Boolean Functions Whose Restrictions are Highly Nonlinear

Constanza Riera
Høgskolen i Bergen
Nygårdsgt. 112
Bergen 5008, Norway
Email: csr@hib.no

Matthew G. Parker
Selmer Centre, Inst. for Informatikk
University of Bergen
Bergen 5020, Norway
Email: matthew@ii.uib.no

***Abstract*—We construct Boolean functions whose non-trivial restrictions are either highly nonlinear with respect to the Walsh-Hadamard or the negahadamard transform. We generalise these properties, identify group actions that preserve them, and obtain complementary sets from our functions.**

I. Introduction

This paper investigates spectral properties of basic classes of Boolean function. Typical cryptanalysis considers Walsh-Hadamard spectra of Boolean functions, and we examine spectra with respect to more general transform sets. This is one in a series of papers that tackles such ideas [2], [4], [8]–[10]. We also propose two new types of multivariate complementary set to add to the one proposed in [7]. The first construction generates Boolean functions whose restrictions remain highly nonlinear with respect to the Walsh-Hadamard transform (WHT). We then modify the construction so that, instead, the restrictions remain highly nonlinear with respect to the negahadamard transform (NHT). Re-expressing these results in terms of unitary matrices facilitates a significant generalisation, where each of the two constructions is shown to retain its spectral properties with respect to an infinite class of unitary transforms. We highlight unitary group actions that preserve the spectral properties of the two constructions, and show that each of the two constructions leads to a new type of multivariate complementary set.

II. Background

Denote the set of Boolean functions in m variables by $\mathcal{B}_m$. Let $S \subset \{0,1,\ldots,m-1\} := \{s_0, s_1, \ldots, s_{t-1}\}$ be an ordered set of size $t \le m$, and let $\bar{S} := \{0,1,\ldots,m-1\} \setminus S$. Let $x_S := (x_{s_0}, x_{s_1}, \ldots, x_{s_{t-1}}) \in \mathbb{F}_2^t$. For $f \in \mathcal{B}_m$, and $a \in \mathbb{F}_2^t$, a constant, the *restriction* of $f(x)$ to $x_S = a$ is denoted by $f_{a,S} \in \mathcal{B}_{m-t}$, and satisfies $f_{a,S}(x_{\bar{S}}) = f(x)$ if $x_S = a$, and is undefined otherwise. The Walsh-Hadamard spectrum of $f_{a,S}$ is defined as

$$\grave{\mathcal{F}}^H_{a,S}(w) := 2^{\frac{t-m}{2}} \sum_{x \in \mathbb{F}_2^{m-t}} (-1)^{f_{a,S}(x) + x \cdot w}, \qquad (1)$$

where $w \in \mathbb{F}_2^{m-t}$, and $x \cdot w := \sum_{i=0}^{m-1} x_i w_i$. Denote $\grave{\mathcal{F}}^H_S := \{\grave{\mathcal{F}}^H_{a,S} \mid \forall a \in \mathbb{F}_2^t\}$ as the set of 2^t Walsh-Hadamard spectra of the restrictions of $f(x)$ to x_S. The nonlinearity of $f_{a,S}$ is given by

$$\text{nl}(f_{a,S}) := 2^{m-t-1} - 2^{\frac{m-t}{2}-1} \max_{w \in \mathbb{F}_2^{m-t}} |\grave{\mathcal{F}}^H_{a,S}(w)|.$$

'nl' is not so useful for comparing nonlinearities over all choices of S, so instead we propose *peak-to-average power ratio*, $\mathcal{P}_H(\grave{f})$, where $\grave{f} := (-1)^f$,

$$\mathcal{P}_H(\grave{f}_{a,S}) := \max_{w \in \mathbb{F}_2^{m-t}} \left(|\grave{\mathcal{F}}^H_{a,S}(w)|^2 \right),$$

and

$$\text{nl}(f_{a,S}) = 2^{\frac{m-t}{2}-1} \left(2^{\frac{m-t}{2}} - \sqrt{\mathcal{P}_H(\grave{f}_{a,S})} \right).$$

Define peak-to-average power ratio over all restrictions of $\grave{f}$ by

$$\mathcal{P}^r_H(\grave{f}) := \max_{a \in \mathbb{F}_2^{|S|}, S \subset \{0,1,\ldots,m-1\}} \left(\mathcal{P}_H(\grave{f}_{a,S}) \right),$$

where $1 \le \mathcal{P}^r_H(\grave{f}) \le 2^m$. *Construction* $\mathbb{III}$ generates functions, $f' \in \mathcal{B}_n$, from functions, $f \in \mathcal{B}_m$, $n > m$, that satisfy $\mathcal{P}^r_H(\grave{f}') \le 2^m$, irrespective of the size of n relative to m [1].

