Skew, bent and fractious: a confession

Paul Leopardi

Mathematical Sciences Institute, Australian National University.
Presented on 3 October 2013 at AustMS 2013, Sydney.

Corrected, 4 October 2013
Acknowledgements

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

National Computational Infrastructure.

Australian Mathematical Sciences Institute.

Australian National University.
Result 1: anti-amicability

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

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

The graph of anti-amicability of the canonical basis matrices of the neutral Clifford algebra $\mathbb{R}_{2,2}$ is strongly regular with parameters $(\nu, k, \lambda = \mu) = (16, 6, 2)$ is the $4 \times 4$ lattice graph and not the Shrikande graph.
Overview

- What led to this investigation?
- Key concepts.
- Specific construction.
- Why is Result 1 true?
Motivation

Anti-amicability of $4 \times 4$ Hadamard matrices: 24 components.
A long history and a deep literature

- Difference sets.
  Bruck (1955), Hall (1956), Menon (1960, 1962),
  Mann (1965), Turyn (1965), Baumert (1969),
  Kantor (1975, 1985), Ma (1994), ...

- Bent functions.
  Dillon (1974), Rothaus (1976), Dempwolff (2006), ...

- 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 $(v, k, \lambda, n)$ 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 $\lambda$ solutions $(d_i, d_j)$ with $d_i, d_j$ in $D$.

The parameter $n := k - \lambda$.

(Dillon 1974).
Hadamard difference sets

A \((v, k, \lambda, n)\) difference set with \(v = 4n\) is called a Hadamard difference set.

**Theorem 1**

*(Menon 1962)*

A Hadamard difference set has parameters of the form

\[(v, k, \lambda, n) = (4N^2, 2N^2 - N, N^2 - N, N^2)\]

or

\[(4N^2, 2N^2 + N, N^2 + N, N^2)\].

*(Menon 1962, Dillon 1974).*
Bent functions

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

\[
H_1 := \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix},
\]

\[
H_m := H_{m-1} \otimes H_1, \quad \text{for } m > 1.
\]

For a boolean function \(f : \mathbb{Z}_2^m \rightarrow \mathbb{Z}_2\), 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 Boolean function \( f : \mathbb{Z}_2^m \rightarrow \mathbb{Z}_2 \) is \textit{bent} if its Hadamard transform has constant magnitude.

In other words,

\[
|H_m[f]| = C[1, \ldots, 1]^T.
\]

for some constant \( C \).

(Dillon 1974)
Bent functions and Hadamard difference sets

**Theorem 2**

*(Dillon 1974, 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.

**Theorem 3**

*(Dillon 1974, Remark 6.2.4)*

Bent functions exist on \( \mathbb{Z}_2^m \) only when \( m \) is even.
A simple graph $\Gamma$ of order $v$ is strongly regular with parameters $(v, k, \lambda, \mu)$ if

- each vertex has degree $k$,
- each adjacent pair of vertices has $\lambda$ common neighbours, and
- each nonadjacent pair of vertices has $\mu$ common neighbours.

(Brouwer, Cohen and Neumaier 1989)
**Bent functions and strongly regular graphs**

The **Cayley graph** of a binary function \( f : \mathbb{Z}_2^m \rightarrow \mathbb{Z}_2 \) 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 \( \mathbb{Z}_2^m \).

**Theorem 4**

*(Bernasconi and Codenotti 1999, Lemma 12)*

The Cayley graph of a bent function on \( \mathbb{Z}_2^m \) is a strongly regular graph with \( \lambda = \mu \).

**Theorem 5**

*(Bernasconi, Codenotti and VanderKam 2001, Theorem 3)*

Bent functions are the only binary functions on \( \mathbb{Z}_2^m \) whose Cayley graph is a strongly regular graph with \( \lambda = \mu \).
The groups $G_{1,1}$ and $\mathbb{Z}_2^2$

The $2 \times 2$ orthogonal matrices

$$e_1 := \begin{bmatrix} 1 & -1 \\ 1 & -1 \end{bmatrix}, \quad e_2 := \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$$

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

$$0 \leftrightarrow 00 \leftrightarrow \{\pm I\},$$

$$1 \leftrightarrow 00 \leftrightarrow \{\pm e_1\},$$

$$2 \leftrightarrow 10 \leftrightarrow \{\pm e_2\},$$

$$3 \leftrightarrow 11 \leftrightarrow \{\pm e_1 e_2\}.$$
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 $\mathbb{Z}_2^{2m}$:

$$
0 \leftrightarrow 00\ldots00 \leftrightarrow \{ \pm I \},
$$

$$
1 \leftrightarrow 00\ldots01 \leftrightarrow \{ \pm I_{(2)}^{\otimes(m-1)} \otimes e_1 \},
$$

$$
2 \leftrightarrow 00\ldots10 \leftrightarrow \{ \pm I_{(2)}^{\otimes(m-1)} \otimes e_2 \},
$$

$$
\ldots
$$

$$
2^{2m} - 1 \leftrightarrow 11\ldots11 \leftrightarrow \{ \pm (e_1e_2)^{\otimes m} \}.
$$
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, $(I, e_1, e_2, e_1 e_2)$ is one such ordered basis.

We define a function $\gamma_m : \mathbb{Z}_{2^{2m}} \rightarrow G_{m,m}$ 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, $\gamma_1(1) = \gamma_1(01) := e_1$. 
The sign function \( s_1 \) on \( \mathbb{Z}_4 \) and \( \mathbb{Z}_2^2 \)

We use the function \( \gamma_1 \) 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 notation, we see that \([s_1] = [1, -1, 1, 1]^T\).
The sign function $s_m$ on $\mathbb{Z}_{2^m}$ and $\mathbb{Z}_2^{2^m}$

We use the function $\gamma_m$ 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 $\mathbb{Z}_2^{2^m}$. 
If we define $\odot : \mathbb{Z}_2 \times \mathbb{Z}_2^{2m-2} \rightarrow \mathbb{Z}_2^{2m}$ as concatenation of bit vectors, e.g. $01 \odot 1111 := 011111$, it becomes 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.
Proof of Result 1: \( s_m \) is bent

Recall that \([s_1] = [1, -1, 1, 1]^T\).

We show that \( s_1 \) is bent by forming

\[
H_2[s_1] = \begin{bmatrix}
1 & 1 & 1 & 1 \\
1 & -1 & 1 & 1 \\
1 & 1 & -1 & 1 \\
1 & 1 & 1 & -1 \\
1 & -1 & 1 & 1
\end{bmatrix}
\begin{bmatrix}
1 \\
1 \\
1 \\
1
\end{bmatrix} = \begin{bmatrix}
2 \\
2 \\
-2 \\
2
\end{bmatrix}.
\]
Proof of Result 1: $s_m$ is bent

Recall that for $m > 1$, $H_{2m} = H_2 \otimes H_{2m-2}$ and $[s_m] = [s_1] \otimes [s_{m-1}]$.

Therefore

$$H_{2m}[s_m] = H_2[s_1] \otimes H_{2m-2}[s_{m-1}] = (H_2[s_1])^{(\otimes m)},$$

which has constant absolute value.
The $4 \times 4$ lattice graph

Image from
http://mathworld.wolfram.com/LatticeGraph.html