $\iota : \mathbb{F}_2^{k-1} \to \mathbb{Z}_{2^{k-1}}$, which is defined by $\iota(\mathbf{c}) = \sum_{j=0}^{k-2} c_j 2^j$ where $\mathbf{c} = (c_0, c_1, \ldots, c_{k-2})$.

Lemma 8 *For a generalized Boolean* $f \in \mathcal{GB}_n^{2^k}$, $f(\mathbf{x}) = a_0(\mathbf{x}) + 2a_1(\mathbf{x}) + \cdots + 2^{k-1}a_{k-1}(\mathbf{x})$, $a_i \in \mathcal{B}_n$, *we have*

$$\mathcal{H}_f(\boldsymbol{u}) = \frac{1}{2^{k-1}} \sum_{(\boldsymbol{c},\boldsymbol{d}) \in \mathbb{F}_2^{k-1} \times \mathbb{F}_2^{k-1}} (-1)^{\boldsymbol{c}\cdot\boldsymbol{d}} \zeta_{2^k}^{\iota(\boldsymbol{d})} \mathcal{W}_{f_{\boldsymbol{c}}}(\boldsymbol{u}), \tag{7}$$

where $f_{\boldsymbol{c}}(\mathbf{x}) = c_0 a_0(\mathbf{x}) \oplus c_1 a_1(\mathbf{x}) \oplus \cdots \oplus c_{k-2} a_{k-2}(\mathbf{x}) \oplus a_{k-1}(\mathbf{x})$ *are the component functions of* f.

The next lemma is known and easy to show.

Lemma 9 *If* b, c *are bits and* z *is a complex number, then*

$$2z^b = (1 + (-1)^b) + (1 - (-1)^b)z,$$

$$\left(1 + (-1)^b z\right)(-1)^{bc} = \begin{cases} 1 + z & \text{if } b = 0 \\ (1 - z)(-1)^c & \text{if } b = 1. \end{cases}$$

In the next theorem, we generalize Lemma 8 with respect to our root-Hadamard transforms. The proof is interestingly enough, similar to the proof of Lemma 8, with some appropriate changes.

Theorem 10 *For a generalized Boolean* $f \in \mathcal{GB}_n^{2^k}$, A *and* L *as in Definition* 1, *and* $f(\mathbf{x}) = a_0(\mathbf{x}) + 2a_1(\mathbf{x}) + \cdots + 2^{k-1}a_{k-1}(\mathbf{x})$, $a_i \in \mathcal{B}_n$, *we have*

$$\mathcal{U}_{L,A,f}(\boldsymbol{u}) = \frac{1}{2^{k-1}} \sum_{(\boldsymbol{c},\boldsymbol{d}) \in \mathbb{F}_2^{k-1} \times \mathbb{F}_2^{k-1}} (-1)^{\boldsymbol{c}\cdot\boldsymbol{d}} \zeta_{2^k}^{\iota(\boldsymbol{d})} \mathcal{T}_{L,A,f_{\boldsymbol{c}}}(\boldsymbol{u}), \tag{8}$$

where $f_{\boldsymbol{c}}(\mathbf{x}) = c_0a_0(\mathbf{x})\oplus c_1a_1(\mathbf{x})\oplus\cdots\oplus c_{k-2}a_{k-2}(\mathbf{x})\oplus a_{k-1}(\mathbf{x})$ *are the component functions of* f.

Proof Denoting $\gamma_{\mathbf{c}} = \prod_{i=0}^{k-2}\left(1+(-1)^{c_i}\zeta_{2^{k-i}}\right)$, where $\mathbf{c} = (c_0, c_1, \ldots, c_{k-2}) \in \mathbb{F}_2^{k-1}$, we compute

$$2^{n/2}\mathcal{U}_{L,A,f}(\mathbf{u}) = \sum_{\mathbf{x}\in\mathbb{F}_2^n}\zeta_{2^k}^{f(\mathbf{x})}(-1)^{\mathbf{u}\cdot\mathbf{x}}\lambda_L(\mathbf{x}) = \sum_{\mathbf{x}\in\mathbb{F}_2^n}\zeta_{2^k}^{\sum_{i=0}^{k-1}f_i(\mathbf{x})2^i}(-1)^{\mathbf{u}\cdot\mathbf{x}}\lambda_L(\mathbf{x})$$

$$= \sum_{\mathbf{x}\in\mathbb{F}_2^n}(-1)^{f_{k-1}(\mathbf{x})+\mathbf{u}\cdot\mathbf{x}}\lambda_L(\mathbf{x})\prod_{i=0}^{k-2}\zeta_{2^{k-i}}^{f_i(\mathbf{x})}$$

