Twin bent functions and Clifford algebras

Paul C. Leopardi

Mathematical Sciences Institute, The Australian National University.
paul.leopardi@anu.edu.au

Abstract. This paper examines a pair of bent functions on $\mathbb{Z}_2^{2m}$ and their relationship to a necessary condition for the existence of an automorphism of an edge-coloured graph whose colours are defined by the properties of a canonical basis for the real representation of the Clifford algebra $\mathbb{R}_{m,m}$. Some other necessary conditions are also briefly examined.

1 Introduction

A recent paper [7] constructs a sequence of edge-coloured graphs Δ_m ($m \geqslant 1$) with two edge colours, and makes the conjecture that for $m \geqslant 1$, there is an automorphism of Δ_m that swaps the two edge colours. This conjecture can be refined into the following question.

Question 1. Consider the sequence of edge coloured graphs Δ_m ($m \geqslant 1$) as defined in [7], each with red subgraph $\Delta_m[-1]$, and blue subgraph $\Delta_m[1]$. For which $m \geqslant 1$ is there an automorphism of Δ_m that swaps the subgraphs $\Delta_m[-1]$ and $\Delta_m[1]$?

Considering that it is known that $\Delta_m[-1]$ is a strongly regular graph, a more general question is:

Question 2. For which parameters (n, k, λ, μ) is there a an edge coloured graph Γ on n vertices, with two edge colours, red (with subgraph $\Gamma[-1]$) and blue (with subgraph $\Gamma[1]$), such that the red subgraph $\Gamma[-1]$ is a strongly regular graph with parameters (n, k, λ, μ), and such that there exists an automorphism of Γ that swaps $\Gamma[-1]$ with $\Gamma[1]$?

These questions were asked (in a slightly different form) at the workshop on "Algebraic design theory with Hadamard matrices" in Banff in July 2014. This paper examines some of the necessary conditions for the graph Δ_m to have an automorphism as per Question 1. Question 2 remains open for future investigation.

Considering that $\Delta_m[-1]$ is a strongly regular graph, the first necessary condition is that $\Delta_m[1]$ is also a strongly regular graph, with the same parameters. This is proven as Theorem 22 in Section 5. Some other necessary conditions are addressed in Section 6.

2 A monomial representation and a related bent function

The following definitions and results appear in the paper on Hadamard matrices and Clifford algebras [7], and are presented here for completeness, since they are used below. Further details and proofs can be found in that paper, unless otherwise noted.

The signed group $\mathbb{G}_{p,q}$ of order 2^{1+p+q} is extension of $\mathbb{Z}_2$ by $\mathbb{Z}_2^{p+q}$, defined by the signed group presentation

$$\begin{aligned}\mathbb{G}_{p,q} := \Big\langle\ & \mathbf{e}_{\{k\}}\ (k \in S_{p,q})\ \mid \\ & \mathbf{e}_{\{k\}}^2 = -1\ (k<0), \quad \mathbf{e}_{\{k\}}^2 = 1\ (k>0), \\ & \mathbf{e}_{\{j\}}\mathbf{e}_{\{k\}} = -\mathbf{e}_{\{k\}}\mathbf{e}_{\{j\}}\ (j \neq k)\Big\rangle,\end{aligned}$$

where $S_{p,q} := \{-q, \ldots, -1, 1, \ldots, p\}$.

The following construction of the real monomial representation $P(\mathbb{G}_{m,m})$ of the group $\mathbb{G}_{m,m}$ is used in [7].

