Generalised complementary arrays

Matthew G. Parker[1] and Constanza Riera[2]

[1] The Selmer Center, Department of Informatics, University of Bergen, PB 7800, N-5020 Bergen, Norway,
matthew@ii.uib.no,
[2] Høgskolen i Bergen , Bergen, Norway,
Constanza.Riera@ii.uib.no

Abstract. We present a generalised setting for the construction of complementary array pairs and its proof, using a unitary matrix notation. When the unitaries comprise multivariate polynomials in complex space, we show that four definitions of conjugation imply four types of complementary pair - types I, II, III, and IV. We provide a construction for complementary pairs of types I, II, and III over $\{1,-1\}$, and further specialize to a construction for all known $2\times 2\times\ldots\times 2$ complementary array pairs of types I, II, and III over $\{1,-1\}$. We present a construction for type-IV complementary array pairs, and call them *Rayleigh quotient pairs*. We then generalise to complementary array sets, provide a construction for complementary sets of types I, II, and III over $\{1,-1\}$, further specialize to a construction for all known $2\times 2\times\ldots\times 2$ complementary array sets of types I, II, and III over $\{1,-1\}$, and derive closed-form Boolean formulas for these cases.

Key words: Complementary sets, complementary arrays, Golay pairs, Rayleigh quotient.

1 Introduction

A length $\mathtt{d}$ sequence of complex numbers, $A:=(a_0,a_1,\ldots,a_{\mathtt{d}-1})\in\mathbb{C}^{\mathtt{d}}$, can be written as a univariate polynomial, $A(z):=a_0+a_1z+\ldots+a_{\mathtt{d}-1}z^{\mathtt{d}-1}$, and the *aperiodic autocorrelation* of A comprises the coefficients of $A(z)\overline{A(z^{-1})}$, where $\overline{A(z^{-1})}$ means conjugate the coefficients of $A(z^{-1})$. Then (A,B) are a *Golay complementary pair* of sequences [1,2,4,3] if

$$\lambda_{AB}:=A(z)\overline{A(z^{-1})}+B(z)\overline{B(z^{-1})}=c\in\mathbb{R}.$$

A $\mathtt{d}_0\times\mathtt{d}_1\times\ldots\times\mathtt{d}_{m-1}$ array of complex numbers, $A\in\bigotimes_{k=0}^{m-1}\mathbb{C}^{\mathtt{d}_k}$, can be written as a multivariate polynomial, $A(\mathbf{z})$, where $\mathbf{z}:=(z_0,z_1,\ldots,z_{m-1})$ and $A(\mathbf{z})$ has

maximum degree $\mathtt{d}_k - 1$ in z_k. Then a size S *complementary set* of arrays is a set of S m-dimensional arrays, $A_S = \{A_0, A_1, \ldots, A_{S-1}\}$, such that

$$\lambda_{A_S}(\mathbf{z}) := \sum_{s=0}^{S-1} A_s(\mathbf{z})\overline{A_s(\mathbf{z}^{-1})} = c \in \mathbb{R}, \tag{1}$$

where $\mathbf{z}^{-1} := (z_0^{-1}, z_1^{-1}, \ldots, z_{m-1}^{-1})$. Complementary pairs and, more generally, sets are attractive because the sum of their aperiodic autocorrelations, λ_{A_S}, has zero sidelobes, i.e. $\lambda_{A_S}(\mathbf{z})$ has no dependence on $\mathbf{z}$. This means that the *Fourier transform* of λ_{A_S} is completely flat, as $\lambda_{A_S}(\mathbf{e}) = c$, a constant, for $\mathbf{e} = (e_0, e_1, \ldots, e_{m-1}) \in \mathbb{C}^m$, $|e_k| = 1$, $\forall k$. Golay proposed a construction for complementary sequence pairs with sequence elements taken from alphabet $\{1, -1\}$ [1,2,4,3]. This was extended by Turyn and others [5,6], and generalised to sets [7,8,9,10], to other alphabets [11,12,13] to arrays [14,15,16,9,17,18,19,20], to near-complementarity [15,21], and to complete complementary codes [22]. A typical requirement is that any pair so constructed comprises elements taken from some highly constrained complex alphabet (such as, for instance, $\{1, -1\}$ or $\{1, i, -1, -i\}$, $i = \sqrt{-1}$) - one difficulty with complementary construction lies in devising methods to suitably restrict the alphabet. In this paper we examine four types of complementarity, types I, II, III, and IV, of which type-I is the conventional type. We first express the pair construction as a 2×2 unitary transform action, where we derive unitarity without defining, explicitly, addition, multiplication, and conjugacy, apart from a few necessary constraints. The approach allows us to propose λ-pairs: from a λ_{AB} pair, (A, B), and a λ_{CD} pair, (C, D), one constructs a λ_{FG} pair, (F, G), where $\lambda_{FG} = \lambda_{AB}\lambda_{CD}$. We then specialise to the case where the 2×2 unitary matrix contains m-variate complex polynomial elements. By defining conjugacy in three different ways one establishes that unitarity is preserved when evaluating the polynomial elements of this matrix over the m-fold unit circle, real axis, or imaginary axis, so as to obtain constructions for complementary array pairs of types I, II, and III, respectively. We specialise to constructions for the alphabet $\{1, -1\}$, and to $2 \times 2 \times \ldots \times 2$ arrays [3]. A fourth definition of conjugacy yields type-IV, leading to the characterisation and construction of *Rayleigh quotient pairs*. We then generalise to complementary array sets and, in particular, develop constructions for complementary sets of $2 \times 2 \times \ldots \times 2$ arrays over the alphabet $\{1, -1\}$ for types I, II, and III. We derive closed-form Boolean formulae for these constructions.

Whilst types I, II, and III have been proposed and explored in other recent papers [23,24,25,26], the method of proof in this paper is both more concise and

[3] This may seem restrictive but, as discussed in [19,20], array dimensions can be combined whilst preserving (near-)complementarity. For instance, properties for a $2 \times 2 \times 3$ array imply properties for a set of 4×3, 2×6 arrays, or length 12 sequences.

more general, allowing characterisation and constructions beyond the $2\times2\times\ldots\times 2$ case, and is applicable to scenarios beyond complex polynomials. Moreover the definition and construction of Rayleigh quotient pairs is new, arising from a consideration of results in [27,28]. Although the formula for the construction of complementary sets of Boolean functions of type-I was first stated in [16] and proved in [9], the proof here is more succinct, facilitating the development of new formulae for complementary sets of Boolean functions of types II and III.

2 New contexts for the complementary pair construction

Let Γ be a set and let '$\circ$', '$+$', and '$*$' act on Γ, where $\circ, + : \Gamma^2 \to \Gamma$, and $* : \Gamma \to \Gamma$. Let '$-$' and '$/$' be the inverses of '$+$' and '$\circ$', respectively, where, $\forall a, b \in \Gamma$, $-(+(a,b),b) = a$, and $/(\circ(a,b),b) = \frac{a\circ b}{b} = a$. In any equation, let '$*$' take precedence over '$\circ$' which, itself, takes precedence over '$+$'. Let $A, B, C, D \in \Gamma$. A modified and generalised construction for complementary pair (F, G), given complementary pairs (A, B) and (C, D), and based on [5,14,17,19], is

$$F = C \circ A + D^* \circ B, \qquad G = D \circ A - C^* \circ B. \tag{2}$$

Theorem 1 *Given (2), the identity,*

$$F \circ F^* + G \circ G^* = (A \circ A^* + B \circ B^*) \circ (C \circ C^* + D \circ D^*),$$

holds if the following conditions on '$\circ$', '$+$', and '$*$' are met:

- *'$*$' is an involution and is also distributive over '$\circ$' and '$+$'.*
- *'$\circ$' is distributive over '$+$'.*
- *Both '$\circ$' and '$+$' are associative and commutative.*

Proof. From (2),

$$\begin{aligned}
F \circ F^* &= (C \circ A + D^* \circ B) \circ (C \circ A + D^* \circ B)^* \\
&= (C \circ A + D^* \circ B) \circ (C^* \circ A^* + (D^*)^* \circ B^*) && * \text{ distrib. over } \circ, + \\
&= (C \circ A + D^* \circ B) \circ (C^* \circ A^* + D \circ B^*) && * \text{ an involution} \\
&= C \circ A \circ C^* \circ A^* + D^* \circ B \circ C^* \circ A^* && \circ \text{ distrib. over } + \\
&\qquad + C \circ A \circ D \circ B^* + D^* \circ B \circ D \circ B^* \\
&= C \circ C^* \circ A \circ A^* + A^* \circ B \circ C^* \circ D^* && \circ \text{ commut., assoc.} \\
&\qquad + A \circ B^* \circ C \circ D + D \circ D^* \circ B \circ B^* \\
&= C \circ C^* \circ A \circ A^* + D \circ D^* \circ B \circ B^* && + \text{ commut., assoc.} \\
&\qquad + A^* \circ B \circ C^* \circ D^* + A \circ B^* \circ C \circ D
\end{aligned}$$

Likewise,

$$G \circ G^* = D \circ D^* \circ A \circ A^* + C \circ C^* \circ B \circ B^* - A^* \circ B \circ C^* \circ D^* - A \circ B^* \circ C \circ D,$$

and the theorem follows from $F \circ F^* + G \circ G^*$. □

Let U be a 2×2 matrix with elements in Γ, with multiplication of matrices taken with respect to '$\circ$' and '$+$' in the obvious way. Let $\dagger$ take $U := \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ to $U^\dagger := \left(\begin{smallmatrix} a^* & c^* \\ b^* & d^* \end{smallmatrix}\right)$ (i.e. transpose-'conjugate'). Then U is called *unitary* with respect to '$\circ$', '$+$', and '$*$', if $UU^\dagger = I$, where I is the 2×2 identity matrix.

Definition: (C, D) is called a λ_{CD}*-pair*, where $\lambda_{CD} := C \circ C^* + D \circ D^*$.

We abbreviate (2) to

$$\begin{pmatrix} F \\ G \end{pmatrix} = \begin{pmatrix} C & D^* \\ D & -C^* \end{pmatrix} \begin{pmatrix} A \\ B \end{pmatrix} = \sqrt{\lambda} T \begin{pmatrix} A \\ B \end{pmatrix}, \tag{3}$$

where $\lambda := \lambda_{CD}$ and $T := \frac{1}{\sqrt{C \circ C^* + D \circ D^*}} \left(\begin{smallmatrix} C & D^* \\ D & -C^* \end{smallmatrix}\right)$ is unitary [4]. One associates λ with unitary, T, and with its constituent pair, (C, D). By definition, T is a complete complementary code [22], where the matrix elements are not fixed elements of the space, but are variables.

The inner product, $\langle \cdot, \cdot \rangle$, of two length S vectors, $u, v \in \Gamma^S$, is given by $\langle u, v \rangle := uv^\dagger = u_0 \circ v_0^* + u_1 \circ v_1^* + \ldots + u_{S-1} \circ v_{S-1}^* = \sum_{i=0}^{S-1} u_i \circ v_i^*$, and u and v are called *orthogonal* if $\langle u, v \rangle = 0$.

