Twin bent functions and Clifford algebras

Paul Leopardi

Mathematical Sciences Institute, Australian National University.
For presentation at the University of Newcastle.
Originally presented at ADTHM, 8 July 2014.

25 September 2014

Australian National University

Acknowledgements

Richard Brent, Padraig Ó Catháin, Bill Martin, Judy-anne Osborn.

National Computational Infrastructure.

Australian Mathematical Sciences Institute.

Australian National University.

Restricted amicability/anti-amicability graphs

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, red and blue:

- Matrices A_j and A_k are connected by a red edge if they have disjoint support and are anti-amicable.
- Matrices A_j and A_k are connected by a blue edge if they have disjoint support and are amicable.
- Otherwise there is no edge between A_j and A_k.

We call Δ_m the *restricted amicability / anti-amicability graph* of the Clifford algebra $\mathbb{R}_{m,m}$.

(L 2014)

Results

Theorem 1

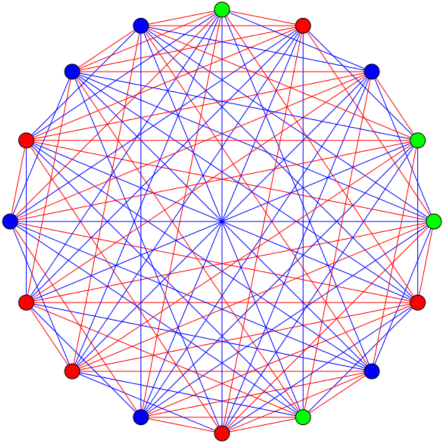
(L 2014)
The graph of anti-amicability of the canonical basis matrices of the neutral Clifford algebra $\mathbb{R}_{m,m}$ is strongly regular with parameters

$$(\nu, k, \lambda = \mu) = (4^m, 2^{2m-1} - 2^{m-1}, 2^{2m-2} - 2^{m-1}).$$

Theorem 2

The graph of amicability with disjoint support of the canonical basis matrices of the neutral Clifford algebra $\mathbb{R}_{m,m}$ is also strongly regular with the same parameters as those in Theorem 1.

The graphs from Theorem 1 and Theorem 2 are the red and the blue subgraphs of Δ_m.
They are isomorphic.

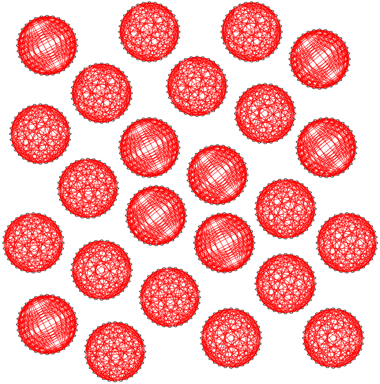


Δ_2

Overview

- What led to this investigation?
- Key concepts.
- Constructions.
- Proof of Theorem 2.
- Conclusion and open question.

Motivation



Anti-amicability of 4×4 Hadamard matrices: 24 components.

(L 2014)

A long history and a deep literature

- Difference sets.
  Bruck (1955), Hall (1956), Menon (1960, 1962), Mann (1965), Turyn (1965), Baumert (1969), Dembowski (1969), McFarlane (1973), Dillon (1974), Kantor (1975, 1985), Ma (1994), ...
- Bent functions.
  Dillon (1974), Rothaus (1976), Canteaut et al. (2001), Canteaut and Charpin (2003), Dempwolff (2006), Tokareva (2011), ...
- Strongly regular graphs.
  Brouwer, Cohen and Neumaier (1989), Ma (1994), Bernasconi and Codenotti (1999), Bernasconi, Codenotti and VanderKam (2001) ...

Difference sets

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 $n := k - \lambda$.

(Dillon 1974).

Hadamard difference sets

A (v, k, λ, n) difference set with $v = 4n$ is called a *Hadamard difference set.*

Lemma 3

(Menon 1962)

A Hadamard difference set has parameters of the form

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

(Menon 1962, Dillon 1974).

Hadamard transforms

H_m, the Sylvester Hadamard matrix of order 2^m, is defined by

$$H_1 := \begin{bmatrix} 1 & 1 \\ 1 & - \end{bmatrix}; \quad H_m := H_{m-1} \otimes H_1, \quad \text{for } m > 1.$$

For a boolean function $f : \mathbb{Z}_2^m \to \mathbb{Z}_2$, define the vector $[f]$ by

$$[f] = [(-1)^{f(0)}, (-1)^{f(1)}, \ldots, (-1)^{f(2^m-1)}]^T,$$

where $f(i)$ uses the binary expansion of i.