The 2×2 orthogonal matrices

$$\mathrm{E}_1 := \begin{bmatrix} . & - \\ 1 & . \end{bmatrix}, \quad \mathrm{E}_2 := \begin{bmatrix} . & 1 \\ 1 & . \end{bmatrix}$$

generate $P(\mathbb{G}_{1,1})$, the real monomial representation of group $\mathbb{G}_{1,1}$. The cosets of $\{\pm I\} \equiv \mathbb{Z}_2$ in $P(\mathbb{G}_{1,1})$ are ordered using a pair of bits, as follows.

$$\begin{aligned} 0 &\leftrightarrow 00 \leftrightarrow \{\pm I\}, \\ 1 &\leftrightarrow 00 \leftrightarrow \{\pm \mathrm{E}_1\}, \\ 2 &\leftrightarrow 10 \leftrightarrow \{\pm \mathrm{E}_2\}, \\ 3 &\leftrightarrow 11 \leftrightarrow \{\pm \mathrm{E}_1\mathrm{E}_2\}. \end{aligned}$$

For $m > 1$, the real monomial representation $P(\mathbb{G}_{m,m})$ of the group $\mathbb{G}_{m,m}$ consists of matrices of the form $G_1 \otimes G_{m-1}$ with G_1 in $P(\mathbb{G}_{1,1})$ and G_{m-1} in $P(\mathbb{G}_{m-1,m-1})$. The cosets of $\{\pm I\} \equiv \mathbb{Z}_2$ in $P(\mathbb{G}_{m,m})$ are ordered by concatenation of pairs of bits, where each pair of bits uses the ordering as per $P(\mathbb{G}_{1,1})$, and the pairs are ordered as follows.

$$\begin{aligned} 0 &\leftrightarrow 00\ldots00 \leftrightarrow \{\pm I\}, \\ 1 &\leftrightarrow 00\ldots01 \leftrightarrow \{\pm I_{(2)}^{\otimes(m-1)} \otimes \mathrm{E}_1\}, \\ 2 &\leftrightarrow 00\ldots10 \leftrightarrow \{\pm I_{(2)}^{\otimes(m-1)} \otimes \mathrm{E}_2\}, \\ &\ldots \\ 2^{2m}-1 &\leftrightarrow 11\ldots11 \leftrightarrow \{\pm(\mathrm{E}_1\mathrm{E}_2)^{\otimes m}\}. \end{aligned}$$

(Here $I_{(2)}$ is used to distinguish this 2×2 unit matrix from the $2^m \times 2^m$ unit matrix I.) In this paper, this ordering is called the *Kronecker product ordering* of the cosets of $\{\pm I\}$ in $P(\mathbb{G}_{m,m})$.

The Kronecker product ordering of the canonical basis matrices of $P(\mathbb{R}_{m,m})$ the real monomial representation of the Clifford algebra $\mathbb{R}_{m,m}$ is given by an ordered transversal of $\{\pm I\} \equiv \mathbb{Z}_2$ in $P(\mathbb{G}_{m,m})$, using the Kronecker product ordering. For example, $(I, \mathrm{E}_1, \mathrm{E}_2, \mathrm{E}_1\mathrm{E}_2)$ is the Kronecker product ordering of the canonical basis matrices of $P(\mathbb{R}_{1,1})$.

Definition 3. *For some transversal of $\mathbb{Z}_2$ in $P(\mathbb{G}_{m,m})$, in the Kronecker product ordering, we define a function $\gamma_m : \mathbb{Z}_{2^{2m}} \to P(\mathbb{G}_{m,m})$ to choose the corresponding canonical basis matrix for $P(\mathbb{R}_{m,m})$. The Kronecker product ordering then defines a corresponding function on $\mathbb{Z}_2^{2m}$, which we also call γ_m. For example, $\gamma_1(1) = \gamma_1(01) := \mathrm{E}_1$.*

We recall here a number of well-known properties of the representation $P(\mathbb{G}_{m,m})$.

