INCOMPLETE DRAFT: Classifying bent functions by their Cayley graphs

Paul Leopardi *

INCOMPLETE DRAFT: 18 April 2017

Abstract

1 Introduction

Binary bent functions are important combinatorial objects. Besides the well-known application of bent functions and their generalizations to cryptography [1] [36, 4.1-4.6], bent functions have well-studied connections to Hadamard difference sets [10], symmetric designs with the symmetric difference property [11, 18], projective two-weight codes [12] and strongly regular graphs.

In two papers, Bernasconi and Codenotti [2], and then Bernasconi, Codenotti and Vanderkam [3] explored some of the connections between bent functions and strongly regular graphs. While these papers established that the Cayley graph of a binary bent function (whose value at 0 is 0) is a strongly regular graph with certain parameters, they leave open the question of which strongly regular graphs with these parameters be so obtained. Kantor, in 1983 [19], showed that the number of non-isomorphic projective linear two weight codes with certain parameters, Hadamard difference sets, and symmetric designs with certain properties, grows at exponentially with dimension. This result suggests that the number of strongly regular graphs obtained as Cayley graphs of bent functions also increases at least exponentially with dimension.

*University of Melbourne mailto:paul.leopardi@gmail.com

In a recent paper, the author found an example of two infinite series of bent functions whose Cayley graphs have the same strongly regular parameters at each dimension, but are not isomorphic if the dimension 8 or more [23].

The goal of the current paper is to further explore the connections between bent functions, their Cayley graphs, and related combinatorial objects, and in particular to examine the relationship between various equivalence classes of bent functions, in particular, the relationship between the extended affine equivalence classes and equivalence classes defined by isomorphism of Cayley graphs. As well as a theoretical study of bent functions of all dimensions, an empirical study is conducted into bent functions of dimension at most 8, using SageMath [34] and SageMathCloud [32].

The remainder of the paper is organized as follows. Section 2 covers the concepts, definitions and known results used later in the paper. Some of these concepts and definitions are novel, such as new notions of equivalence of bent functions. Section 3 contains the main theoretical results of the paper. Section 4 lists some of the properties of the equivalence classes of bent functions for dimension up to 8. Section 5 describes the SageMath and SageMathCloud code that has been used to obtain and display these empirical results. Section 6 puts these results in the context of questions that are still open.

2 Key concepts

This section presents some of the key concepts used in the remainder of the paper.

We first define the primary objects of study, bent functions and their Cayley graphs.

2.1 Bent functions

Bent Boolean functions can be defined in a number of equivalent ways. The definition used here involves the Walsh Hadamard Transform.

Definition 1. *The Walsh Hadamard transform of a Boolean function* $f : \mathbb{Z}_2^m \to \mathbb{Z}_2$ *is*

$$W_f(y) := \sum_{x \in \mathbb{Z}_2^{2m}} (-1)^{\langle x,y \rangle} + f(x)$$

Definition 2. *A Boolean function $f : \mathbb{Z}_2^m \to \mathbb{Z}_2$ is bent if and only if its Walsh Hadamard transform has constant magnitude 2^{-m} [10, p. 74] [30, p. 300].*

The remainder of this paper refers to bent Boolean functions simply as bent functions.

Remark: Bent functions can also be characterized as those Boolean functions whose Hamming distance from any affine Boolean function is the maximum possible [28, Theorem 3.3].

The characterization of bent functions given by Definition 2 immediately implies the existence of dual functions:

Definition 3. *For a bent function f, the function $\widetilde{f}$, defined by*

$$(-1)^{\widetilde{f}(x)} := 2^{-m} \sum_{y \in \mathbb{Z}_2^{2m}} (-1)^{f(y)+\langle x,y \rangle}$$

is called the dual of f [35].

Remark: The function $\widetilde{f}$ is also a bent function on $\mathbb{Z}_2^{2m}$ [30, p. 301].

2.2 Weights and weight classes

Definition 4. *The Hamming weight of a Boolean function is the cardinality of its support. For f on $\mathbb{Z}_2^{2m}$*

$$\operatorname{supp}(f) := \{x \in \mathbb{Z}_2^{2m} \mid f(x) = 1\}, \quad \operatorname{wt}(f) := |\operatorname{supp}(f)|.$$

The remainder of this paper refers to Hamming weights simply as weights.

Since a bent function of a given dimension can have only one of two weights, the weights can be used to define equivalence classes of bent functions here called *weight classes*.