$$= \frac{1}{2^{k-1}}\sum_{\mathbf{x}\in\mathbb{F}_2^n}(-1)^{f_{k-1}(\mathbf{x})+\mathbf{u}\cdot\mathbf{x}}\lambda_L(\mathbf{x})\prod_{i=0}^{k-2}\left(1+\zeta_{2^{k-i}}+\left(1-\zeta_{2^{k-i}}\right)(-1)^{f_i(\mathbf{x})}\right)$$

$$= \frac{1}{2^{k-1}}\sum_{\mathbf{x}\in\mathbb{F}_2^n}(-1)^{f_{k-1}(\mathbf{x})+\mathbf{u}\cdot\mathbf{x}}\lambda_L(\mathbf{x})$$

$$\cdot\sum_{\mathbf{c}\in\mathbb{F}_2^{k-1}}(-1)^{\sum_{i=0}^{k-2}c_if_i(\mathbf{x})}\prod_{i=0}^{k-2}\left(1+(-1)^{c_i}\zeta_{2^{k-i}}\right) \text{ (by Lemma 9)}$$

$$= \frac{1}{2^{k-1}}\sum_{\mathbf{c}\in\mathbb{F}_2^{k-1}}\gamma_{\mathbf{c}}\sum_{\mathbf{x}\in\mathbb{F}_2^n}(-1)^{f_{\mathbf{c}}(\mathbf{x})+\mathbf{u}\cdot\mathbf{x}}\lambda_L(\mathbf{x}) = \frac{1}{2^{k-1}}\sum_{\mathbf{c}\in\mathbb{F}_2^{k-1}}\gamma_{\mathbf{c}}\mathcal{T}_{L,A,f_{\mathbf{c}}}(\mathbf{u}).$$

The theorem follows after easily expressing $\gamma_{\mathbf{c}}$ as a sum of powers of the complex roots of 1 (or simply using [20, Lemma 5]). □

The next lemma will be used later.

Lemma 11 (Inversion Lemma) *We let* $F_{\boldsymbol{u}} : \mathbb{F}_2^n \to \mathbb{C}$ *be a class of complex-valued functions indexed by* $\boldsymbol{u} \in \mathbb{F}_2^{k-1}$. *Then, for every* $\boldsymbol{c} \in \mathbb{F}_2^{k-1}$, *we have*

$$F_{\boldsymbol{c}}(\boldsymbol{a}) = \frac{1}{2^{k-1}}\sum_{\boldsymbol{u},\boldsymbol{v}\in\mathbb{F}_2^{k-1}}(-1)^{(\boldsymbol{u}+\boldsymbol{c})\cdot\boldsymbol{v}}F_{\boldsymbol{u}}(\boldsymbol{a}).$$

Proof Observe that

$$\sum_{\mathbf{u},\mathbf{v}\in\mathbb{F}_2^{k-1}}(-1)^{(\mathbf{u}+\mathbf{c})\cdot\mathbf{v}}F_{\mathbf{u}}(\mathbf{a}) = \sum_{\mathbf{u}\in\mathbb{F}_2^{k-1}}F_{\mathbf{u}}(\mathbf{a})\sum_{\mathbf{v}\in\mathbb{F}_2^{k-1}}(-1)^{(\mathbf{u}+\mathbf{c})\cdot\mathbf{v}} = 2^{k-1}F_{\mathbf{c}}(\mathbf{a}),$$

by [3, Lemma 2.9], and our result follows. □

In the spirit of the Hadamard and nega-Hadamard complementary notions, we define a root-transform complementarity notion next. For $L = \{R_j\}_{j\in K}$, a partition of $\{0, 1, \ldots, n-$

1} and $A = \{\alpha_j\}_{j\in K}$, a set of complex roots of 1, we say that a set $S = \{g_i\}_{i=1}^M$ of functions in $\mathcal{GB}_n^q$ (q may be 2) is *LA-complementary* if

$$\sum_{i=1}^{M} \mathcal{C}^p_{L,A,g_i}(\mathbf{u}) = 0, \text{ for all } \mathbf{u} \neq 0.$$

Moreover, two tuples $S_1 = (f_i)_{i=1}^M$, $S_2 = (g_i)_{i=1}^M$ of (generalized or not) Boolean functions are *LA-crosscomplementary* if

$$\sum_{i=1}^{M} \mathcal{C}^p_{L,A,f_i,g_i}(\mathbf{u}) = 0, \text{ for all } \mathbf{u} \neq 0.$$

We give such an example below.