Lemma 4. *The group $\mathbb{G}_{m,m}$ and its real monomial representation $P(\mathbb{G}_{m,m})$ satisfy the following properties.*

1. *Pairs of elements of $\mathbb{G}_{m,m}$ (and therefore $P(\mathbb{G}_{m,m})$) either commute or anti-commute: for $g, h \in \mathbb{G}_{m,m}$, either $hg = gh$ or $hg = -gh$.*
2. *The matrices $E \in P(\mathbb{G}_{m,m})$ are orthogonal: $EE^T = E^T E = I$.*
3. *The matrices $E \in P(\mathbb{G}_{m,m})$ are either symmetric and square to give I or skew and square to give $-I$: either $E^T = E$ and $E^2 = I$ or $E^T = -E$ and $E^2 = -I$.*

The following properties of the diagonal elements of $P(\mathbb{G}_{m,m})$ are less well-known.

Lemma 5. *The set of diagonal matrices $D_m \subset P(\mathbb{G}_{m,m})$ forms a subgroup of order 2^{m+1} of $P(\mathbb{G}_{m,m})$, consisting of the union of the following cosets of $\{\pm I\}$, listed in Kronecker product order.*

$$\begin{aligned}
00\ldots00 &\leftrightarrow \{\pm I\},\\
00\ldots11 &\leftrightarrow \{\pm I_{(2)}^{\otimes(m-1)} \otimes \mathrm{E}_1 E_2\},\\
&\ldots\\
11\ldots1100 &\leftrightarrow \{\pm(\mathrm{E}_1\mathrm{E}_2)^{\otimes(m-1)} \otimes I_{(2)}\},\\
11\ldots11 &\leftrightarrow \{\pm(\mathrm{E}_1\mathrm{E}_2)^{\otimes m}\}.
\end{aligned}$$

Each coset of D_m in $P(\mathbb{G}_{m,m})$ consists of a set of 2^{m+1} monomial matrices, all of which have the same support.

Definition 6. *We use the basis element selection function γ_m of Definition 3 to define the* sign-of-square *function $\sigma_m : \mathbb{Z}_2^{2m} \to \mathbb{Z}_2$ as*

$$\sigma_m(i) := \begin{cases} 1 \leftrightarrow \gamma_m(i)^2 = -I \\ 0 \leftrightarrow \gamma_m(i)^2 = I, \end{cases}$$

for all i in $\mathbb{Z}_2^{2m}$.

Since each $\gamma_m(i)$ is orthogonal (from Lemma 4), $\sigma_m(i) = 1$ if and only if $\gamma_m(i)$ is skew.

Definition 7. *[6, p. 74].*

A Boolean function $f : \mathbb{Z}_2^m \to \mathbb{Z}_2$ is bent *if its Hadamard transform has constant magnitude. Specifically:*

1. *The Sylvester Hadamard matrix H_m, of order 2^m, is defined by*
$$H_1 := \begin{bmatrix} 1 & 1 \\ 1 & - \end{bmatrix},$$
$$H_m := H_{m-1} \otimes H_1, \quad \text{for} \quad m > 1.$$
2. *For a Boolean function $f : \mathbb{Z}_2^m \to \mathbb{Z}_2$, define the vector $\underline{f}$ by*
$$\underline{f} := [(-1)^{f[0]}, (-1)^{f[1]}, \ldots, (-1)^{f[2^m-1]}]^T,$$
where the value of $f[i], i \in \mathbb{Z}_{2^m}$ is given by the value of f on the binary digits of i.
3. *In terms of these two definitions, the Boolean function $f : \mathbb{Z}_2^m \to \mathbb{Z}_2$ is bent if*
$$\left|H_m \underline{f}\right| = C[1, \ldots, 1]^T.$$
for some constant C.

The following lemma is proven in [7].

Lemma 8. *The function σ_m is a bent function on $\mathbb{Z}_2^{2m}$.*

3 A second bent function

The basis element selection function γ_m also gives rise to a second function, τ_m on $\mathbb{Z}_{2^{2m}}$ as follows.