Lemma 1 *Let* $\left(\begin{smallmatrix} C' \\ D' \end{smallmatrix}\right) = V \left(\begin{smallmatrix} C \\ D \end{smallmatrix}\right)$. *Then* $\lambda_{C'D'} = \lambda_{CD}$ *if* V *is unitary.*

Proof. Let $v := \left(\begin{smallmatrix} C \\ D \end{smallmatrix}\right)$, and express λ_{CD} of (C, D) as the inner product of v with itself, i.e. $\lambda_{CD} = \langle v, v \rangle$. Then $\langle Vv, Vv \rangle = v^\dagger V^\dagger V v = v^\dagger v = \langle v, v \rangle$. □

We summarise theorem 1 in terms of λ_{AB}, λ_{CD},and λ_{FG}:

$$\lambda_{FG} = \lambda_{CD} \circ \lambda_{AB}. \tag{4}$$

2.1 Polynomial context

The above presentation is very general, allowing one to examine different scenarios without having to re-prove complementarity. In this paper we consider just a few special cases, where we focus, primarily, on varying the definition of '$*$'. Let Γ be the space of complex multivariate rational functions. Let '$\circ$' and '$+$' be conventional multiplication and addition of complex multivariate rational functions, respectively. Henceforth, although we deal with rational functions, i.e. the powers of our variables may be negative, for brevity we shall refer to rational functions as polynomials. Let $A(z_0, z_1, \ldots, z_{m-1}) = A(\mathbf{z})$ be an m-variate

[4] '$\sqrt{\lambda}$' is the member or members of Γ that satisfy $\sqrt{\lambda} \circ \sqrt{\lambda} = \lambda$ - such a root must necessarily exist in Γ.

polynomial with complex coefficients, of minimum degree zero and maximum degree $\mathtt{d}_k - 1$ in z_k. We can interpret $A(\mathbf{z})$ as a $\mathtt{d}_0 \times \mathtt{d}_1 \times \ldots \times \mathtt{d}_{m-1}$ array of complex numbers. We write A for both polynomial and array interpretations, where meaning is clear from context. Then $A_{\mathbf{l}}$, $\mathbf{l} = (l_0, l_1, \ldots, l_{m-1}) \in \mathbb{Z}^{+m}$, is the coefficient of the monomial $\prod_{k=0}^{m-1} z_k^{l_k}$ in $A(\mathbf{z})$, i.e. the $\mathbf{l}$th element of the m-dimensional array, A, where $A_{\mathbf{l}} = 0$, $\forall \mathbf{l}$ where $l_k \geq \mathtt{d}_k$ for one or more k. The first three definitions of '$*$', acting on A are as follows:

$$\begin{array}{ll} \text{Type-I:} & A^*(z_0, z_1, \ldots, z_{m-1}) := \overline{A(z_0^{-1}, z_1^{-1}, \ldots, z_{m-1}^{-1})} := \overline{A(\mathbf{z}^{-1})}. \\ \text{Type-II:} & A^*(z_0, z_1, \ldots, z_{m-1}) := \overline{A(\mathbf{z})}. \\ \text{Type-III:} & A^*(z_0, z_1, \ldots, z_{m-1}) := \overline{A(-\mathbf{z})}, \end{array} \tag{5}$$

where $\overline{A}$ means conjugate the complex coefficients of A. The above three definitions for '$*$' are all involutions, as required. For instance, let $A(\mathbf{z}) = 2 + iz_0 - 3z_1 + z_0z_1$. Then $A^*(\mathbf{z}) = 2 - iz_0^{-1} - 3z_1^{-1} + z_0^{-1}z_1^{-1}$ or $2 - iz_0 - 3z_1 + z_0z_1$ or $2 + iz_0 + 3z_1 + z_0z_1$, for types I or II or III, respectively.

Let pairs $A(\mathbf{z}), B(\mathbf{z})$, and $C(\mathbf{y}), D(\mathbf{y})$, and $F(\mathbf{x}), G(\mathbf{x})$, be m-variate, m'-variate, and $m'' = m + m'$-variate polynomials, respectively, where the variable elements of $\mathbf{y}$ and $\mathbf{z}$ are disjoint, and where $\mathbf{x} = \mathbf{y}|\mathbf{z}$ is the concatenation of $\mathbf{y}$ and $\mathbf{z}$. A generalised spectral analysis in the complex plane requires us to evaluate these polynomials, and $\sqrt{\lambda(\mathbf{y})}T(\mathbf{y})$, by assigning every variable to a complex number. For brevity, define $\sqrt{\lambda}T(\mathbf{y}) := \sqrt{\lambda(\mathbf{y})}T(\mathbf{y})$. If, after evaluation at a point $\mathbf{y} = \mathbf{e} \in \mathbb{C}^{m'}$, $\sqrt{\lambda}T(\mathbf{e})(\sqrt{\lambda}T(\mathbf{e}))^\dagger \neq \lambda(\mathbf{e})I$, then the complementary pair property does not carry over to spectral evaluation $\mathbf{y} = \mathbf{e}$. This leads to natural restrictions on the evaluation space, so as to preserve unitarity in complex space. For example, for type-I, although, $\lambda(y)T(y)T^\dagger(y) = \begin{pmatrix} 1+y^2 & y^{-1} \\ y & -1-y^{-2} \end{pmatrix}\begin{pmatrix} 1+y^{-2} & y^{-1} \\ y & -1-y^2 \end{pmatrix} = (3 + y^2 + y^{-2})I = \lambda(y)I$ holds for both $y = 3$ and $y = i$, $i = \sqrt{-1}$, one finds that $\sqrt{\lambda}T(i)(\sqrt{\lambda}T(i))^\dagger = \lambda(i)I = I$, but $\sqrt{\lambda}T(3)(\sqrt{\lambda}T(3))^\dagger = \begin{pmatrix} 10 & \frac{1}{3} \\ 3 & \frac{-10}{9} \end{pmatrix}\begin{pmatrix} 10 & 3 \\ \frac{1}{3} & \frac{-10}{9} \end{pmatrix} \neq \lambda(3)I = \frac{109}{9}I$. Let $\mathbb{E} \subset \mathbb{C}^{m'}$ be the subset of complex space where evaluation and conjugation commute:

$$\mathbb{E} := \{\mathbf{e} \quad | \quad \mathbf{e} \in \mathbb{C}^{m'}, (\sqrt{\lambda}T(\mathbf{e}))^\dagger = (\sqrt{\lambda}T)^\dagger(\mathbf{e})\},$$

where $\mathbf{e} := (e_0, e_1, \ldots, e_{m'-1})$. We call $\mathbb{E}$ the *commuting evaluation set*. For our example $i \in \mathbb{E}$ but $3 \notin \mathbb{E}$. One finds that

$$\begin{array}{lll} \text{Type-I:} & \mathbb{E} = \{\mathbf{e} \quad | \quad |e_j| = 1, \forall j\} & (m'\text{-fold unit circle}), \\ \text{Type-II:} & \mathbb{E} = \mathbb{R}^{m'} & (m'\text{-fold real axis}), \\ \text{Type-III:} & \mathbb{E} = \mathbb{I}^{m'} & (m'\text{-fold imaginary axis}). \end{array}$$

Evaluations of A in the complex plane are the multi-set $\{A(\mathbf{z}=\mathbf{e}) \quad | \quad \mathbf{e} \in \mathbb{C}^{m'}\}$. When $\mathtt{d}_k = 2, \forall k$, these spectral evaluations can be realised, to within row normalisation, by the action of a special set of unitary transforms on the array, A. For $r \in \mathbb{R}$, and $|\beta| = 1$, evaluation of $a_0 + a_1 z$ at both $z = r\beta$ and $z = \frac{-\beta}{r}$ is given by $V \begin{pmatrix} a_0 \\ a_1 \end{pmatrix}$, for V a matrix from the evaluation set, E,

$$E := \{\begin{pmatrix} 1 & r\beta \\ 1 & \frac{-\beta}{r} \end{pmatrix} \quad | \quad r \in \mathbb{R}, |\beta| = 1\}.$$

Restrictions to the commuting evaluation set put constraints on r or β: $r = 1$ for type-I, $\beta = 1$ for type-II, and $\beta = i$ for type-III. Row normalisation of E then gives *unitary evaluation set*, $\mathcal{E}$,

$$\mathcal{E} := \{\frac{1}{\sqrt{1+r^2}} \begin{pmatrix} 1 & 0 \\ 0 & r \end{pmatrix} \begin{pmatrix} 1 & r\beta \\ 1 & \frac{-\beta}{r} \end{pmatrix} \quad | \quad r \in \mathbb{R}, |\beta| = 1\},$$

which, for types I, II and III, yields *unitary commuting evaluation sets* [25]

$$\begin{aligned}
\mathcal{E}_I &= \{\tfrac{1}{\sqrt{2}} \begin{pmatrix} 1 & \beta \\ 1 & -\beta \end{pmatrix} \quad | \quad r = 1, |\beta| = 1\}, \\
\mathcal{E}_{II} &= \{\tfrac{1}{\sqrt{1+r^2}} \begin{pmatrix} 1 & r \\ r & -1 \end{pmatrix} \quad | \quad r \in \mathbb{R}, \beta = 1\} = \{\begin{pmatrix} \cos\phi & \sin\phi \\ \sin\phi & -\cos\phi \end{pmatrix} \quad | \quad \forall\phi\}, \qquad (6) \\
\mathcal{E}_{III} &= \{\tfrac{1}{\sqrt{1+r^2}} \begin{pmatrix} 1 & ri \\ r & -i \end{pmatrix} \quad | \quad r \in \mathbb{R}, \beta = i\} = \{\begin{pmatrix} \cos\phi & i\sin\phi \\ \sin\phi & -i\cos\phi \end{pmatrix} \quad | \quad \forall\phi\}.
\end{aligned}$$

From (6) the normalisation factors of types I, II, and III for the $\mathtt{d}_k = 2$ case, $0 \le k < m'$, are $2^{\frac{-m'}{2}}$, $\prod_{k=0}^{m'-1} \frac{1}{\sqrt{(1+r_k^2)}}$, and $\prod_{k=0}^{m'-1} \frac{1}{\sqrt{(1+r_k^2)}}$, respectively. So one must normalise $\lambda(\mathbf{y}) = C(\mathbf{y})C^*(\mathbf{y}) + D(\mathbf{y})D^*(\mathbf{y})$ by dividing by $2^{m'}$, $\prod_{k=0}^{m'-1}(1+y_k^2)$, and $\prod_{k=0}^{m'-1}(1-y_k^2)$, for types I, II, and III, respectively. But the normalisation argument can be extended to any combination of array dimensions, $\mathtt{d}_k$, even if we can't specify the associated $\mathtt{d}_k \times \mathtt{d}_k$ unitaries explicitly. One makes the first row of the kth matrix equal to $(1, \beta, \beta^2, \ldots, \beta^{\mathtt{d}_k-1})$, $(1, r, r^2, \ldots, r^{\mathtt{d}_k-1})$, and $(1, ri, -r^2, \ldots, r^{\mathtt{d}_k-1} i^{\mathtt{d}_k-1})$, for types I, II, and III, respectively. Then, for types I, II, and III, $\lambda(\mathbf{y})$ must be divided by $\prod_{k=0}^{m'-1} \mathtt{d}_k$, $\prod_{k=0}^{m'-1}(1 + y_k^2 + y_k^4 + \ldots + y_k^{2(\mathtt{d}_k-1)})$, and $\prod_{k=0}^{m'-1}(1 - y_k^2 + y_k^4 - \ldots + (-1)^{\mathtt{d}_k-1} y_k^{2(\mathtt{d}_k-1)})$, respectively.

