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

Paul C. Leopardi *

Submitted: 11 April 2015

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 \((\nu, k, \lambda, \mu)\) coincide. Even so, the corresponding graphs in the two sequences are not isomorphic, except in the first 3 cases. The proof of this non-isomorphism is a simple consequence of a theorem of Radon.

1 Introduction

A recent paper of the author [3] describes a generalization of Williamson’s construction for Hadamard matrices [6] using the real monomial representation of the basis elements of the Clifford algebras \(\mathbb{R}_{m,m}\). In that paper, the following three conjectures appear:

Conjecture 1. For all \(m \geq 0\) 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. For all \(m \geq 0\), 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.

*School of Mathematical and Physical Sciences, The University of Newcastle.

mailto:paul.leopardi@newcastle.edu.au
Conjecture 3. For all $m \geq 0$, 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 $T$.

The author’s subsequent paper on bent functions [4] refines Conjecture 1 into the following question.

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

(The term transversal graph and the definitions of $\Delta_m$, $\Delta_m[-1]$, and $\Delta_m[1]$ are given in the relevant papers and are repeated in the next section.)

In this paper it is proved that Conjecture 3 fails for $m \geq 4$, and as a consequence, so do Conjectures 1 and 2. This also resolves Question 1: the only values for which such an automorphism exists are 1, 2, and 3.

The paper is organized as follows. Section 2 repeats the relevant definitions from the previous two papers [3, 4], and includes further definitions as necessary. Section 3 states and proves the main results.

2 Preliminaries

This section sets out the main definitions and properties used in this paper. It is mostly based on the previous papers [3, 4] with a few additions.

Clifford algebras and their real monomial representations.

The following definitions and results appear in the paper on Hadamard matrices and [3], 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 and Clifford algebras, 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

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

where $S_{p,q} := \{-q, \ldots, -1, 1, \ldots, p\}$. 
The following construction of the real monomial representation \( P(G_{m,m}) \) of the group \( G_{m,m} \) is used in [3].

The \( 2 \times 2 \) orthogonal matrices

\[
E_1 := \begin{bmatrix} \cdot & -1 \\ 1 & \cdot \end{bmatrix}, \quad E_2 := \begin{bmatrix} \cdot & 1 \\ 1 & \cdot \end{bmatrix}
\]

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

\[
\begin{align*}
0 & \leftrightarrow 00 \leftrightarrow \{\pm I\}, \\
1 & \leftrightarrow 01 \leftrightarrow \{\pm E_1\}, \\
2 & \leftrightarrow 10 \leftrightarrow \{\pm E_2\}, \\
3 & \leftrightarrow 11 \leftrightarrow \{\pm E_1E_2\}.
\end{align*}
\]

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

\[
\begin{align*}
0 & \leftrightarrow 00 \ldots 00 \leftrightarrow \{\pm I\}, \\
1 & \leftrightarrow 00 \ldots 01 \leftrightarrow \{\pm I^{\otimes(m-1)}_1 \otimes E_1\}, \\
2 & \leftrightarrow 00 \ldots 10 \leftrightarrow \{\pm I^{\otimes(m-1)}_2 \otimes E_2\}, \\
\ldots \\
2^m - 1 & \leftrightarrow 11 \ldots 11 \leftrightarrow \{\pm (E_1E_2)^{\otimes m}\}.
\end{align*}
\]

This ordering is called the Kronecker product ordering of the cosets of \( \{\pm I\} \) in \( P(G_{m,m}) \).

Recall that the group \( G_{m,m} \) and its real monomial representation \( P(G_{m,m}) \) satisfy the following properties.

1. Pairs of elements of \( G_{m,m} \) (and therefore \( P(G_{m,m}) \)) either commute or anticommute: for \( g, h \in G_{m,m} \), either \( hg = gh \) or \( hg = -gh \).

2. The matrices \( E \in P(G_{m,m}) \) are orthogonal: \( EE^T = E^TE = I \).

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

**Definition.** We define the function $\gamma_m : \mathbb{Z}_{2^m} \to P(\mathbb{G}_{m,m})$ to choose the corresponding basis matrix from the positive signed basis of $P(\mathbb{R}_{m,m})$, using the Kronecker product ordering. This ordering also defines a corresponding function on $\mathbb{Z}_{2^m}$, which we also call $\gamma_m$.