Definition 9. *We define the* non-diagonal-symmetry *function τ_m on $\mathbb{Z}_{2^{2m}}$ and $\mathbb{Z}_2^{2m}$ as follows.*

For i in $\mathbb{Z}_2^2$:

$$\tau_1(i) := \begin{cases} 1 & \text{if } i = 10, \text{ so that } \gamma_1(i) = \pm \mathrm{E}_2, \\ 0 & \text{otherwise.} \end{cases}$$

For i in $\mathbb{Z}_2^{2m-2}$:

$$\begin{aligned} \tau_m(00 \odot i) &:= \tau_{m-1}(i), \\ \tau_m(01 \odot i) &:= \sigma_{m-1}(i), \\ \tau_m(10 \odot i) &:= \sigma_{m-1}(i) + 1, \\ \tau_m(11 \odot i) &:= \tau_{m-1}(i). \end{aligned}$$

where $\odot$ denotes concatenation of bit vectors, and σ is the sign-of-square function, as above.

It is easy to verify that $\tau_m(i) = 1$ if and only if $\gamma_m(i)$ is symmetric but not diagonal. This can be checked directly for τ_1. For $m > 1$ it results from properties of the Kronecker product of square matrices, specifically that $(A \otimes B)^T = A^T \otimes B^T$, and that $A \otimes B$ is diagonal if and only if both A and B are diagonal.

The first main result of this paper is the following.

Theorem 10. *The function τ_m is a bent function on $\mathbb{Z}_2^{2m}$.*

The proof of Theorem 10 uses the following result, due to Tokareva [11], and stemming from the work of Canteaut, Charpin and others [4, Theorem V.4][5, Theorem 2].

Lemma 11. *[11, Theorem 1] If a binary function f on $\mathbb{Z}_2^{2m}$ can be decomposed into four functions f_0, f_1, f_2, f_3 on $\mathbb{Z}_2^{2m-2}$ as*

$$f(00 \odot i) =: f_0(i), \qquad f(01 \odot i) =: f_1(i),$$
$$f(10 \odot i) =: f_2(i), \qquad f(11 \odot i) =: f_3(i),$$

where all four functions are bent, with dual functions such that $\tilde{f}_0 + \tilde{f}_1 + \tilde{f}_2 + \tilde{f}_3 = 1$, then f is bent.

Proof of Theorem 10. In Lemma 11, set $f_0 = f_3 := \tau_{m-1}, f_1 = \sigma_{m-1}, f_2 = \sigma_{m-1} + 1$. Clearly, $\tilde{f}_0 = \tilde{f}_3$. Also, $\tilde{f}_2 = \tilde{f}_1 + 1$, since $H_{m-1}[f_2] = -H_{m-1}[f_1]$. Therefore $\tilde{f}_0 + \tilde{f}_1 + \tilde{f}_2 + \tilde{f}_3 = 1$. Thus, these four functions satisfy the premise of Lemma 11, as long as both σ_{m-1} and τ_{m-1} are bent.

It is known that σ_m is bent for all m. It is easy to show that τ_1 is bent, directly from its definition. Therefore τ_m is bent. □

4 Bent functions and Hadamard difference sets

The following well known properties of Hadamard difference sets and bent functions are noted in [7].

Definition 12. *[6, pp. 10 and 13].*

The k-element set D is a (v, k, λ, n) difference set *in an abelian group G of order v if for every non-zero element g in G, the equation $g = d_i - d_j$ has exactly λ solutions (d_i, d_j) with d_i, d_j in D. The parameter $n := k - \lambda$. A (v, k, λ, n) difference set with $v = 4n$ is called a* Hadamard difference set*.*

Lemma 13. *[6, Remark 2.2.7] [8, 9]. A Hadamard difference set has parameters of the form*

$$(v, k, \lambda, n) = (4N^2, 2N^2 - N, N^2 - N, N^2)$$
$$\text{or} \quad (4N^2, 2N^2 + N, N^2 + N, N^2).$$

Lemma 14. *[6, Theorem 6.2.2] The Boolean function $f : \mathbb{Z}_2^m \to \mathbb{Z}_2$ is bent if and only if $D := f^{-1}(1)$ is a Hadamard difference set.*

Together, these properties, along with Lemma 8 and Theorem 10, are used here to prove the following result.