Definition: (C, D) is a *perfect* type-I, II, or III pair, iff $\lambda = c$, $c\prod_{k=0}^{m'-1}(1 + y_k^2 + y_k^4 + \ldots + y_k^{2(\mathtt{d}_k-1)})$, or $c\prod_{k=0}^{m'-1}(1 - y_k^2 + y_k^4 - \ldots + (-1)^{\mathtt{d}_k-1} y_k^{2(\mathtt{d}_k-1)})$, respectively, where $c \in \mathbb{R}$.

For instance, the conventional Golay complementary pair of sequences of length $\mathtt{d}$ is here called a perfect type-I pair, (C, D), where $m' = 1$, and $\mathtt{d}_0 = \mathtt{d}$.

Example: Let $\sqrt{\lambda}T = \begin{pmatrix} 1 & y \\ -y & -1 \end{pmatrix}$. Then T is a type-III unitary but not a type-I or II unitary, as $\lambda T T^\dagger = \lambda I$ for '$*$' of type-III, but not for '$*$' of types I or II.

However, for this very special case ($C = 1, D = -y$) is a perfect type-I, II, and III pair, as $\lambda_{CD} = 2$, or $1 + y^2$, or $1 - y^2$ for types I or II or III, respectively. Instead, let $C = 1+y_0+y_1-y_0y_1$, $D = 1-y_0-y_1-y_0y_1$. Then (C, D) is a perfect type-II pair as $\lambda_{CD} = 2(1+y_0^2)(1+y_1^2)$, but not a perfect type-I or type-III pair. Evaluating $C(y_0, y_1)$ and $D(y_0, y_1)$ at $y_0 \in \{\pm 1\}$, $y_1 \in \{0, \infty\}$ (four points on the 2-fold real axis) gives $\lambda_{CD}(\pm 1, \{0, \infty\}) = 4, 4, 4\infty, 4\infty$. Normalising λ_{CD} by dividing by $(1 + y_0^2)(1 + y_1^2)$ in each case gives $\left(\frac{\lambda_{CD}}{(1+y_0^2)(1+y_1^2)}\right)_{y_0\in\{\pm1\},y_1\in\{0,\infty\}} = 2, 2, 2, 2$. This is equivalent to applying the type-II unitary commuting evaluation matrix $H \otimes I \in \mathcal{E}_{II}^{\otimes 2}$ to C and to D, where $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, to obtain

$$
\begin{aligned}
(\hat{C}, \hat{D}) &= \left(\begin{pmatrix} \sqrt{2} \\ 0 \\ 0 \\ \sqrt{2} \end{pmatrix}, \begin{pmatrix} 0 \\ \sqrt{2} \\ -\sqrt{2} \\ 0 \end{pmatrix} \right) \\
&= \left(\begin{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \\ -1 \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ -1 \\ -1 \\ -1 \end{pmatrix} \end{pmatrix} \right),
\end{aligned}
$$

and then verifying that the sum of the point-products of $\hat{C}$ with itself and of $\hat{D}$ with itself is $\hat{C}.\hat{C} + \hat{D}.\hat{D} = (2, 2, 2, 2)^T$. In general the two arrays, C and D, satisfy $\hat{C}.\hat{C} + \hat{D}.\hat{D} = (2, 2, 2, 2)^T$ for $\hat{C} = \left(\begin{pmatrix} \cos\phi_0 & \sin\phi_0 \\ \sin\phi_0 & -\cos\phi_0 \end{pmatrix} \otimes \begin{pmatrix} \cos\phi_1 & \sin\phi_1 \\ \sin\phi_1 & -\cos\phi_1 \end{pmatrix} \right) C$, $\forall \phi_0, \phi_1$, and similarly for $\hat{D}$.

Whilst $\mathcal{E}_I^{\otimes m}$ is the m-dimensional *Fourier* transform, $\mathcal{E}_{II}^{\otimes m}$ and $\mathcal{E}_{III}^{\otimes m}$ are less familiar, although types I, II, and III may make sense to some as characterising the three axes of a *Bloch sphere* in the context of qubit quantum systems [29]. We have discussed evaluations when $\mathtt{d}_k = 2$, $\forall k$, and proposed suitable normalisation, irrespective of the value of $\mathtt{d}_k$, even if one does not know the associated $\mathtt{d}_k \times \mathtt{d}_k$ evaluation unitary. But for type-I a unitary is known for general $\mathtt{d}_k = \mathtt{d}$, by replacing $\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & \beta \\ 1 & -\beta \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & \beta \end{pmatrix}$, $|\beta| = 1$, in (6) by $\frac{1}{\sqrt{\mathtt{d}}}\begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \alpha & \alpha^2 & \dots & \alpha^{\mathtt{d}-1} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & \alpha^{\mathtt{d}-1} & \alpha^{\mathtt{d}-2} & \dots & \alpha \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & \beta & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & \beta^{\mathtt{d}-1} \end{pmatrix}$, where $\alpha = e^{2\pi i/\mathtt{d}}$ and $|\beta| = 1$. For types II and III, although it remains an open problem for us to characterise these generalisations, we can still envisage unitary evaluation sets, $\mathcal{E}$, without explicit characterisation. In this context, let $\lambda = \lambda(\mathbf{y})$ be an m'-variate polynomial, and let $\lambda_U := U\lambda$ for U taken from some m'-variate unitary evaluation set $\mathcal{E}' = \mathcal{E}'_0 \otimes \mathcal{E}'_1 \otimes \ldots \otimes \mathcal{E}'_{m'-1}$. We then obtain an evaluated form of (4), for λ_{AB}, λ_{CD}, and λ_{FG} m-variate, m'-variate, and $m'' = m + m'$-variate, respectively:

$$\lambda_{U'',FG} = \lambda_{U',CD}\lambda_{U,AB}, \tag{7}$$

for $U'' = U' \otimes U$, $U' \in \mathcal{E}'$, $U \in \mathcal{E}$, and $\mathcal{E}'' = \mathcal{E}' \otimes \mathcal{E}$. Let $\|U\lambda\|_\infty$ be the maximum size of an element in array $U\lambda$. Let $\lambda_{\max,\mathcal{E}} := \max_{U\in\mathcal{E}}(\|U\lambda\|_\infty)$. Then a variant of (7) is

$$\lambda_{\max,\mathcal{E}'',FG} = \lambda_{\max,\mathcal{E}',CD}\lambda_{\max,\mathcal{E},AB}, \tag{8}$$

which allows one to characterise and construct *near-complementary* λ-pairs [15,21], i.e. where $\lambda_{\mathcal{E}'',FG}$ is not constant, but 'near-constant'. (One could, similarly, replace 'max' by 'min' throughout). Equations (7) and (8) become identical when (A, B) and (C, D) are perfect, in which case, from (4), (F, G) is also perfect.

3 Pair recursion

To recurse (3) for polynomials, we combine (3) and lemma 1, to give

$$\begin{aligned}\begin{pmatrix} F_j(\mathbf{z}_j) \\ G_j(\mathbf{z}_j) \end{pmatrix} &= \left(U_j(\mathbf{y}_j) \begin{pmatrix} C_j(\mathbf{y}_j) & D_j^*(\mathbf{y}_j) \\ D_j(\mathbf{y}_j) & -C_j^*(\mathbf{y}_j) \end{pmatrix} V_j(\mathbf{y}_j) \right)^{(\dagger)} \begin{pmatrix} F_{j-1}(\mathbf{z}_{j-1}) \\ G_{j-1}(\mathbf{z}_{j-1}) \end{pmatrix} \\ &= \left(U_j(\mathbf{y}_j)\sqrt{\lambda_j}T_j(\mathbf{y}_j)V_j(\mathbf{y}_j) \right)^{(\dagger)} \begin{pmatrix} F_{j-1}(\mathbf{z}_{j-1}) \\ G_{j-1}(\mathbf{z}_{j-1}) \end{pmatrix},\end{aligned} \tag{9}$$

where $\sqrt{\lambda_j}T_j(\mathbf{y}_j)$ abbreviates $\sqrt{\lambda_j}(\mathbf{y}_j)T_j(\mathbf{y}_j)$, U_j and V_j are 2×2 unitary, $\forall j$, with $\mathbf{y}_j := (z_{\mu_j}, z_{\mu_j+1}, \ldots, z_{mu_j+m_j-1})$, $\mu_j = \sum_{k=0}^{j-1} m_k$, $\mathbf{z}_j = \mathbf{y}_j|\mathbf{z}_{j-1}$, $\forall j$, and '(†)' means optional transpose-conjugate. U_j, V_j, and (†) are inserted to generate symmetry classes by lemma 1. If the starting conditions are $F_{-1} = G_{-1} = 1$, then one obtains λ-pair $(\mathcal{F}, \mathcal{G}) := (F_{n-1}, G_{n-1})$, where $\lambda = \prod_{j=0}^{n-1} \lambda_j$.

3.1 Coefficients restricted to $\{1, -1\}$

To construct λ-pairs whose coefficients are from a restricted alphabet, one must choose (C_j, D_j), U_j and V_j, appropriately. Let $\mathbf{d}_j := (\mathtt{d}_{\mu_j}, \mathtt{d}_{mu_j+1}, \ldots, \mathtt{d}_{\mu_j+m_j-1})$. Wlog we assume C_j and D_j have minimum degree zero and maximum degree $\mathtt{d}_{\mu_j+k} - 1$ in z_{μ_j+k}, so as to facilitate the mapping to and from arrays. Let $\mathbf{y}_j^{\mathbf{d}_j-\mathbf{1}}$ mean $\prod_{k=0}^{m_j-1} z_{\mu_j+k}^{\mathtt{d}_{\mu_j+k}-1}$ - this term is added for type-I below so as to facilitate this mapping to and from arrays. Here is a recursive formula to generate all known λ-pairs of types I, II, and III, with coefficients restricted to $\{1, -1\}$, where (F_{-1}, G_{-1}) and (C_j, D_j) have only $\{1, -1\}$ coefficients, $\forall j$:

$$\begin{aligned}
&\text{I:} \quad \begin{pmatrix} F_j \\ G_j \end{pmatrix} = \tfrac{\pm 1}{\sqrt{2}} \begin{pmatrix} 1 & 0 \\ 0 & \pm 1 \end{pmatrix} \left(\sqrt{\lambda_j}T_j(\mathbf{y}_j) \begin{pmatrix} 1 & 0 \\ 0 & \mathbf{y}_j^{\mathbf{d}_j-\mathbf{1}} \end{pmatrix} \right)^{(T)} \begin{pmatrix} 1 & 1 \\ \pm 1 & \mp 1 \end{pmatrix} \begin{pmatrix} F_{j-1} \\ G_{j-1} \end{pmatrix}, \\
&\text{II:} \quad \begin{pmatrix} F_j \\ G_j \end{pmatrix} = \tfrac{\pm 1}{\sqrt{2}} \begin{pmatrix} 1 & 0 \\ 0 & \pm 1 \end{pmatrix} \left(\sqrt{\lambda_j}T_j(\mathbf{y}_j) \right)^{(\dagger)} \begin{pmatrix} 1 & 1 \\ \pm 1 & \mp 1 \end{pmatrix} \begin{pmatrix} F_{j-1} \\ G_{j-1} \end{pmatrix}, \\
&\text{III:} \quad \begin{pmatrix} F_j \\ G_j \end{pmatrix} = \tfrac{\pm 1}{\sqrt{2}} \left(\sqrt{\lambda_j}T_j(\mathbf{y}_j) \right)^{(\dagger)} \begin{pmatrix} \pm 1 & 1 \\ \mp 1 & 1 \end{pmatrix} \begin{pmatrix} F_{j-1} \\ G_{j-1} \end{pmatrix}.
\end{aligned} \tag{10}$$

In all three cases, the final pair, $\left(\begin{smallmatrix}F'_j\\G'_j\end{smallmatrix}\right)$, is given by $\left(\begin{smallmatrix}1&0\\0&\pm1\end{smallmatrix}\right)\left(\begin{smallmatrix}F_j\\G_j\end{smallmatrix}\right)$, where one does not distinguish between $\left(\begin{smallmatrix}F'_j\\G'_j\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}G'_j\\F'_j\end{smallmatrix}\right)$. The use of '$(T)$', ('transpose'), instead of '$(\dagger)$' for type-I, is just a convenience to ensure positive powers of z_{μ_j+k}, $\forall j,k$, throughout. The expression for type-I is, essentially, a re-formulation of expressions in [19,20].

