# Twin bent functions, strongly regular Cayley graphs, and Hurwitz-Radon theory 

Paul Leopardi


#### Abstract

The real monomial representations of Clifford algebras give rise to two sequences of bent functions. For each of these sequences, the corresponding Cayley graphs are strongly regular graphs, and the corresponding sequences of strongly regular graph parameters coincide. Even so, the corresponding graphs in the two sequences are not isomorphic, except in the first 3 cases. The proof of this nonisomorphism is a simple consequence of a theorem of Radon.


2010 MSC: 05E30, 11T71, 15A24, 15B34
Keywords: Bent functions, Strongly regular graphs, Clifford algebras, Hurwitz-Radon

## 1. Introduction

Two recent papers $[10,11]$ describe and investigate two infinite sequences of bent functions and their Cayley graphs. The bent function $\sigma_{m}$ on $\mathbb{Z}_{2}^{2 m}$ is described in the first paper [10], on generalizations of Williamson's construction for Hadamard matrices. The bent function $\tau_{m}$ on $\mathbb{Z}_{2}^{2 m}$ is described in the second paper [11], which investigates some of the properties of the two sequences of bent functions. In this second paper it is shown that the bent functions $\sigma_{m}$ and $\tau_{m}$ both correspond to Hadamard difference sets with the same parameters

$$
\left(v_{m}, k_{m}, \lambda_{m}, n_{m}\right)=\left(4^{m}, 2^{2 m-1}-2^{m-1}, 2^{2 m-2}-2^{m-1}, 2^{2 m-2}\right)
$$

and that their corresponding Cayley graphs are both strongly regular with the same parameters $\left(v_{m}, k_{m}, \lambda_{m}, \lambda_{m}\right)$.

The main result of the current paper is the following.
Theorem 1.1. The Cayley graphs of the bent functions $\sigma_{m}$ and $\tau_{m}$ are isomorphic only when $m=1,2$, or 3 .

Paul Leopardi; University of Melbourne, Australian Government-Bureau of Meteorology (email: paul.leopardi@gmail.com).

The remainder of the paper is organized as follows. Section 2 outlines some of the background of this investigation. Section 3 includes further definitions used in the subsequent sections. Section 4 proves the main result, and resolves the conjectures and the question raised by the previous papers. Section 5 puts these results in context, and suggests future research.

## 2. Background

A recent paper of the author [10] describes a generalization of Williamson's construction for Hadamard matrices [16] using the real monomial representation of the basis elements of the Clifford algebras $\mathbb{R}_{m, m}$.

Briefly, the general construction uses some

$$
A_{k} \in\{-1,0,1\}^{n \times n}, \quad B_{k} \in\{-1,1\}^{b \times b}, \quad k \in\{1, \ldots, n\},
$$

where the $A_{k}$ are monomial matrices, and constructs

$$
\begin{equation*}
H:=\sum_{k=1}^{n} A_{k} \otimes B_{k} \tag{H0}
\end{equation*}
$$

such that

$$
\begin{equation*}
H \in\{-1,1\}^{n b \times n b} \quad \text { and } \quad H H^{T}=n b I_{(n b)} \tag{H1}
\end{equation*}
$$

i.e. $H$ is a Hadamard matrix of order $n b$. The paper [10] focuses on a special case of the construction, satisfying the conditions

$$
\begin{align*}
A_{j} * A_{k}=0 \quad(j \neq k), & \sum_{k=1}^{n} A_{k} \in\{-1,1\}^{n \times n} \\
A_{k} A_{k}^{T} & =I_{(n)} \\
A_{j} A_{k}^{T}+\lambda_{j, k} A_{k} A_{j}^{T}= & 0 \quad(j \neq k)  \tag{1}\\
B_{j} B_{k}^{T}-\lambda_{j, k} B_{k} B_{j}^{T} & =0 \quad(j \neq k) \\
\lambda_{j, k} & \in\{-1,1\} \\
\sum_{k=1}^{n} B_{k} B_{k}^{T} & =n b I_{(b)}
\end{align*}
$$

where $*$ is the Hadamard matrix product.
In Section 3 of the paper [10], it is noted that the Clifford algebra $\mathbb{R}^{2^{m} \times 2^{m}}$ has a canonical basis consisting of $4^{m}$ real monomial matrices, corresponding to the basis of the algebra $\mathbb{R}_{m, m}$, with the following properties:

Pairs of basis matrices either commute or anticommute. Basis matrices are either symmetric or skew, and so the basis matrices $A_{j}, A_{k}$ satisfy

$$
\begin{equation*}
A_{k} A_{k}^{T}=I_{\left(2^{m}\right)}, \quad A_{j} A_{k}^{T}+\lambda_{j, k} A_{k} A_{j}^{T}=0 \quad(j \neq k), \quad \lambda_{j, k} \in\{-1,1\} \tag{2}
\end{equation*}
$$

Additionally, for $n=2^{m}$, we can choose a transversal of $n$ canonical basis matrices that satisfies conditions (1) on the $A$ matrices,

$$
\begin{equation*}
A_{j} * A_{k}=0 \quad(j \neq k), \quad \sum_{k=1}^{n} A_{k} \in\{-1,1\}^{n \times n} \tag{3}
\end{equation*}
$$

Section 3 also contains the definition of $\Delta_{m}$, the restricted amicability / anti-amicability graph of $\mathbb{R}_{m, m}$, and the subgraphs $\Delta_{m}[-1]$ and $\Delta_{m}[1]$, as well as the term "transversal graph". These definitions are repeated here since they are used in the conjectures and question below.

Definition 2.1. [10, p. 225]
Let $\Delta_{m}$ be the graph whose vertices are the $n^{2}=4^{m}$ positive signed basis matrices of the real representation of the Clifford algebra $\mathbb{R}_{m, m}$, with each edge having one of two labels, -1 or 1 :

- Matrices $A_{j}$ and $A_{k}$ are connected by an edge labelled by -1 ("red") if they have disjoint support and are anti-amicable, that is, $A_{j} A_{k}^{-1}$ is skew.
- Matrices $A_{j}$ and $A_{k}$ are connected by an edge labelled by 1 ("blue") if they have disjoint support and are amicable, that is, $A_{j} A_{k}^{-1}$ is symmetric.
- Otherwise there is no edge between $A_{j}$ and $A_{k}$.

The subgraph $\Delta_{m}[-1]$ consists of the vertices of $\Delta_{m}$ and all edges in $\Delta_{m}$ labelled by -1 . Similarly, the subgraph $\Delta_{m}[1]$ contains all of the edges of $\Delta_{m}$ that are labelled by 1.

A transversal graph for the Clifford algebra $\mathbb{R}_{m, m}$ is any induced subgraph of $\Delta_{m}$ that is a complete graph on $2^{m}$ vertices. That is, each pair of vertices in the transversal graph represents a pair of matrices, $A_{j}$ and $A_{k}$ with disjoint support.

The following three conjectures appear in Section 3 of the paper [10]:
Conjecture 2.2. For all $m \geqslant 0$ there is a permutation $\pi$ of the set of $4^{m}$ canonical basis matrices, that sends an amicable pair of basis matrices with disjoint support to an anti-amicable pair, and vice-versa.

Conjecture 2.3. For all $m \geqslant 0$, for the Clifford algebra $\mathbb{R}_{m, m}$, the subset of transversal graphs that are not self-edge-colour complementary can be arranged into a set of pairs of graphs with each member of the pair being edge-colour complementary to the other member.

Conjecture 2.4. For all $m \geqslant 0$, for the Clifford algebra $\mathbb{R}_{m, m}$, if a graph $T$ exists amongst the transversal graphs, then so does at least one graph with edge colours complementary to those of $T$.

Note that Conjecture 2.2 implies Conjecture 2.3, which in turn implies Conjecture 2.4.
The significance of these conjectures can be seen in relation to the following result, which is Part 1 of Theorem 10 of the paper [10].

Lemma 2.5. If $b$ is a power of $2, b=2^{m}, m \geqslant 0$, the amicability / anti-amicability graph $P_{b}$ of the matrices $\{-1,1\}^{b \times b}$ contains a complete two-edge-coloured graph on $2 b^{2}$ vertices with each vertex being a Hadamard matrix. This graph is isomorphic to $\Gamma_{m, m}$, the amicability / anti-amicability graph of the group $\mathbb{G}_{m, m}$.