Theorem 15. *The sets $\sigma_m^{-1}(1)$ and $\tau_m^{-1}(1)$ are both Hadamard difference sets, with the same parameters*

$$(v_m, k_m, \lambda_m, n_m) = (4^m, 2^{2m-1} - 2^{m-1}, 2^{2m-2} - 2^{m-1}, 2^{2m-2}).$$

Proof. Both σ_m and τ_m are bent functions, as per Lemma 8 and Theorem 10 respectively. Therefore, by Lemma 14, both $\sigma_m^{-1}(1)$ and $\tau_m^{-1}(1)$ are Hadamard difference sets. In both cases, the relevant abelian group is $\mathbb{Z}_2^{2m}$, with order 4^m. Thus in Lemma 13 we must set $N = 2^{m-1}$ to obtain that either

$$(v_m, k_m, \lambda_m, n_m) = (4^m, 2^{2m-1} - 2^{m-1}, 2^{2m-2} - 2^{m-1}, 2^{2m-2}) \text{ or}$$
$$(v_m, k_m, \lambda_m, n_m) = (4^m, 2^{2m-1} + 2^{m-1}, 2^{2m-2} + 2^{m-1}, 2^{2m-2}).$$

Since $\sigma_m(i) = 1$ if and only if $\gamma_m(i)$ is skew, and $\tau_m(i) = 1$ if and only if $\gamma_m(i)$ is symmetric but not diagonal, not only are these conditions mutually exclusive, but also, for all $m \geqslant 1$, the number of i for which $\sigma_m(i) = \tau_m(i) = 0$ is positive. These are the i for which $\gamma_m(i)$ is diagonal. Thus $k_m = 2^{2m-1} - 2^{m-1}$ rather than $2^{2m-1} + 2^{m-1}$. The result follows immediately. □

As a check, the parameters k_m can also be calculated directly, using the recursive definitions of each of σ_m and τ_m.

5 Bent functions and strongly regular graphs

This section examines the relationship between the bent functions σ_m and τ_m and the subgraphs $\Delta_m[-1]$ and $\Delta_m[1]$ mentioned above. First we revise some known properties of Cayley graphs and strongly regular graphs, as noted in the previous paper on Hadamard matrices and Clifford algebras [7], including the result of Bernasconi and Codenotti [1] on the relationship between bent functions and strongly regular graphs.

First we recall a special case of the definition of a Cayley graph.

Definition 16. *The* Cayley graph *of a binary function $f : \mathbb{Z}_2^m \to \mathbb{Z}_2$ is the undirected graph with adjacency matrix F given by $F_{i,j} = f(g_i + g_j)$, for some ordering $(g_1, g_2, \ldots)$ of $\mathbb{Z}_2^m$.*

Now, the definition of a strongly regular graph.

Definition 17. *[2, 3, 10]. A simple graph Γ of order v is* strongly regular *with parameters (v, k, λ, μ) if*

- *each vertex has degree k,*
- *each adjacent pair of vertices has λ common neighbours, and*
- *each nonadjacent pair of vertices has μ common neighbours.*

The result of Bernasconi and Codenotti [1] on the relationship between bent functions and strongly regular graphs is the following.

Lemma 18. *[1, Lemma 12]. The Cayley graph of a bent function on Z_2^m is a strongly regular graph with $\lambda = \mu$.*

We use this result to examine the graph Δ_m as defined here.