Example: Let $m_0 = m_1 = 1$, $\mathtt{d}_0 = 3$, $\mathtt{d}_1 = 2$, $F_0 = 1 + z_0 + z_0^2$, and $G_0 = 1 - z_0 - z_0^2$. Then, for type-III, $\lambda' = F_0F_0^* + G_0G_0^* = 2(1 - z_0^2 + z_0^4)$, so (F_0, G_0) is a perfect type-III pair. Let $\mathbf{y}_1 = (z_1)$, $C_1 = 1 + z_1$ and $D_1 = 1 + z_1$. Then $\lambda_1 = C_1C_1^* + D_1D_1^* = 2(1 - z_1^2)$, so (C_1, D_1) is a perfect type-III pair. Then applying a particular instance of the type-III construction of (10)

$$\begin{aligned}\begin{pmatrix}F_1\\G_1\end{pmatrix} &= \tfrac{1}{\sqrt{2}}\begin{pmatrix}1+z_1 & 1-z_1\\ 1+z_1 & -1+z_1\end{pmatrix}\begin{pmatrix}1&1\\-1&1\end{pmatrix}\begin{pmatrix}1+z_0+z_0^2\\1-z_0-z_0^2\end{pmatrix}\\ &= \sqrt{2}\begin{pmatrix}1-z_0-z_0^2+z_1+z_0z_1+z_0^2z_1\\1+z_0+z_0^2+z_1-z_0z_1-z_0^2z_1\end{pmatrix},\end{aligned}$$

and one can verify that $\lambda = F_1F_1^* + G_1G_1^* = 4(1 - z_1^2)(1 - z_0^2 + z_0^4) = \lambda_1\lambda'$, as expected, so (F_1, G_1) is type-III perfect. Evaluation of normalised λ is the evaluation of $\frac{\lambda}{(1-z_1^2)(1-z_0^2+z_0^4)}$ on the imaginary axis, which is the constant, 4.

When $\mathtt{d}_{\mu_j+k} = 2, \forall j,k$ then, from (6), as well as type-I unitary evaluation, we also know explicit type-II and III unitary evaluations. Moreover, when $m_j = 1$, $\forall j$ then, to within symmetry, we can identify a unique T_j, $\forall j$, for each of I, II, and III, such that (C_j, D_j) are perfect, and (F_{-1}, G_{-1}) and (C_j, D_j) have only $\{1, -1\}$ coefficients, $\forall j$. We obtain

$$\begin{aligned}\text{I:}\quad \begin{pmatrix}F_j\\G_j\end{pmatrix} &= \tfrac{\pm1}{\sqrt{2}}\begin{pmatrix}1&0\\0&\pm1\end{pmatrix}\begin{pmatrix}1+z_j & z_j-1\\1-z_j & -z_j-1\end{pmatrix}\begin{pmatrix}1&1\\\pm1&\mp1\end{pmatrix}\begin{pmatrix}F_{j-1}\\G_{j-1}\end{pmatrix}\\ &= \pm2HP_{\gamma,j}\begin{pmatrix}1&0\\0&z_j\end{pmatrix}P_{\theta,j}\begin{pmatrix}F_{j-1}\\G_{j-1}\end{pmatrix},\\ \text{II:}\quad \begin{pmatrix}F_j\\G_j\end{pmatrix} &= \tfrac{\pm1}{\sqrt{2}}\begin{pmatrix}1&0\\0&\pm1\end{pmatrix}\begin{pmatrix}1+z_j & 1-z_j\\1-z_j & -1-z_j\end{pmatrix}\begin{pmatrix}1&1\\\pm1&\mp1\end{pmatrix}\begin{pmatrix}F_{j-1}\\G_{j-1}\end{pmatrix}\\ &= \pm\sqrt{2}\begin{pmatrix}1&z_j\\z_j&-1\end{pmatrix}O_jP_{\theta,j}\begin{pmatrix}F_{j-1}\\G_{j-1}\end{pmatrix},\\ \text{III:}\quad \begin{pmatrix}F_j\\G_j\end{pmatrix} &= \tfrac{\pm1}{\sqrt{2}}\begin{pmatrix}1+z_j & 1-z_j\\1+z_j & -1+z_j\end{pmatrix}\begin{pmatrix}\pm1&1\\\mp1&1\end{pmatrix}\begin{pmatrix}F_{j-1}\\G_{j-1}\end{pmatrix}\\ &= \pm\sqrt{2}\begin{pmatrix}1&z_j\\z_j&1\end{pmatrix}O_j\begin{pmatrix}F_{j-1}\\G_{j-1}\end{pmatrix},\end{aligned} \tag{11}$$

where $O_j \in \{\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right), \left(\begin{smallmatrix}1&0\\0&-1\end{smallmatrix}\right)\}$, and $P_{\gamma_j}, P_{\theta_j} \in \{\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right), \left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)\}$. In all three cases, the final pair, $\left(\begin{smallmatrix}F'_j\\G'_j\end{smallmatrix}\right)$, is given by $O_{j+1}\left(\begin{smallmatrix}F_j\\G_j\end{smallmatrix}\right)$, where one does not distinguish between $\left(\begin{smallmatrix}F'_j\\G'_j\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}G'_j\\F'_j\end{smallmatrix}\right)$.

4 Type-IV: the Rayleigh quotient pair

(5) gave three types of involution, '$*$'. Here is a fourth, where we must also modify the definition of '$\circ$' accordingly. Let M be an m-dimensional unitary Hermitian matrix (i.e. $M^\dagger = M$, $MM^\dagger = I$), where M is of size $\mathtt{d}_0 \times \mathtt{d}_1 \times \ldots \times \mathtt{d}_{m-1}$. Remembering that $A(z_0, z_1, \ldots, z_{m-1})$ can be interpreted as an m-dimensional array, A, define '$*$' as

$$\text{Type-IV:} \qquad A^* := MA. \tag{12}$$

Remember that $A_{\mathbf{l}}$, $\mathbf{l} \in \mathbb{Z}^{*m}$, is the $\mathbf{l}$th coefficient of the monomial $\prod_{k=0}^{m-1} z_k^{l_k}$ in $A(\mathbf{z})$. Then, for $A(z_0, z_1, \ldots, z_{m-1})$ and $B(z_0, z_1, \ldots, z_{m-1})$, both of degree less than $\mathtt{d}_k$ in z_k, $\forall k$, the *inner-product* of A and B is given by

$$\langle A(\mathbf{z}), B(\mathbf{z})\rangle = \langle A, B\rangle = \sum_{\mathbf{l}\in\mathbb{Z}^{*m}} A_{\mathbf{l}}\overline{B_{\mathbf{l}}},$$

i.e., viewing A and B as arrays, the inner-product is element-wise. For $\mathbf{y}$ and $\mathbf{z}$ disjoint vectors of variables, we define '$\circ$' as

$$\begin{aligned} \text{Type-IV:} \qquad & C(\mathbf{y}) \circ A(\mathbf{z}) := C(\mathbf{y})A(\mathbf{z}) \\ & A(\mathbf{z}) \circ B(\mathbf{z}) := \langle A, B\rangle, \end{aligned} \tag{13}$$

i.e. '$\circ$' is conventional polynomial multiplication between polynomials in disjoint variables (a tensor-product of the associated arrays), but is the inner-product of polynomials in the same variables. It can be verified that '$*$' is an involution, and that the required distributivity, commutativity, and associativity relationships hold between '$*$', '$\circ$' and '$+$', apart from the caveat that '$*$' is not distributive over '$\circ$' when '$\circ$' acts as the inner-product, i.e. $(C(\mathbf{y})\circ C'(\mathbf{y}))^* \neq C^*(\mathbf{y})\circ C'^*(\mathbf{y}) = \langle C^*(\mathbf{y}), C'^*(\mathbf{y})\rangle$. But this scenario is not required in the proof of theorem 2.

The definition of the *Rayleigh quotient* of A with respect to M is given by

$$\mathrm{RQ}(A, M) := \frac{\langle A, MA\rangle}{\langle A, A\rangle},$$

where M is unitary Hermitian. We have that $|\mathrm{RQ}| \leq 1$, with $\mathrm{RQ}(A, M) = \pm 1$ iff A is an eigenvector (eigenarray) of M. It follows that

$$\mathrm{RQ}(A, M) = \frac{A \circ A^*}{\langle A, A\rangle}, \tag{14}$$

We similarly define the *Rayleigh quotient pair* of (A, B) with respect to M by

$$\mathrm{RQ}_2((A, B), M) := \frac{\langle A, MA\rangle + \langle B, MB\rangle}{\langle A, A\rangle + \langle B, B\rangle}.$$

We have that $|\mathrm{RQ}_2| \leq 1$, with $\mathrm{RQ}_2((A,B),M) = \pm 1$ iff both A and B are eigenvectors of M. The type-IV definition of '$*$' and '$\circ$' implies that

$$\mathrm{RQ}_2((A,B),M) = \frac{A \circ A^* + B \circ B^*}{\langle A,A\rangle + \langle B,B\rangle}. \tag{15}$$

Let M_{y_j} be a $\mathtt{d}_{\mu_j} \times \mathtt{d}_{\mu_j+1} \times \ldots \times \mathtt{d}_{\mu_j+m_j-1}$ Hermitian unitary matrix, and let $M_j = M_{y_j} \otimes M_{j-1}$, $\forall j$, where $M_{-1} = 1$ and $\mathcal{M} := M_{n-1}$. We apply construction (9) for '$*$' and '$\circ$' of type-IV, with respect to M_{y_j} at step j. Then $(\mathcal{F},\mathcal{G}) := (F_{n-1},G_{n-1})$ is a λ-pair, where $\lambda = \prod_{j=0}^{n-1}\lambda_j$ (note that, in this case, the λ_j are complex numbers, not polynomials). In particular,

$$\mathrm{RQ}_2((\mathcal{F},\mathcal{G}),\mathcal{M}) = \frac{\mathcal{F}\circ\mathcal{F}^* + \mathcal{G}\circ\mathcal{G}^*}{\langle\mathcal{F},\mathcal{F}\rangle + \langle\mathcal{G},\mathcal{G}\rangle} = \frac{\lambda}{\langle\mathcal{F},\mathcal{F}\rangle + \langle\mathcal{G},\mathcal{G}\rangle}, \tag{16}$$

where $F_{-1} = G_{-1} = 1$. If both C_j and D_j are eigenvectors of M_{y_j}, $\forall j$, then both $\mathcal{F}$ and $\mathcal{G}$ are eigenvectors of $\mathcal{M}$. So we have a way of computing sets of eigenvectors of $\mathcal{M} = \bigotimes_{j=0}^{n-1} M_{y_j}$ given a set of eigenvectors, $\{C_j, D_j \mid M_{y_j}C_j = C_j, M_{y_j}D_j = D_j\}$, $\forall j$. Trivial eigenvectors of $\mathcal{M}$ can be obtained by assigning $C_j = D_j^*$, $\forall j$, and are not interesting - the interesting eigenvectors are obtained if $C_j \neq D_j$ for one or more j.

