The selfnegadual properties of generalised quadratic Boolean functions

Lars Eirik Danielsen and Matthew G. Parker

Department of Informatics, University of Bergen, PO Box 7803, N-5020 Bergen, Norway
{larsed,matthew}@ii.uib.no
http://www.ii.uib.no/~{larsed,matthew}

Abstract. We define and characterise selfnegadual generalised quadratic Boolean functions by establishing a link, both to the multiplicative order of symmetric binary matrices, and also to the Hermitian self-dual $\mathbb{F}_4$-linear codes. This facilitates a novel way to classify Hermitian self-dual $\mathbb{F}_4$-linear codes.

Keywords: generalised Boolean functions; selfnegadual functions; negabent functions; bent functions; negaHadamard transform; Walsh Hadamard transform; Fourier eigenspectra; selfdual codes; quantum codes

1 Introduction

In this paper an n-variable generalised quadratic Boolean function refers to a function in $\mathrm{ZRM}(2,n)$ (the quaternary Reed-Muller code). To be explicit, if $f : \mathbb{F}_2^n \rightarrow \mathbb{Z}_4$ is of the form:

$$f(x) = 2(\sum_{j<k} a_{jk}x_jx_k) + 2(\sum_j b_jx_j + c) + \sum_j a_{jj}x_j + d \tag{1}$$

where $a_{jk}, a_{jj}, b_j, c, d \in \mathbb{F}_2$, then it is a function in $\mathrm{ZRM}(2,n)$. We consider f and its phase representation, i^f, where $i^2 = -1$, and $i^f = (i^{f(x)}, x \in \mathbb{F}_2^n)$, is interpreted as a column vector of 2^n elements. When $a_{jj} = d = 0$, $\forall j$, then $f/2$ is a quadratic Boolean function. We consider a map from f to an $n \times n$ binary symmetric matrix, $A_f = (a_{ij})$, where the off-diagonal part refers to Boolean quadratic terms, the diagonal part refers to $\mathbb{Z}_4$-linear terms, and the binary linear coefficients, b_i, together with the constant term, c, is called the *binary affine offset*, and is ignored for the map to a matrix. To simplify notation, and without loss of generality, we assume, throughout this paper, that $c = d = 0$.

Recent papers [4,8,11] have classified and constructed Boolean functions that are *selfdual*, i.e. their phase representations are eigenvectors of the *Walsh-Hadamard* transform - such functions are therefore bent. Another direction is to classify and construct Boolean functions that are *negabent* or *bent-negabent* (both bent and negabent) [15,16]. We show that a function in $\mathrm{ZRM}(2,n)$ can never be both selfdual and negabent. Let a function be called *selfnegadual* if its phase representation is an eigenvector of the *negaHadamard* transform - such functions are therefore negabent and it turns out that they are also bent. We show that there are no quadratic selfnegadual Boolean functions, but that there are selfnegadual functions in $\mathrm{ZRM}(2,n)$. So, in this paper, we answer the following question:

Question 1. `Which functions in` $\mathrm{ZRM}(2,n)$ `are selfnegadual?`

The main result of this paper is to characterise those functions in $\mathrm{ZRM}(2,n)$ that are *selfnegadual.*

We came at this problem from an unusual direction. Our initial question was in the context of the study of multiplicative orders of symmetric binary matrices. Let A be such a matrix, and let it have order p if $A^p = I$, the identity, and $A^j \neq I$, for $1 \leq j < p$. We say that $\mathrm{ord}(A) = p$, where A can only have an order if A has maximum rank. If $f \in \mathrm{ZRM}(2,n)$ is selfdual, then $\mathrm{ord}(A_f) = 2$ [4]. If f is negabent then $A_f + I$ has maximum rank [15]. However, if $\mathrm{ord}(A_f) = 2$ then $A_f + I$ cannot have maximum rank. This motivates the question:

Question 2. `For which` $n \times n$ `symmetric binary matrices,` A`, is ord`(A) `and ord`$(A+I)$ `jointly minimised to 3?`

An $n \times n$ symmetric binary matrix, A, represents an n-vertex undirected graph with possible loops. For ω primitive in $\mathbb{F}_4$, the rowspace of matrix $A + wI$ is a Hermitian selfdual $\mathbb{F}_4$-additive code of blocklength n. The graphical interpretation has been used to aid in classifying all selfdual $\mathbb{F}_4$-additive codes up to blocklength 12 [7]. A small subset of these matrices, $A + \omega I$, generate selfdual $\mathbb{F}_4$-additive codes that are also selfdual $\mathbb{F}_4$-linear of blocklength n - all selfdual $\mathbb{F}_4$-linear codes can be represented in this way. So we have the question:

Question 3. `For which` $n \times n$ `symmetric binary matrices,` A`, is the` $\mathbb{F}_4$`-additive code generated by` $A + wI$ `also` $\mathbb{F}_4$`-linear?`

Question 3 has been characterised by Van den Nest [17]. Our contribution is to show that questions 2 and 3 are the same question, and also the same as question 1 to within a binary affine offset.

In section 2 we characterise dualities of functions with respect to Walsh-Hadamard and negaHadamard transforms. In section 3 we look at orders of symmetric binary matrices, show how they relate to dualities of a function, and show that order is preserved by action of the orthogonal group. In section 4 we show how selfduality and selfnegaduality relate to linear selfdual codes over $\mathbb{F}_2$ and $\mathbb{F}_4$, respectively, and also, by interpreting the symmetric matrix as an undirected graph, show how a modified form of *local complementation* [2] on the graph preserves selfnegaduality. In section 5 we use graphical interpretation, and orthogonal equivalence, to classify all Hermitian selfdual $\mathbb{F}_4$-linear codes up to $n = 18$.