III. Constructions

A. *Construction* $\mathbb{III}$

Let $K := \{K_0, K_1, \ldots, K_{m-1}\}$ be an m-wise partition of $\{0,1,\ldots,n-1\}$, where $\bigcup_{i=0}^{m-1} K_i = \{0,1,\ldots,n-1\}$, and $K_i \cap K_j = \emptyset$, $i \ne j$. Let $k := (k_0, k_1, \ldots, k_{m-1})$, $k_j := |K_j|$, $\forall j$, $\mathcal{K}_j := \sum_{i,l \in K_j, i<l} x_i x_l \in \mathcal{B}_n$, and $\mathcal{K} := \sum_{j=0}^{m-1} \mathcal{K}_j$. Let $y := (y_0, y_1, \ldots, y_{m-1})$, where $y_j := \sum_{i \in K_j} x_i, 0 \le j < m$. For $f \in \mathcal{B}_m$, define the *expansion* of f with respect to K by

$$\langle f \rangle_K := f(y) \in \mathcal{B}_n,$$

and abbreviate to $\langle f \rangle$ if K is clear from context.

$$\textbf{Construction } \mathbb{III}: \qquad f'(x) = \langle f \rangle + \mathcal{K}. \qquad (2)$$

[1] *Construction* '$\mathbb{I}$' is reserved for functions described in [7].

For f' so constructed, we can show that

$$\mathcal{P}^r_H(\grave{f}') = \mathcal{P}^r_H(\grave{f}) \leq 2^m. \qquad (3)$$

We defer proofs of (3) and (6) until the end of section IV. For $n \gg m$, Construction $\mathbb{II}$ generates functions, f', whose nontrivial restrictions are highly nonlinear with respect to the WHT. Proposition 38 of [1] is a sub-case of Construction $\mathbb{II}$, where $\deg(f) \leq 2$, and all k_j are equal.

Example: Let $f := x_0x_1 + x_1x_2 \in \mathcal{B}_3$. Then $f_{-,\emptyset} = f$, $f_{0,\{0\}} = x_1x_2$, $f_{1,\{0\}} = x_1x_2 + x_1$, $f_{0,\{1\}} = 0$, $f_{1,\{1\}} = x_0 + x_2$, $f_{0,\{2\}} = x_0x_1$, $f_{1,\{2\}} = x_0x_1 + x_1$, $f_{00,\{0,1\}} = f_{10,\{0,1\}} = f_{00,\{0,2\}} = f_{11,\{0,2\}} = f_{01,\{1,2\}} = 0$, $f_{01,\{0,1\}} = x_2$, $f_{11,\{0,1\}} = x_2 + 1$, $f_{10,\{0,2\}} = f_{01,\{0,2\}} = x_1$, $f_{10,\{1,2\}} = x_0$, $f_{11,\{1,2\}} = x_0+1$, $f_{000,\{0,1,2\}} = f_{100,\{0,1,2\}} = f_{010,\{0,1,2\}} = f_{001,\{0,1,2\}} = f_{101,\{0,1,2\}} = f_{111,\{0,1,2\}} = 0$, $f_{110,\{0,1,2\}} = f_{011,\{0,1,2\}} = 1$.

Computations give, $\forall a$, $\mathcal{P}_H(\grave{f}_{-,\emptyset}) = \mathcal{P}_H(\grave{f}_{a,\{0,1\}}) = \mathcal{P}_H(\grave{f}_{a,\{0,2\}}) = \mathcal{P}_H(\grave{f}_{a,\{1,2\}}) = 2$, $\mathcal{P}_H(\grave{f}_{a,\{0\}}) = \mathcal{P}_H(\grave{f}_{a,\{2\}}) = \mathcal{P}_H(\grave{f}_{a,\{0,1,2\}}) = 1$, $\mathcal{P}_H(\grave{f}_{a,\{1\}}) = 4$. So $\mathcal{P}^r_H(\grave{f}) = 4$.

Let $K := \{0,3\}\{1,4\}\{2,5\}$. Then, by (2), $\langle f \rangle = (x_0 + x_3)(x_1 + x_4) + (x_1 + x_4)(x_2 + x_5)$, $\mathcal{K} = x_0x_3 + x_1x_4 + x_2x_5$, and $f' = x_0x_1 + x_0x_3 + x_0x_4 + x_1x_2 + x_1x_3 + x_1x_4 + x_1x_5 + x_2x_4 + x_2x_5 + x_3x_4 + x_4x_5$. One can verify that $\mathcal{P}^r_H(\grave{f}') = \mathcal{P}^r_H(\grave{f}) = 4$, in agreement with (3).