Definition 19. *Let Δ_m be the graph whose vertices are the $n^2 = 4^m$ canonical basis matrices of the real representation of the Clifford algebra $\mathbb{R}_{m,m}$, with each edge having one of two colours, -1 (red) and 1 (blue):*

- *Matrices A_j and A_k are connected by a red edge if they have disjoint support and are anti-amicable, i.e. $A_j A_k^{-1}$ is skew.*
- *Matrices A_j and A_k are connected by a blue edge if they have disjoint support and are amicable, i.e. $A_j A_k^{-1}$ is symmetric.*
- *Otherwise there is no edge between A_j and A_k.*

We call this graph the restricted amicability / anti-amicability graph *of the Clifford algebra $\mathbb{R}_{m,m}$, the restriction being the requirement that an edge only exists for pairs of matrices with disjoint support.*

Definition 20. *For a graph Γ with edges coloured by -1 (red) and 1 (blue), $\Gamma[-1]$ denotes the* red subgraph *of Γ, the graph containing all of the vertices of Γ, and all of the red (-1) coloured edges. Similarly, $\Gamma[1]$ denotes the* blue subgraph *of Γ.*

The following theorem is presented in [7].

Theorem 21. *For all $m \geqslant 1$, the graph $\Delta_m[-1]$ is strongly regular, with parameters $v_m = 4^m$, $k_m = 2^{2m-1} - 2^{m-1}$, $\lambda_m = \mu_m = 2^{2m-2} - 2^{m-1}$.*

Unfortunately, the proof given there is incomplete, proving only that $\Delta_m[-1]$ is strongly regular, without showing why $k_m = 2^{2m-1} - 2^{m-1}$ and $\lambda_m = \mu_m = 2^{2m-2} - 2^{m-1}$. In this section, we rectify this by proving the following.

Theorem 22. *For all $m \geqslant 1$, both graphs $\Delta_m[-1]$ and $\Delta_m[1]$ is strongly regular, with parameters $v_m = 4^m$, $k_m = 2^{2m-1} - 2^{m-1}$, $\lambda_m = \mu_m = 2^{2m-2} - 2^{m-1}$.*

Proof. Since each vertex of Δ_m is a canonical basis element of the Clifford algebra $\mathbb{R}_{m,m}$, we can impose the Kronecker product ordering on the vertices, labelling each vertex A by $\gamma_m{-}1(A) \in \mathbb{Z}_2^{2m}$. The colour $\kappa_m(a,b)$ of each edge $(\gamma_m(a), \gamma_m(b))$ of Δ_m depends on $a + b$ in the following way:

$\kappa_m(a,b) := \tau_m(a+b) - \sigma_m(a+b)$, that is,

$$\kappa_m(a,b) = \begin{cases} -1, & \sigma_m(a+b) = 1 \quad (\Leftrightarrow \gamma_m(a+b) \text{ is skew}), \\ 0, & \sigma_m(a+b) = \tau_m(a+b) = 0 \quad (\Leftrightarrow \gamma_m(a+b) \text{ is diagonal}), \\ 1, & \tau_m(a+b) = 1 \quad (\Leftrightarrow \gamma_m(a+b) \text{ is symmetric but not diagonal}). \end{cases}$$

Thus $\Delta_m[-1]$ is isomorphic to the Cayley graph of σ_m on $\mathbb{Z}_2^{2m}$, and $\Delta_m[1]$ is isomorphic to the Cayley graph of τ_m on $\mathbb{Z}_2^{2m}$. Since, by Lemma 8 and Theorem 10, both σ_m and τ_m are bent functions on $\mathbb{Z}_2^{2m}$, Lemma 18 implies that both $\Delta_m[-1]$ and $\Delta_m[1]$ are strongly regular graphs.

It remains to determine the graph parameters. Firstly, v_m is the number of vertices, which is 4^m.

Since $\Delta_m[-1]$ is regular, we can determine k_m by examining one vertex, $\gamma_m(0)$. The edges $(\gamma_m(0), \gamma_m(b))$ of $\Delta_m[-1]$ are those for which $\sigma_m(b) = 1$, that is, the edges where b is in the Hadamard difference set $\sigma_m^{-1}(1)$. Thus, by Theorem 15, $k_m = 2N^2 - N = 2^{2m-1} - 2^{m-1}$, where $N = 2^{m-1}$.