The graphs used in Conjectures 2 and 3 and Question 1.

The following definitions appear in the previous two papers [3, 4], and are repeated here for completeness, because Conjectures 2 and 3 and Question 1 depend on these definitions.

**Definition 1.** Let $\Delta_m$ 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 labels, $-1$ or $1$:

- Matrices $A_j$ and $A_k$ are connected by an edge labelled by $-1$ if they have disjoint support and are anti-amicable, that is, $A_jA_k^{-1}$ is skew.
- Matrices $A_j$ and $A_k$ are connected by an edge labelled by $1$ if they have disjoint support and are amicable, that is, $A_jA_k^{-1}$ is symmetric.
- Otherwise there is no edge between $A_j$ and $A_k$.

The graph $\Delta_m$ is composed of two subgraphs: $\Delta_m[-1]$ denotes the red subgraph of $\Delta_m$, the graph containing all of the vertices of $\Delta_m$, and all of edges labelled with $-1$; and $\Delta_m[1]$ denotes the blue subgraph of $\Delta_m$, the graph containing all of the vertices of $\Delta_m$, and all of edges labelled with $1$.

As noted in the paper on Clifford algebras and Hadamard matrices [3], 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.

**Two bent functions and their strongly regular Cayley graphs.**

The previous two papers [3, 4] define two bent functions on $\mathbb{Z}_{2^m}$, $\sigma_m$ and $\tau_m$, respectively. (For the definition and properties of bent functions, see the previous two papers [3, 4] and references therein.)
In the paper on bent functions [4], the following two properties of $\sigma_m$ are noted.

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

2. For $i \in \mathbb{Z}_{2^m}$, $\sigma_m(i) = 1$ if and only if the number of 1 digits in the base 4 representation of $i$ is odd.

Thus the subgraph $\Delta_m[-1]$ is isomorphic to Cayley graph of $\sigma_m$, the graph whose vertices are labelled by $\mathbb{Z}_{2^m}$, where there is an edge between $i$ and $j$ if and only if $\sigma_m(i + j) = 1$.

The paper on bent functions [4] also notes that $\tau_m(i) = 1$ if and only if $\gamma_m(i)$ is symmetric but not diagonal. Thus the subgraph $\Delta_m[1]$ is isomorphic to Cayley graph of $\sigma_m$. It is also easily verified that $\tau_m(i) = 1$ if and only if the number of digits 1 or 2 in the base 4 representation of $i$ is non zero, and the number of 1 digits is even.

The paper on bent functions [4] uses the characterization of $\Delta_m[1]$ and $\Delta_m[1]$ as Cayley graphs of bent functions to prove the following theorem.

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

**Hurwitz-Radon theory.**

A set of real orthogonal matrices $\{A_1, A_2, \ldots, A_s\}$ is called a Hurwitz-Radon family [1, 2, 5] 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

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

As stated by Geramita and Pullman [1, Theorem A], Radon [5] proved the following result, which is used as a lemma in this paper.

**Lemma 1.** Any Hurwitz-Radon family of order $n$ has at most $\rho(n) - 1$ members.
3 Main Results

Here we state and prove the main results of this paper.

**Theorem 2.** For $m \geq 4$ the following hold.

1. There exist transversal graphs that do not have an edge-colour complement, and therefore Conjecture 3 does not hold.

2. As a consequence, Conjectures 1 and 2 also do not hold.

3. Question 1 is resolved. The only $m \geq 1$ 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.

The proof of Theorem 2 follows from the following two lemmas. The first lemma puts an upper bound on the size of the maximum clique in $\Delta_m[-1]$.

**Lemma 2.** The order of the largest clique in the red subgraph $\Delta_m[-1]$ is at most $\rho(2^m)$, where $\rho$ is the Hurwitz-Radon function. Therefore $\rho(2^m) < 2^m$ for $m \geq 4$.