B. Construction $\mathbb{III}$

Define the *negahadamard* spectrum of $f_{a,S}$ as

$$\grave{\mathcal{F}}^N_{a,S}(w) := 2^{\frac{t-m}{2}} \sum_{x \in \mathbb{F}_2^{m-t}} i^{2(f_{a,S}(x) + x \cdot w) + \text{ wt}(x)}, \qquad (4)$$

where $i := \sqrt{-1}$ and 'wt(.)' denotes Hamming weight. Denote $\grave{\mathcal{F}}^N_S := \{\grave{\mathcal{F}}^N_{a,S} \mid \forall a \in \mathbb{F}_2^t\}$ as the set of 2^t negahadamard spectra of the restrictions of $f(x)$ to x_S. Define *peak-to-average power ratio* of $\grave{f}_{a,S}$ with respect to the NHT by,

$$\mathcal{P}_N(\grave{f}_{a,S}) := \max_{w \in \mathbb{F}_2^{m-t}} \left(|\grave{\mathcal{F}}^N_{a,S}(w)|^2 \right),$$

and peak-to-average power ratio over all restrictions of $\grave{f}$ by

$$\mathcal{P}^r_N(\grave{f}) := \max_{a \in \mathbb{F}_2^{|S|}, S \subset \{0,1,\ldots,m-1\}} \left(\mathcal{P}_N(\grave{f}_{a,S}) \right),$$

where $1 \leq \mathcal{P}^r_N(\grave{f}) \leq 2^{m-1}$.

$$\textbf{Construction } \mathbb{III}\textbf{:} \qquad \langle f \rangle. \qquad (5)$$

For $\langle f \rangle \in \mathcal{B}_n$, we can show that

$$\mathcal{P}^r_N(\langle \grave{f} \rangle) = \mathcal{P}^r_N(\grave{f}) \leq 2^{m-1}. \qquad (6)$$

So, for $n \gg m$, Construction $\mathbb{III}$ generates functions, f', whose restrictions are highly nonlinear with respect to the NHT.

Example (continued): Computations give, $\forall a$, $\mathcal{P}_N(\grave{f}_{a,\{0\}}) = \mathcal{P}_N(\grave{f}_{a,\{2\}}) = 2$, $\mathcal{P}_N(\grave{f}_{-,\emptyset}) = \mathcal{P}_N(\grave{f}_{a,\{1\}}) = \mathcal{P}_N(\grave{f}_{a,\{0,1\}}) = \mathcal{P}_N(\grave{f}_{a,\{0,2\}}) = \mathcal{P}_N(\grave{f}_{a,\{1,2\}}) = \mathcal{P}_N(\grave{f}_{a,\{0,1,2\}}) = 1$. So $\mathcal{P}^r_N(\grave{f}) = 2$.
One can verify that $\mathcal{P}^r_N(\langle \grave{f} \rangle) = \mathcal{P}^r_N(\grave{f}) = 2$, in agreement with (6).

In section V we establish peak-to-average properties of Constructions $\mathbb{II}$ and $\mathbb{III}$ with respect to an infinitely larger set of transforms than just WHT and NHT. To do so we first recast $\grave{\mathcal{F}}^H_S$ and $\grave{\mathcal{F}}^N_S$ in terms of unitary [2] matrices. This clarifies subsequent generalisations.

IV. Matrix characterisation

Interpret $\grave{f} = (-1)^f$ as an m-variate array, $\grave{f} \in (\mathbb{C}^2)^{\otimes m}$, with elements indexed by members of $\mathbb{F}_2^m$, i.e. $\grave{f}_j := (-1)^{f(j)}$, $j \in \mathbb{F}_2^m$. Define unitary matrices $H := \frac{1}{\sqrt{2}}\left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)$, and $I := \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Comparing with (1), the WHT of $f_{a,s} \in (\mathbb{C}^2)^{\otimes m-t}$ is given by

$$\grave{\mathcal{F}}^H_{a,S} := H^{\otimes m-t} \grave{f}_{a,S}, \qquad (7)$$

where $\grave{\mathcal{F}}^H_{a,S} \in (\mathbb{C}^2)^{\otimes m-t}$, and $H^{\otimes l} = \bigotimes_{i=0}^{l-1} H$ is the l-fold tensor product of H with itself, such that the wth element of $\grave{\mathcal{F}}^H_{a,S}$ is given by $\grave{\mathcal{F}}^H_{a,S,w} = \grave{\mathcal{F}}^H_{a,S}(w)$, $w \in \mathbb{F}_2^{m-t}$.

Let $2^m \times 2^m$ unitary, U_j, denote m-fold tensor product $U_j := I \otimes I \otimes \ldots \otimes U \otimes \ldots \otimes I$, with 2×2 unitary, U, being in the jth position from the left (numbering from zero). For $S \subset \{0,1,\ldots,m-1\}$, let $U_S := \prod_{j \in S} U_j$, [3] . Then $\grave{\mathcal{F}}^H_S \in (\mathbb{C}^2)^{\otimes m}$, the concatenation of $\grave{\mathcal{F}}^H_{a,S}$, $\forall a \in \mathbb{F}_2^t$, is given by

$$\grave{\mathcal{F}}^H_S := H_{\bar{S}} \grave{f} = (\grave{\mathcal{F}}^H_{a,S}, \forall a \in \mathbb{F}_2^t), \qquad (8)$$

and

$$\mathcal{P}^r_H(\grave{f}) := \max_{S \subset \{0,1,\ldots,m-1\}, w \in \mathbb{F}_2^m} \left(|\grave{\mathcal{F}}^H_{S,w}|^2 \right).$$