5 Set recursion

The λ-pair construction (9) is generalised to a λ-set construction of size S, as follows:

$$\mathbf{F}_j := \begin{pmatrix} F_{j,0}(\mathbf{z}_j) \\ F_{j,1}(\mathbf{z}_j) \\ \ldots \\ F_{j,S-1}(\mathbf{z}_j) \end{pmatrix} = \Big(\mathcal{U}_j(\mathbf{y}_j)\sqrt{\lambda_j}\mathcal{T}_j(\mathbf{y}_j)\mathcal{V}_j(\mathbf{y}_j)\Big)^{(\dagger)} \begin{pmatrix} F_{j-1,0}(\mathbf{z}_{j-1}) \\ F_{j-1,1}(\mathbf{z}_{j-1}) \\ \ldots \\ F_{j-1,S-1}(\mathbf{z}_{j-1}) \end{pmatrix}, \tag{17}$$

where $\mathcal{U}_j$ and $\mathcal{V}_j$ are unitary, $\forall j$, $\mathbf{y}_j := (z_{\mu_j}, z_{\mu_j+1}, \ldots, z_{\mu_j+m_j-1})$, $\mu_j = \sum_{i=0}^{j-1} m_i$, and $\mathbf{z}_j = \mathbf{y}_j|\mathbf{z}_{j-1}$, $\forall j$. From starting conditions ($F_{-1,s} = 1, 0 \leq s < S$), one obtains λ-set ($\mathcal{F} := F_{n-1,s}, 0 \leq s < S$), where $\lambda = \prod_{j=0}^{n-1}\lambda_j$.

5.1 Size-2^t sets

A special case is when $S = 2^t$ and $\sqrt{\lambda_j}\mathcal{T}_j$ decomposes as $\sqrt{\lambda_j}\mathcal{T}_j = \bigotimes_{k=0}^{t-1}\sqrt{\lambda_{j,k}}T_{j,k}$, where $\sqrt{\lambda_{j,k}}T_{j,k} = \left(\begin{smallmatrix} C_{j,k} & D_{j,k}^* \\ D_{j,k} & -C_{j,k}^* \end{smallmatrix}\right)$ is a matrix function of $m_{j,k}$ variables. For this decomposition of the construction, unitary evaluation sets of types I, II, and III are then just a t-fold tensoring of the evaluations described in (6), where $m_j = \sum_{k=0}^{t-1} m_{j,k}$. It follows that

Definition: $\mathcal{F}$ is a perfect type-I, II, or III set iff, $\forall j,k$, $\lambda_j = c$, $c\prod_{k=0}^{t-1}(1+z_{\mu_j+k}^2)$, and $c\prod_{k=0}^{t-1}(1-z_{\mu_j+k}^2)$, for types I, II, and III, respectively, where $c \in \mathbb{R}$.

5.2 Size-2^t sets of $2 \times 2 \times \ldots \times 2$ bipolar arrays

If we further restrict, such that $m_{j,k} = 1$ and $\mathtt{d}_{\mu_j+k} = \mathtt{d}_{tj+k} = 2, \forall j, k$, and where the constructed polynomials have coefficients restricted to $\{1, -1\}$ then, generalising (11), and observing that $\mu_j = tj$, one can substitute in for $\mathcal{U}_j\sqrt{\lambda_j}\mathcal{T}_j\mathcal{V}_j$ in (17) to obtain

$$\begin{aligned}
\text{I:} \quad & \begin{pmatrix} F_{j,0}(\mathbf{z}_j) \\ F_{j,1}(\mathbf{z}_j) \\ \ldots \\ F_{j,2^t-1}(\mathbf{z}_j) \end{pmatrix} = \pm H^{\otimes t} P_{\gamma,j} \bigotimes_{k=0}^{t-1} \begin{pmatrix} 1 & 0 \\ 0 & z_{tj+k} \end{pmatrix} O_j P_{\theta,j} \begin{pmatrix} F_{j-1,0,}(\mathbf{z}_{j-1}) \\ F_{j-1,1}(\mathbf{z}_{j-1}) \\ \ldots \\ F_{j-1,2^t-1,}(\mathbf{z}_{j-1}) \end{pmatrix}. \\
\text{II:} \quad & \begin{pmatrix} F_{j,0}(\mathbf{z}_j) \\ F_{j,1}(\mathbf{z}_j) \\ \ldots \\ F_{j,2^t-1}(\mathbf{z}_j) \end{pmatrix} = \pm \bigotimes_{k=0}^{t-1} \begin{pmatrix} 1 & z_{tj+k} \\ z_{tj+k} & -1 \end{pmatrix} O_j P_{\theta,j} \begin{pmatrix} F_{j-1,0}(\mathbf{z}_{j-1}) \\ F_{j-1,1}(\mathbf{z}_{j-1}) \\ \ldots \\ F_{j-1,2^t-1}(\mathbf{z}_{j-1}) \end{pmatrix}. \\
\text{III:} \quad & \begin{pmatrix} F_{j,0}(\mathbf{z}_j) \\ F_{j,1}(\mathbf{z}_j) \\ \ldots \\ F_{j,2^t-1}(\mathbf{z}_j) \end{pmatrix} = \pm \bigotimes_{k=0}^{t-1} \begin{pmatrix} 1 & z_{tj+k} \\ z_{tj+k} & 1 \end{pmatrix} O_j P_{\theta,j} \begin{pmatrix} F_{j-1,0}(\mathbf{z}_{j-1}) \\ F_{j-1,1}(\mathbf{z}_{j-1}) \\ \ldots \\ F_{j-1,2^t-1}(\mathbf{z}_{j-1}) \end{pmatrix},
\end{aligned} \tag{18}$$

where $P_{\gamma,j}, P_{\theta,j}$ are $2^t \times 2^t$ permutation matrices, and $O_j := \text{diag}(o_j)$, $o_j \in \{1, -1\}^{2^t}$. For type-I, when comparing with (11), the application of O_j on the right-hand side is no longer redundant so is included. For type-III, the inclusion of $P_{\theta,j}$ is for the same reason. In all three cases, the final set, $\begin{pmatrix} F'_{j,0}(\mathbf{z}_j) \\ F'_{j,1}(\mathbf{z}_j) \\ \ldots \\ F'_{j,2^t-1}(\mathbf{z}_j) \end{pmatrix}$, is given by $O_{j+1}\begin{pmatrix} F_{j,0}(\mathbf{z}_j) \\ F_{j,1}(\mathbf{z}_j) \\ \ldots \\ F_{j,2^t-1}(\mathbf{z}_j) \end{pmatrix}$, where one does not distinguish between $\begin{pmatrix} F_{j,0}(\mathbf{z}_j) \\ F_{j,1}(\mathbf{z}_j) \\ \ldots \\ F_{j,2^t-1}(\mathbf{z}_j) \end{pmatrix}$ and $P_{\theta,j+1}\begin{pmatrix} F_{j,0}(\mathbf{z}_j) \\ F_{j,1}(\mathbf{z}_j) \\ \ldots \\ F_{j,2^t-1}(\mathbf{z}_j) \end{pmatrix}$.

6 Generalised Boolean λ-sets

We now develop closed-form Boolean expressions for a special case of the sets described by subsection 5.1, where $\mathtt{d}_{\mu_j+k} = 2$, $\forall j, k$, and where the coefficients are in $\{1, -1\}$. Let $\mu_{j,k} = \mu_j + \sum_{i=0}^{k-1} m_{j,i}$, and $C_{j,k}$ and $D_{j,k}$ be polynomials in $\mathbf{y}_{j,k}$, where $\mathbf{y}_{j,k} = (z_{\mu_{j,k}}, z_{\mu_{j,k}+1}, \ldots, z_{\mu_{j,k}+m_{j,k}-1})$. In (17), let $\sqrt{\lambda_j}\mathcal{T}_j = \bigotimes_{k=0}^{t-1}\sqrt{\lambda_{j,k}}T_{j,k}$, where $\sqrt{\lambda_{j,k}}T_{j,k} = \begin{pmatrix} C_{j,k} & D^*_{j,k} \\ D_{j,k} & -C^*_{j,k} \end{pmatrix}$. As we are recursing we can, WLOG, assign $\mathcal{U}_j = I$, $\forall j < n-1$, i.e. only $\mathcal{U}_{n-1}$ is not constrained to identity if our final λ-set is $\mathcal{F} = \mathbf{F}_{n-1}$. We restrict to a $\{1, -1\}$ alphabet, for both $C_{j,k}$

and $D_{j,k}$, and for the resulting F_j, by assigning $\mathcal{V}_j = \left(\begin{smallmatrix}1 & 1\\ 1 & -1\end{smallmatrix}\right)^{\otimes t} O_j P_{\theta,j}$. We have

$$\left(\sqrt{\lambda_j}\mathcal{T}_j \left(\begin{smallmatrix}1 & 1\\ 1 & -1\end{smallmatrix}\right)^{\otimes t}\right) = \bigotimes_{k=0}^{t-1} \left(\begin{smallmatrix}C_{j,k} + D^*_{j,k} & C_{j,k} - D^*_{j,k}\\ D_{j,k} - C^*_{j,k} & D_{j,k} + C^*_{j,k}\end{smallmatrix}\right). \tag{19}$$

(19) is, essentially, an array generalisation of Turyn's construction [5], in more general context. To begin with, set $O_j = P_{\theta,j} = I$, $\forall j$, and ignore (†). Then (17) simplifies to

$$\mathbf{F}_j = \bigotimes_{k=0}^{t-1} \left(\begin{smallmatrix}C_{j,k} + D^*_{j,k} & C_{j,k} - D^*_{j,k}\\ D_{j,k} - C^*_{j,k} & D_{j,k} + C^*_{j,k}\end{smallmatrix}\right) \mathbf{F}_{j-1}. \tag{20}$$

As $C_{j,k}$ and $D_{j,k}$ are $2 \times 2 \times \ldots \times 2$ arrays with elements from $\{1, -1\}$, then they can be represented by Boolean functions $c_{j,k}, d_{j,k} : \mathbb{F}_2^{m_{j,k}} \to \mathbb{F}_2$, of $\mathbf{u}_{j,k}$, where $\mathbf{u}_{j,k} := (x_{\mu_{j,k}}, x_{\mu_{j,k}+1}, \ldots, x_{\mu_{j,k}+m_{j,k}-1}) \in \mathbb{F}_2^{m_{j,k}}$, and where $C_{j,k} = (-1)^{c_{j,k}}$ and $D_{j,k} = (-1)^{d_{j,k}}$. Our claim is that, given $c_{j,k}, d_{j,k}$, and $f_{j-1,s}$ Boolean functions $\forall k, s$, and that $C^*_{j,k}, D^*_{j,k}$ have elements in $\{1, -1\}$, $\forall j, k$, then $f_{j,s}$ is a Boolean function $\forall s$.