2 Bentness and selfdualities of functions - definitions

For two length-n vectors, $u = (u_0, u_1, \ldots, u_{n-1})^T$ and $v = (v_0, v_1, \ldots, v_{n-1})^T$, let $u{\cdot}v = \sum_{j=0}^{n-1} u_j v_j$ be the dot-product of u and v, and $uv = (u_0v_0, u_1v_1, \ldots, u_{n-1}v_{n-1})^T$. Let $w(x)$ be the Hamming weight of x.

For $f : \mathbb{F}_2^n \to \mathbb{Z}_4$ in ZRM$(2,n)$, let $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ be the 2×2 Hadamard matrix, and $N = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}$, $i^2 = -1$, be the 2×2 negaHadamard matrix. Let '$\otimes$' indicate the tensor product of matrices.

We define f to be a *bent* function in ZRM$(2,n)$ if

$$F_k = 2^{-n/2} \sum_{j \in \mathbb{F}_2^n} i^{f(x)+2j\cdot k},$$

satisfies $|F_k| = 1$, $\forall k \in \mathbb{F}_2^n$. Alternatively we can write

$$F = H^{\otimes n} i^f.$$

In such a case we can define the *dual* of f by $i^{\hat{f}} = F$, where $\hat{f}$ is also a *bent* function in ZRM$(2,n)$.

We define f to be a *negabent* function in ZRM$(2,n)$ if

$$F_k = \alpha 2^{-n/2} \sum_{j \in \mathbb{F}_2^n} i^{f(x)+2j\cdot k+w(j)},$$

satisfies $|F_k| = 1$, $\forall k \in \mathbb{F}_2^n$, where α is an arbitrary constant that satisfies $|\alpha| = 1$. Alternatively we can write

$$F = \alpha N^{\otimes n} i^f.$$

In such a case we can define the *negadual* of f by $i^{\tilde{f}} = F$, where $\tilde{f}$ is then a bent function in ZRM$(2,n)$.

We summarise the bent and negabent properties in Table 1, as well as the dualities that we discuss in this paper, where $s, r, r' \in \mathbb{F}_2^n$. For brevity, except in the case of selfdual and selfnegadual, we do not make explicit the global multiplicative constants or eigenvalues in these expressions, using symbols α and α' to indicate arbitrary constants that need only satisfy $|\alpha| = |\alpha'| = 1$. In [4] the cases of $\alpha = 1$ and $\alpha = -1$ were used to distinguish between selfdual and anti-selfdual, respectively, but we refer, here to the union of these two simply as selfdual. For selfnegadual, observe that $N^3 = e^{\pi i/4} I$. For some eigenvalue, α, and eigenvector, v, of $N^{\otimes n}$, we have $N^{\otimes n} v = \alpha v$. Therefore $(N^{\otimes n})^3 v = \alpha^3 v = e^{n\pi i/4} v$. Therefore $\alpha \in \{e^{(n+8k)\pi i/12}, k = 0, 1, 2\}$. Choosing f from ZRM$(2,n)$ and selfnegadual restricts α to the alphabet $\{e^{hi\pi/4}\}$, for some integer, h. Theorem 2 and lemma 12 will show that, for such an f, then n must be even. It then follows, uniquely, that $\alpha = e^{-ni\pi/4}$.

If f is bent then its dual, $\hat{f}$, is also bent. But if f is negabent, then its dual, $\tilde{f}$, is only negabent if f is also bent. A selfdual function is bent and a selfnegadual

Table 1: Spectral dualities

Property of $f \in \mathrm{ZRM}(2,n)$	equation satisfied by f
bent	$i^{\hat{f}} = H^{\otimes n} i^f$
negabent	$i^{\tilde{f}} = \alpha N^{\otimes n} i^f$
selfdual	$i^f = \pm H^{\otimes n} i^f$
selfnegadual	$i^f = e^{-ni\pi/4} N^{\otimes n} i^f$
P-dual	$i^{f(x)} = \alpha H^{\otimes n} i^{f(x+s)+2r\cdot x}$
	$= \alpha' H^{\otimes n} i^{f(x)+2r'\cdot x}$
P-negadual	$i^{f(x)} = \alpha N^{\otimes n} i^{f(x+s)+2r\cdot x}$
	$= \alpha' N^{\otimes n} i^{f(x)+2r'\cdot x}$

function is bent-negabent, where bentness of the selfnegadual function follows because $H^{\otimes n} i^{f(x)} = e^{ni\pi/4} H^{\otimes n} N^{\otimes n} i^{f(x)} = e^{ni\pi/4} i^{f(x)+\sum_j x_j}$.

Selfdual and selfnegadual are special cases of *P-dual* and *P-negadual*, respectively. If $f - \hat{f}$ or $f - \tilde{f}$ are of the form $2r \cdot x + c$, for some $r \in \mathbb{F}_2^n$, $c \in \mathbb{F}_4$, then f is P-dual or P-negadual, respectively.

3 Matrix orders and function dualities

We wish to characterise the $n \times n$ binary symmetric matrices, A, such that both $\mathrm{ord}(A)$ and $\mathrm{ord}(A+I)$ are as small as possible. We call A a (p,q)-matrix if A has order p and $A+I$ has order q, where p or q equals '$-$' if A or $A+I$, respectively, does not have maximum rank. Trivially, if $\mathrm{ord}(A) = 1$, then $A = I$ and $A+I$ cannot have maximum rank, in which case A is a $(1,-)$-matrix. Likewise, if $\mathrm{ord}(A) = 2$ then $A+I$ cannot have maximum rank, as $(A+I)^2 = A^2 + I = 0$, in which case A is a $(2,-)$-matrix. One can trivially obtain $(-,1)$ and $(-,2)$ matrices by replacing A by $A+I$ in the above. So our first candidate of interest is for A to be a $(3,3)$-matrix and, indeed, such symmetric binary matrices do exist. After some preliminary lemmas, we present, by considering the conditions on $f \in \mathrm{ZRM}(2,n)$ for selfduality and selfnegaduality, two theorems for $(2,-)$ matrices (theorem 1), and $(3,3)$ matrices (theorem 2), respectively.