Example (continued): For $S = \{0,2\}$,

$$\begin{aligned}
\grave{\mathcal{F}}^H_{00,S} &= H\grave{f}_{00,S} &&= H \left(\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right) &&= \left(\begin{smallmatrix} \sqrt{2} \\ 0 \end{smallmatrix}\right) \\
\grave{\mathcal{F}}^H_{10,S} &= H\grave{f}_{10,S} &&= H \left(\begin{smallmatrix} 1 \\ -1 \end{smallmatrix}\right) &&= \left(\begin{smallmatrix} 0 \\ \sqrt{2} \end{smallmatrix}\right) \\
\grave{\mathcal{F}}^H_{01,S} &= H\grave{f}_{01,S} &&= H \left(\begin{smallmatrix} 1 \\ -1 \end{smallmatrix}\right) &&= \left(\begin{smallmatrix} 0 \\ \sqrt{2} \end{smallmatrix}\right) \\
\grave{\mathcal{F}}^H_{11,S} &= H\grave{f}_{11,S} &&= H \left(\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right) &&= \left(\begin{smallmatrix} \sqrt{2} \\ 0 \end{smallmatrix}\right).
\end{aligned}$$

Therefore,

$$\begin{aligned}
\grave{\mathcal{F}}^H_S &= H_{\bar{S}} \grave{f} \\
&= \frac{1}{\sqrt{2}} \begin{pmatrix}
1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\
1 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & -1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 1 & 0 & -1 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & -1
\end{pmatrix}
\begin{pmatrix} 1 \\ 1 \\ 1 \\ -1 \\ 1 \\ 1 \\ -1 \\ 1 \end{pmatrix} \\
&= \sqrt{2}\,(1,0,0,1,0,1,1,0)^T.
\end{aligned}$$

Similarly, for $S = \{1\}$, we get $\grave{\mathcal{F}}^H_S = 2\,(1,0,0,0,0,0,0,1)^T$. Computing over all subsets, S, we establish, as before, that $\mathcal{P}^r_H(\grave{f}) = 4$, where the maximum occurs for $S = \{1\}$.

[2] A unitary matrix, U, satisfies $UU^\dagger = I$ for I the identity.

[3] $(A \otimes B)(C \otimes D) = AC \otimes BD$, so $U_jU'_k = I \otimes I \otimes \ldots \otimes U \otimes \ldots \otimes U' \otimes \ldots I = U'_kU_j$, for $j \neq k$, and U, U' 2×2 unitaries.

Define unitary $N := \frac{1}{\sqrt{2}}\left(\begin{smallmatrix} 1 & i \\ 1 & -i \end{smallmatrix}\right)$. Comparing with (4), the NHT of $f_{a,s} \in (\mathbb{C}^2)^{\otimes m-t}$ is given by

$$\grave{\mathcal{F}}^N_{a,S} := N^{\otimes m-t}\grave{f}_{a,S}, \tag{9}$$

The concatenation of $\grave{\mathcal{F}}^N_{a,S}$, $\forall a \in \mathbb{F}_2^t$, is given by

$$\grave{\mathcal{F}}^N_S := N_{\bar{S}}\grave{f} = (\grave{\mathcal{F}}^N_{a,S}, \forall a \in \mathbb{F}_2^t), \tag{10}$$

and

$$\mathcal{P}^r_N(\grave{f}) := \max_{S\subset\{0,1,\ldots,m-1\},w\in\mathbb{F}_2^m}\left(|\grave{\mathcal{F}}^N_{S,w}|^2\right).$$

Example (continued): For $S = \{2\}$,

$$\begin{aligned}\grave{\mathcal{F}}^N_{0,S} = N^{\otimes 2}\grave{f}_{0,S} &= N^{\otimes 2}\begin{pmatrix} 1 \\ 1 \\ 1 \\ -1 \end{pmatrix} = \begin{pmatrix} 1+i \\ 0 \\ 0 \\ 1-i \end{pmatrix} \\ \grave{\mathcal{F}}^N_{1,S} = N^{\otimes 2}\grave{f}_{1,S} &= N^{\otimes 2}\begin{pmatrix} 1 \\ 1 \\ -1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1-i \\ 1+i \\ 0 \end{pmatrix}.\end{aligned}$$