Definition 5. *A bent function f on $\mathbb{Z}_2^{2m}$ has weight [10, Theorem 6.2.10]*

$$\begin{aligned} &\operatorname{wt}(f) = 2^{2m-1} - 2^{m-1} \quad (\textit{weight class number } \operatorname{wc}(f) = 0), \textit{ or} \\ &\operatorname{wt}(f) = 2^{2m-1} + 2^{m-1} \quad (\textit{weight class number } \operatorname{wc}(f) = 1). \end{aligned}$$

2.3 The Cayley graph of a Bent function

The Cayley graph of a bent function f with $f(0) = 0$ is defined in terms of the Cayley graph for a general Boolean function with f with $f(0) = 0$.

The Cayley graph of a Boolean function.

Definition 6. *For a Boolean function $f : \mathbb{Z}_2^{2m} \to \mathbb{Z}_2$, with $f(0) = 0$ we consider the simple undirected* Cayley graph $\mathrm{Cay}(f)$ *[2, 3.1] where the vertex set $V(\mathrm{Cay}(f)) = \mathbb{Z}_2^{2m}$ and for $i, j \in \mathbb{Z}_2^{2m}$, the edge (i, j) is in the edge set $E(\mathrm{Cay}(f))$ if and only if $f(i + j) = 1$.*

Note especially that in contrast with the paper of Bernasconi and Codenotti [2], this paper defines Cayley graphs only for Boolean functions f with $f(0) = 0$, since the use of Definition 6 with a function f for which $f(0) = 1$ would result in a graph with loops rather than a simple graph.

Bent functions and strongly regular graphs. We repeat below in Proposition 1 the result of Bernasconi and Codenotti [2] that the Cayley graph of a bent function is strongly regular. The following definition is used fix the notation used in this paper.

Definition 7. *A simple graph Γ of order v is* strongly regular *[4, 6, 33] 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.*

Proposition 1. *The Cayley graph $\mathrm{Cay}(f)$ of a bent function f on $\mathbb{Z}_2^{2m}$ (with $f(0) = 0$) is a strongly regular graph with $\lambda = \mu$ [2, Lemma 12].*

The parameters of $\mathrm{Cay}(f)$ are [10, Theorem 6.2.10] [14, Theorem 3.2]

$$\begin{aligned}(v, k, \lambda) =& (4^m, 2^{2m-1} - 2^{m-1}, 2^{2m-2} - 2^{m-1}) \\ \text{or} \quad & (4^m, 2^{2m-1} + 2^{m-1}, 2^{2m-2} + 2^{m-1}).\end{aligned}$$

2.4 The two block designs of a bent function

The adjacency matrix of $\mathrm{Cay}(f)$ can also be interpreted as the incidence matrix of a block design. In this case we do not need $f(0) = 0$.

Definition 8. *A symmetric block design described by Kantor [18, Section 5], and further investigated by Dillon and Schatz [11] [29, Theorem 3.29], can be defined by the incidence matrix $D(f)$ where*

$$D(f)_{c,x} := f(x) + \langle c, x \rangle + \widetilde{f}(c). \tag{1}$$

This is a symmetric block design with the symmetric difference property*, which we call the* SDP design *of f.*

2.5 Projective two-weight binary codes

Definition 9. *[5] [37]*

A two-weight binary code with parameters $[n, k, d]$ is a k dimensional subspace of $\mathbb{Z}_2^n$ with minimum Hamming distance d, such that the set of Hamming weights of the non-zero vectors has size 2.

Bouyukliev, Fack, Willems and Winne [5, p. 60] define projective codes as follows. "A generator matrix G of a linear code $[n, k]$ code C is any matrix of rank k (over $\mathbb{Z}_2$) with rows from C. . . . A linear $[n, k]$ code is called projective if no two columns of a generator matrix G are linearly dependent, i.e., if the columns of G are pairwise different points in a projective $(k-1)$-dimensional space."

Remark: In the case of $\mathbb{Z}_2$, no two columns are equal.

2.6 More concepts of equivalence of bent functions

The following concepts of equivalence of bent functions are used in this paper.

Extended affine equivalence.

Definition 10. *For bent functions $f, g : \mathbb{Z}_2^{2m} \to \mathbb{Z}_2$, f is extended affine equivalent [36, Section 1.4] to g if and only if*

$$g(x) = f(Ax + b) + \langle c, x \rangle + \delta$$

for some $A \in GL(2m, 2)$, $b, c \in \mathbb{Z}_2^{2m}$, $\delta \in \mathbb{Z}_2$.