Let $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. The following lemma is easily verified.

Lemma 1.

$$\begin{aligned} HX &= ZH, & HZ &= XH, \\ NX &= iZXN, & NZ &= XN. \end{aligned}$$

For $r \in \mathbb{F}_2^n$, U a 2×2 matrix, $U^0 = I$, the identity, and $U^1 = U$, let $U_r = \bigotimes_{0 \le j < n} U^{r_j}$, be a $2^n \times 2^n$ matrix constructed using the tensor product.

Lemma 2. *For f bent,*

$$H^{\otimes n} i^{f(x+r)} = i^{\hat{f}(x)+2r\cdot x}.$$

Proof. By lemma 1 and Table 1,

$$\begin{aligned} H^{\otimes n} i^{f(x+r)} &= H^{\otimes n} X_r i^{f(x)} \\ &= Z_r H^{\otimes n} i^{f(x)} = Z_r i^{\hat{f}(x)} = i^{\hat{f}(x)+2r\cdot x}. \end{aligned}$$

□

Lemma 3. *For f negabent,*

$$N^{\otimes n} i^{f(x+r)} = \alpha i^{\tilde{f}(x+r)+2r\cdot x+w(r)},$$

and

$$N^{\otimes n} i^{f(x)+2r\cdot x} = \alpha i^{\tilde{f}(x+r)}.$$

Proof. By lemma 1 and Table 1,

$$\begin{aligned} N^{\otimes n} i^{f(x+r)} &= N^{\otimes n} X_r i^{f(x)} \\ &= i^{w(r)} Z_r X_r N^{\otimes n} i^{f(x)} = \alpha Z_r X_r i^{\tilde{f}(x)+w(r)} = \alpha i^{\tilde{f}(x+r)+2r\cdot x+w(r)}. \end{aligned}$$

For the second part,

$$N^{\otimes n} i^{f(x)+2r\cdot x} = N^{\otimes n} Z_r i^{f(x)} = X_r N^{\otimes n} i^{f(x)} = \alpha X_r i^{\tilde{f}(x)} = \alpha i^{\tilde{f}(x+r)}.$$

□

Lemma 4. *For $f \in ZRM(2,n)$, and for any $r \in \mathbb{F}_2^n$,*

$$f(x+r) = f(x) + 2A_f r\cdot x + f(r) - f(0).$$

Proof. From (1), $f(x) = 2q(x) + 2b\cdot x + a\cdot x + f(0)$, where q is a homogeneous quadratic, and $b, a \in \mathbb{F}_2^n$. Then $2q(x+r) = 2(q(x) + A_q r\cdot x + q(r))$, $2b\cdot(x+r) = 2b\cdot x + 2b\cdot r$, and $a\cdot(x+r) = a\cdot x + 2ar\cdot x + a\cdot r$. Therefore $f(x+r) = 2q(x+r) + 2b\cdot(x+r) + a\cdot(x+r) + f(0) = (2q(x)+2b\cdot x+a\cdot x+f(0)) + 2(A_q r+ar)\cdot x + (2q(r)+2b\cdot r+a\cdot r)$. Observe that $A_f r = A_q r + ar$. □

Theorem 1. *If f is selfdual or anti-selfdual then A_f is a $(2,-)$-matrix, and $f(r) = -f(A_f r) + 2f(0)$, $\forall r \in \mathbb{F}_2^n$. Conversely, if A_f is a $(2,-)$-matrix, then $A_{\hat{f}} = A_f$, i.e. f is P-dual, and $f(r) = -\hat{f}(A_f r) + f(0) + \hat{f}(0)$, $\forall r \in \mathbb{F}_2^n$.*

Proof. Using Table 1, lemmas 2 and 4, if f is selfdual or anti-selfdual,

$$H^{\otimes n} i^{f(x+r)} = H^{\otimes n} i^{f(x)+2A_f r\cdot x+f(r)-f(0)} = \alpha i^{f(x)+2r\cdot x}.$$

Similarly,

$$H^{\otimes n} i^{f(x+A_f r)} = H^{\otimes n} i^{f(x)+2A_f^2 r\cdot x+f(A_f r)-f(0)} = \alpha i^{f(x)+2A_f r\cdot x}, \qquad \alpha \in \pm 1.$$

Then, as $H^{\otimes n}$ is self-inverse,

$$\alpha i^{f(x)+2r\cdot x-f(r)+f(0)} = \alpha^{-1} i^{f(x)+2A_f^2 r\cdot x+f(A_f r)-f(0)},$$

from which $A_f^2 = I$ and $f(r) = -f(A_f r) + 2f(0)$. For the converse, we have that

$$H^{\otimes n} i^{f(x+r)} = H^{\otimes n} i^{f(x)+2A_f r\cdot x+f(r)-f(0)} = i^{\hat{f}(x)+2r\cdot x},$$

and

$$H^{\otimes n} i^{\hat{f}(x+A_f r)} = H^{\otimes n} i^{\hat{f}(x)+2A_{\hat{f}} A_f r\cdot x+\hat{f}(A_f r)-\hat{f}(0)} = i^{f(x)+2A_f r\cdot x}.$$

Combining gives

$$i^{\hat{f}(x)+2r\cdot x-f(r)+f(0)} = i^{\hat{f}(x)+2A_{\hat{f}} A_f r\cdot x+\hat{f}(A_f r)-\hat{f}(0)}.$$

□

Let $\mathcal{E}_f$ be the eigenspace of A_f associated with the eigenvalue 1 (we are working mod 2, so all eigenvectors have eigenvalue 1).