The *Hadamard transform* of f is the vector $H_m[f]$.

(Dillon 1974)

Bent functions

The Boolean function $f : \mathbb{Z}_2^m \to \mathbb{Z}_2$ is *bent*

if its Hadamard transform has constant magnitude:

$|H_m[f]| = C[1, \ldots, 1]^T$ for some constant C.

Each bent function f on $\mathbb{Z}_2^m$ has a *dual* function $\widetilde{f}$ given by

$$(H_m[f])_i =: 2^{m/2}(-1)^{\widetilde{f}(i)}.$$

(Dillon 1974, Tokareva 2011)

Bent functions and Hadamard difference sets

Lemma 4

(Dillon 1974, Theorem 6.2.2)

The Boolean function $f : \mathbb{Z}_2^m \to \mathbb{Z}_2$ is bent if and only if the set $f^{-1}(1)$ is a Hadamard difference set.

Lemma 5

(Dillon 1974, Remark 6.2.4)

Bent functions exist on $\mathbb{Z}_2^m$ only when m is even.

(Dillon 1974)

Strongly regular graphs

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.

(Brouwer, Cohen and Neumaier 1989)

Bent functions and strongly regular graphs

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 $\mathbb{Z}_2^m$.

Lemma 6

(Bernasconi and Codenotti 1999, Lemma 12)
The Cayley graph of a bent function on Z_2^m is a strongly regular graph with $\lambda = \mu$.

Lemma 7

(Bernasconi, Codenotti and VanderKam 2001, Theorem 3)
Bent functions are the only binary functions on Z_2^m whose Cayley graph is a strongly regular graph with $\lambda = \mu$.

The groups $\mathbb{G}_{1,1}$ and $\mathbb{Z}_2^2$

The 2×2 orthogonal matrices

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

generate the group $\mathbb{G}_{1,1}$ of order 8, an extension of $\mathbb{Z}_2$ by $\mathbb{Z}_2^2$, with $\mathbb{Z}_2 \simeq \{I, -I\}$, and cosets

$$0 \leftrightarrow 00 \leftrightarrow \{\pm I\},$$
$$1 \leftrightarrow 01 \leftrightarrow \{\pm \mathrm{e}_1\},$$
$$2 \leftrightarrow 10 \leftrightarrow \{\pm \mathrm{e}_2\},$$
$$3 \leftrightarrow 11 \leftrightarrow \{\pm \mathrm{e}_1 \mathrm{e}_2\}.$$

(L 2005)

The groups $\mathbb{G}_{m,m}$ and $\mathbb{Z}_2^{2m}$

For $m > 1$, the group $\mathbb{G}_{m,m}$ of order 2^{2m+1} consists of matrices of the form $g_1 \otimes g_{m-1}$ with g_1 in $\mathbb{G}_{1,1}$ and g_{m-1} in $\mathbb{G}_{m-1,m-1}$.

This group is an extension of $\mathbb{Z}_2 \simeq \{\pm I\}$ by $\mathbb{Z}_2^{2m}$:

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

(L 2005)

Canonical basis matrices of $\mathbb{R}_{m,m}$

A *canonical ordered basis* of the matrix representation of the Clifford algebra $\mathbb{R}_{m,m}$ is given by an ordered transversal of $\mathbb{Z}_2 \simeq \{\pm I\}$ in $\mathbb{Z}_2^{2m}$.

For example, $(I, \mathrm{e}_1, \mathrm{e}_2, \mathrm{e}_1\mathrm{e}_2)$ is one such ordered basis.

We define a function $\gamma_m : \mathbb{Z}_{2^{2m}} \to \mathbb{G}_{m,m}$ to choose the corresponding canonical basis matrix for $\mathbb{R}_{m,m}$ for some transversal, and use binary expansion to get a function on $\mathbb{Z}_2^{2m}$.

For example, $\gamma_1(1) = \gamma_1(01) := \mathrm{e}_1$.