Let us first derive for $t = 1$, and subsequently develop for more general t. For $t = 1$, $\left(\begin{smallmatrix}F_{j,0}\\ F_{j,1}\end{smallmatrix}\right) = \left(\begin{smallmatrix}C_{j-1} + D^*_{j-1} & C_{j-1} - D^*_{j-1}\\ D_{j-1} - C^*_{j-1} & D_{j-1} + C^*_{j-1}\end{smallmatrix}\right) \left(\begin{smallmatrix}F_{j-1,0}\\ F_{j-1,1}\end{smallmatrix}\right)$ gives

$$\begin{aligned} F_{j,0} &= (C_{j-1} = D^*_{j-1}) C_{j-1} F_{j-1,0} + (C_{j-1} = -D^*_{j-1}) C_{j-1} F_{j-1,1},\\ F_{j,1} &= (D_{j-1} = -C^*_{j-1}) D_{j-1} F_{j-1,0} + (D_{j-1} = C^*_{j-1}) D_{j-1} F_{j-1,1}. \end{aligned} \tag{21}$$

Conditions $(C_{j-1} = D^*_{j-1}) \in \{0, 1\}$ and $(C_{j-1} = -D^*_{j-1}) \in \{0, 1\}$ are mutually exclusive, and similarly for $(D_{j-1} = -C^*_{j-1})$ and $(D_{j-1} = C^*_{j-1})$. So $F_{j,0}$ and $F_{j,1}$ have elements only from the alphabet $\{1, -1\}$ if C_{j-1}, D_{j-1}, $F_{j-1,0}$ and $F_{j-1,1}$ have elements only from $\{1, -1\}$. Assuming that C^*_j and D^*_j have coefficients in $\{1, -1\}$ if C_j and D_j do [5] , then let $C^*_j = (-1)^{c^*_j}$ and $D^*_j = (-1)^{d^*_j}$. Then, from (21),

$$\begin{aligned} &f_{j,0} = (c_{j-1} + d^*_{j-1} + 1)(c_{j-1} + f_{j-1,0}) + (c_{j-1} + d^*_{j-1})(c_{j-1} + f_{j-1,1}),\\ &f_{j,1} = (c^*_{j-1} + d_{j-1})(d_{j-1} + f_{j-1,0}) + (c^*_{j-1} + d_{j-1} + 1)(d_{j-1} + f_{j-1,1}).\\ &\qquad\qquad\qquad\qquad \Rightarrow\\ &\begin{pmatrix} f_{j,0}\\ f_{j,1}\end{pmatrix} = \begin{pmatrix} c_{j-1} + d^*_{j-1} + 1 & c_{j-1} + d^*_{j-1}\\ c^*_{j-1} + d_{j-1} & c^*_{j-1} + d_{j-1} + 1\end{pmatrix} \begin{pmatrix} f_{j-1,0}\\ f_{j-1,1}\end{pmatrix} + \begin{pmatrix} c_{j-1}\\ d_{j-1}\end{pmatrix}. \end{aligned} \tag{22}$$

Consider the optional '†', i.e.
$\left(\begin{smallmatrix}F_{j,0}\\ F_{j,1}\end{smallmatrix}\right) = \left(\begin{smallmatrix}C_{j-1} + D^*_{j-1} & C_{j-1} - D^*_{j-1}\\ D_{j-1} - C^*_{j-1} & D_{j-1} + C^*_{j-1}\end{smallmatrix}\right)^{\dagger} \left(\begin{smallmatrix}F_{j-1,0}\\ F_{j-1,1}\end{smallmatrix}\right) = \left(\begin{smallmatrix}C^*_{j-1} + D_{j-1} & D^*_{j-1} - C_{j-1}\\ C^*_{j-1} - D_{j-1} & D^*_{j-1} + C_{j-1}\end{smallmatrix}\right) \left(\begin{smallmatrix}F_{j-1,0}\\ F_{j-1,1}\end{smallmatrix}\right)$.
In general this possibility does not preserve the $\{1, -1\}$ alphabet as $(C^*_{j-1} = D_{j-1})$ and $(D^*_{j-1} = -C_{j-1})$ are not, in general, mutually exclusive conditions,

[5] The type-IV definition of '$*$' does not satisfy this requirement in general.

and neither are ($C^*_{j-1} = -D_{j-1}$) and ($D^*_{j-1} = C_{j-1}$). However mutual exclusivity is realised in this case when $c^*_{j-1} + d_{j-1} = c_{j-1} + d^*_{j-1}$, from which

$$\begin{pmatrix} f_{j,0} \\ f_{j,1} \end{pmatrix} = \begin{pmatrix} c_{j-1} + d^*_{j-1} + 1 & c_{j-1} + d^*_{j-1} \\ c_{j-1} + d^*_{j-1} & c_{j-1} + d^*_{j-1} + 1 \end{pmatrix} \begin{pmatrix} f_{j-1,0} \\ f_{j-1,1} \end{pmatrix} + \begin{pmatrix} c^*_{j-1} \\ d^*_{j-1} \end{pmatrix} + c_{j-1}c^*_{j-1} + d_{j-1}d^*_{j-1}. \tag{23}$$

For reasons of page count we do not develop (23) further in this paper.

Now consider more general t. Let $\mathbf{f}_j := (f_{j,s}, s \in \mathbb{F}_2^t)$, where $f_{j,s} : \mathbb{F}_2^{\mu_{j+1}} \to \mathbb{F}_2$ is a function of $(x_0, x_1, \ldots, x_{\mu_{j+1}-1})$, $\forall s$. Then, from (20) and (22),

$$\mathbf{f}_j := \log_{-1}(\mathbf{F}_j) = \bigotimes_{k=0}^{t-1} \begin{pmatrix} c_{j,k} + d^*_{j,k} + 1 & c_{j,k} + d^*_{j,k} \\ c^*_{j,k} + d_{j,k} & c^*_{j,k} + d_{j,k} + 1 \end{pmatrix} \mathbf{f}_{j-1} + \mathbf{v}_j,$$

where $\mathbf{v}_j = ((s+\mathbf{1})\cdot\mathbf{c}_j + s\cdot\mathbf{d}_j, s \in \mathbb{F}_2^t)$, $\mathbf{c}_j = (c_{j,k}, 0 \le k < t)$, and $\mathbf{d}_j = (d_{j,k}, 0 \le k < t)$. Let $w_{j,k} = c_{j,k} + d^*_{j,k} : \mathbb{F}_2^{m_{j,k}} \to \mathbb{F}_2$. Then $w^*_{j,k} = c^*_{j,k} + d_{j,k}$ and

$$\mathbf{f}_j = \bigotimes_{k=0}^{t-1} \begin{pmatrix} w_{j,k} + 1 & w_{j,k} \\ w^*_{j,k} & w^*_{j,k} + 1 \end{pmatrix} \mathbf{f}_{j-1} + \mathbf{v}_j. \tag{24}$$

Unwrapping (24), and setting, wlog, $\mathbf{f}_{-1} = \mathbf{0}$, gives

$$\begin{aligned} \mathbf{f}_j &= \textstyle\prod_{q=0}^{j} \bigotimes_{k=0}^{t-1} \begin{pmatrix} w_{q,k} + 1 & w_{q,k} \\ w^*_{q,k} & w^*_{q,k} + 1 \end{pmatrix} \mathbf{f}_{-1} + \mathbf{v}_j \\ &\qquad + \textstyle\sum_{q=0}^{j-1} \prod_{r=q+1}^{j} \bigotimes_{k=0}^{t-1} \begin{pmatrix} w_{r,k} + 1 & w_{r,k} \\ w^*_{r,k} & w^*_{r,k} + 1 \end{pmatrix} \mathbf{v}_q \\ &= \mathbf{v}_j + \textstyle\sum_{q=0}^{j-1} \prod_{r=q+1}^{j} \bigotimes_{k=0}^{t-1} \begin{pmatrix} w_{r,k} + 1 & w_{r,k} \\ w^*_{r,k} & w^*_{r,k} + 1 \end{pmatrix} \mathbf{v}_q \\ &= \mathbf{v}_j + \textstyle\sum_{q=0}^{j-1} \bigotimes_{k=0}^{t-1} \left(\prod_{r=q+1}^{j} \begin{pmatrix} w_{r,k} + 1 & w_{r,k} \\ w^*_{r,k} & w^*_{r,k} + 1 \end{pmatrix} \right) \mathbf{v}_q, \end{aligned} \tag{25}$$

where the '$\prod$' sign means 'multiply matrices on the left', e.g. $\prod_{j=0}^{1} M_j = M_1 M_0$.

We now present two alternative derivations, A and B, taking (25) as their starting point. They yield different, but equivalent, expressions for $\mathbf{f}_j$.

6.1 Derivation A

We require extra notation. For $g : \mathbb{F}_2^a \to \mathbb{F}_2$ for some positive integer, a, then, for $b \in \mathbb{F}_2$, define

$$\begin{aligned} g^{*b} &:= g, && b = 0, \\ &:= g^*, && b = 1. \end{aligned}$$

More generally, for $a = (a_0, a_1, \ldots, a_{t-1}) \in \mathbb{Z}^{+\,t}$, $g_k : \mathbb{F}_2^{a_k} \to \mathbb{F}_2$, $\mathbf{g} = (g_0, g_1, \ldots, g_{t-1}) : ((\mathbb{F}_2^{a_k} \to \mathbb{F}_2), 0 \le k < t)$, and $b \in \mathbb{F}_2^t$, then

$$\mathbf{g} \wedge b := \mathbf{g}^{*b} + b := (g_0^{*b_0}, g_1^{*b_1}, \ldots, g_{t-1}^{*b_{t-1}}) + b. \tag{26}$$

Define a recursive extension of '$\wedge$':

$$\bigwedge_{p=i}^{j} \mathbf{g}_p := \mathbf{g}_i \wedge (\bigwedge_{p=i+1}^{j} \mathbf{g}_p), \qquad i < j,$$

where $\mathbf{g}_p : ((\mathbb{F}_2^{a_{k_p}} \to \mathbb{F}_2), 0 \le k_i < t)$, and $\bigwedge_{p=j}^{j} \mathbf{g}_p = \mathbf{g}_j$.

Let $\mathbf{w}_j = (w_{j,0}, w_{j,1}, \ldots, w_{j,t-1})$. Then, for $b = (b_0, b_1, \ldots, b_{t-1}) \in \mathbb{F}_2^t$, assign $\mathbf{h}_q = \bigwedge_{p=q+1}^{j+1} \mathbf{w}_p$, where $\mathbf{w}_{j+1} = s$. Then, from (25),

$$\mathbf{f}_j = (f_{j,s}, s \in \mathbb{F}_2^t), \qquad f_{j,s} = \sum_{q=0}^{j} \mathbf{v}_q(\mathbf{h}_q). \tag{27}$$

Proof. (of (27), sketch) - Observe that, for $\mathbf{v} = \begin{pmatrix} \mathbf{v}(0) \\ \mathbf{v}(1) \end{pmatrix}$, $\begin{pmatrix} w+1 & w \\ w & w+1 \end{pmatrix} \mathbf{v} = \begin{pmatrix} \mathbf{v}(w) \\ \mathbf{v}(w+1) \end{pmatrix}$. Therefore $\mathbf{v}' = \begin{pmatrix} w+1 & w \\ w^* & w^*+1 \end{pmatrix} \mathbf{v} = \begin{pmatrix} \mathbf{v}(w) \\ \mathbf{v}(w^*+1) \end{pmatrix}$, i.e. $\mathbf{v}' = (v'_s = \mathbf{v}(w^{*s} + s) = \mathbf{v}(w \wedge s), s \in \mathbb{F}_2)^T$. Now observe that $\mathbf{v}' = \begin{pmatrix} w_2+1 & w_2 \\ w_2^* & w_2^*+1 \end{pmatrix} \begin{pmatrix} w_1+1 & w_1 \\ w_1^* & w_1^*+1 \end{pmatrix} \mathbf{v} = \begin{pmatrix} w_2+1 & w_2 \\ w_2^* & w_2^*+1 \end{pmatrix} \begin{pmatrix} \mathbf{v}(w_1) \\ \mathbf{v}(w_1^*+1) \end{pmatrix} = \begin{pmatrix} \mathbf{v}(w_1^{*w_2} + w_2) \\ \mathbf{v}(w_1^{*(w_2^*+1)} + w_2^*+1) \end{pmatrix}$. Therefore $\mathbf{v}' = (v'_s = \mathbf{v}(w_1 \wedge (w_2 \wedge s)) = \mathbf{v}(\bigwedge_{p=1}^{3} w_p)), s \in \mathbb{F}_2)^T$, where $w_3 = s$.

