The selfnegadual properties of generalised quadratic Boolean functions

Lars Danielsen, Matthew Parker

The selfnegadual properties of generalised quadratic Boolean functions

Lars Eirik Danielsen and Matthew G. Parker

The Selmer Center, Department of Informatics, University of Bergen, PB 7800,
N-5020 Bergen, Norway,
larsed@ii.uib.no, matthew@ii.uib.no

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 $f:\mathbb{F}_2^n \to \mathbb{Z}_4$ 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 $i^f = (i^{f(k)})$, $k \in \mathbb{F}_2^n$, is interpreted as a column vector of 2^n elements. When $a_{jj} = d = 0$, $\forall j$, then f 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, 7] 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) [13, 14]. 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 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 [13]. 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 [6]. 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 [15]. 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

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

We summarise, in table 1, the dualities that we discuss in this paper, where $s, r, r' \in \mathbb{F}_2^n$, and $w(x)$ is the Hamming weight of x. 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 11 will show that, for such an f, then n must be even. It then follows, uniquely, that $\alpha = e^{-ni\pi/4}$.

Table 1. Spectral dualities

Property of $f \in$ ZRM$(2, n)$	equation satisfied by f
bent	$i^{\hat{f}} = \alpha H^{\otimes n} i^f$
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	$i^{f(x)} = \alpha H^{\otimes n} i^{f(x+s)+r\cdot x}$
	$= \alpha' H^{\otimes n} i^{f(x)+r'\cdot x}$
P-negadual	$i^{f(x)} = \alpha N^{\otimes n} i^{f(x+s)+r\cdot x}$
	$= \alpha' N^{\otimes n} i^{f(x)+r'\cdot x}$

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 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 binary affine 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 ord(A) and 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. 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 $X = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ and $Z = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$. 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,*

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

Proof. By lemma 1 and table 1,

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

□

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 $r \in \mathbb{F}_2^n$, $r \neq 0$,*

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

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

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

Proof. Using table 1, lemmas 2 and 4,

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

Similarly,

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

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

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

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

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

and

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

Combining gives

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

□

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

Proof. Using table 1, lemmas 3 and 4,

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

and

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

But, by lemma 4, we can equate these equations and the first part of the theorem follows. For the second part we obtain, in a similar fashion,

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

leading to $A_f + I = A_f A_{\tilde{f}}$ and $f(A_{\tilde{f}}r) = f(r) - \tilde{f}(r) + w(r)$. The argument is completed by constraining $\mathrm{ord}(A_f) = 3$, and $A_f + I$ to be of maximum rank, in which case A_f is a $(3,3)$ matrix and $A_f^2 + A_f + I = 0$. □

Before continuing, we summarise function dualities of f in terms of the associated orders of A_f.

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 $A^2 + A + I = 0$. In the full paper we discuss the binary offsets, b in (1), required to make a P-dual or P-negadual function, f, selfdual or selfnegadual, respectively, for A_f a $(2,-)$ or $(3,3)$ matrix, respectively. For A_f a given $(2,-)$ matrix the set of valid b vectors is of size the binary eigenspace of A_f but, for A_f a given $(3,3)$ matrix, there is only one valid b vector, as follows from condition $f(A_f r) = w(r)$, $\forall r \neq 0$, in theorem 2.

Lemma 5. *[1, 11] 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 6. *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 5, is impossible as A_f has no ones on its diagonal. □

Lemma 7. *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 6, f cannot be a quadratic Boolean function. □

Remark: The result of lemma 7 can also be deduced from the thesis of Van den Nest [15], 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.

Lemma 8. *For A a symmetric $n \times n$ matrix, and $U \in \mathcal{O}_n$, then UAU^T is a (p, q)-matrix iff A is a (p, q)-matrix.*

Proof. We have that $(UAU^T)^p = UA^pU^T = I$. For $0 < j < p$, we need to show that $UA^jU^T \neq I$. But if $UA^jU^T = I$ then UA^j is the matrix inverse of U^T, and there is only one inverse of U^T, namely U, so $U^j = I$ and $UA^jU^T \neq I$. The same argument holds if we replace A by $A + I$, and p by q. Moreover, if A_f or $A_f + I$ are not of maximum rank, then neither are their orthogonal transformations, so non-order is also preserved by the action of $\mathcal{O}_n$. □

Corollary 1. *(of lemma 8) 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 9. *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, $A = \begin{pmatrix} 0 & P \\ P^T & 0 \end{pmatrix}$, 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 [15] 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 [15] 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 10. *[15] 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 2. *$A + \omega I$ is the codespace of a Hermitian selfdual $\mathbb{F}_4$-linear code iff A is a $(3, 3)$ matrix.*

Proof. Follows from lemma 10 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 11. *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 [6] 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 12. *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 11, $V^2 = V$, 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, 12]. As a consequence of lemma 10 and corollary 2, 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 [8, 9]. 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, 8, 9, 12]

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

Conjecture 1. Given two $n \times n$ (3,3) matrices A and A', there always exists an orthogonal matrix $U \in \mathcal{O}_n$ such that $A' = UAU^T$.

By our classification, we verify this conjecture numerically for $n \leq 18$. Also note that it has been shown by Janusz [10] that all selfdual binary codes of length n are equivalent under the action of $\mathcal{O}_n$. It is known [10] 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 $2n$, we choose the matrix $C = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right) \otimes I_n$. Starting from C, we then apply orthogonal transforms until one representative from each equivalence class has been found. (Which is verified by checking the *mass formula* [12].) In practice, we achieve this by generating $C' = (PM)C(PM)^T$ for all the $\binom{n}{4}$ non-trivial permutations P. C' is then

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.

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.: 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
7. 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
8. 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. `arXiv:1007.2555` (2010)
9. Harada, M., Munemasa, A.: Classification of quaternary Hermitian self-dual codes of length 20. `arXiv:1012.0898` (2010)
10. Janusz, G.J.: Parametrization of self-dual codes by orthogonal matrices. Finite Fields Appl. **13**(3) (2007) 450–491
11. MacWilliams, J.: Orthogonal Matrices Over Finite Fields. The American Mathematical Monthly. **76**(2) (1969) 152–164
12. 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
13. 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)
14. 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
15. Van den Nest, M.: Local Equivalence of Stabilizer States and Codes. PhD thesis, K. U. Leuven, Belgium (May 2005)