Example 12 Let $A = \left\{e^{\frac{2\pi i}{4}}, e^{\frac{2\pi i}{8}}\right\}$ and $L = \{\{0, 2\}, \{1, 3\}\}$. Consider the generalized Boolean function $f \in \mathcal{GB}_4^4$, defined by $f(\mathbf{x}) = x_1 + x_2 + x_3 + x_4 + 2f_1(\mathbf{x})$ where f_1 is any Boolean function in the set S_F (see Table 1). Then,

$$\mathcal{C}^p_{L,A,f}(\mathbf{u}) = \begin{cases} 16, & \mathbf{u} = \mathbf{0} \\ -8i, & \mathbf{u} = (0, 1, 0, 1) \\ 0, & \text{otherwise} \end{cases}.$$

Furthermore, let $g \in \mathcal{GB}_4^4$, defined by $g(\mathbf{x}) = x_1x_2 + x_3 + x_4 + x_1x_4 + 2g_1(\mathbf{x})$, where g_1 is a Boolean function in the set S_G (see Table 2). Then,

$$\mathcal{C}^p_{L,A,g}(\mathbf{u}) = \begin{cases} 16, & \mathbf{u} = \mathbf{0} \\ 8i, & \mathbf{u} = (0, 1, 0, 1) \\ 0, & \text{otherwise} \end{cases}.$$

Clearly, $\mathcal{C}^p_{L,A,f}(\mathbf{u}) + \mathcal{C}^p_{L,A,g}(\mathbf{u}) = 0$, for all $\mathbf{u} \neq 0$. In other words, the generalized Boolean functions f, g are LA-complementary.

Theorem 13 *Let $S = \{f_i\}_{i\in I}$, $f_i \in \mathcal{GB}_n^{2^k}$, be a set of generalized Boolean functions and A, L as in Definition 1. Then S forms an LA-complementary set if and only if for all $\boldsymbol{a}, \boldsymbol{c} \in \mathbb{F}_2^{k-1}$, $S_{\boldsymbol{a}} = \{f_{\boldsymbol{a}}\}_{f\in S}$, $S_{\boldsymbol{c}} = \{f_{\boldsymbol{c}}\}_{f\in S}$ form a binary LA-crosscomplementary set.*

Table 1 Set of Boolean functions S_F

$x_1x_2 + x_3x_2 + x_1x_4 + x_3x_4 + x_4$
$x_1x_2 + x_3 + x_1x_4 + x_4$
$x_1x_2 + x_3x_2 + x_3 + x_1x_4 + x_3x_4 + x_4$
$x_1 + x_2x_3 + x_3x_4 + x_4$
$x_2x_1 + x_4x_1 + x_1 + x_2x_3 + x_3x_4 + x_4$
$x_2x_1 + x_4x_1 + x_1 + x_3 + x_4$
$x_2x_1 + x_4x_1 + x_1 + x_2x_3 + x_3 + x_3x_4 + x_4$
$x_1 + x_2 + x_2x_3 + x_3x_4$
$x_2x_1 + x_4x_1 + x_1 + x_2 + x_2x_3 + x_3x_4$
$x_1 + x_2 + x_2x_3 + x_3 + x_3x_4$
$x_2x_1 + x_4x_1 + x_1 + x_2 + x_3$
$x_2x_1 + x_4x_1 + x_1 + x_2 + x_2x_3 + x_3 + x_3x_4$

Table 2 Set of Boolean functions S_G

$x_1x_2 + x_1x_3x_2 + x_3x_2 + x_1x_3 + x_1x_4 + x_1x_3x_4$
$x_1x_2 + x_1x_3x_2 + x_4x_2 + x_1x_3 + x_1x_4 + x_1x_3x_4 + x_3x_4 + x_4$
$x_1x_2 + x_1x_3x_2 + x_3x_2 + x_1x_3 + x_3 + x_1x_4 + x_1x_3x_4$
$x_1x_2 + x_1x_3x_2 + x_4x_2 + x_1x_3 + x_3 + x_1x_4 + x_1x_3x_4 + x_3x_4 + x_4$
$x_2x_1 + x_2x_3x_1 + x_3x_1 + x_3x_4x_1 + x_4x_1 + x_1 + x_2x_3$
$x_2x_1 + x_2x_3x_1 + x_3x_1 + x_3x_4x_1 + x_4x_1 + x_1 + x_2x_4 + x_3x_4 + x_4$
$x_2x_1 + x_2x_3x_1 + x_3x_1 + x_3x_4x_1 + x_4x_1 + x_1 + x_2x_3 + x_3$
$x_2x_1 + x_2x_3x_1 + x_3x_1 + x_3x_4x_1 + x_4x_1 + x_1 + x_3 + x_2x_4 + x_3x_4 + x_4$
$x_2x_3x_1 + x_3x_1 + x_3x_4x_1 + x_1 + x_2 + x_2x_4 + x_3x_4$
$x_2x_1 + x_2x_3x_1 + x_3x_1 + x_3x_4x_1 + x_4x_1 + x_1 + x_2 + x_2x_4 + x_3x_4$
$x_2x_3x_1 + x_3x_1 + x_3x_4x_1 + x_1 + x_2 + x_2x_3 + x_4$
$x_2x_1 + x_2x_3x_1 + x_3x_1 + x_3x_4x_1 + x_4x_1 + x_1 + x_2 + x_2x_3 + x_4$
$x_2x_3x_1 + x_3x_1 + x_3x_4x_1 + x_1 + x_2 + x_3 + x_2x_4 + x_3x_4$
$x_2x_1 + x_2x_3x_1 + x_3x_1 + x_3x_4x_1 + x_4x_1 + x_1 + x_2 + x_3 + x_2x_4 + x_3x_4$
$x_2x_3x_1 + x_3x_1 + x_3x_4x_1 + x_1 + x_2 + x_2x_3 + x_3 + x_4$
$x_2x_1 + x_2x_3x_1 + x_3x_1 + x_3x_4x_1 + x_4x_1 + x_1 + x_2 + x_2x_3 + x_3 + x_4$