The definitions of $\Gamma_{m, m}$ and $\mathbb{G}_{m, m}$ are given in Section 3 of the paper [10], and the definition of $\mathbb{G}_{m, m}$ is repeated below. For the current paper, it suffices to note that $\Delta_{m}$ is a subgraph of $\Gamma_{m, m}$, and so, therefore, are all of the transversal graphs.

An $n$-tuple of $A$ matrices of order $n=2^{m}$ satisfying properties (2) and (3) yields a corresponding transversal graph $T$. As noted in Section 5 of the paper [10], if Conjecture 2.4 were true, this would guarantee the existence of an edge-colour complementary transversal graph $\bar{T}$. In turn, because Lemma 2.5 guarantees the existence of a complete two-edge-coloured graph isomorphic to $\Gamma_{m, m}$ within $P_{b}$, and because $\Delta_{m}$ is a subgraph of $\Gamma_{m, m}$, the graph $P_{b}$ would have to contain a two-edge-coloured subgraph isomorphic to $\bar{T}$. This would imply the existence of an $n$-tuple of $B$ matrices of order $n$ satisfying the condition (1) such that the construction (H0) would satisfy the Hadamard condition (H1), with a matrix of order $n^{2}$.

The author's subsequent paper on bent functions [11] refines Conjecture 2.2 into the following question.

Question 2.6. Consider the sequence of edge-coloured graphs $\Delta_{m}$ for $m \geqslant 1$, each with red subgraph $\Delta_{m}[-1]$, and blue subgraph $\Delta_{m}[1]$. For which $m \geqslant 1$ is there an automorphism of $\Delta_{m}$ that swaps the subgraphs $\Delta_{m}[-1]$ and $\Delta_{m}[1]$ ?

The main result of this paper, Theorem 1.1, leads to the resolution of these conjectures and this question.

## 3. Further definitions and properties

This section sets out the remainder of the definitions and properties used in this paper. It is based on the previous papers $[10,11]$ with additions.

### 3.1. Clifford algebras and their real monomial representations

The following definitions and results appear in the paper on Hadamard matrices and Clifford algebras [10], and are presented here for completeness, since they are used below. Further details and proofs can be found in that paper, and in the paper on bent functions [11], unless otherwise noted. An earlier paper on representations of Clifford algebras [9] contains more background material.

The signed group [4] $\mathbb{G}_{p, q}$ of order $2^{1+p+q}$ is extension of $\mathbb{Z}_{2}$ by $\mathbb{Z}_{2}^{p+q}$, defined by the signed group presentation

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

where $S_{p, q}:=\{-q, \ldots,-1,1, \ldots, p\}$.
The $2 \times 2$ orthogonal matrices

$$
\mathrm{E}_{1}:=\left[\begin{array}{cc}
0 & -1 \\
1 & 0
\end{array}\right], \quad \mathrm{E}_{2}:=\left[\begin{array}{ll}
0 & 1 \\
1 & 0
\end{array}\right]
$$

generate $P\left(\mathbb{G}_{1,1}\right)$, the real monomial representation of group $\mathbb{G}_{1,1}$. The cosets of $\{ \pm I\} \equiv \mathbb{Z}_{2}$ in $P\left(\mathbb{G}_{1,1}\right)$ are ordered using a pair of bits, as follows.

$$
\begin{aligned}
& 0 \leftrightarrow 00 \leftrightarrow\{ \pm I\}, \\
& 1 \leftrightarrow 01 \leftrightarrow\left\{ \pm \mathrm{E}_{1}\right\}, \\
& 2 \leftrightarrow 10 \leftrightarrow\left\{ \pm \mathrm{E}_{2}\right\}, \\
& 3 \leftrightarrow 11 \leftrightarrow\left\{ \pm \mathrm{E}_{1} \mathrm{E}_{2}\right\} .
\end{aligned}
$$

For $m>1$, the real monomial representation $P\left(\mathbb{G}_{m, m}\right)$ of the group $\mathbb{G}_{m, m}$ consists of matrices of the form $G_{1} \otimes G_{m-1}$ with $G_{1}$ in $P\left(\mathbb{G}_{1,1}\right)$ and $G_{m-1}$ in $P\left(\mathbb{G}_{m-1, m-1}\right)$. The cosets of $\{ \pm I\} \equiv \mathbb{Z}_{2}$ in $P\left(\mathbb{G}_{m, m}\right)$ are ordered by concatenation of pairs of bits, where each pair of bits uses the ordering as per $P\left(\mathbb{G}_{1,1}\right)$,
and the pairs are ordered as follows.