Applying these techniques to (25) yields (27), where more general t implies function vectors, $\mathbf{w}_j$. □

Remark: Potential confusion is possible here by reading $\mathbf{v}(\mathbf{h})$ and similar, incorrectly, as $\mathbf{v} \times (\mathbf{h})$. The real meaning should be clear from the proof of (27), and by context in the ensuing discussion.

Re-introducing more general O_j and $P_{\theta,j}$ to (20) modifies (27). In particular, $P_{\theta,j}$ is a $2^t \times 2^t$ permutation matrix. Let $\theta_j := (\theta_{0,j}, \theta_{1,j}, \ldots, \theta_{t-1,j}) : \mathbb{F}_2^t \to \mathbb{F}_2^t$ represent this permutation, and let it act on $\mathbf{w}_j$, i.e. define $\mathbf{w}_{\theta,j} := (\theta_{0,j}(\mathbf{w}_j), \theta_{1,j}(\mathbf{w}_j), \ldots, \theta_{t-1,j}(\mathbf{w}_j))$, where $\theta_{k,j}(\mathbf{w}_j) : \mathbb{F}_2^t \to \mathbb{F}_2$. Then

$$\mathbf{f}_j = (f_{j,s}, s \in \mathbb{F}_2^t), \qquad f_{j,s} = \sum_{q=0}^{j} \mathbf{v}_q(\mathbf{h}_{\theta,q}) + o_q(\mathbf{w}_q), \tag{28}$$

where $\mathbf{h}_{\theta,q} = \bigwedge_{p=q+1}^{j+1} \mathbf{w}_{\theta,p}$, $p \le j$, $\mathbf{w}_{\theta,j+1} = s$, and $o_q : \mathbb{F}_2^t \to \mathbb{F}_2$ is arbitrary.

The action of '$\wedge$' and '$\bigwedge$', in the context of (28), is simplified if, $\forall j,k$, $w^*_{j,k} = w_{j,k}$ or $w^*_{j,k} = w_{j,k} + 1$:

- $w^*_{j,k} = w_{j,k}$, $\forall j,k$: From (26), if $g^*_k = g_k$, then $\mathbf{g}^{*b} + b = \mathbf{g} + b$. So the action of '$\wedge$' on $w_{j,k}$ becomes '+', $\mathbf{h}_{\theta,q} = s + \sum_{p=q+1}^{j} \mathbf{w}_{\theta,p}$, and (28) becomes

$$\mathbf{f}_j = (f_{j,s}, s \in \mathbb{F}_2^t), \qquad f_{j,s} = \sum_{q=0}^{j} \mathbf{v}_q(\mathbf{h}_{\theta,q}) + o_q(\mathbf{w}_q). \tag{29}$$

- $w^*_{j,k} = w_{j,k} + 1$, $\forall j,k$: From (26), if $g^*_k = g_k + 1$, then $\mathbf{g}^{*b} + b = \mathbf{g}$. So $\bigwedge_{p=q+1}^{j+1} \mathbf{w}_p = \mathbf{w}_{q+1}$, $\mathbf{h}_{\theta,q} = \mathbf{w}_{\theta,q+1}$, and (28) becomes

$$\mathbf{f}_j = (f_{j,s}, s \in \mathbb{F}_2^t), \qquad f_{j,s} = \mathbf{v}_j(s) + o_j(\mathbf{w}_j) + \sum_{q=0}^{j-1} \mathbf{v}_q(\mathbf{w}_{\theta,q+1}) + o_q(\mathbf{w}_q). \quad (30)$$

  ♢ Consider, $\forall k$, and one or more j,

  Condition X: $c^*_{j,k} = c_{j,k} + a, d^*_{j,k} = d_{j,k} + a + 1, a \in \mathbb{F}_2 \Rightarrow w^*_{j,k} = w_{j,k} + 1$.

  If, wlog, one sets $a = 0$, then condition X implies that $D_{j,k} - C^*_{j,k} = -(C_{j,k} + D^*_{j,k})$, and $D_{j,k} + C^*_{j,k} = C_{j,k} - D^*_{j,k}$, leading to factorisation of the matrix in (20):

$$\begin{pmatrix} C_{j,k} + D^*_{j,k} & C_{j,k} - D^*_{j,k} \\ D_{j,k} - C^*_{j,k} & D_{j,k} + C^*_{j,k} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} C_{j,k} + D^*_{j,k} & 0 \\ 0 & D_{j,k} + C^*_{j,k} \end{pmatrix}.$$

  If, for fixed j, condition X holds $\forall k$, $0 \le k < t$, then one can employ permutations γ_j and θ_j on the columns of the two matrix factors. Thus, (20) becomes

$$F_j = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}^{\otimes t} P_{\gamma,j} \bigotimes_{k=0}^{t-1} \begin{pmatrix} C_{j,k} + D^*_{j,k} & 0 \\ 0 & D_{j,k} + C^*_{j,k} \end{pmatrix} P_{\theta,j} F_{j-1},$$

  and, in Boolean terms, this extra permutation generalises $\mathbf{v}_j$ to $\mathbf{v}_{\gamma,j} := (\gamma_{0,j}(\mathbf{v}_j), \gamma_{1,j}(\mathbf{v}_j), \ldots, \gamma_{t-1,j}(\mathbf{v}_j))$, where $\gamma_j = (\gamma_{0,j}, \gamma_{1,j}, \ldots, \gamma_{t-1,j}) : \mathbb{F}_2^t \to \mathbb{F}_2^t$ is a permutation, and $\gamma_{k,j}(\mathbf{v}_j) : \mathbb{F}_2^t \to \mathbb{F}_2$, and we obtain,

$$\mathbf{f}_j = (f_{j,s}, s \in \mathbb{F}_2^t), \qquad f_{j,s} = \mathbf{v}_{\gamma,j}(s) + o_j(\mathbf{w}_j) + \sum_{q=0}^{j-1} \mathbf{v}_{\gamma,q}(\mathbf{w}_{\theta,q+1}) + o_q(\mathbf{w}_q), \quad (31)$$

  where γ_j is the identity permutation $\forall j$ where condition X does not hold.

6.2 Derivation B

Let $J = \left(\begin{smallmatrix} 1 & 1 \\ 1 & 1 \end{smallmatrix}\right)$, $I = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, and let $e_{j,k} = w_{j,k} + w^*_{j,k} + 1$. For U some 2×2 unitary, let $U_k = \bigotimes_{i=0}^{t-1} V^{(i)}$, where $V^{(i)} = I$, $\forall i \neq k$, and $V^{(k)} = U$. From (25),

$$\begin{aligned} \mathbf{f}_j &= \mathbf{v}_j + \textstyle\sum_{q=0}^{j-1} \bigotimes_{k=0}^{t-1} \left(\sum_{p=0}^{j} \begin{pmatrix} w_{p,k} & 0 \\ 0 & w^*_{p,k} \end{pmatrix} J \left(\prod_{r=q+1}^{p-1} e_{r,k} \right) + I \right) \mathbf{v}_q \\ &= \mathbf{v}_j + \textstyle\sum_{q=0}^{j-1} \left(I^{\otimes t} + \sum_{k=0}^{t-1} \sum_{p=0}^{j} \begin{pmatrix} w_{p,k} & 0 \\ 0 & w^*_{p,k} \end{pmatrix}_k J_k \left(\prod_{r=q+1}^{p-1} e_{r,k} \right) \right) \mathbf{v}_q \\ &\quad + ((\ldots) J_k J_{k'} + \ldots + (\ldots) J_k J_{k'} J_{k''} + \ldots + (\ldots) J^{\otimes t}) \, \mathbf{v}_q, \end{aligned}$$

where $\prod_{r=q+1}^{p-1} e_{r,k} = 0$ and 1 for $q \geq p$ and $q = p-1$, respectively. But $J_k J_{k'} \mathbf{v}_q = J_k J_{k'} J_{k''} \mathbf{v}_q = \ldots = J^{\otimes t} \mathbf{v}_q = 0$. So

$$\mathbf{f}_j = \sum_{q=0}^{j} \mathbf{v}_q + \sum_{q=0}^{j-1} \sum_{k=0}^{t-1} \sum_{p=0}^{j} \begin{pmatrix} w_{p,k} & 0 \\ 0 & w^*_{p,k} \end{pmatrix}_k J_k \left(\prod_{r=q+1}^{p-1} e_{r,k} \right) \mathbf{v}_q.$$

With re-arranging,

$$\mathbf{f}_j = \sum_{p=0}^{j} \left(\mathbf{v}_p + \sum_{k=0}^{t-1} \begin{pmatrix} w_{p,k} & 0 \\ 0 & w^*_{p,k} \end{pmatrix}_k J_k \sum_{q=0}^{p-1} \left(\prod_{r=q+1}^{p-1} e_{r,k} \right) \mathbf{v}_q \right).$$

Re-introduce more general O_j and $P_{\theta,j}$ to (20). Abbreviate $\theta_{p,k}(\mathbf{w}_p)$ to $\theta_{p,k}$, and let $e_{\theta,r,k} := \theta_{r,k} + \theta^*_{r,k} + 1$. Then

$$\mathbf{f}_j = \sum_{p=0}^{j} \left(\mathbf{v}_p + o_p(\mathbf{w}_p) + \sum_{k=0}^{t-1} \begin{pmatrix} \theta_{p,k} & 0 \\ 0 & \theta^*_{p,k} \end{pmatrix}_k J_k \sum_{q=0}^{p-1} \left(\prod_{r=q+1}^{p-1} e_{\theta,r,k} \right) \mathbf{v}_q \right). \quad (32)$$

(32) is simplified if, $\forall j, k$, $w^*_{j,k} = w_{j,k}$ or $w^*_{j,k} = w_{j,k} + 1$:

- $w^*_{j,k} = w_{j,k}$: $e_{j,k}$ reduces to 1 and (32) becomes

$$\mathbf{f}_j = \sum_{p=0}^{j} \left(\mathbf{v}_p + o_p(\mathbf{w}_p) + \sum_{k=0}^{t-1} \theta_{p,k} \sum_{q=0}^{p-1} (c_{q,k} + d_{q,k}) \right). \quad (33)$$

- $w^*_{j,k} = w_{j,k} + 1$: $e_{j,k}$ reduces to 0 and 1 for $0 \leq j < p$ and $j = p$, respectively, so (32) becomes

$$\mathbf{f}_j = \mathbf{v}_j + \sum_{p=0}^{j} \left(o_p(\mathbf{w}_p) + \sum_{k=0}^{t-1} \theta_{p,k} (c_{p-1,k} + d_{p-1,k}) + c_{p-1,k} \right). \quad (34)$$

  ♢ If condition X holds for one or more j, then $\mathbf{v}_j$ becomes $\mathbf{v}_{\gamma,j}$, and

$$\mathbf{f}_j = \mathbf{v}_{\gamma,j} + \sum_{p=0}^{j} \left(o_p(\mathbf{w}_p) + \sum_{k=0}^{t-1} \theta_{p,k} (c_{\gamma,p-1,k} + d_{\gamma,p-1,k}) + c_{\gamma,p-1,k} \right). \quad (35)$$

  where γ_j is the identity permutation $\forall j$ where condition X does not hold.