General linear equivalence.

Definition 11. *For bent functions $f, g : \mathbb{Z}_2^{2m} \to \mathbb{Z}_2$, f is general linear equivalent to g if and only if*

$$g(x) = f(Ax)$$

for some $A \in GL(2m, 2)$.

Extended translation equivalence.

Definition 12. *For bent functions $f, g : \mathbb{Z}_2^{2m} \to \mathbb{Z}_2$, f is extended translation equivalent to g if and only if*

$$g(x) = f(x + b) + \langle c, x \rangle + \delta$$

for $b, c \in \mathbb{Z}_2^{2m}$, $\delta \in \mathbb{Z}_2$.

Cayley equivalence.

Definition 13. *For $f, g : \mathbb{Z}_2^{2m} \to \mathbb{Z}_2$, with both f and g bent, we call f and g Cayley equivalent, and write $f \equiv g$, if and only if $f(0) = g(0) = 0$ and $\mathrm{Cay}(f) \equiv \mathrm{Cay}(g)$ as graphs.*

Equivalently, $f \equiv g$ if and only if $f(0) = g(0) = 0$ and there exists a bijection $\pi : \mathbb{Z}_2^{2m} \to \mathbb{Z}_2^{2m}$ such that

$$g(x + y) = f\big(\pi(x) + \pi(y)\big) \quad \text{for all } x, y \in \mathbb{Z}_2^{2m}.$$

Extended Cayley equivalence.

Definition 14. *For $f, g : \mathbb{Z}_2^{2m} \to \mathbb{Z}_2$, with both f and g bent, if there exist $\delta, \epsilon \in \{0, 1\}$ such that $f + \delta \equiv g + \epsilon$, we call f and g extended Cayley (EC) equivalent and write $f \cong g$.*

Extended Cayley equivalence is an equivalence relation on the set of all bent functions on $\mathbb{Z}_2^{2m}$.

Remark: While extended affine equivalence has been well studied, general linear equivalence and extended translation equivalence are less often used, and the two notions of Cayley equivalence are apparently new.

3 Theoretical results

This section contains a number of theoretical results that serve a few purposes. Firstly, in order to classify bent functions by their Cayley graphs, it helps to understand the relationship between Cayley equivalence and other concepts of equivalence of bent functions, especially if this helps to cut down the search space needed for the classification. A similar consideration applies to the duals of bent functions. Secondly, some empirical observations made in the classification of bent functions in small dimensions can be explained by theoretical results. Thirdly, theoretical results can improve our understanding of the relationships between some of the concepts introduced in the previous section, notably dual bent functions, SDP designs, projective two-weight codes, and strongly regular graphs.

3.1 Different concepts of equivalence

General linear equivalence implies Cayley equivalence. Firstly, general linear equivalence implies Cayley equivalence. Specifically, the following result applies.

Theorem 1. *If f is bent with $f(0) = 0$ and $g(x) := f(Ax)$ where $A \in GL(2m, 2)$, then g is bent with $g(0) = 0$ and $f \equiv g$.*

Proof.

$$g(x + y) = f\big(A(x + y)\big) = f(Ax + Ay) \quad \text{for all } x, y \in \mathbb{Z}_2^{2m}.$$

□

Extended affine, translation, and Cayley equivalence. Secondly, if f is bent with $f(0) = 0$, and a bent function h is extended affine equivalent to f, then a bent function g can be found that is Cayley equivalent to h and extended translation equivalent to f.

Theorem 2. *For $A \in GL(2m, 2)$, $b, c \in \mathbb{Z}_2^{2m}$, $\delta \in \mathbb{Z}_2$, $f : \mathbb{Z}_2^{2m} \to \mathbb{Z}_2$, the function*

$$h(x) := f(Ax + b) + \langle c, x\rangle + \delta$$

can be expressed as $h(x) = g(Ax)$ where

$$g(x) := f(x + b) + \langle (A^{-1})^T c, x\rangle + \delta,$$

and therefore if f is bent and $h(0) = 0$ then $h \equiv g$.