Therefore,

$$\begin{aligned}\grave{\mathcal{F}}^N_S &= N_{\bar{S}}\grave{f} \\ &= \frac{1}{2}\begin{pmatrix} 1 & i & i & -1 & 0 & 0 & 0 & 0 \\ 1 & -i & i & 1 & 0 & 0 & 0 & 0 \\ 1 & i & -i & 1 & 0 & 0 & 0 & 0 \\ 1 & -i & -i & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & i & i & -1 \\ 0 & 0 & 0 & 0 & 1 & -i & i & 1 \\ 0 & 0 & 0 & 0 & 1 & i & -i & 1 \\ 0 & 0 & 0 & 0 & 1 & -i & -i & -1 \end{pmatrix}\begin{pmatrix} 1 \\ 1 \\ 1 \\ -1 \\ 1 \\ 1 \\ -1 \\ 1 \end{pmatrix} \\ &= (1+i, 0, 0, 1-i, 0, 1-i, 1+i, 0)^T.\end{aligned}$$

For $\mathcal{W}$ a set of $2^m \times 2^m$ unitaries, define peak-to-average power ratio of $\grave{f}$ with respect to $\mathcal{W}$ by

$$\mathcal{P}_{\mathcal{W}}(\grave{f}) := \max_{W\in\mathcal{W},w\in\mathbb{F}_2^m}\left(|(W\grave{f})_w|^2\right).$$

Let $\mathcal{D}$ be the set of all $2^n \times 2^n$ unitaries where any member of $\mathcal{D}$ only has one non-zero entry per row and column. Let $\mathcal{U}$ be a set of $2^n \times 2^n$ unitaries, and $\mathcal{DU}$ be the set of $2^n \times 2^n$ unitaries, $\{DW, D \in \mathcal{D}, W \in \mathcal{U}\}$. Then, for $h \in \mathcal{B}_n$,

$$\mathcal{P}_{\mathcal{U}}(\grave{h}) = \mathcal{P}_{\mathcal{DU}}(\grave{h}). \tag{11}$$

We abbreviate, $\forall D \in \mathcal{D}$, this equivalence by

$$D\mathcal{U} \simeq \mathcal{U}, \quad \text{and} \quad D\mathcal{U}\grave{h} \simeq \mathcal{U}\grave{h}.$$

Proof: (of (3) and (6) - sketch) Let $V := \bigcup_{j=0}^{m-1} V_j$, where $V_j \subset K_j$. Let $O_V := \{j \mid |V_j| \text{ odd}\}$. Then we can show that $H_V\grave{f}' \simeq \langle H_{O_V}\grave{f}\rangle$ and $N_V\langle\grave{f}\rangle \simeq \langle N_{O_V}\grave{f}\rangle$, so over all choices for V, the spectral elements with respect to the WHT (resp. NHT) of the restrictions of $\grave{f}'$ (resp. $\langle\grave{f}\rangle$), comprise, to within phase and position, multiplicities of the spectral elements with respect to the WHT (resp. NHT) of the restrictions of $\grave{f}$, where magnitudes are unchanged [4]. ■

V. Generalised nonlinearities

For $\mathcal{V}$ a set of 2×2 unitaries we say that $W \in \mathcal{V}^{\otimes n}$ iff $W = \otimes_{j=0}^{n-1}U_j$, and $U_j \in \mathcal{V}$, $\forall j$. Using this notation, $\mathcal{P}_{\{I,H\}^{\otimes m}}(\grave{f}) = \mathcal{P}^r_H(\grave{f})$, and $\mathcal{P}_{\{I,N\}^{\otimes m}}(\grave{f}) = \mathcal{P}^r_N(\grave{f})$.

Let $V_{\mathbb{II}} := \{\left(\begin{smallmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{smallmatrix}\right), \quad \forall\theta \in \mathbb{R}\}$, and $V_{\mathbb{IIII}} := \{\left(\begin{smallmatrix} \cos\theta & i\sin\theta \\ \sin\theta & -i\cos\theta \end{smallmatrix}\right), \quad \forall\theta \in \mathbb{R}\}$, be infinite sets of 2×2 unitaries, called *type*-$\mathbb{II}$, and *type*-$\mathbb{IIII}$ unitaries, respectively [2], [8], [9]. We can show that

$$\mathcal{P}_{V_{\mathbb{II}}^{\otimes n}}(\grave{f}') \leq 2^m. \tag{12}$$

$$\mathcal{P}_{V_{\mathbb{IIII}}^{\otimes n}}(\langle\grave{f}\rangle) \leq 2^{m-1}. \tag{13}$$

By (11), equations (12) and (13) have (3) and (6), respectively, as special cases as, for any $S \in \{0, 1, \ldots, n-1\}$, $H_S \in \{I, H\}^{\otimes n} \subset \{DV_{\mathbb{II}}^{\otimes n}, \forall D \in \mathcal{D}\}$ and $N_S \in \{I, N\}^{\otimes n} \subset \{DV_{\mathbb{IIII}}^{\otimes n}, \forall D \in \mathcal{D}\}$. To sketch proofs for (12) and (13), we introduce *Type*-$\mathbb{I}$ unitaries, $V_{\mathbb{I}} = \{\frac{1}{\sqrt{2}}\left(\begin{smallmatrix} 1 & \alpha \\ 1 & -\alpha \end{smallmatrix}\right), \quad |\alpha| = 1\}$. Let $\#(\grave{h})$ be the number of non-zero elements of $\grave{h}$. The following results are critical to our proofs.

$$\#(N^{\otimes n}\grave{f}') \leq 2^m. \tag{14}$$

$$\#(H^{\otimes n}\langle\grave{f}\rangle) \leq 2^{m-1}. \tag{15}$$

Remark 1: Every entry of every matrix in $V_{\mathbb{I}}^{\otimes n}$ has the same magnitude.