Proof We first assume that S forms an LA-complementary set. Then $\sum_{f\in S}\mathcal{C}^p_{L,A,f}(\mathbf{v}) = 0$, for $\mathbf{v} \neq \mathbf{0}$. From Theorem 5, we know that $\mathcal{C}^p_{L,A,f}(\mathbf{v}) = \lambda_L(\mathbf{v})\sum_{\mathbf{u}\in\mathbb{F}_2^n}|\mathcal{U}_{L,A,f}(\mathbf{u})|^2(-1)^{\mathbf{v}\cdot\mathbf{u}}$, and using our assumption along with Theorem 10 we obtain (we divide throughout by $\lambda_L(\mathbf{v})$)

$$
\begin{aligned}
0 &= \sum_{\mathbf{u}\in\mathbb{F}_2^n}\sum_{f\in S}|\mathcal{U}_{L,A,f}(\mathbf{u})|^2(-1)^{\mathbf{v}\cdot\mathbf{u}} \\
&= \sum_{\substack{\mathbf{u}\in\mathbb{F}_2^n \\ \mathbf{a},\mathbf{b},\mathbf{c},\mathbf{d}\in\mathbb{F}_2^{k-1}}} (-1)^{(\mathbf{a},\mathbf{c})\cdot(\mathbf{b},\mathbf{d})}\zeta_{2^k}^{\iota(\mathbf{b})+\iota(\mathbf{d})}\sum_{f\in S}\mathcal{T}_{L,A,f_\mathbf{a}}(\mathbf{u})\mathcal{T}_{L,A,f_\mathbf{c}}(\mathbf{u})(-1)^{\mathbf{v}\cdot\mathbf{u}} \\
&= \sum_{\mathbf{a},\mathbf{b},\mathbf{c},\mathbf{d}\in\mathbb{F}_2^{k-1}} (-1)^{(\mathbf{a},\mathbf{c})\cdot(\mathbf{b},\mathbf{d})}\zeta_{2^k}^{\iota(\mathbf{b})+\iota(\mathbf{d})}\sum_{\mathbf{u}\in\mathbb{F}_2^n}\sum_{f\in S}\mathcal{T}_{L,A,f_\mathbf{a}}(\mathbf{u})\mathcal{T}_{L,A,f_\mathbf{c}}(\mathbf{u})(-1)^{\mathbf{v}\cdot\mathbf{u}} \\
&= \sum_{\mathbf{a},\mathbf{b},\mathbf{c},\mathbf{d}\in\mathbb{F}_2^{k-1}} (-1)^{(\mathbf{a},\mathbf{c})\cdot(\mathbf{b},\mathbf{d})}\zeta_{2^k}^{\iota(\mathbf{b})+\iota(\mathbf{d})}\sum_{f\in S}\mathcal{C}^p_{L,A,f_\mathbf{a},f_\mathbf{c}}(\mathbf{v}) \\
&= \sum_{\mathbf{d}\in\mathbb{F}_2^{k-1}}\left(\sum_{\mathbf{a},\mathbf{b},\mathbf{c}\in\mathbb{F}_2^{k-1}} (-1)^{(\mathbf{a},\mathbf{c})\cdot(\mathbf{b},\mathbf{d})}\zeta_{2^k}^{\iota(\mathbf{b})}\sum_{f\in S}\mathcal{C}^p_{L,A,f_\mathbf{a},f_\mathbf{c}}(\mathbf{v})\right)\zeta_{2^k}^{\iota(\mathbf{d})},
\end{aligned}
$$

and since $\{\zeta_{2^k}^{\iota(\mathbf{d})}\}_{\mathbf{d}\in\mathbb{F}_2^{k-1}}$ is a basis of $\mathbb{Q}(\zeta_{2^k})$, then, for all $\mathbf{d} \in \mathbb{F}_2^{k-1}$,