Lemma 5. *If f is selfdual or anti-selfdual, and $e \in \mathcal{E}_f$, then so is $f + 2e \cdot x$. Conversely, if both f and $f + 2e \cdot x$ are selfdual or anti-selfdual, then $e \in \mathcal{E}_f$. Consequently, if f is selfdual or anti-selfdual, then so are $|\mathcal{E}_f|$ binary linear offsets of f.*

Proof. Assume $f(0) = 0$. Then, from theorem 1, if f is selfdual or anti-selfdual, then $f(r) + f(A_f r) = 0$. For $e \in \mathcal{E}_f$ we have $A_f e = e$, so $(A_f + I)e = 0$, mod 2, and $2(A_f + I)e = 0$, mod 4. Therefore $f(r) + f(A_f r) + 2(A_f + I)e \cdot r = 0$. But $2(A_f + I)e \cdot r = 2(A_f + I)r \cdot e$, so $(f(r) + 2r \cdot e) + (f(A_f r) + 2A_f r \cdot e) = 0$, so $f + 2e \cdot x$ is selfdual. The converse is similarly proved, and the argument is easily generalised to $f(0)$ other than 0. □

Theorem 2. *If f is selfnegadual then A_f is a $(3,3)$-matrix, and $f(A_f r) = w(r) + f(0)$, $\forall r \in \mathbb{F}_2^n$. Conversely, if A_f is a $(3,3)$-matrix then $A_{\tilde{f}} = A_f$, f is P-negadual, and $f(r) = \tilde{f}(r) - \tilde{f}(A_f r) + f(0) + w(r)$.*

Proof. Using Table 1, lemmas 3 and 4, if f is selfnegadual,

$$N^{\otimes n} i^{f(x)+2A_f r\cdot x} = \alpha i^{f(x+A_f r)} = \alpha i^{f(x)+2A_f^2 r\cdot x+f(A_f r)-f(0)},$$

and

$$N^{\otimes n} i^{f(x+r)-f(r)+f(0)} = \alpha i^{f(x+r)+2r\cdot x+w(r)-f(r)+f(0)} = \alpha i^{f(x)+2(A_f+I)r\cdot x+w(r)}.$$

But, by lemma 4, we can equate these equations. So, taking the righthand expressions of both lines we get $f(x) + 2A_f^2 r \cdot x = f(x) + 2(A_f + I)r \cdot x$ and $f(A_f r) - f(0) = w(r)$. Therefore $A_f^2 = A_f + I$, mod 2, (implying that both A_f

and $A_f + I$ have order 3), and $f(A_f r) = w(r) + f(0)$, and the first part of the theorem follows. For the second part we obtain, in a similar fashion,

$$i^{\tilde{f}(x)+2A_{\tilde{f}}A_f r\cdot x+\tilde{f}(A_f r)-\tilde{f}(0)} = i^{\tilde{f}(x)+2(A_{\tilde{f}}+I)r\cdot x+\tilde{f}(r)-f(r)+\tilde{f}(0)+f(0)+w(r)},$$

leading to $A_{\tilde{f}}A_f = A_{\tilde{f}}+I$ and $f(r) = \tilde{f}(r)-\tilde{f}(A_f r)+f(0)+w(r)$. The argument is completed by observing that A_f a $(3,3)$ matrix implies that $A_f + I$ has maximum rank, with inverse A_f. So, as $A_{\tilde{f}}(A_f + I) = I$, then $A_{\tilde{f}} = A_f$. □

It is later shown in lemma 12 that, if A_f is a $(3,3)$ matrix, then n must be even.

From the equation $f(A_f r) = w(r) + f(0)$ of theorem 2, it is evident that, if A_f is a $(3,3)$ matrix then f is uniquely defined, to within a constant:

Corollary 1. *If f is selfnegadual then $f + 2e \cdot x$ is not selfnegadual $\forall e \in \mathbb{F}_2^n$, $e \neq 0$.*

It remains to derive an expression for the binary vector $b \in \mathbb{F}_2^n$ of (1). Let $\mu = (\mu_0, \mu_1, \ldots, \mu_{n-1})$, where μ_i is the Hamming weight of column i of A_f. Let $a \in \mathbb{F}_2^n$ be the diagonal of A_f, and let $\mathbf{1}$ be the all-ones vector of length-n.

Lemma 6. *If f is selfnegadual, then*

$$b = \frac{1}{2}\langle \mu + a + \mathbf{1}\rangle_4,$$

where $\langle * \rangle_4$ means reduce, mod 4.

Proof. Wlog we can restrict to $f(0) = 0$. Then, from theorem 2, $f(A_f r) = w(r)$. Therefore, as $(A_f + I)A_f = I$, then $f(r) = w((A_f + I)r)$. When r has Hamming weight 1, then $f(r) = (a + 2b) \cdot r$, and $w((A_f + I)r) = \mu \cdot r - 2a \cdot r + 1$. So $2b = \mu + a + \mathbf{1}$. □

Examples: Let $g = 2x_0x_1 + x_1$, where $n = 2$. Then A_g is a $(3,3)$ matrix. Moreover $\mu = (1,2)$, and $a = (0,1)$. So $2b = (1,2) + (0,1) + (1,1) = (2,0)$ and, from lemma 6, $f = 2x_0x_1 + 2x_0 + x_1$ is selfnegadual.

Now let $g = 2(x_0x_1 + x_0x_2 + x_0x_5 + x_1x_3 + x_1x_5 + x_2x_4 + x_2x_5 + x_3x_4 + x_3x_5 + x_4x_5) + x_5$, where $n = 6$. Then A_g is a $(3,3)$ matrix. Moreover $\mu = (3,3,3,3,3,6)$, and $a = (0,0,0,0,0,1)$. So $2b = (4,4,4,4,4,8) = (0,0,0,0,0,0)$ and $f = g$ is selfnegadual.