Proof: (for (12) - sketch) From (14) and Remark 1, it follows that $\mathcal{P}_{V_{\mathbb{I}}^{\otimes n}}(N^{\otimes n}\grave{f}') \leq 2^m$. (12) follows by observing that $V_{\mathbb{II}} \simeq NV_{\mathbb{I}}$. ■

Proof: (for (13) - sketch) From (15) and Remark 1, it follows that $\mathcal{P}_{V_{\mathbb{I}}^{\otimes n}}(H^{\otimes n}\langle\grave{f}\rangle) \leq 2^{m-1}$. (13) follows by observing that $V_{\mathbb{IIII}} \simeq HV_{\mathbb{I}}$. ■

VI. Group actions preserving nonlinearity

Constructions $\mathbb{II}$ and $\mathbb{IIII}$ give $\grave{f}'$ and $\langle\grave{f}\rangle$, for which (12) and (13) hold, respectively. Furthermore, groups exist under whose action properties (12) and (13) are preserved. First we establish matrix representations for these groups.

$V_{\mathbb{II}}$ group

$V_{\mathbb{II}} \cup ZV_{\mathbb{II}}$ is a matrix group as, for $U \in V_{\mathbb{II}}$, $UV_{\mathbb{II}} \in ZV_{\mathbb{II}}$.

Affine group

Two Boolean functions $f, g \in \mathcal{B}_n$ are *affine equivalent* if

$$g(x) = f(Ax + b) + d \cdot x + c, \tag{16}$$

for A a binary invertible $n \times n$ matrix, $b, d \in \mathbb{F}_2^n$ and $c \in \mathbb{F}_2$. We recast affine equivalence by the *affine group* in matrix form. Let $X := \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, $Z := \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$, and $Y := XZ = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$, be 2×2 unitary (Pauli) matrices. Define $X_j^k := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = \delta_{z,uz}$, where $u = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, $z = (x_j, x_k)^T$, i.e. elements of X_j^k are one at positions (z, uz) and zero otherwise, $\forall z \in \mathbb{F}_2^2$ - (one should remember that matrix $X_j^k \in (\mathbb{C}^2)^{\otimes 2} \times (\mathbb{C}^2)^{\otimes 2}$ is a $2^2 \times 2^2$ matrix with

[4] In particular, the proof implies that $\grave{f}'$ and $\langle f\rangle$ are bent and negabent, respectively, for k_j even $\forall j$.

both rows and columns indexed by elements from $\mathbb{F}_2^2$). Define matrix group [5] ,

$$\mathcal{A}_n = \langle\langle -1, X_j, Z_j, X_j^k, \forall j, k \in \{0, 1, \ldots, n-1\}, j \neq k \rangle\rangle.$$

Then $f, g \in \mathcal{B}_n$ are affine equivalent iff $\exists W \in \mathcal{A}_n$, such that $\grave{f} = W\grave{g}$.

Extended orthogonal group

The functions $f, g \in \mathcal{B}_n$ are *extended orthogonal equivalent* if (16) holds for $AA^T = I$, and $b = d$ of even weight. Define $V_{0,1,2,3}$ as the $2^4 \times 2^4$ unitary, $V_{0,1,2,3} := \delta_{z,uz}$, where $u = \left(\begin{smallmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{smallmatrix}\right)$, and $z = (x_0, x_1, x_2, x_3)^T$. Based on theorem 19 of [5], the *orthogonal group* has the following unitary representation for $n > 4$,

$$\mathcal{O}_n := \langle\langle V_{0,1,2,3}, P_{j,k}, \forall j, k \in \{0, 1, \ldots, n-1\}, j \neq k \rangle\rangle,$$

where $P_{j,k}$ is the 4×4 permutation matrix swapping tensor positions j and k, i.e. $P_{j,k} := \left(\begin{smallmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{smallmatrix}\right) = \delta_{z,uz}$, where $u = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, and $z = (x_j, x_k)^T$. Repeated action of $P_{j,k}$ at various pairs, j, k, generates the symmetric group, S_n The *extended orthogonal group*, $\mathcal{E}_n$, for $n > 4$, has the following matrix representation,

$$\begin{aligned} \mathcal{E}_n := \langle\langle -1, V_{0,1,2,3}, Y_{j,k}, P_{j,k}, \\ \forall j, k \in \{0, 1, \ldots, n-1\}, j \neq k \rangle\rangle, \end{aligned}$$

where $Y_{j,k} := \left(\begin{smallmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \\ 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{smallmatrix}\right)$ takes the role of even-weight vector $b = d$ in (16). Then $f, g \in \mathcal{B}_n$ are extended orthogonal equivalent iff $\exists W \in \mathcal{E}_n$, such that $\grave{f} = W\grave{g}$. Observe that $\mathcal{O}_n \subset \mathcal{E}_n \subset \mathcal{A}_n$.