Proof. Let $y := Ax$. Then

$$\begin{aligned} g(Ax) = g(y) &= f(y + b) + \langle (A^{-1})^T c, y\rangle + \delta \\ &= f(y + b) + \langle c, A^{-1}y\rangle + \delta \\ &= f(Ax + b) + \langle c, x\rangle + \delta = h(x). \end{aligned}$$

If f is bent, then so are g and h. Therefore, by Theorem 1, if $h(0) = 0$ then $h \equiv g$. □

Therefore, to determine which strongly regular graphs occur in the extended Cayley equivalence classes within the extended affine equivalence class of a bent function $f : \mathbb{Z}_2^{2m} \to \mathbb{Z}_2$, for which $f(0) = 0$, we need only examine the extended translation equivalent functions of the form

$$f(x + b) + \langle c, x\rangle + f(b),$$

for each $b, c \in \mathbb{Z}_2^{2m}$. This cuts down the required search space considerably.

3.2 Weight classes, dual functions, and SDP designs

Weight classes and dual bent functions. We first note a connection between weight classes and dual bent functions that makes it a little easier to reason about dual bent functions. The following lemma expresses the dual bent function in terms of weight classes.

Lemma 1. *For a bent function $f : \mathbb{Z}_2^{2m} \to \mathbb{Z}_2$, and $x \in \mathbb{Z}_2^{2m}$,*

$$\widetilde{f}(x) = \mathrm{wc}\left(y \mapsto f(y) + \langle x, y\rangle\right)$$

The proof of Lemma 1 relies on the following lemma about weight classes.

Lemma 2. *For a bent function $f : \mathbb{Z}_2^{2m} \to \mathbb{Z}_2$,*

$$\mathrm{wc}\left(f\right) = 2^{-m}\,\mathrm{wt}\left(f\right) - 2^{m-1} + 2^{-1},$$

so that

$$\mathrm{wt}\left(f\right) = 2^{m}\,\mathrm{wc}\left(f\right) + 2^{2m-1} - 2^{m-1}.$$

Proof. If $\mathrm{wt}\left(f\right) = 2^{2m-1} - 2^{m-1}$ then

$$\begin{aligned} 2^{-m}\,\mathrm{wt}\left(f\right) - 2^{m-1} + 2^{-1} &= 2^{-m}(2^{2m-1} - 2^{m-1}) - 2^{m-1} + 2^{-1} \\ &= 2^{m-1} - 2^{-1} - 2^{m-1} + 2^{-1} = 0. \end{aligned}$$

If $\mathrm{wt}\left(f\right) = 2^{2m-1} + 2^{m-1}$ then

$$\begin{aligned} 2^{-m}\,\mathrm{wt}\left(f\right) - 2^{m-1} + 2^{-1} &= 2^{-m}(2^{2m-1} + 2^{m-1}) - 2^{m-1} + 2^{-1} \\ &= 2^{m-1} + 2^{-1} - 2^{m-1} + 2^{-1} = 1. \end{aligned}$$

□

Proof of Lemma1. Let $h(y) := y \mapsto f(y) + \langle x, y\rangle$. Then

$$\begin{aligned} (-1)^{\widetilde{f}(x)} &= 2^{-m} \sum_{y \in \mathbb{Z}_2^{2m}} (-1)^{f(y)+\langle x,y\rangle} \\ &= 2^{-m} \left(\sum_{f(y)+\langle x,y\rangle=0} 1 - \sum_{f(y)+\langle x,y\rangle=1} 1 \right) \\ &= 2^{-m} \left(2^{2m} - 2\,\mathrm{wt}\left(h\right)\right) \\ &= 2^{m} - 2^{1-m}\,\mathrm{wt}\left(h\right) \\ &= 2^{m} - 2^{1-m}(2^{m}\,\mathrm{wc}\left(h\right) + 2^{2m-1} - 2^{m-1}) \\ &= 2^{m} - 2\,\mathrm{wc}\left(h\right) - 2^{m} + 1 \\ &= 1 - 2\,\mathrm{wc}\left(h\right) = (-1)^{\mathrm{wc}(h)}, \end{aligned}$$

where we have used Lemma 2. □

The following propositions are based on well known results, but are useful in understanding the relationship between the duality of bent functions and various concepts of equivalence.

Firstly, general linear equivalence of bent functions f and g implies general linear equivalence of their duals, $\widetilde{f}$ and $\widetilde{g}$, which implies Cayley equivalence of $\widetilde{f}$ and $\widetilde{g}$.

Proposition 2. *[10, Remark 6.2.7]*
For a bent function $f : \mathbb{Z}_2^{2m} \to \mathbb{Z}_2$, and $A \in GL(2m, 2)$, if

$$g(x) := f(Ax)$$

then

$$\widetilde{g}(x) = \widetilde{f}\big((A^T)^{-1}x\big),$$

and therefore by Theorem 1, $\widetilde{g} \equiv \widetilde{f}$.
If, in addition, $f = \widetilde{f}$ then $\widetilde{g} \equiv g$.