$$
\begin{aligned}
0 & \leftrightarrow 00 \ldots 00 \leftrightarrow\{ \pm I\}, \\
1 & \leftrightarrow 00 \ldots 01 \leftrightarrow\left\{ \pm I_{(2)}^{\otimes(m-1)} \otimes \mathrm{E}_{1}\right\}, \\
2 & \leftrightarrow 00 \ldots 10 \leftrightarrow\left\{ \pm I_{(2)}^{\otimes(m-1)} \otimes \mathrm{E}_{2}\right\}, \\
& \ldots \\
2^{2 m}-1 & \leftrightarrow 11 \ldots 11 \leftrightarrow\left\{ \pm\left(\mathrm{E}_{1} \mathrm{E}_{2}\right)^{\otimes m}\right\} .
\end{aligned}
$$

This ordering is called the Kronecker product ordering of the cosets of $\{ \pm I\}$ in $P\left(\mathbb{G}_{m, m}\right)$.
The group $\mathbb{G}_{m, m}$ and its real monomial representation $P\left(\mathbb{G}_{m, m}\right)$ satisfy the following properties.

1. Pairs of elements of $\mathbb{G}_{m, m}$ (and therefore $P\left(\mathbb{G}_{m, m}\right)$ ) either commute or anticommute: for $g, h \in$ $\mathbb{G}_{m, m}$, either $h g=g h$ or $h g=-g h$.
2. The matrices $E \in P\left(\mathbb{G}_{m, m}\right)$ are orthogonal: $E E^{T}=E^{T} E=I$.
3. The matrices $E \in P\left(\mathbb{G}_{m, m}\right)$ 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 $E^{2}=-I$.

Taking the positive signed element of each of the $2^{2 m}$ cosets listed above defines a transversal of $\{ \pm I\}$ in $P\left(\mathbb{G}_{m, m}\right)$ which is also a monomial basis for the real representation of the Clifford algebra $\mathbb{R}_{m, m}$ in Kronecker product order, called this basis the positive signed basis of $P\left(\mathbb{R}_{m, m}\right)$.

The function $\gamma_{m}: \mathbb{Z}_{2^{2 m}} \rightarrow P\left(\mathbb{G}_{m, m}\right)$ chooses the corresponding basis matrix from the positive signed basis of $P\left(\mathbb{R}_{m, m}\right)$, using the Kronecker product ordering. This ordering also defines a corresponding function on $\mathbb{Z}_{2}^{2 m}$, also called $\gamma_{m}$.

### 3.2. Hurwitz-Radon theory

The key concept used in the proof of Lemma 4.1 below is that of a Hurwitz-Radon family of matrices. A set of real orthogonal matrices $\left\{A_{1}, A_{2}, \ldots, A_{s}\right\}$ is called a Hurwitz-Radon family $[6,7,13]$ if

1. $A_{j}^{T}=-A_{j}$ for all $j=1, \ldots, s$, and
2. $A_{j} A_{k}=-A_{k} A_{j}$ for all $j \neq k$.

The Hurwitz-Radon function $\rho$ is defined by

$$
\rho\left(2^{4 d+c}\right):=2^{c}+8 d, \quad \text { where } 0 \leqslant c<4 .
$$

As stated by Geramita and Pullman [6], Radon [13] proved the following result, which is used as a lemma in this paper.

Lemma 3.1. [6, Theorem A]
Any Hurwitz-Radon family of order $n$ has at most $\rho(n)-1$ members.

### 3.3. The two sequences of bent functions

The previous two papers [10, 11] define two binary functions on $\mathbb{Z}_{2}^{2 m}, \sigma_{m}$ and $\tau_{m}$, respectively. Their key properties are repeated below. See the two papers for the proofs and for more details and references on bent functions.

The function $\sigma_{m}: \mathbb{Z}_{2}^{2 m} \rightarrow \mathbb{Z}_{2}$ has the following properties.

1. For $i \in \mathbb{Z}_{2}^{2 m}, \sigma_{m}(i)=1$ if and only if the number of digits equal to 1 in the base 4 representation of $i$ is odd.
2. Since each matrix $\gamma_{m}(i)$ is orthogonal, $\sigma_{m}(i)=1$ if and only if the matrix $\gamma_{m}(i)$ is skew.
3. The function $\sigma_{m}$ is bent.