Before continuing, we summarise function dualities of f in terms of the associated orders of A_f. For instance, we indicate the property 'A_f has an order' by the row 'ord(A_f)', and indicate the property 'f is bent' by the column 'f bent'. There is a $\surd$ ('tick') symbol at the intersection of this row and column to indicate that one property implies the other. The $-$ symbol indicates that the row/column properties do not imply each other. The $\surd$ symbol is replaced by a number (2 or 3) if the order of A_f or $A_f + I$ is known explicitly.

property of:	f	f	f	$f + \sum_j x_j$	f
	bent	negabent	P-dual	P-dual	P-negadual
$\mathrm{ord}(A_f)$	$\surd$	–	2	–	3
$\mathrm{ord}(A_f + I)$	–	$\surd$	–	2	3

Remarks: The condition in the proof of theorem 2 that $A + I$ has maximum rank is important, as both $(3, -)$ and $(-, 3)$ matrices exist. For A of order 3, $(A^3 + I) = (A^2 + A + I)(A + I)$, and the condition that $(A + I)$ has maximum rank is equivalent to the condition that $A^2 + A + I = 0$.

Lemma 7. *[1,13] An invertible binary symmetric matrix can be factored in the form MM^T iff it has at least one nonzero term on the main diagonal.*

If $f \in \mathrm{ZRM}(2, n)$ is such that A_f has zero diagonal, then f is a quadratic Boolean function.

Lemma 8. *If f is a bent quadratic Boolean function, then A_f has even order.*

Proof. If A_f has odd order, p, then we can write $A_f = B^2$, where $B = A_f^{\frac{p+1}{2}}$. But, B is symmetric as A_f is symmetric so $A_f = BB^T$ which, by lemma 7, is impossible as A_f has no ones on its diagonal. □

Lemma 9. *There are no selfnegadual quadratic Boolean functions.*

Proof. By theorem 2, A_f has order 3 if $f \in \mathrm{ZRM}(2, n)$ is selfnegadual. Therefore, by lemma 8, f cannot be a quadratic Boolean function. □

Remark: The result of lemma 9 can also be deduced from the thesis of Van den Nest [17], in the context of $\mathbb{F}_4$-additive and $\mathbb{F}_4$-linear codes.

We identify an action which preserves the (p, q) property of a matrix. An orthogonal matrix, U, satisfies $UU^T = I$. The set of $n \times n$ binary orthogonal matrices forms a group, $\mathcal{O}_n$, under multiplication. Then it is trivial to show that UAU^T is a (p, q)-matrix iff A is a (p, q)-matrix, and corollary 2 follows immediately from this observation.

Corollary 2. *For $U \in \mathcal{O}_n$ and $f(x) \in ZRM(2, n)$, and by theorems 1 and 2, if $f(x)$ is selfdual then so is $f(Ux)$ and, if $f(x)$ is selfnegadual then so is $f(Ux)$.*

4 Graphs and code dualities

Let A be an $n \times n$ symmetric binary matrix. Then A can be used to generate codes, and can also be interpreted as an adjacency matrix for an undirected graph, where the graph of A has loops if its diagonal is non-zero. The next lemma is well-known.

Lemma 10. *If A has zero diagonal, and if $A^2 = I$ then the linear space generated by the rows of $A{+}I$ is a self-orthogonal binary linear code of dimension rank$(A{+}I)$. In particular, if A is the adjacency matrix for a bipartite graph with equal-size partitions, then $A + I$ generates a selfdual binary linear code.*

Proof. The rows of A are pairwise orthogonal as $A^2 = I$. Therefore the rows of $A + I$ are pairwise orthogonal as A is symmetric. The linear space generated by $A + I$ is self-orthogonal because $(A + I)(A + I)^T = 0$. For the last part, $A = \left(\begin{smallmatrix} 0 & P \\ P^T & 0 \end{smallmatrix}\right)$, P square, so $A + I$ spans a self-dual code. □

An *additive* code over $\mathbb{F}_4 = \{0, 1, \omega, \overline{\omega} = \omega + 1\}$ of length n is a $\mathbb{F}_2$-linear subgroup of $\mathbb{F}_4^n$. We define the *dual* of the code $\mathcal{C}$ with respect to the *trace inner product* as $\mathcal{C}^\perp = \{\boldsymbol{u} \in \mathbb{F}_4^n \mid \sum_{i=1}^n (u_i\overline{c_i} + \overline{u_i}c_i) = 0 \text{ for all } \boldsymbol{c} \in \mathcal{C}\}$, and say that it is *selfdual* if $\mathcal{C} = \mathcal{C}^\perp$. A *linear* code over $\mathbb{F}_4$ which is selfdual with respect to the *Hermitian inner product*, i.e., $\boldsymbol{u} \cdot \overline{\boldsymbol{v}}$, is also selfdual additive with respect to the trace inner product. However, most selfdual additive codes are not $\mathbb{F}_4$-linear. Two selfdual additive codes over $\mathbb{F}_4$ are *equivalent* if we can obtain one from the other by permuting, scaling, and conjugating coordinates. Equivalence of selfdual linear codes is defined similarly, with the exception that conjugating single coordinates is not permitted.

It is known [17] that any selfdual additive code has a *standard form* $n \times n$ generator matrix of the form $A + \omega I$, where I is the identity matrix and A is a binary symmetric matrix. It is also known [17] that two codes are equivalent iff the corresponding graphs are related via *local complementation* (LC) [2]. Given a generator matrix of standard form, conjugating a coordinate is equivalent to complementing a diagonal element in A. Hence, for selfdual additive codes considered up to equivalence, this diagonal can always be set to zero. For selfdual linear codes (represented by overdefined $n \times n$ generator matrices), the diagonal is of importance and can in fact never be zero.