Type-$\mathbb{II}$ invariance

$V_{\mathbb{II}} \cup ZV_{\mathbb{II}}$ is a group so

$$\mathcal{P}_{V_{\mathbb{II}}^{\otimes n}}(W\grave{f}') = \mathcal{P}_{V_{\mathbb{II}}^{\otimes n}}(\grave{f}'), \qquad \forall W \in V_{\mathbb{II}}^{\otimes n}. \tag{17}$$

In general there exist $W \in \{I, H\}^{\otimes n}$ and $h \in \mathcal{B}_n$, such that $\grave{h} = W\grave{f}'$. But it is currently unclear to us whether $\exists W \in \{DV_{\mathbb{II}}^{\otimes n}, \forall D \in \mathcal{D}\}$, $W \not\in \{I, H\}^{\otimes n}$, such that $\grave{h} = W\grave{f}'$.

$$\mathcal{P}_{V_{\mathbb{II}}^{\otimes n}}(W\grave{f}') = \mathcal{P}_{V_{\mathbb{II}}^{\otimes n}}(\grave{f}'), \qquad \forall W \in \mathcal{E}_n. \tag{18}$$

Proof: (of (18), sketch) One can verify that $N^{\otimes 4}V_{0,1,2,3} \simeq N^{\otimes 4}$, $N^{\otimes 2}Y_{j,k} \simeq N^{\otimes 2}$, and $N^{\otimes 2}P_{j,k} \simeq N^{\otimes 2}$ so, for $W \in \mathcal{E}_n$, $N^{\otimes n}W\grave{f}' \simeq N^{\otimes n}\grave{f}'$, and the proof follows, like (12), by Remark 1 and (14). ■

Type-$\mathbb{III}$ invariance

$$\mathcal{P}_{V_{\mathbb{III}}^{\otimes n}}(W\langle\grave{f}\rangle) = \mathcal{P}_{V_{\mathbb{III}}^{\otimes n}}(\langle\grave{f}\rangle), \qquad \forall W \in \mathcal{A}_n. \tag{19}$$

Proof: (of (19), sketch) One can verify that $H^{\otimes 2}X_j^k \simeq H^{\otimes 2}$, $HX \simeq H$, and $HZ \simeq H$ so, for $W \in \mathcal{A}_n$, $H^{\otimes n}W\langle\grave{f}\rangle \simeq H^{\otimes n}\langle\grave{f}\rangle$, and the proof follows, like (13), by remark 1 and (15). ■

VII. Complementary sets

A size 2^m complementary set, $C_{\mathcal{W}}^n := \{f^j \mid j \in \mathbb{F}_2^m\}$, of arrays, $f^j \in (\mathbb{C}^2)^{\otimes n}$, with respect to a set, $\mathcal{W}$, of $2^n \times 2^n$ unitaries is defined by the property,

$$\sum_{j \in \mathbb{F}_2^m} |\grave{\mathcal{F}}_w^{W,j}|^2 = 2^m, \quad \forall w \in \mathbb{F}_2^n, W \in \mathcal{W},$$

where $\grave{\mathcal{F}}^{W,j} = W\grave{f}^j$. Previous work [7] proposed *Construction* $\mathbb{I}$ for a set of functions, $h \in \mathbb{F}_2^n$, where, for $n = tm$,

$$h = \sum_{i=0}^{t-1} \theta_i(z_i) \cdot \theta_{i+1}(z_{i+1}) + g_i(z_i), \tag{20}$$

where $z_i = (x_{im}, x_{im+1}, + \ldots, x_{(i+1)m-1}) \in \mathbb{F}_2^m$, $\theta_i : \mathbb{F}_2^m \rightarrow \mathbb{F}_2^m$, are permutations, and $g_i(z_i) \in \mathcal{B}_m$. These functions satisfy,

$$\mathcal{P}_{V_{\mathbb{I}}^{\otimes n}}(\grave{h}) \leq 2^m.$$

Let

$$C_{V_{\mathbb{I}}^{\otimes n}}^n = \{h + j \cdot z_{t-1} \mid j \in \mathbb{F}_2^m\}.$$

Then $C_{V_{\mathbb{I}}^{\otimes n}}^n$ is a *type-$\mathbb{I}$ complementary set* of size 2^m. Constructions $\mathbb{II}$ and $\mathbb{III}$ similarly lead to complementary sets. For $y = (y_0, y_1, \ldots, y_{m-1})$, $y_j = \sum_{i \in K_j} x_i$, let

$$C_{V_{\mathbb{II}}^{\otimes n}}^n = \{f' + j \cdot y \mid j \in \mathbb{F}_2^m\}.$$