The function $\tau_{m}: \mathbb{Z}_{2}^{2 m} \rightarrow \mathbb{Z}_{2}$ has the following properties.

1. For $i \in \mathbb{Z}_{2}^{2 m}, \tau_{m}(i)=1$ if and only if the number of digits equal to 1 or 2 in the base 4 representation of $i$ is non zero, and the number of digits equal to 1 is even.
2. The value $\tau_{m}(i)=1$ if and only if the matrix $\gamma_{m}(i)$ is symmetric but not diagonal.
3. The function $\tau_{m}$ is bent.

### 3.4. The relevant graphs

For a binary function $f: \mathbb{Z}_{2}^{2 m} \rightarrow \mathbb{Z}_{2}$, with $f(0)=0$ we consider the simple undirected Cayley graph $\operatorname{Cay}(f)[1,3.1]$ where the vertex set $V(\operatorname{Cay}(f))=\mathbb{Z}_{2}^{2 m}$ and for $i, j \in \mathbb{Z}_{2}^{2 m}$, the edge $(i, j)$ is in the edge set $E(\operatorname{Cay}(f))$ if and only if $f(i+j)=1$.

In the paper on Hadamard matrices [10] it is shown that since $\sigma_{m}(i)=1$ if and only if $\gamma_{m}(i)$ is skew, the subgraph $\Delta_{m}[-1]$ is isomorphic to the Cayley graph Cay $\left(\sigma_{m}\right)$.

The paper on bent functions [11] notes that since $\tau_{m}(i)=1$ if and only if $\gamma_{m}(i)$ is symmetric but not diagonal, the subgraph $\Delta_{m}[1]$ is isomorphic to the Cayley graph Cay $\left(\tau_{m}\right)$. In that paper, these isomorphisms and the characterization of Cay $\left(\sigma_{m}\right)$ and $\operatorname{Cay}\left(\tau_{m}\right)$ as Cayley graphs of bent functions are used to prove the following theorem.
Theorem 3.2. [11, Theorem 5.2]
For all $m \geqslant 1$, both graphs $\Delta_{m}[-1]$ and $\Delta_{m}[1]$ are strongly regular, with parameters $v_{m}=4^{m}$, $k_{m}=2^{2 m-1}-2^{m-1}, \lambda_{m}=\mu_{m}=2^{2 m-2}-2^{m-1}$.

## 4. Proof of Theorem 1.1 and related results

Here we prove the main result, and examine its implications for Conjectures 2.2 to 2.4 and Question 2.6.

The proof of Theorem 1.1 follows from the following two lemmas. The first lemma puts an upper bound on the clique number of the graph $\operatorname{Cay}\left(\sigma_{m}\right) \simeq \Delta_{m}[-1]$.
Lemma 4.1. The clique number of the graph $\operatorname{Cay}\left(\sigma_{m}\right)$ is at most $\rho\left(2^{m}\right)$, where $\rho$ is the Hurwitz-Radon function. Therefore $\rho\left(2^{m}\right)<2^{m}$ for $m \geqslant 4$.

Proof. If we label the vertices of the graph Cay $\left(\sigma_{m}\right)$ with the elements of $Z_{2}^{2 m}$, then any clique in this graph is mapped to another clique if a constant is added to all of the vertices. Thus without loss of generality we can assume that we have a clique of order $s+1$ with one of the vertices labelled by 0 . If we then use $\gamma_{m}$ to label the vertices with elements of $\mathbb{R}_{m, m}$ to obtain the isomorphic graph $\Delta_{m}[-1]$, we have one vertex of the clique labelled with the identity matrix $I$ of order $2^{m}$. Since the clique is in $\Delta_{m}[-1]$, the other vertices $A_{1}$ to $A_{s}$ (say) must necessarily be skew matrices that are pairwise anti-amicable,

$$
A_{j} A_{k}^{T}=-A_{k} A_{j}^{T} \quad \text { for all } j \neq k
$$

But then

$$
A_{j} A_{k}=-A_{k} A_{j} \quad \text { for all } j \neq k
$$

and therefore $\left\{A_{1}, \ldots, A_{s}\right\}$ is a Hurwitz-Radon family. By Lemma 3.1, $s$ is at most $\rho\left(2^{m}\right)-1$ and therefore the size of the clique is at most $\rho\left(2^{m}\right)$.