Equation pairs (28) and (32), (29) and (33), (30) and (34), and (31) and (35), are all equivalent. In subsections 6.3, 6.4, and 6.5, we assign these equations to type-I, II, and III, as appropriate. To equate (29) with (33), observe that

$$v_{p-1}(\mathbf{w}_p + s) = v_{p-1}(s) + \sum_{k=0}^{t-1} w_{p,k} (c_{p-1,k} + d_{p-1,k}).$$

To equate (30) with (34), observe that

$$v_{p-1}(\mathbf{w}_p) = \sum_{k=0}^{t-1} w_{p,k} (c_{p-1,k} + d_{p-1,k}) + c_{p-1,k}.$$

6.3 Type-I Boolean

From (5), the action of '$*$' on $C_{j,k}(\mathbf{y}_{j,k}) = (-1)^{c_{j,k}(\mathbf{u}_{j,k})}$ takes $c_{j,k}$ to $c^*_{j,k} = c_{j,k}(\mathbf{u}_{j,k} + \mathbf{1})$. In general we cannot simplify (28) and (32) further but both $w^*_{j,k} = w_{j,k}$ and $w^*_{j,k} = w_{j,k} + 1$ could occur as special cases, in which case (29) and (30) or (33) and (34) are the constructions, respectively. Moreover, if condition X holds for one or more j, then one can further generalise (30) and (34) to (31) and (35), respectively. The special case where $c_{j,k} = 0$, $d_{j,k} = x_{j,k}$, $\forall j, k$, allows for the application of (31) or (35) to generate the type-I complementary set of size 2^t first proposed in [9].

6.4 Type-II Boolean

From (5), the '$*$' has an identity action on $C_{j,k}(\mathbf{y}_{j,k}) = (-1)^{c_{j,k}(\mathbf{u}_{j,k})}$, so $C^*_{j,k} = C_{j,k}$ and $c^*_{j,k} = c_{j,k}$. Similarly for $d_{j,k}$. So $w^*_{j,k} = w_{j,k}$ and (29) or (33) is the construction.

6.5 Type-III Boolean

From (5), the action of '$*$' on $C_{j,k}(\mathbf{y}_{j,k}) = (-1)^{c_{j,k}(\mathbf{u}_{j,k})}$ takes $c_{j,k}$ to $c^*_{j,k} = c_{j,k} + l_{j,k}$, where $l_{j,k} = \mathbf{u}_{j,k} \cdot \mathbf{1} = x_{\mu_{j,k}} + x_{\mu_{j,k}+1} + \ldots + x_{\mu_{j,k}+m_{j,k}-1}$. Similarly for $d_{j,k}$. So $w_{j,k} = w^*_{j,k} = c_{j,k} + d_{j,k} + l_{j,k}$, and (29) or (33) is the construction. The only difference between types II and III is the definition of $w_{j,k}$.

6.6 Comments on the closed-form Boolean expressions

The equivalent type-I expressions of (31) and (35) are also equivalent to that previously stated in [16] and derived in [9], but the proof given here is more concise, and demonstrating, via condition X, that both θ and γ permutations are possible for type-I. We can characterise the Boolean λ-pairs, i.e. $t = 1$, as follows. From (24), with $t = 1$, we obtain

$$\begin{aligned} f_{0,j} &= (c_j + d^*_j)(f_{0,j-1} + f_{1,j-1}) + c_j + f_{0,j-1}, \\ f_{1,j} &= (c^*_j + d_j)(f_{0,j-1} + f_{1,j-1}) + d_j + f_{1,j-1}, \end{aligned} \tag{36}$$

where, for types I, II and III, $c^*_j = c_j(\mathbf{u}_j + \mathbf{1})$, $c^*_j = c_j$, and $c^*_j = c_j + l_j$, respectively, where $l_j = \mathbf{u}_j \cdot \mathbf{1}$. For type-IV in section 4, when C_j and D_j are both eigenvectors (eigenarrays) of M_{y_j}, $\forall j$, then $C^*_j = C_j$ and $D^*_j = D_j$, $\forall j$, which is then the same as type-II. So one can, in that case, use the type-II pair construction. The papers [27,28] examine the Rayleigh quotient of $2 \times 2 \times \ldots \times 2$ arrays from the alphabet $\{1, -1\}$, being a special case of section 4, where $\mathcal{M} = H^{\otimes m}$, and $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. The matrix $H^{\otimes m}$ is the *Walsh-Hadamard transform*, and an

eigenvector of $H^{\otimes m}$, with elements from $\{1, -1\}$, can be described by a Boolean function, in which case it is called an *(anti-)self-dual Boolean function.* [28] gave a secondary construction for a self-dual Boolean function in Theorem 4.9, and that construction is the same as (36) in the type-II case, i.e. the construction of theorem 4.9 of [28] is a special case of the complementary pair construction. It was this observation, amongst others, that motivated the generalisations of this paper. Closed-form Boolean function constructions for complementary sets of types II and III have also been given in [26], that overlap with the functions constructed by (29) and (33), but are not identical to them.

References

1. M.J.E. Golay. Multislit spectroscopy. *J. Opt. Soc. Amer.*, **39**:437–444, 1949.
2. M.J.E. Golay. Static multislit spectrometry and its application to the panoramic display of infrared spectra. *J. Opt. Soc. Amer.*, **41**:468–472, 1951.
3. M.J.E. Golay. Complementary series. *IRE Trans. Inform. Theory*, **IT-7**:82–87, 1961.
4. H.S. Shapiro. Extremal problems for polynomials and power series. Master's thesis, Mass. Inst. of Technology, 1951.
5. R.J. Turyn. Hadamard matrices, Baumert-Hall units, four-symbol sequences, pulse compression, and surface wave encodings. *J. Combin. Theory (A)*, **16**:313–333, 1974.
6. J.A. Davis and J. Jedwab. Peak-to-mean power control in OFDM, Golay complementary sequences, and Reed-Muller codes. *IEEE Trans. Inform. Theory*, **45**:2397–2417, 1999.
7. C.C. Tseng and C.L. Liu. Complementary sets of sequences. *IEEE Trans. Inform. Theory*, **18**, 5:644–652, 1972.
8. H.D. Lüke. Sets of one and higher dimensional Welti codes and complementary codes. *IEEE Trans. Aerospace Electron. Systems*, **AES-21**:170–179, 1985.
9. M.G. Parker and C. Tellambura. A Construction for Binary Sequence Sets with Low Peak-to-Average Power Ratio. *Reports in Informatics*, University of Bergen, **242**, ISSN 0333–3590, Feb. 2003.
10. K.-U. Schmidt. Complementary Sets, Generalized Reed-Muller Codes, and Power Control for OFDM. *IEEE Trans. Inform. Theory*, **53**, 2:808–814, Feb. 2007
11. C.V. Chong, R. Venkataramani, and V. Tarokh. A new construction of 16-QAM Golay complementary sequences. *IEEE Trans. Inform. Theory*, **49**:2953–2959, 2003.
12. R. Craigen and C. Koukouvinos. A theory of ternary complementary pairs. *J. Combin. Theory (Series A)*, **96**:358–375, 2001.
13. R. Craigen, W. Holzmann, and H. Kharaghani. Complex Golay sequences: structure and applications. *Discrete Math.*, **252**:73–89, 2002.
14. M. Dymond. *Barker arrays: existence, generalization and alternatives.* PhD thesis, University of London, 1992.

15. M.G. Parker and C. Tellambura. Generalised Rudin-Shapiro Constructions. *WCC2001 International Workshop on Coding and Cryptography*, Paris(France), Jan 8–12, 2001. *Electronic Notes in Discrete Mathematics*, 6, April 2001 Guest Editors: Daniel Augot and Claude Carlet.
16. M.G. Parker and C. Tellambura. A Construction for Binary Sequence Sets with Low Peak-to-Average Power Ratio. *Int. Symp. Inform. Theory, Lausanne, Switzerland*, 239, June 30–July 5, 2002.
17. P.B. Borwein and R.A. Ferguson. A Complete Description of Golay Pairs for Lengths up to 100. *Math. Comp.*, **73**, 246:967–985, 2003.
18. S. Matsufuji, R. Shigemitsu, Y. Tanada, and N. Kuroyanagi. Construction of Complementary Arrays. *Proc. of Sympotic'04*, 78–81, 2004.
19. J. Jedwab and M.G. Parker. Golay complementary array pairs. *Designs, Codes and Cryptography*, **44**:209–216, 2007.
20. F. Fiedler, J. Jedwab and M.G. Parker. A Multi-dimensional Approach to the Construction and Enumeration of Golay Complementary Sequences. *J. Combinatorial Theory (Series A)*, **115**: 753–776, 2008.
21. K.-U. Schmidt. On Cosets of the Generalized First-Order Reed-Muller Code with Low PMEPR. *IEEE Trans. Inform. Theory*, **52**, 7:3220–3232, July 2006.
22. N. Suehiro. Complete Complementary Codes Composed of N-multiple Shift Orthogonal Sequences. *IEICE Trans. Fundamentals of Electronics, Communications and Computer Sciences (in Japanese)*, **J65-A**, 11:1247–1253, 1982.
23. M.G. Parker. Close encounters with Boolean functions of three different kinds. Invited talk, *Lecture Notes in Computer Science*, **5228**:15–19 September 2008.
24. T.E. Bjørstad and M.G. Parker. Equivalence Between Certain Complementary Pairs of Types I and III, in Enhancing Cryptographic Primitives with Techniques from Error Correcting Codes. Invited talk at *NATO Science for Peace and Security Series - D: Information and Communication Security*, **23**, Edited by: B. Preneel, S. Dodunekov, V. Rijmen and S. Nikova, June 2009.
25. M.G. Parker. Polynomial Residue Systems via Unitary Transforms. Invited talk in post-proceedings of *Contact Forum Coding Theory and Cryptography III*, The Royal Flemish Acadamy of Belgium for Science and the Arts, Brussels, Belgium.
26. C. Riera and M.G. Parker. Boolean functions whose restrictions are highly nonlinear. Invited talk at *ITW 2010 Dublin - IEEE Information Theory Workshop*, 30 August – 3 Sept. 2010.
27. L.E. Danielsen, M.G. Parker, and P. Solé. The Rayleigh quotient of bent functions. *Lecture Notes in Computer Science*, **5921**, 418–432, 2009.
28. C. Carlet, L.E. Danielsen, M.G. Parker, and P. Solé. Self-dual bent functions. *Int. J. Inform. and Coding Theory*, **1**, 4:384–399, 2010.
29. M.A. Nielsen, and I.L. Chuang *Quantum Computation and Quantum Information.* Cambridge University Press, 2001.