Since $\Delta_m[-1]$ is a strongly regular graph, it holds that

$$(v_m - k_m - 1)\mu_m = k_m(k_m - 1 - \lambda_m)$$

[10, p. 158] and hence, since $\lambda_m = \mu_m$, we must have $(v_m - 1)\lambda_m = k_m(k_m - 1)$ and therefore

$$\lambda_m = k_m(k_m - 1)/(v_m - 1).$$

We now note that

$$\begin{aligned} k_m(k_m - 1) &= (2N^2 - N)(2N^2 - N - 1) = (N^2 - N)(4N^2 - 1) \\ &= (2^{2m-2} - 2^{m-1})(v_m - 1), \end{aligned}$$

so that $\lambda_m = \mu_m = 2N^2 - N = 2^{2m-2} - 2^{m-1}$.

Running through these arguments again, with $\Delta_m[1]$ substituted for $\Delta_m[-1]$ and τ_m substituted for σ_m, yields the same parameters for $\Delta_m[1]$. □

Remark. A more elementary derivation of the value of λ_m for $\Delta_m[-1]$ follows.

There are $k_m(k_m-1)$ ordered pairs (a, b) with $a \neq b$ and $\sigma_m(a) = \sigma_m(b) = 1$. Since $k_m(k_m-1) = (N^2-N)(4N^2-1)$, this gives exactly $N^2-N = 2^{2m-2}-2^{m-1}$ ordered pairs for each of other $4^m - 1$ vertices of $\Delta_m[-1]$.

Also, considering that $\sigma_m^{-1}(1)$ is a Hadamard difference set, and for $c \in \mathbb{Z}_2^{2m}$, $c \neq 0$, consider one of the pairs (a, b) such that $\sigma_m(a) = \sigma_m(b) = 1$ and $c = a + b$. Thus $b = a + c$ and $\sigma_m(a) = \sigma_m(a + c) = 1$. Therefore, the graph $\Delta_m[-1]$ contains the edges $(\gamma_m(0), \gamma_m(a))$, $(\gamma_m(0), \gamma_m(b))$, $(\gamma_m(c), \gamma_m(a))$, and $(\gamma_m(c), \gamma_m(b))$. Thus, in the graph $\Delta_m[-1]$, the vertices $\gamma_m(0)$ and $\gamma_m(c)$ have the two vertices $\gamma_m(a)$ and $\gamma_m(b)$ in common. This is true whether or not there is an edge between $\gamma_m(0)$ and $\gamma_m(c)$. The pair (b, a) yields the same four edges. Running through all such pairs (a, b) and using Theorem 15 again, we see that $\lambda_m = \mu_m = 2N^2 - N = 2^{2m-2} - 2^{m-1}$.

6 Other necessary conditions

This section examines two other necessary conditions for the existence of an automorphism of Δ_m that swaps $\Delta_m[-1]$ with $\Delta_m[1]$. The first condition follows.

Theorem 23. *If an automorphism $\theta : \Delta_m \to \Delta_m$ exists that swaps $\Delta_m[-1]$ with $\Delta_m[1]$, then there is an automorphism $\Theta : \Delta_m \to \Delta_m$ that also swaps $\Delta_m[-1]$ with $\Delta_m[1]$, leaving $\gamma_m(0)$ fixed.*

Proof. For the purposes of this proof, assume the Kronecker product ordering of the canonical basis elements of $\mathbb{R}_{m,m}$ and define the one-to-one mapping $\phi : \mathbb{Z}_2^{2m} \to \mathbb{Z}_2^{2m}$ such that $\theta(\gamma_m(a)) = \gamma_m(\phi(a))$ for all $a \in \mathbb{Z}_2^{2m}$. The condition that θ swaps $\Delta_m[-1]$ with $\Delta_m[1]$ is equivalent to the condition

$$\kappa_m(\phi(a) + \phi(b)) = -\kappa_m(a + b),$$

where κ_m is as defined in the proof of Theorem 22 above.