The second lemma puts a lower bound on the clique number of the graph Cay $\left(\tau_{m}\right) \simeq \Delta_{m}[1]$.
Lemma 4.2. The clique number of the graph $\operatorname{Cay}\left(\tau_{m}\right)$ is at least $2^{m}$.
Proof. We construct a clique of order $2^{m}$ in $\operatorname{Cay}\left(\tau_{m}\right)$ with the vertices labelled in $\mathbb{Z}_{2}^{2 m}$, using the following set of vertices, denoted in base 4:

$$
C_{m}:=\{00 \ldots 00,00 \ldots 02,00 \ldots 20, \ldots, 22 \ldots 22\}
$$

The set $C_{m}$ is closed under addition in $\mathbb{Z}_{2}^{2 m}$, and therefore forms a clique of order $2^{m}$ in $\operatorname{Cay}\left(\tau_{m}\right)$, since the sum of any two distinct elements of $C_{m}$ is in the support of $\tau_{m}$.

With these two lemmas in hand, the proof of Theorem 1.1 follows easily.
Proof of Theorem 1.1. The result is a direct consequence of Lemmas 4.1 and 4.2. For $m \geqslant 4$, the clique numbers of the graphs Cay $\left(\sigma_{m}\right)$ and $\operatorname{Cay}\left(\tau_{m}\right)$ are different, and therefore these graphs cannot be isomorphic.

Lemmas 4.1 and 4.2 , along with Theorem 1.1 imply the failure of the conjectures 2.2 to 2.4 , as well as the resolution of Question 2.6, as follows.

Theorem 4.3. For $m \geqslant 4$ the following hold.

1. There exist transversal graphs that do not have an edge-colour complement, and therefore Conjecture 2.4 does not hold.
2. As a consequence, Conjectures 2.2 and 2.3 also do not hold.
3. Question 2.6 is resolved. The only $m \geqslant 1$ for which there is an automorphism of $\Delta_{m}$ that swaps the subgraphs $\Delta_{m}[-1]$ and $\Delta_{m}[1]$ are $m=1,2$ and 3 .

Proof. Assume that $m \geqslant 4$. A transversal graph is a subgraph of $\Delta_{m}$ which is a complete graph of order $2^{m}$. The edges of a transversal graph are labelled with the colour red (if the edge is contained in $\Delta_{m}[-1]$ ) or blue (if the edge is contained in $\Delta_{m}[1]$ ). By Lemma 4.1, the largest clique of $\Delta_{m}[-1]$ is of order $\rho\left(2^{m}\right)<2^{m}$, and by Lemma 4.2, the largest clique of $\Delta_{m}[1]$ is of order $2^{m}$. If we take a blue clique of order $2^{m}$ as a transversal graph, this cannot have an edge-colour complement in $\Delta_{m}$, because no red clique can be this large. More generally, we need only take a transversal graph containing a blue clique with order larger than $\rho\left(2^{m}\right)$ to have a clique with no edge-colour complement in $\Delta_{m}$. This falsifies Conjecture 2.4.

Since Conjecture 2.4 fails for $m \geqslant 4$, the pairing of graphs described in Conjecture 2.3 is impossible for $m \geqslant 4$. Thus Conjecture 2.3 is also false.

Finally, Conjecture 2.2 fails as a direct consequence of Theorem 1.1 since, for $m \geqslant 4$, the subgraphs $\Delta_{m}[-1]$ and $\Delta_{m}[1]$ are not isomorphic. Therefore, for $m \geqslant 4$, there can be no automorphism of $\Delta_{m}$ that swaps these subgraphs.

## 5. Discussion

The result of Lemma 4.1 is well known. For example, the graph $\Delta_{m}[-1]$ is the complement of the graph $V^{+}$of Yiu [17], and the result for $V^{+}$in his Theorem 2 is equivalent to Lemma 4.1.