Lemma 11. *[17] For A and B symmetric, a Hermitian selfdual $\mathbb{F}_4$-additive code, generated by $A + \omega B$, is $\mathbb{F}_4$-linear iff $AA^T + BB^T + AB^T = 0$. Moreover, if $B = I$, this condition reduces to $A^2 + A + I = 0$.*

Corollary 3. *$A + \omega I$ is the codespace of a Hermitian selfdual $\mathbb{F}_4$-linear code iff A is a $(3, 3)$ matrix.*

Proof. Follows from lemma 11 as the condition $A^2 + A + I = 0$ immediately implies that both A and $A + I$ have order 3. □

Let G_A be the n-vertex graph of A with an edge between i and j iff $a_{ij} = 1$, and a loop at vertex j iff $a_{jj} = 1$.

Lemma 12. *If A is a $(3, 3)$ matrix, then all vertices of G_A have odd degree, disregarding loops. In such a case, n, the number of vertices, must be even.*

Proof. Since A is a $(3, 3)$ function, $A^2 = A + I$. Hence the diagonal entries in A^2 must be the complements of the diagonal entries of A. This criterion is satisfied iff there is an odd number of 1s among the off-diagonal entries in each row of A. The number of edges of a graph equals the sum of the vertex degrees divided by 2. But, if all vertex degrees are odd, then n must be even. □

Remark: It is also a well-known fact that all codewords of selfdual $\mathbb{F}_4$-linear codes have even weight, which amounts to the same thing.

It is known [7] that *local complementation* (LC) acting on G_A, where loops are ignored, preserves, to within equivalence, the $\mathbb{F}_4$ additive selfdual code generated by $A + \omega I$. However, for those additive codes that are also linear codes, one has to modify local complementation to take account of loops, so that the additive code remains linear after local complementation. We first describe this modified form of local complementation (LC*) and then prove that it preserves linearity of the $\mathbb{F}_4$ codespace. Let $\mathcal{N}_j \subset \{0, 1, \ldots, n-1\}$ be the set of vertices that are neighbours to vertex j in G_A (not including j itself). Let LC* at vertex j of G_A produce the graph $G_{A'}$.

Modified local complementation (LC*):

LC* on G_A at vertex j is realised by

$$\begin{array}{ll} a'_{ik} = a'_{ki} = a_{ik} + 1 & i, k \in \mathcal{N}_j, \\ a'_{ik} = a'_{ki} = a_{ik} & \text{otherwise.} \\ a'_{ii} = a_{ii} + 1 & i \in j \bigcup \mathcal{N}_j, \\ a'_{ii} = a_{ii} & \text{otherwise.} \end{array}$$

Lemma 13. *Let $G_{A'}$ be the graph resulting from LC* on G_A at some vertex. If A is a $(3,3)$-matrix, then A' is also a $(3,3)$-matrix.*

Proof. Let LC* act on G_A at vertex j. Let $D = (d_{ik})$ and $V = (v_{ik})$ be $n \times n$ binary matrices such that $d_{jj} = 1$ and $d_{ik} = 0$ otherwise, and $v_{ik} = 1$, $\forall i, k \in \mathcal{N}_j, i \neq k$, and $v_{ik} = 0$ otherwise. Then, by the LC* rule, one can see that $A' = A + D + V$. A' is a $(3,3)$-matrix iff $A'^2 = A' + I$. But $A'^2 = (A + D + V)^2 = (A^2 + D^2 + V^2) + (AD + DA) + (AV + VA) + (DV + VD)$. But $A^2 = A + I$ as A is a $(3,3)$-matrix. Moreover it is easily verified that $D^2 = D$. Using lemma 12, $V^2 = V$, and $AD + DA = AV + VA$. D and V are row/column disjoint, so $DV + VD = 0$. Therefore, $A'^2 = A + I + D + V = A' + I$, as required. □

The modified local complementation proposed in [3] differs crucially from ours - when doing a local complementation at vertex j, they do not flip the diagonal at j, whereas we do.

5 Code classification

Selfdual linear codes over $\mathbb{F}_4$ have been classified up to length 16 [5,14]. As a consequence of lemma 11 and corollary 3, we can use the correspondence to (3,3) matrices to devise a new algorithm and classify codes of length 18. During the process of extending the result to length 20, we became aware that codes of length 18 and 20 have already been classified independently in two preprints recently made available online [9,10]. However, we still give an overview of our approach, since it gives different theoretical insights and highlights the connection between selfdual codes and selfnegadual Boolean functions.

Table 2: Number of selfdual linear codes over $\mathbb{F}_4$ of length n [5,9,10,14]

n	2	4	6	8	10	12	14	16	18	20
	1	1	2	3	5	10	21	55	245	3427

It has been shown in theorem 3.1 of [11] that all $(2,-)$ symmetric matrices are orthogonally equivalent to one of a small set of canonical forms. We use a similar proof method to obtain the following theorem.

Theorem 3. [1]
Let A be a $(3,3)$ matrix of size $n \times n$. Then A is orthogonally congruent to the canonical form $C_n = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right) \otimes I_{n/2}$, where $I_{n/2}$ is the $n/2 \times n/2$ identity matrix, i.e. there always exists an orthogonal matrix, $U \in \mathcal{O}_n$, such that

$$A = U(\left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right) \otimes I_{n/2})U^T.$$

Proof. We make repeated use of the identity $A^2 + A + I = 0$. Let $v = (1, 0, 0, \ldots, 0)$ be of length n. Then $vv^T = 1$. We aim to convert, in t steps, A to C_n by successive actions of the form $V_t A V_t^T$, where $V_t \in \mathcal{O}_n$. Then $U = V_{t-1} \ldots V_1 V_0$. Moreover, wlog we consider only the case of $A = (a_{ij})$ where $a_{00} = 0$ because, when $a_{00} = 1$ then we can orthogonally transform $A^2 = A + I$ instead to obtain C_n. Then $C_n = UA^2U^T = U(A+I)U^T = UAU^T + I$, and so $(XU)A(U^TX) = C_n$.