**Proof.** If we label the vertices of the subgraph $\Delta_m[-1]$ with the elements of $\mathbb{Z}_{2^m}$, then any clique in this subgraph is mapped to another clique if a constant is added to all of the vertices. Thus without loss of generality we can assume that one of the vertices is labelled 0. If we then use $\gamma_m$ to label the vertices with elements of $\mathbb{R}_{m,m}$, we have one vertex labelled with the identity matrix $I$ of order $2^m$, and (since we have a clique in $\Delta_m[-1]$) the other vertices $A_1$ to $A_s$ (say) must necessarily be skew matrices that are pairwise anti-amicable:

$$A_jA_k^T = -A_kA_j^T$$

for all $j \neq k$.

But then

$$A_jA_k = -A_kA_j$$

for all $j \neq k$,

and therefore $\{A_1, \ldots, A_s\}$ is a Hurwitz-Radon family. By Lemma 1, $s$ is at most $\rho(2^m) - 1$ and therefore the size of the clique is at most $\rho(2^m)$.

The second lemma puts a lower bound on the size of the maximum clique in $\Delta_m[1]$.

**Lemma 3.** The order of the largest clique in the blue subgraph $\Delta_m[1]$ is at least $2^m$.
**Proof.** We construct a clique of order $2^m$ in $\Delta_m[1]$ with the vertices labelled in $\mathbb{Z}_2^{2m}$, using the following vertices denoted in base 4:

\[
\begin{align*}
&00 \ldots 02 \\
&00 \ldots 20 \\
&\ldots \\
&22 \ldots 22
\end{align*}
\]

This set is closed under addition in $\mathbb{Z}_2^{2m}$, and therefore forms a clique of order $2^m$ in $\Delta_m[1]$. 

With these two lemmas in hand, the proof of Theorem 2 follows easily. **Proof of Theorem 2.** Assume that $m \geq 4$. 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 -1 (red) or 1 (blue). By Lemma 2, the largest clique of $\Delta_m[-1]$ is of order $\rho(2^m) < 2^m$, and by Lemma 3, 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 $\rho(2^m)$. This falsifies Conjecture 3.

Since Conjecture 3 fails for $m \geq 4$, the pairing of graphs described in Conjecture 2 is impossible for $m \geq 4$. Thus Conjecture 2 is also false.

Finally, Conjecture 1 fails as a direct consequence of Lemmas 2 and 3 since, for $m \geq 4$, the difference between $\Delta_m[-1]$ and $\Delta_m[1]$ in the order of the largest clique means that these two subgraphs of $\Delta_m$ cannot be isomorphic. Therefore, for $m \geq 4$, there can be no automorphism of $\Delta_m$ that swaps the edge colours.

**Remark.** As a result of Theorems 1 and 2, we see that we have two sequences of strongly regular graphs, $\Delta_m[-1]$ and $\Delta_m[1]$ ($m \geq 1$), sharing the same parameters, $v_m = 4^m$, $k_m = 2^{2m-1} - 2^{m-1}$, $\lambda_m = \mu_m = 2^{2m-2} - 2^{m-1}$, 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 [Table 1] is remarkable in the light of Theorem 2.

**Acknowledgements.** Thanks to Christine Leopardi for her hospitality at Long Beach. Thanks to Robert Craigen, 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, and concluded while the author was a Visiting Fellow and a Casual Academic at the University of Newcastle, Australia.
References

[1] A. V. Geramita and N. J. Pullman. A theorem of hurwitz and radon and orthogonal projective modules. *Proceedings of the American Mathematical Society*, 42(1):51–56, (1974).

[2] A. Hurwitz. Über die Komposition der quadratischen Formen. *Math. Ann.*, 88(1-2):1–25, (1922).

[3] 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).

[4] P. Leopardi. Twin bent functions and Clifford algebras. Accepted for publication in Springer Proceedings in Mathematics and Statistics (PROMS): Algebraic Design Theory and Hadamard Matrices. Preprint: arXiv:1501.05477 [math.CO], (2015).

[5] J. Radon. Lineare Scharen orthogonaler Matrizen. *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, 1(1):1–14, (1922).

[6] J. Williamson. Hadamard’s determinant theorem and the sum of four squares. *Duke Math. J.*, 11:65–81, (1944).