$$
\begin{aligned}
0 &= \sum_{\mathbf{a},\mathbf{b},\mathbf{c}\in\mathbb{F}_2^{k-1}} (-1)^{(\mathbf{a},\mathbf{c})\cdot(\mathbf{b},\mathbf{d})}\zeta_{2^k}^{\iota(\mathbf{b})}\sum_{f\in S}\mathcal{C}^p_{L,A,f_\mathbf{a},f_\mathbf{c}}(\mathbf{v}) \\
&= \sum_{\mathbf{b}\in\mathbb{F}_2^{k-1}}\left(\sum_{\mathbf{a},\mathbf{c}\in\mathbb{F}_2^{k-1}} (-1)^{(\mathbf{a},\mathbf{c})\cdot(\mathbf{b},\mathbf{d})}\sum_{f\in S}\mathcal{C}^p_{L,A,f_\mathbf{a},f_\mathbf{c}}(\mathbf{v})\right)\zeta_{2^k}^{\iota(\mathbf{b})},
\end{aligned}
$$

which, by the same reason as above, renders, for all $\mathbf{b}, \mathbf{d} \in \mathbb{F}_2^{k-1}$,

$$\sum_{\mathbf{a},\mathbf{c}\in\mathbb{F}_2^{k-1}} (-1)^{(\mathbf{a},\mathbf{c})\cdot(\mathbf{b},\mathbf{d})} \sum_{f\in S} \mathcal{C}^p_{L,A,f_\mathbf{a},f_\mathbf{c}}(\mathbf{v}) = 0.$$

Inverting the previous equation using Lemma 11, we obtain $\sum_{f\in S} \mathcal{C}^p_{L,A,f_\mathbf{a},f_\mathbf{c}}(\mathbf{v}) = 0$. The reciprocal follows easily from the identity

$$\begin{aligned}\sum_{f\in S} \mathcal{C}^p_{L,A,f}(\mathbf{v}) &= \lambda_L(\mathbf{v}) \sum_{\mathbf{u}\in\mathbb{F}_2^n} \sum_{f\in S} |\mathcal{U}_{L,A,f}(\mathbf{u})|^2 (-1)^{\mathbf{v}\cdot\mathbf{u}} \\ &= \lambda_L(\mathbf{v}) \sum_{\mathbf{a},\mathbf{b},\mathbf{c},\mathbf{d}\in\mathbb{F}_2^{k-1}} (-1)^{(\mathbf{a},\mathbf{c})\cdot(\mathbf{b},\mathbf{d})} \zeta_{2^k}^{\iota(\mathbf{b})+\iota(\mathbf{d})} \sum_{f\in S} \mathcal{C}^p_{L,A,f_\mathbf{a},f_\mathbf{c}}(\mathbf{v}).\end{aligned}$$

The theorem is shown. □

Corollary 14 *Let $\{f, g\}$ be two generalized Boolean functions in $\mathcal{GB}_n^{2^k}$. Then $\{f, g\}$ forms an P-complementary (respectively, N-complementary) pair if and only if for all $\boldsymbol{a}, \boldsymbol{c} \in \mathbb{F}_2^{k-1}$, $\{f_a, f_c\}$ and $\{g_a, g_c\}$ form a (binary) P-crosscomplementary (respectively, N-crosscomplementary) pair.*

5 Transforms and complementary constructions

It is well known [12] that a Boolean function f has flat spectrum with respect to the nega-Hadamard spectrum if $f + s_2$ (where s_2 is the quadratic elementary symmetric polynomial) has flat spectrum with respect to the Walsh-Hadamard transform. Thus, it is natural to ask whether some connection exists between the Walsh-Hadamard and the nega-Hadamard transforms defined on generalized Boolean functions. To that effect, we show the first claim of our next result (see [1] for the particular case of $k = 1$). We can also relate the root-Hadamard transform and the generalized Hadamard transform.

We let $A = \{\alpha_1, \ldots, \alpha_r\}$ be a set of roots of unity $\alpha_j = e^{\frac{2\pi i}{k_j}}$ such that $k_j = 2^{m_j}$, $m_j \leq k$, $K = \{k_j\}_{1\leq j\leq r}$ and $L = \{R_s\}_{s\in K}$ be a partition of the index set $\{0, \ldots, n-1\} = \bigsqcup_{s\in K} R_s$, $|L| = |K| = r$. For $J \subseteq K$, we let A_J be A with α_s replaced by 1 for all $s \in J$. Let $s_1(\mathbf{x}) = \bigoplus_{j=1}^{n} x_j$, $s_2(\mathbf{x}) = \bigoplus_{1\leq j<k\leq n} x_j x_k$, and in general $s_t(\mathbf{x}) = \bigoplus_{1\leq j_1<\ldots<j_t\leq n} x_{j_1}\cdots x_{j_1}$ be the symmetric polynomials of degree 1, 2, t, respectively, all reduced modulo 2. We will use here Lemma 5 from [17]:

Lemma 15 ([17]) *Let $\mathbf{x} \in \mathbb{V}_n$. Then,*

$$\begin{aligned} wt(\mathbf{x}) \pmod 4 &= s_1(\mathbf{x}) + 2s_2(\mathbf{x}) \\ wt(\mathbf{x}) \pmod{2^k} &= wt(\mathbf{x}) \pmod{2^{k-1}} + 2^{k-1} s_{2^{k-1}}(\mathbf{x}) \end{aligned}$$

Theorem 16 *We have:*

(*i*) *Let $n \geq 1$, $k \geq 1$, $f \in \mathcal{GB}_n^{2^k}$ and $g \in \mathcal{GB}_n^{2^{k+1}}$ defined by $g(\mathbf{x}) = 2f(\mathbf{x}) + 2^{k-1}s_1(\mathbf{x}) + 2^k s_2(\mathbf{x})$ (the sum is taken modulo 2^{k+1}). Then, $\mathcal{N}_f^{(2^k)}(\boldsymbol{u}) = \mathcal{H}_g^{(2^{k+1})}(\boldsymbol{u})$, for all $\boldsymbol{u} \in \mathbb{F}_2^n$.*

(*ii*) *Let* $n \geq 1$, $k \geq 1$, $f, h_K, h_J \in \mathcal{GB}_n^{2^k}$ *defined by* $h_K(\mathbf{x}) = f(\mathbf{x}) - \sum_{s\in K} 2^{k-m_s} \sum_{j=0}^{s-1} s_{2^j}(\mathbf{x}_{R_s})$, $h_J(\mathbf{x}) = f(\mathbf{x}) - \sum_{s\in J} 2^{k-m_s} \sum_{j=0}^{s-1} s_{2^j}(\mathbf{x}_{R_s})$ (*the sum is taken modulo* 2^k), *where* $\mathbf{x}_{R_s}$ *is the restriction of* $\mathbf{x}$ *to the indices in* R_s. *Then,*

$$\mathcal{U}_{L,A,h_K}^{(2^k)}(\boldsymbol{u}) = \mathcal{H}_f^{(2^k)}(\boldsymbol{u}) \text{ and } \mathcal{U}_{L,A,h_J}^{(2^k)}(\boldsymbol{u}) = \mathcal{U}_{L,A_J,f}^{(2^k)}(\boldsymbol{u}), \text{ for all } \boldsymbol{u} \in \mathbb{F}_2^n.$$

Proof We compute

$$\begin{aligned}
\mathcal{H}_g^{(2^{k+1})}(\mathbf{u}) &= 2^{-n/2} \sum_{\mathbf{x}\in\mathbb{F}_2^n} \zeta_{2^{k+1}}^{g(\mathbf{x})} (-1)^{\mathbf{u}\cdot\mathbf{x}} \\
&= 2^{-n/2} \sum_{\mathbf{x}\in\mathbb{F}_2^n} \zeta_{2^k}^{f(\mathbf{x})} (-1)^{\mathbf{u}\cdot\mathbf{x}} i^{s_1(\mathbf{x})+2s_2(\mathbf{x})} \\
&= 2^{-n/2} \sum_{\mathbf{x}\in\mathbb{F}_2^n} \zeta_{2^k}^{f(\mathbf{x})} (-1)^{\mathbf{u}\cdot\mathbf{x}} i^{wt(\mathbf{x})} = \mathcal{N}_f^{(2^k)}(\mathbf{u}).
\end{aligned}$$

The two claims of (*ii*) are similar so we will show only the first part. Note that, by Lemma 15, $wt(\mathbf{x}) \pmod{2^s} = \sum_{j=0}^{s-1} s_{2^j}(\mathbf{x})$. We compute

$$\begin{aligned}
\mathcal{U}_{L,A,h_K}^{(2^k)}(\mathbf{u}) &= 2^{-n/2} \sum_{\mathbf{x}\in\mathbb{F}_2^n} \zeta_{2^k}^{g(\mathbf{x})} (-1)^{\mathbf{u}\cdot\mathbf{x}} \lambda_L(\mathbf{x}) \\
&= 2^{-n/2} \sum_{\mathbf{x}\in\mathbb{F}_2^n} \zeta_{2^k}^{f(\mathbf{x}) - \sum_{s\in K} 2^{k-m_s} \sum_{j=0}^{s-1} s_{2^j}(\mathbf{x}_{R_s})} (-1)^{\mathbf{u}\cdot\mathbf{x}} \prod_{s\in K} \alpha_s^{wt(\mathbf{x}_{R_s})} \\
&= 2^{-n/2} \sum_{\mathbf{x}\in\mathbb{F}_2^n} \zeta_{2^k}^{f(\mathbf{x})} \prod_{s\in K} \alpha_s^{-wt(\mathbf{x}_{R_s})} (-1)^{\mathbf{u}\cdot\mathbf{x}} \prod_{s\in K} \alpha_s^{wt(\mathbf{x}_{R_s})} \\
&= 2^{-n/2} \sum_{\mathbf{x}\in\mathbb{F}_2^n} \zeta_{2^k}^{f(\mathbf{x})} (-1)^{\mathbf{u}\cdot\mathbf{x}} = \mathcal{H}_f^{(2^k)}(\mathbf{u}),
\end{aligned}$$