Functions of the form

$$f(x) := \sum_{k=0}^{m-1} x_{2k}x_{2k+1}$$

are self dual bent functions, $f = \widetilde{f}$ [10, Remark 6.3.2]. There are many other self dual bent functions [8, 13].

The following proposition displays a relationship between the extended translation class of a bent function f

Proposition 3. *[10, Remark 6.2.7] [7, Proposition 8.7]*
For a bent function $f : \mathbb{Z}_2^{2m} \to \mathbb{Z}_2$, and $b, c \in \mathbb{Z}_2^{2m}$, if

$$g(x) := f(x + b) + \langle c, x\rangle$$

then

$$\widetilde{g}(x) = \widetilde{f}(x + c) + \langle b, x\rangle + \langle b, c\rangle.$$

This result has many implications. First, recall that a bent function is not necessarily extended affine equivalent to its dual [22].

Weight classes and the SDP design matrix.

Theorem 3. *For every bent function f, the weight class matrix of f equals the incidence matrix of the SDP design of f.*

Specifically, for a bent function $f : \mathbb{Z}_2^{2m} \to \mathbb{Z}_2$, and $b, c \in \mathbb{Z}_2^{2m}$,

$$\begin{aligned} M_{wc}(f)_{c,b} &:= \mathrm{wc}\left(x \mapsto f(x+b) + \langle c, x\rangle + f(b)\right) = f(b) + \langle c, b\rangle + \widetilde{f}(c) \\ &= D(f)_{c,b}, \end{aligned}$$

where $D(f)$ is defined by (1).

Proof. Let $g(x) := f(x+b) + \langle c, x\rangle + f(b)$. Then by change of variable $y := x + b$,

$$\begin{aligned} \mathrm{wc}\,(g) &= \mathrm{wc}\left(y \mapsto f(y) + \langle c, y\rangle + \langle c, b\rangle + f(b)\right) \\ &= \mathrm{wc}\left(y \mapsto f(y) + \langle c, y\rangle\right) + \langle c, b\rangle + f(b) \\ &= \widetilde{f}(c) + \langle c, b\rangle + f(b), \end{aligned}$$

as a consequence of Lemma 1. □

Quadratic bent functions have only two extended Cayley classes.

Theorem 4. *For each $m > 0$, the extended affine equivalence class of quadratic bent functions $q : \mathbb{Z}_2^{2m} \to \mathbb{Z}_2$ contains exactly two extended Cayley equivalence classes, corresponding to the two possible weight classes of $x \mapsto q(x+b) + \langle c, x\rangle + q(b)$.*

The proof of this theorem is quite long and is given in Appendix A.

3.3 Bent functions, linear codes and strongly regular graphs

From bent function to linear code.

Definition 15. *[12, Corollary 10]*

For a bent function $f : \mathbb{Z}_2^{2m} \to \mathbb{Z}_2$, define the linear code $C(f)$ by the generator matrix

$$\begin{aligned} M_C(f)_{x,y} &\in \mathbb{Z}_2^{2^{2m} \times \mathrm{wt}(f)}, \\ M_C(f)_{x,y} &:= \langle x, \mathrm{supp}\,(f)\,(y)\rangle, \end{aligned}$$

with x in lexicographic order of $\mathbb{Z}_2^{2m}$ and $\mathrm{supp}\,(f)\,(y)$ in lexicographic order of $\mathrm{supp}\,(f)$.

The 4^m words of the code $C(f)$ are the rows of the generator matrix $M_C(f)$.

Proposition 4. *[12, Corollary 10]*

For a bent function $f : \mathbb{Z}_2^{2m} \to \mathbb{Z}_2$, the linear code $C(f)$ is a projective two-weight binary code. The possible weights of non-zero code words are:

$$\begin{cases} 2^{2m-2}, 2^{2m-2} - 2^{m-1} & \text{if } \mathrm{wc}\,(f) = 0. \\ 2^{2m-2}, 2^{2m-2} + 2^{m-1} & \text{if } \mathrm{wc}\,(f) = 1. \end{cases}$$

From linear code to strongly regular graph.