Given the above we have that $vAv^T = 0$ and $vA^2v^T = 1$. We create the $n \times n$ matrix,

$$V = \begin{pmatrix} v \\ vA = a_0 \\ v_2 \\ v_3 \\ \cdots \\ v_{n-1} \end{pmatrix},$$

and we wish to choose v_j so that $vv_j^T = vAv_j^T = v_kv_j^T = 0$, $2 \leq j, k < n$, $j \neq k$, in which case $V \in \mathcal{O}_n$. If we can do this then

$$V^TAV = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right) \oplus B,$$

where B is a $(3,3)$ matrix of size $(n-2) \times (n-2)$. The proof follows by induction on B, to obtain C_n.

It remains to show that we can always select the v_j so that $V \in \mathcal{O}_n$. Let us further assume that $a_{01} = 0$. If this is not the case then it can always be

[1] We thank Prof. Alexander Pott for suggesting the proof strategy used for this theorem.

made so by the action PAP^T, where P is a row/column permutation satisfying $PP^T = I$, iff $a_0 \neq (011\ldots11)$. Let us assume, for now, that $a_0 \neq (011\ldots11)$. Then, by orthogonality, we require V to be of the form $V = 1 \oplus R$, where R is an $(n-1) \times (n-1)$ orthogonal matrix. But non-trivial binary orthogonal matrices are of even dimension so R is orthogonal iff $R = Q(I_k \oplus R')Q^T$, where I_k is the $k \times k$ identity, k odd, Q is some permutation, and R' is an $(n-1-k) \times (n-1-k)$ orthogonal matrix. For suitable k we can make R' orthogonal by choosing it to be $R' = J_{n-1-k} + I_{n-1-k}$, were J_k is the all-ones matrix of dimension k, on condition that $a_0 = (0, 0, a_{02}, \ldots, a_{0(n-1)})$ has odd weight, which it does by lemma 12. Permutation Q always exists, so R can be made orthogonal, and therefore V can be made orthogonal. We just need to show that $a_0 \neq (011\ldots11)$ can be avoided. Imagine that A is such that $a_0 = (011\ldots11)$. Then swap row and column 0 of A with row and column $j > 0$, and call this D. This is an orthogonal conjugation so D is also $(3,3)$. Then $D = (d_{ij})$ has $d_{00} = 1$ so now orthogonally conjugate D^2, as mentioned previously. Self-duality of the associated $\mathbb{F}_4$-additive code [7] implies that $w(d_0 + d_j) > 1$, so the first row of D^2 is never equal to $(011\ldots11)$. □

Example (to illustrate proof of theorem 3) Let $A = \begin{pmatrix} 111111 \\ 100101 \\ 100011 \\ 110010 \\ 101100 \\ 111000 \end{pmatrix}$. Then A is a $(3,3)$ matrix. As $a_{00} = 1$ we conjugate $A^2 = \begin{pmatrix} 011111 \\ 110101 \\ 101011 \\ 110110 \\ 101110 \\ 111001 \end{pmatrix}$ instead. As $a_0 = (011111)$ we swap a_0 and, say, a_2 to get D. As $d_{00} = 1$ we orthogonally conjugate $D^2 = \begin{pmatrix} 001011 \\ 001101 \\ 111111 \\ 011010 \\ 101100 \\ 111000 \end{pmatrix}$. Choose $V = \begin{pmatrix} 100000 \\ 001011 \\ 010000 \\ 000111 \\ 001101 \\ 001110 \end{pmatrix}$. Then $VDV^T = \left(\begin{smallmatrix} 01 \\ 11 \end{smallmatrix}\right) \oplus \begin{pmatrix} 0010 \\ 0001 \\ 1010 \\ 0101 \end{pmatrix}$. ... and so on ....

Corollary 4. *(of theorem 3) Given two $(3,3)$ matrices, A and A', of size $n \times n$, there always exists an orthogonal matrix $U \in \mathcal{O}_n$ such that $A' = UAU^T$.*

By our classification, we verify theorem 3 numerically for $n \leq 18$. Also note that it has been shown by Janusz [12] that all selfdual binary codes of length n are equivalent under the action of $\mathcal{O}_n$. It is known [12] that $\mathcal{O}_n$ is generated by all matrices of the form PM, where P is a permutation matrix and $M = \begin{pmatrix} I_{n-4} & 0 \\ 0 & I_4 + J_4 \end{pmatrix}$, where J_4 is the 4×4 all-one matrix. As a canonical representative for selfdual $\mathbb{F}_4$-linear codes of length n, we choose the matrix $C_n = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right) \otimes I_{n/2}$. Starting from C_n, we then apply orthogonal transforms until one representative from each equivalence class has been found. (Which is verified by checking the *mass formula* [14].) In practice, we achieve this by generating $C' = (PM)C_n(PM)^T$ for all the $\binom{n/2}{4}$ non-trivial permutations P. Then C' is treated as a graph with loops and checked for isomorphism against all previously seen graphs. If C' is new, the corresponding code is output, and the complete LC*-orbit of C', using modified local complementation, is generated and stored. (This is not strictly necessary, but speeds up the algorithm, since

LC*-operations are faster than orthogonal transforms.) We proceed recursively, generating matrices $(PM)C'(PM)^T$, and so on, until all codes are found. With this algorithm, classifying all codes of length $n \leq 18$ was achieved in about two hours of CPU time on a standard desktop computer.