and the theorem is shown. □

Two of us introduced the next concept in [14]. We call a function $f \in \mathcal{GB}_n^q$ a *landscape* function if there exist $t \geq 1$, $m_i \in \mathbb{N}_0$, $\ell_i \in 2\mathbb{N}_0 + 1$, $1 \leq i \leq t$, such that

$$\{|\mathcal{H}_f(\mathbf{u})|\}_{\mathbf{u}\in \mathrm{supp}(\mathcal{H}_f)} = \{2^{\frac{m_1}{2}} \ell_1, \ldots, 2^{\frac{m_t}{2}} \ell_t\}.$$

We call the set of pairs $\{(m_1, \ell_1), (m_2, \ell_2), \ldots\}$, the *levels* of f, and $t+1$ (if 0 belongs to the Walsh-Hadamard spectrum), or t (if 0 is not in the spectrum) the *length* of f.

We can deduce this corollary (the second claim of the next result was also shown in [1]).

Corollary 17 *Let* $f, h \in \mathcal{B}_n$, *where* $h(\mathbf{x}) = f(\mathbf{x}) + s_2(\mathbf{x})$. *If* n *is even, then* f *is negabent if and only if* h *is bent. Furthermore,* f *is negaplateaued if and only if* h *is plateaued. In general,* f *is negalandscape* (*defined as above, via the nega-Hadamard transform*) *if and only if* h *is landscape.*

Proof By Theorem 16 (*i*), for $k = 1$, we have that if $f \in \mathcal{B}_n$ and $g \in \mathcal{GB}_n^4$ defined by $g(\mathbf{x}) = 2f(\mathbf{x}) + s_1(\mathbf{x}) + 2s_2(\mathbf{x})$, then, $\mathcal{N}_f^{(2)}(\mathbf{u}) = \mathcal{H}_g^{(4)}(\mathbf{u})$, for all $\mathbf{u} \in \mathbb{F}_2^n$. Since the decomposition of g is $g(\mathbf{x}) = a_0(\mathbf{x}) + 2a_1(\mathbf{x})$, where $a_0(\mathbf{x}) = s_1(\mathbf{x})$, and $a_1(\mathbf{x}) = f(\mathbf{x}) + s_2(\mathbf{x})$, this implies, by [10], that, when n is even, g is gbent if and only if a_1 and $a_0 + a_1$ are bent Boolean

functions. This implies that g is gbent if and only if $f+s_2$ and s_1+f+s_2 are bent Boolean functions. Since s_1 is a linear Boolean function, this implies that f is negabent if and only if $h=f+s_2$ is bent, giving yet another proof to this known result [12].

Further, by Corollary 1 of [14], we see that, if $g:\mathbb{F}_2^n\to\mathbb{Z}_{2^k}$ is a function given by $g(\mathbf{x})=a_0(\mathbf{x})+2a_1(\mathbf{x})+\cdots+2^{k-1}a_{k-1}$, and $s\geq 0$ is an integer, then, g is s-gplateaued if and only if, for each $\mathbf{c}\in\mathbb{F}_2^{k-1}$, the Boolean function $g_{\mathbf{c}}$ defined as $g_{\mathbf{c}}(\mathbf{x})=\mathbf{c}\cdot(a_0(\mathbf{x}),\ldots,a_{k-2}(\mathbf{x}))+a_{k-1}(\mathbf{x})$ is an s-plateaued (if $n+s$ is even), respectively, an $(s+1)$-plateaued function (if $n+s$ is odd), with some extra conditions on the Walsh-Hadamard coefficients. In particular, taking $k=1$, this implies that f is negaplateaued if and only if $f+s_1+s_2$ is plateaued (no extra conditions on the Walsh-Hadamard coefficients), which again implies that $f+s_2$ is plateaued.