The main consequence of Theorem 4.3 is that for $m>3$ there is at least one $n$-tuple of $A$ matrices, with $n=2^{m}$ such that no $n$-tuple of $B$ matrices of order $n$ can be found to satisfy construction (H0) under condition (H1). The proof of Theorem 5 of the Hadamard construction paper [10] shows by construction that for any $m$, and any $n$-tuple of $A$ matrices satisfying (1), there is an $n$-tuple of $B$ matrices of order $n c$ that satisfies construction (H0) under condition (H1), where $c=M(n-1)$, with

$$
M(q):=\left\{\begin{array}{l}
\left\lceil\frac{q}{2}\right\rceil+1, \quad \text { if } q \equiv 2,3,4 \quad(\bmod 8),  \tag{4}\\
\left\lceil\frac{q}{2}\right\rceil \text { otherwise } .
\end{array}\right.
$$

Thus Theorem 5 remains valid. The question remains as to whether the the order $n c$ is tight or can be reduced. In the special case where the $n$-tuple of $A$ matrices is mutually amicable, the answer is given by Corollary 15 of the paper [10]: The set of $\{-1,1\}$ matrices of order $c$ contains an $n$-tuple of mutually anti-amicable Hadamard matrices. So in this special case, the required order can be reduced from $n c$ to $c$. This leads to the following question.

Question 5.1. In the general case, for any $m>1, n=2^{m}$, for any $n$-tuple of $A$ matrices satisfying (1), does there always exist an n-tuple of $B$ matrices of order $c$ that satisfies construction (HO) under condition (H1), where $c=M(n-1)$, with $M$ defined by (4)?

As a result of Theorems 3.2 and 4.3, we see that we have two sequences of strongly regular graphs, $\Delta_{m}[-1]$ and $\Delta_{m}[1](m \geqslant 1)$, sharing the same parameters, $v_{m}=4^{m}, k_{m}=2^{2 m-1}-2^{m-1}, \lambda_{m}=\mu_{m}=$ $2^{2 m-2}-2^{m-1}$, but the graphs are isomorphic only for $m=1,2,3$. For these three values of $m$, the existence of automorphisms of $\Delta_{m}$ that swap $\Delta_{m}[-1]$ and $\Delta_{m}[1]$ as subgraphs [10, Table 1] is remarkable in the light of Theorem 4.3.

A paper of Bernasconi and Codenotti describes the relationship between bent functions and their Cayley graphs, implying that a bent function corresponding to a $(v, k, \lambda, n)$ Hadamard difference set has a Cayley graph that is strongly regular with parameters $(v, k, \lambda, \mu)$ where $\lambda=\mu$ [1, Lemma 12]. The current paper notes that for two specific sequences of bent functions, $\sigma_{m}$ and $\tau_{m}$, the corresponding Cayley graphs are not necessarily isomorphic.

This raises the subject of classifying bent functions via their Cayley graphs, raising the following questions.

Question 5.2. Which strongly regular graphs with parameters $(v, k, \lambda, \lambda)$ occur as Cayley graphs of bent functions?

Question 5.3. What is the relationship between other classifications of bent functions and the classification via Cayley graphs?

This classification is the topic of a paper in preparation [8].
With respect to the specific bent functions $\sigma_{m}$ and $\tau_{m}$ investigated here, one of the anonymous reviewers of an earlier draft of this paper has asked whether each of these functions are part of a larger class of bent functions.

The function $\sigma_{m}$ is a quadratic form, as can be seen from its definition and its recursive identity [10, Lemma 7]. Specifically, $\sigma_{m}(0)=0$, and, in terms of algebraic normal form, using a particular convention for the mapping of bits to Boolean variables, the identity is $\sigma_{1}\left(x_{0}, x_{1}\right)=x_{0} x_{1}+x_{0}$, and

$$
\begin{gathered}
\sigma_{m+1}\left(x_{0}, x_{1}, \ldots, x_{2 m}, x_{2 m+1}\right)=\sigma_{m}\left(x_{0}, x_{1}\right)+\sigma_{m}\left(x_{2}, x_{3}, \ldots, x_{2 m}, x_{2 m+1}\right) \\
=x_{0} x_{1}+x_{0}+x_{2} x_{3}+x_{2}+\ldots+x_{2 m} x_{2 m+1}+x_{2 m}
\end{gathered}
$$

In a paper in preparation [8], it is proven that all quadratic bent functions with the same dimension and weight have isomorphic Cayley graphs.