Definition 16. *Given $f : \mathbb{Z}_2^{2m} \to \mathbb{Z}_2$, form the linear code $C(f)$.*

The graph $R(f)$ is defined as:

Vertices of $R(f)$ are code words of $C(f)$.

For $v, w \in C(f)$, edge $(u, v) \in R(f)$ if and only if

$$\begin{cases} \mathrm{wt}\,(u+v) = 2^{2m-2} - 2^{m-1} & (\mathrm{wc}\,(f) = 0). \\ \mathrm{wt}\,(u+v) = 2^{2m-2} + 2^{m-1} & (\mathrm{wc}\,(f) = 1). \end{cases}$$

Since $C(f)$ is a projective two-weight binary code, $R(f)$ is a strongly regular graph [9, Theorem 2].

The graph $R(f)$ is the Cayley graph of the extended dual.

Theorem 5. *For $f : \mathbb{Z}_2^{2m} \to \mathbb{Z}_2$, with $f(0) = 0$,*

$$R(f) \equiv \mathrm{Cay}\left(\widetilde{f} + \mathrm{wc}\,(f)\right).$$

Proof. We examine W_f, the Walsh Hadamard transform of f.

$$\begin{aligned} W_f(y) &= \sum_{x \in \mathbb{Z}_2^{2m}} (-1)^{\langle x,y \rangle} + f(x) = \sum_{f(x)=0} (-1)^{\langle x,y \rangle} + f(x) - 2 \sum_{f(x)=1} (-1)^{\langle x,y \rangle} \\ &= \sum_{x \in \mathbb{Z}_2^{2m}} (-1)^{\langle x,y \rangle} - 2 \sum_{f(x)=1} (-1)^{\langle x,y \rangle}. \end{aligned}$$

But

$$\sum_{x \in \mathbb{Z}_2^{2m}} (-1)^{\langle x,y \rangle} = \begin{cases} 4^m & (y = 0) \\ 0 & \text{otherwise,} \end{cases}$$

as per the Sylvester Hadamard matrices.

So, for $y \neq 0$,

$$W_f(y) = -2 \sum_{f(x)=1} (-1)^{\langle x,y \rangle},$$

so

$$\sum_{f(x)=1} (-1)^{\langle x,y \rangle} = \mathrm{wt}\,(f) - 2 \sum_{\substack{f(x)=1 \\ \langle x,y \rangle = 1}} 1 = -W_f(y)/2.$$

But

$$\sum_{\substack{f(x)=1 \\ \langle x,y \rangle = 1}} 1 = \mathrm{wt}\,(C(f)[y])\,,$$

the weight of code $C(f)$ at the point y. So

$$\mathrm{wt}\,(f) - 2\,\mathrm{wt}\,(C(f)[y]) = -W_f(y)/2,$$

and therefore

$$\mathrm{wt}\,(C(f)[y]) = \mathrm{wt}\,(f)\,/2 + W_f(y)/4.$$

We now examine the two possible weight class numbers of f.

If $\mathrm{wc}\,(f) = 0$ then $\mathrm{wt}\,(f) = 2^{2m-1} - 2^{m-1}$. For $y \neq 0$ there are two cases, depending on $\widetilde{f}(y)$:

If $\widetilde{f}(y) = 0$ then $W_f(y) = 2^m$, so

$$\mathrm{wt}\,(C(f)[y]) = 2^{2m-2} - 2^{m-2} + 2^{m-2} = 2^{2m-2} = 4^{m-1}.$$

If $\widetilde{f}(y) = 1$ then $W_f(y) = -2^m$, so

$$\mathrm{wt}\,(C(f)[y]) = 2^{2m-2} - 2^{m-2} - 2^{m-2} = 2^{2m-2} - 2^{m-1} = 4^{m-1} - 2^{m-1}.$$

Similarly, if $\mathrm{wc}\,(f) = 1$ then $\mathrm{wt}\,(f) = 2^{2m-1} + 2^{m-1}$, and so for $y \neq 0$

$$\mathrm{wt}\,(C(f)[y]) = \begin{cases} 4^{m-1} + 2^{m-1} & (\widetilde{f}(y) = 0) \\ 4^{m-1} & (\widetilde{f}(y) = 1). \end{cases}$$

Also, as a consequence of Lemma 1, $\mathrm{wc}\,(f) = \widetilde{f}(0)$, so if $g(y) := \widetilde{f}(y) + \mathrm{wc}\,(f)$ then $g(0) = 0$ and therefore the Cayley graph of g is well defined. □

4 Empirical Observations

4.1 Bent functions in 2 dimensions

One extended affine class, containing the extended translation class: $[f_{2,1}]$ where $f_{2,1}(x) := x_0x_1$ is self dual.