Then $C_{V_{\mathbb{II}}^{\otimes n}}^n$ is a *type-$\mathbb{II}$ complementary set* of size 2^m. For some fixed $r \in \{0, 1, \ldots, m-1\}$, let $y^r = (y_0, y_1, \ldots, y_{r-1}, y_{r+1}, \ldots, y_{m-1})$, and

$$C_{V_{\mathbb{III}}^{\otimes n}}^n = \{\langle f \rangle + j \cdot y^r \mid j \in \mathbb{F}_2^{m-1}\}.$$

Then $C_{V_{\mathbb{III}}^{\otimes n}}^n$ is a *type-$\mathbb{III}$ complementary set* of size 2^{m-1}.

Observe that the upper bounds of (12) and (13) follow immediately from the fact that $C_{V_{\mathbb{II}}^{\otimes n}}^n$ and $C_{V_{\mathbb{III}}^{\otimes n}}^n$ are complementary sets of type-$\mathbb{II}$ and type-$\mathbb{III}$, respectively.

VIII. Final comments

Construction $\mathbb{II}$ may be a step towards the difficult problem of constructing cryptographically-interesting 'k-normal' Boolean functions, $k \ll n/2$, for which infinite constructions do not yet exist [3], [6], where any function affine-equivalent to such a function remains nonlinear up to kth-order restrictions. In contrast, Construction $\mathbb{II}$ yields a basic class of functions whose non-trivial restrictions only remain nonlinear up to extended-orthogonal equivalence, where the extended-orthogonal group is a subgroup of the affine group. Construction $\mathbb{III}$ is a generalisation of the class of affine functions. The constructions and properties mentioned herein focus on Boolean functions, but all results carry over, without modification, to generalised Boolean functions, where one constructs, from $\grave{f} : \mathbb{F}_2^m \rightarrow \mathbb{C}$, functions $\grave{f}', \langle\grave{f}\rangle : \mathbb{F}_2^n \rightarrow \mathbb{C}$, where $\grave{f}'(x) = \langle\grave{f}\rangle(x)\grave{\mathcal{K}}(x)$.

The set of functions constructed using (20) is much larger than that constructed using (2) or (5) [6] , even if one takes

[5] We use '$\langle\langle * \rangle\rangle$' to encompass group generators, as '$\langle * \rangle$' is used in this paper for 'expansion'.

[6] Moreover, section 5 of [7] identifies a further generalisation of (20).

into account symmetries (17), (18), and (19), suggesting that Constructions $\mathbb{II}$ and $\mathbb{III}$ might be generalised further.

References

[1] R. Arratia, B. Bollobas, G. B. Sorkin, The Interlace Polynomial of a Graph, J. Combin. Theory Ser. B, 92, 2, 199–233, 2004.

[2] Tor E. Bjørstad, Matthew G. Parker, Equivalence Between Certain Complementary Pairs of Types I and III, in Enhancing Cryptographic Primitives with Techniques from Error Correcting Codes, Vol. 23, NATO Science for Peace and Security Series, 2009.

[3] A. Canteaut, M. Daum, H. Dobbertin, G. Leander, Finding nonnormal bent functions, Discrete Applied Mathematics, 154 202–218, 2006.

[4] Lars Eirik Danielsen, Matthew G. Parker, Spectral orbits and peak-to-average power ratio of Boolean functions with respect to the I, H, N^n transform, Lecture Notes in Computer Science, LNCS 3486, 373–388, 2005.

[5] Gerald J. Janusz, Parametrization of self-dual codes by orthogonal matrices, Finite Fields and Their Applications, 13, 3, 450–491, 2007.

[6] Gregor Leander, Gary McGuire, Construction of bent functions from near-bent functions, Journal of Comb. Theory, Series A 116 960–970, 2009.

[7] Matthew G. Parker, Chintha Tellambura, A Construction for Binary Sequence Sets with Low Peak-to-Average Power Ratio, Reports in Informatics, University of Bergen, 242, Feb. 2003. http://www.ii.uib.no/publikasjoner/texrap/ps/2003-242.ps.

[8] Matthew G. Parker, Close encounters with Boolean functions of three different kinds, Lecture Notes in Computer Science, LNCS 5228, 15–19 Sept. 2008.

[9] Matthew G. Parker, Polynomial Residue Systems via Unitary Transforms, to appear in post-proceedings of Contact Forum Coding Theory and Cryptography III, Brussels, 2009. http://www.ii.uib.no/~matthew/PRNSUnitary.pdf

[10] Constanza Riera, Matthew G. Parker, Generalised Bent Criteria for Boolean Functions (I), IEEE Trans Inform. Theory, 52, 9, 4142–4159, Sept. 2006.