As for $\tau_{m}$, it is a bent iterative function [2, Theorem V.4] [3, Theorem 2] [15], as can be seen from its definition, and from the proof that it is a bent function [11, Theorem 3.1].

Since the $\mathcal{P} \mathcal{S}^{(-)}$partial spread bent functions are formed using $m$-dimensional subspaces of $\mathbb{Z}^{2 m}$ which are disjoint except for the 0 vector [5, p. 95], these bent functions also have Cayley graphs whose clique number is at least $2^{m}$. It could therefore be speculated that $\tau_{m}$ is also a $\mathcal{P S}{ }^{(-)}$bent function, but exhaustive search using SageMathCloud [14] shows that $\tau_{3}$ cannot be in $\mathcal{P} \mathcal{S}^{(-)}$. Each clique of size 8 in $\operatorname{Cay}\left(\tau_{3}\right)$ that contains the 0 vector intersects each other such clique at two vectors, only one of which is the 0 vector [12].

Acknowledgment: Thanks to Christine Leopardi for her hospitality at Long Beach. Thanks to Robert Craigen, Joanne Hall, William Martin, Padraig Ó Catháin and Judy-anne Osborn for valuable discussions. This work was begun in 2014 while the author was a Visiting Fellow at the Australian National University, continued while the author was a Visiting Fellow and a Casual Academic at the University of Newcastle, Australia, and concluded while the author was an employee of the Bureau of Meteorology of the Australian Government, and an Honorary Fellow of the University of Melbourne. Thanks also to the anonymous reviewers of previous drafts of this paper.

## References

[1] A. Bernasconi, B. Codenotti, Spectral analysis of Boolean functions as a graph eigenvalue problem, IEEE Trans. Comput. 48(3) (1999) 345-351.
[2] A. Canteaut, C. Carlet, P. Charpin, C. Fontaine, On cryptographic properties of the cosets of $R(1, m)$, IEEE Trans. Inform. Theory 47 (4) (2001) 1494-1513.
[3] A. Canteaut, P. Charpin, Decomposing bent functions, IEEE Trans. Inform. Theory 49(8) (2003) 2004-2019.
[4] R. Craigen, Signed groups, sequences, and the asymptotic existence of Hadamard matrices, J. Combin. Theory Ser. A 71(2) (1995) 241-254.
[5] J. F. Dillon, Elementary Hadamard Difference Sets, PhD thesis, University of Maryland College Park, Ann Arbor, USA, 1974.
[6] A. V. Geramita, N. J. Pullman, A theorem of Hurwitz and Radon and orthogonal projective modules, Proc. Amer. Math. Soc. 42(1) (1974) 51-56.
[7] A. Hurwitz, Über die Komposition der quadratischen Formen, Math. Ann. 88(1-2) (1922) 1-25.
[8] P. Leopardi, Classifying bent functions by their Cayley graphs, arXiv:1705.04507 [math.CO].
[9] P. Leopardi, A generalized FFT for Clifford algebras, Bull. Belg. Math. Soc. Simon Stevin 11(5) (2005) 663-688.
[10] P. Leopardi, Constructions for Hadamard matrices using Clifford algebras, and their relation to amicability / anti-amicability graphs, Australas. J. Combin. 58(2) (2014) 214-248.
[11] P. Leopardi, Twin Bent Functions and Clifford Algebras. In: Colbourn C. (eds) Algebraic Design Theory and Hadamard Matrices. Springer Proceedings in Mathematics \& Statistics, vol 133. Springer, Cham.
[12] P. Leopardi, Boolean-Cayley-graphs, (2016). http://tinyurl.com/Boolean-Cayley-graphs SageMathCloud public folder. Last accessed 16 April 2017.
[13] J. Radon, Lineare Scharen orthogonaler Matrizen, Abh. Math. Sem. Univ. Hamburg 1(1) (1922) 1-14.
[14] SageMath, Inc., SageMathCloud Online Computational Mathematics, (2016).
[15] N. Tokareva, On the number of bent functions from iterative constructions: lower bounds and hypotheses, Adv. Math. Commun. 5(4) (2011) 609-621.
[16] J. Williamson, Hadamard's determinant theorem and the sum of four squares, Duke Math. J. 11(1) (1944) 65-81.
[17] P. Y. Yiu, Strongly regular graphs and Hurwitz-Radon numbers, Graphs and Combin. 6(1) (1990) 61-69.