Let $\Phi(a) := \phi(a) + \phi(0)$ for all $a \in Z_2^{2m}$. Then $\Phi(a) + \Phi(b) = \phi(a) + \phi(b)$ for all $a, b \in Z_2^{2m}$, and therefore

$$\kappa_m(\Phi(a) + \Phi(b)) = \kappa_m(\phi(a) + \phi(b)) = -\kappa_m(a + b).$$

Now define $\Theta : \Delta_m \to \Delta_m$ such that $\Theta(\gamma_m(a)) = \gamma_m(\Phi(a))$ for all $a \in \mathbb{Z}_2^{2m}$. □

The second condition is simply to note that if θ swaps $\Delta_m[-1]$ with $\Delta_m[1]$, then for any induced subgraph $\Gamma \subset \Delta_m$ and its image $\theta(\Gamma)$, the corresponding edges (A, B) and $(\theta(A), \theta(B))$ will also have swapped colours. This observation and the properties of $\Delta_m[-1]$ and $\Delta_m[1]$ as strongly regular graphs could be used as the basis for a backtracking search algorithm for $m > 3$ to either find θ or rule out its existence.

Acknowledgements.

This work was first presented at the Workshop on Algebraic Design Theory and Hadamard Matrices (ADTHM) 2014, in honour of the 70th birthday of Hadi Kharaghani. Thanks to Robert Craigen, and William Martin for valuable discussions, and again to Robert Craigen for presenting Questions 1 and 2 at the workshop on "Algebraic design theory with Hadamard matrices" in Banff in July 2014. Thanks also to the Mathematical Sciences Institute at The Australian National University for the author's continuing Visiting Fellowship.

References

1. A. Bernasconi and B. Codenotti. Spectral analysis of Boolean functions as a graph eigenvalue problem. *IEEE Transactions on Computers*, 48(3):345–351, (1999).
2. R. C. Bose. Strongly regular graphs, partial geometries and partially balanced designs. *Pacific J. Math*, 13(2):389–419, (1963).
3. A. Brouwer, A. Cohen, and A. Neumaier. *Distance-Regular Graphs*. Ergebnisse der Mathematik und Ihrer Grenzgebiete, 3 Folge/A Series of Modern Surveys in Mathematics Series. Springer London, Limited, (2011).
4. A. Canteaut, C. Carlet, P. Charpin, and C. Fontaine. On cryptographic properties of the cosets of r (1, m). *Information Theory, IEEE Transactions on*, 47(4):1494–1513, (2001).

5. A. Canteaut and P. Charpin. Decomposing bent functions. *Information Theory, IEEE Transactions on*, 49(8):2004–2019, (2003).
6. J. F. Dillon. *Elementary Hadamard Difference Sets*. PhD thesis, University of Maryland College Park, Ann Arbor, USA, (1974).
7. P. Leopardi. Constructions for Hadamard matrices, Clifford algebras, and their relation to amicability / anti-amicability graphs. *Australasian Journal of Combinatorics*, 58(2):214–248, (2014).
8. P. K. Menon. On difference sets whose parameters satisfy a certain relation. *Proceedings of the American Mathematical Society*, 13(5):739–745, (1962).
9. O. S. Rothaus. On "bent" functions. *Journal of Combinatorial Theory, Series A*, 20(3):300–305, (1976).
10. J. J. Seidel. Strongly regular graphs. In *Surveys in combinatorics (Proc. Seventh British Combinatorial Conf., Cambridge, 1979)*, volume 38 of *London Math. Soc. Lecture Note Ser.*, 157–180. Cambridge Univ. Press, Cambridge-New York, (1979).
11. N. Tokareva. On the number of bent functions from iterative constructions: lower bounds and hypotheses. *Adv. in Math. of Comm.*, 5(4):609–621, (2011).