6 Discussion - further work

It is of interest to consider further how the order of a symmetric binary matrix relates to its associated code and/or graph. We offer here one brief observation that may be worth pursuing:

The optimal Hermitian selfdual additive code over $\mathbb{F}_4$ for $n = 6$ is the *hexacode*, with distance 4. It can be generated by the matrix $A_f + \omega I$, with associated function, $f \in \mathrm{ZRM}(2,6)$ given by $f = 2(x_0x_1 + x_0x_2 + x_1x_2 + x_3x_4 + x_3x_5 + x_4x_5 + x_0x_3 + x_1x_4 + x_2x_5)$, where we zero the diagonal of A_f. The graph, G_{A_f}, is in so-called 'nested-clique' form, specifically the '2-clique of 3-cliques' graph [6]. Let $A_g = (A_f + I)^2$. Then $g = x_0x_1 + x_0x_2 + x_1x_2 + x_3x_4 + x_3x_5 + x_4x_5$, and G_{A_g} is the disjoint sum of two 3-cycles, $C_3 \oplus C_3$. Similarly, the *dodecacode* is the optimal code for $n = 12$ with distance 6. It can be represented by a graph, G_{A_f}, which is a '3-clique of 4-cliques' [6]. Let $A_g = (A_f + I)^2$. Then G_{A_g} is the disjoint sum of two 6-cycles, $C_6 \oplus C_6$. A near-optimal code for $n = 18$, and with distance 6, can be represented by a graph, G_{A_f}, which is a '2-clique of 3-cliques of 3-cliques' [6] (the optimal code has distance 8). Let $A_g = (A_f + I)^6$. Then G_{A_g} is the disjoint sum of two 9-cycles, $C_9 \oplus C_9$. Moreover, for $A_{g'} = (A_f + I)^2$, then $G_{A_{g'}}$ is the disjoint sum of two '3-clique of 3-cliques', which is an optimal code for $n = 9$ with distance 4. These preliminary observations motivate a classification of optimal (or near-optimal) codes and of nested-clique graphs that arise as 'roots' of the disjoint cycles.

Acknowledgement The authors would like to thank the reviewers for their helpful suggestions which improved the quality of the submission. We would also like to thank Prof. Alexander Pott for helping with one of the proofs. This work was supported by the Norwegian Research Council (NFR).

References

1. Albert, A.A.: Symmetric and alternating matrices in an arbitrary field. AMS Trans. **43** (1938) 386–436
2. Bouchet, A.: Graphic presentations of isotropic systems. J. Combin. Theory Ser. B **45**(1) (1988) 58–76
3. Brijder, R., Hoogeboom J.H.: Pivot and Loop Complementation on Graphs and Set Systems. Theory and applications of models of computation, Lecture Notes in Computer Science, LNCS 6108 (2010) 151–162
4. Carlet, C., Danielsen, L.E., Parker, M.G., Solé, P.: Self-dual bent functions. Int. J. Inform. and Coding Theory **1**(4) (2010) 384–399

5. Conway, J.H., Pless, V., Sloane, N.J.A.: Self-dual codes over GF(3) and GF(4) of length not exceeding 16. IEEE Trans. Inform. Theory **25**(3) (1979) 312–322
6. Danielsen, L.E., Parker, M.G.: Spectral orbits and peak-to-average power ratio of Boolean functions with respect to the $\{I, H, N\}^n$ transform. Sequences and Their Applications - SETA 2004, Lecture Notes in Computer Science, LNCS 3486, (2005) 373–388
7. Danielsen, L.E., Parker, M.G.: On the classification of all self-dual additive codes over GF(4) of length up to 12. Journal of Combinatorial Theory, Series A, **113**(7) Oct. (2006) 1351–1367
8. Danielsen, L.E., Parker, M.G., Solé, P.: The Rayleigh quotient of bent functions. 12th IMA International Conference on Cryptography and Coding, 15–17 Dec. 2009, Cirencester, UK, Lecture Notes in Computer Science, LNCS 5921 (2009) 418–432
9. Harada, M., Lam, C., Munemasa, A., Tonchev, V.D.: Classification of generalized Hadamard matrices H(6,3) and quaternary Hermitian self-dual codes of length 18. Electronic J. Combinatorics **17** (2010), #R171.
10. Harada, M., Munemasa, A.: Classification of quaternary Hermitian self-dual codes of length 20. IEEE Trans. Inform. Theory **57**(6) (2011) 3758–3762
11. Hou, X-D.: Classification of self dual quadratic bent functions. Designs, Codes and Cryptography, **63**(2), (2012), 183–198
12. Janusz, G.J.: Parametrization of self-dual codes by orthogonal matrices. Finite Fields Appl. **13**(3) (2007) 450–491
13. MacWilliams, J.: Orthogonal Matrices Over Finite Fields. The American Mathematical Monthly. **76**(2) (1969) 152–164
14. MacWilliams, F.J., Odlyzko, A.M., Sloane, N.J.A., Ward, H.N.: Self-dual codes over GF(4). J. Combin. Theory Ser. A **25**(3) (1978) 288–318
15. Parker, M.G., Pott, A.: On Boolean functions which are bent and negabent. S.W. Golomb, G. Gong, T. Helleseth and H.Y. Song, (Eds.), Sequences, Subsequences, and Consequences, International Workshop, SSC 2007, Los Angeles, CA, USA, May 31 – June 2, 2007, Lecture Notes in Computer Science, LNCS 4893 (2007)
16. Schmidt, K-U., Parker, M.G., Pott, A.: Negabent Functions in the Maiorana-McFarland Class. Sequences and Their Applications - SETA 2008, University of Kentucky, Lexington, KY, Lecture Notes in Computer Science, LNCS 5203 Sept. (2008) 14–18
17. Van den Nest, M.: Local Equivalence of Stabilizer States and Codes. PhD thesis, K. U. Leuven, Belgium (May 2005)