Using Theorem 3.2 of [14], this argument can be also extended to landscape functions, in a similar way as in the plateaued case. □

6 Further comments

In this paper we defined a class of transforms which generalize many others, like generalizes the Walsh-Hadamard, nega-Hadamard, 2^k-Hadamard [17], consta-Hadamard [11] and HN-transforms. For generalized Boolean functions, we describe its behavior on the binary components. Further, we define a notion of complementarity (in the spirit of the Golay sequences) with respect to this transform and furthermore, we describe the complementarity of a generalized Boolean set with respect to the binary components of the elements of that set. Some concrete examples are provided.

There are many questions one can ask on the new transforms. For example, it would be interesting to provide more constructions of root-bent and more generally, root-plateaued functions (surely, Theorem 16 may help). Certainly, finding connections between these transforms, their values, and (relative) difference sets would be quite interesting, as well.

Acknowledgments The authors express their deep appreciation to the editors for promptly handling our paper, as well as to the anonymous referees, whose thorough reading and constructive comments have improved the paper. The research of the first named author was supported by The Puerto Rico Science, Technology and Research Trust under agreement number 2020-00124. This content is only the responsibility of the authors and does not necesarily represent the official views of The Puerto Rico Science, Technology and Research Trust.

References

1. Anbar, N., Kaşikci, C., Meidl, W., Topuzoğlu, A.: Shifted plateaued functions and their differential properties. Cryptogr. Commun. (2020)
2. Carlet, C.: Boolean functions for cryptography and error correcting codes, chapter of the volume. In: Crama, Y., Hammer, P. (eds.) Boolean Models and Methods in Mathematics, Computer Science, and Engineering, pp. 257–397. Cambridge University Press (2010)
3. Cusick, T.W., Stănică, P.: Cryptographic Boolean functions and applications. Elsevier–Academic Press, Cambridge (2017)
4. Davis, J.A., Jedwab, J.: Peak-to-mean power control in OFDM, Golay complementary sequences, and Reed-Muller codes. IEEE Trans. Inf. Theory **45**, 2397–2417 (1999)
5. Fiedler, F., Jedwab, J., Parker, M.G.: A framework for the construction of Golay sequences. IEEE Trans. Inf. Theory **54**, 3114–3129 (2008)
6. Golay, M.J.E.: Multislit spectrometry. J. Optical Soc. Amer. **39**, 437–444 (1949)

7. Golay, M.J.E.: Static multislit spectrometry its application to the panoramic display of infrared spectra. J Optical Soc. Amer. **41**, 468–472 (1951)
8. Jedwab, J., Parker, M.: Golay complementary array pairs. Des Codes Cryptogr **44**, 209–216 (2007)
9. MacWilliams, F.J., Sloane, N.J.A.: The Theory of Error Correcting Codes. North-Holland, Amsterdam (1977)
10. Martinsen, T., Meidl, W., Mesnager, S., Stănică, P.: Decomposing generalized bent and hyperbent functions. IEEE Trans. Inf. Theory **63**, 7804–7812 (2017)
11. Parker, M.G.: The constabent properties of Golay-Davis-Jedwab sequences. Int. Symp. Inf. Theory, Sorrento, p. 302 (2000)
12. Parker, M.G., Pott, A.: On Boolean functions which are bent and negabent. In: Golomb, S.W., Gong, G., Helleseth, T., Song, H.Y. (eds.) Sequences, Subsequences, and Consequences, SSC 2007 LNCS, vol. 4893, pp. 9–23 (2007)
13. Riera, C., Parker, M.G.: Generalized bent criteria for Boolean functions. IEEE Trans. Inf. Theory **52**(9), 4142–4159 (2006)
14. Riera, C., Stănică, P.: Landscape Boolean functions. Adv. Math. Communication **13**(4), 613–627 (2019)
15. Rothaus, O.S.: On bent functions. J. Combin. Theory–Ser. A **20**, 300–305 (1976)
16. Schmidt, K.-U.: On Spectrally Bounded Codes for Multicarrier Communications, Techn. Univ Dresden, Dr. Diss. (2007)
17. Stănică, P.: Weak and strong 2^k-bent functions. IEEE Trans. Inf. Theory **62**(5), 2827–2835 (2016)
18. Stănică, P., Martinsen, T., Gangopadhyay, S., Singh, B.K.: Bent and generalized bent Boolean functions. Designs Codes Cryptogr. **69**, 77–94 (2013)
19. Stănică, P., Gangopadhyay, S., Chaturvedi, A., Gangopadhyay, A.K., Maitra, S.: Investigations on bent and negabent functions via the nega-Hadamard transform. IEEE Trans. Inf. Theory **58**(6), 4064–4072 (2012)
20. Tang, C., Xiang, C., Qi, Y., Feng, K.: Complete characterization of generalized bent and 2^k-bent Boolean functions. IEEE Trans. Inf. Theory **63**, 4668–4674 (2017)
21. Tseng, C., Liu, C.: Complementary sets of sequences. IEEE Trans. Inf. Theory **18**, 644–665 (1972)