Two extended Cayley classes:

Class	Parameters	2-rank	Clique polynomial
0	$(4, 1, 0, 0)$	4	$2t^2 + 4t + 1$
1	K_4	4	$t^4 + 4t^3 + 6t^2 + 4t + 1$

4.2 Bent functions in 4 dimensions

One extended affine class, containing the extended translation class $[f_{4,1}]$ where
$f_{4,1}(x) := x_0x_1 + x_2x_3$ is self dual.

Two extended Cayley classes:

Class	Parameters	2-rank	Clique polynomial
0	$(16, 6, 2, 2)$	6	$8t^4 + 32t^3 + 48t^2 + 16t + 1$
1	$(16, 10, 6, 6)$	6	$16t^5 + 120t^4 + 160t^3 + 80t^2 + 16t + 1$

The Cayley graphs for classes 1 and 2 are isomorphic to those those obtained from the following projective two-weight codes:

Class	Parameters	Generator matrix
1	$[6, 4, 2]$	$\begin{bmatrix} 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix}$
2	$[5, 4, 2]$	$\begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 \end{bmatrix}$

4.3 Bent functions in 6 dimensions

Extended affine classes. In 1996, Tonchev classified the binary projective two-weight $[27, 21, 3]$ and $[35, 6, 16]$ codes listing them in Tables 1 and 2, respectively, of his paper [37]. These tables are repeated as Tables 1.155 and 1.156 in Chapter VII.1 of the Handbook of Combinatorial Designs, Second Edition [38], with a different numbering.

Four extended affine classes, containing the following extended translation classes:

Class	Representative
$[f_{6,1}]$	$f_{6,1} := x_0x_1 + x_2x_3 + x_4x_5$
$[f_{6,2}]$	$f_{6,2} := x_0x_1x_2 + x_0x_3 + x_1x_4 + x_2x_5$
$[f_{6,3}]$	$f_{6,3} := x_0x_1x_2 + x_0x_1 + x_0x_3 + x_1x_3x_4 + x_1x_5 + x_2x_4 + x_3x_4$
$[f_{6,4}]$	$f_{6,4} := x_0x_1x_2 + x_0x_3 + x_1x_3x_4 + x_1x_5 + x_2x_3x_5 + x_2x_3 + x_2x_4 + x_2x_5 + x_3x_4 + x_3x_5$

ET class $[f_{6,1}]$. The function $f_{6,1}(x) = x_0x_1 + x_2x_3 + x_4x_5$ is self dual.

Two extended Cayley classes:

Class	Parameters	2-rank	Clique polynomial
0	$(64, 28, 12, 12)$	8	$64t^8 + 512t^7 + 1792t^6 + 3584t^5 + 5376t^4 + 3584t^3 + 896t^2 + 64t + 1$
1	$(64, 36, 20, 20)$	8	$2304t^6 + 13824t^5 + 19200t^4 + 7680t^3 + 1152t^2 + 64t + 1$

The Cayley graphs for classes 0 and 1 are isomorphic to those those obtained from the following two-weight projective codes as listed by Tonchev [38]:

Class	Parameters	Reference
0	$[35, 6, 16]$	Table 1.156 1, 2 (complement)
1	$[27, 6, 12]$	Table 1.155 1

ET class $[f_{6,2}]$. The function $f_{6,2}(x) = x_0x_1x_2 + x_0x_3 + x_1x_4 + x_2x_5$.

Three extended Cayley classes:

Class	Parameters	2-rank	Clique polynomial
0	$(64, 28, 12, 12)$	8	$64t^8 + 512t^7 + 1792t^6 + 3584t^5 + 5376t^4 + 3584t^3 + 896t^2 + 64t + 1$
1	$(64, 28, 12, 12)$	8	$256t^6 + 1536t^5 + 4352t^4 + 3584t^3 + 896t^2 + 64t + 1$
2	$(64, 36, 20, 20)$	8	$192t^8 + 1536t^7 + 8960t^6 + 19968t^5 + 20224t^4 + 7680t^3 + 1152t^2 + 64t + 1$

Graph 0 is isomorphic to graph 0 of ET class $[f_{6,1}]$, and is also isomorphic to the complement of Royle's $(64, 35, 18, 20)$ strongly regular graph X [31].