(L 2005)

The sign function s_1 on $\mathbb{Z}_4$ and $\mathbb{Z}_2^2$

We use the function γ_1 to define the *sign function* s_1 :

$$s_1(i) := \begin{cases} 1 \leftrightarrow \gamma_1(i)^2 = -I \\ 0 \leftrightarrow \gamma_1(i)^2 = I, \end{cases}$$

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

Using our vector notation, we see that $[s_1] = [1, -1, 1, 1]^T$.

(L 2014)

The sign function s_m on $\mathbb{Z}_{2^{2m}}$ and $\mathbb{Z}_2^{2m}$

We use the function γ_m to define the sign function s_m :

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

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

(L 2014)

Properties of the sign function s_m

If we define $\odot : \mathbb{Z}_2 \times \mathbb{Z}_2^{2m-2} \to \mathbb{Z}_2^{2m}$ as concatenation,

e.g.. $01 \odot 1111 := 011111$, it is easy to verify that

$$s_m(i_1 \odot i_{m-1}) = s_1(i_1) + s_{m-1}(i_{m-1})$$

for all i_1 in $\mathbb{Z}_2$ and i_{m-1} in $\mathbb{Z}_2^{2m-2}$, and therefore

$$[s_m] = [s_1] \otimes [s_{m-1}].$$

Also, since each $\gamma_m(i)$ is orthogonal,

$s_m(i) = 1$ if and only if $\gamma_m(i)$ is skew.

(L 2014)

The symmetry function t_m on $\mathbb{Z}_{2^{2m}}$ and $\mathbb{Z}_2^{2m}$

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

$$t_1(i) := \begin{cases} 1 & \text{if } \gamma_1(i) = \mathrm{e}_2, \\ 0 & \text{otherwise.} \end{cases}$$

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

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

where $\odot$ denotes concatenation.

Properties of the symmetry function t_m

It is easy to verify that $t_m(i) = 1$ if and only if $\gamma_m(i)$ is symmetric but not diagonal.

This can be checked directly for t_1.

For $m > 1$ it results from properties of the Kronecker product:

- $(A \otimes B)^T = A^T \otimes B^T$.
- $A \otimes B$ is diagonal if and only if both A and B are diagonal.

Proof of Theorem 2: t_m is bent

Lemma 8

(Tokareva, 2011 Theorem 1; Canteaut and Charpin, 2003 Theorem 2; Canteaut et al., 2001, Theorem V.4)

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 2: t_m is bent

In Lemma 8, set $f_0 = f_3 := t_{m-1}, f_1 = s_{m-1}, f_2 = s_{m-1} + 1$.

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 $\tilde{f}_0 + \tilde{f}_1 + \tilde{f}_2 + \tilde{f}_3 = 1$.

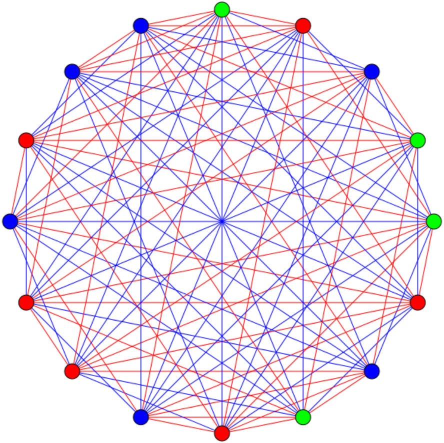
Thus, these four functions satisfy the premise of Lemma 8, as long as both s_{m-1} and t_{m-1} are bent.

I have already shown that s_m is bent for all m.

It is easy to show that t_1 is bent, directly from its definition.

Therefore t_m is bent.

The graphs from Theorem 1 and Theorem 2 are the red and the blue subgraphs of Δ_m.
They are isomorphic.



Δ_2

Open question

For which m is there an isomorphism of $\varDelta_m$ that

swaps all red and blue edges?

Isomorphisms have been constructed for $m = 1, 2, 3$ so far.

(L 2014)

References

[1] Anne Canteaut, Claude Carlet, Pascale Charpin, and Caroline Fontaine. "On cryptographic properties of the cosets of $R(1, m)$." IEEE Transactions on Information Theory, 47.4 (2001): 1494-1513.

[2] Anne Canteaut and Pascale Charpin. "Decomposing bent functions." IEEE Transactions on Information Theory, 49.8 (2003): 2004-2019.

[3] Natalia Tokareva. "On the number of bent functions from iterative constructions: lower bounds and hypotheses." Adv. in Mathematics of Communications (AMC) 5.4 (2011): 609-621.