The Cayley graphs for classes 0 to 2 are isomorphic to those those obtained from the following two-weight projective codes as listed by Tonchev [38]:

Class	Parameters	Reference
0	$[35, 6, 16]$	Table 1.156 1, 2 (complement)
1	$[35, 6, 16]$	Table 1.156 3 (complement)
2	$[27, 6, 12]$	Table 1.155 2

ET class $[f_{6,3}]$. The function

$$f_{6,3}(x) = x_0x_1x_2 + x_0x_1 + x_0x_3 + x_1x_3x_4 + x_1x_5 + x_2x_4 + x_3x_4.$$

Four extended Cayley classes:

Class	Parameters	2-rank	Clique polynomial
0	$(64, 28, 12, 12)$	12	$32t^8 + 256t^7 + 896t^6 + 2048t^5 + 4608t^4 + 3584t^3 + 896t^2 + 64t + 1$
1	$(64, 36, 20, 20)$	12	$160t^8 + 1280t^7 + 9344t^6 + 21504t^5 + 20480t^4 + 7680t^3 + 1152t^2 + 64t + 1$
2	$(64, 28, 12, 12)$	12	$64t^6 + 1024t^5 + 4096t^4 + 3584t^3 + 896t^2 + 64t + 1$
3	$(64, 36, 20, 20)$	12	$160t^8 + 1664t^7 + 9792t^6 + 21504t^5 + 20480t^4 + 7680t^3 + 1152t^2 + 64t + 1$

The Cayley graphs for classes 0 to 3 are isomorphic to those those obtained from the following two-weight projective codes as listed by Tonchev [38]:

Class	Parameters	Reference
0	$[35, 6, 16]$	Table 1.156 4 (complement)
1	$[27, 6, 12]$	Table 1.155 3
2	$[35, 6, 16]$	Table 1.156 5 (complement)
3	$[27, 6, 12]$	Table 1.155 4

ET class $[f_{6,4}]$. The function

$$f_{6,4}(x) = x_0x_1x_2 + x_0x_3 + x_1x_3x_4 + x_1x_5 + x_2x_3x_5 + x_2x_3 + x_2x_4 + x_2x_5 + x_3x_4 + x_3x_5.$$

Three extended Cayley classes:

Class	Parameters	2-rank	Clique polynomial
0	$(64, 28, 12, 12)$	14	$32t^8 + 256t^7 + 896t^6 + 1792t^5 + 4480t^4 + 3584t^3 + 896t^2 + 64t + 1$
1	$(64, 28, 12, 12)$	14	$16t^8 + 128t^7 + 448t^6 + 1280t^5 + 4224t^4 + 3584t^3 + 896t^2 + 64t + 1$
2	$(64, 36, 20, 20)$	14	$176t^8 + 1408t^7 + 9664t^6 + 22272t^5 + 20608t^4 + 7680t^3 + 1152t^2 + 64t + 1$

The Cayley graphs for classes 0 to 2 are isomorphic to those those obtained from the following two-weight projective codes as listed by Tonchev [38]:

Class	Parameters	Reference
0	$[35, 6, 16]$	Table 1.156 7 (complement)
1	$[35, 6, 16]$	Table 1.156 6 (complement)
2	$[27, 6, 12]$	Table 1.155 5

4.4 Bent functions in 8 dimensions

There are $99270589265934370305785861242880 \approx 2^{106}$ bent functions in dimension 8, according to Langevin and Leander [21]. The number of EA classes has not yet been published, let alone a list of representatives.

Extended affine classes up to degree 3. Up to degree 3: Ten extended affine classes, containing the following extended translation classes:

Class	Representative
$[f_{8,1}]$	$f_{8,1} := x_0x_1 + x_2x_3 + x_4x_5 + x_6x_7$
$[f_{8,2}]$	$f_{8,2} := x_0x_1x_2 + x_0x_3 + x_1x_4 + x_2x_5 + x_6x_7$
$[f_{8,3}]$	$f_{8,3} := x_0x_1x_2 + x_0x_6 + x_1x_3x_4 + x_1x_5 + x_2x_3 + x_4x_7$
$[f_{8,4}]$	$f_{8,4} := x_0x_1x_2 + x_0x_2 + x_0x_4 + x_1x_3x_4 + x_1x_5 + x_2x_3 + x_6x_7$
$[f_{8,5}]$	$f_{8,5} := x_0x_1x_2 + x_0x_6 + x_1x_3x_4 + x_1x_4 + x_1x_5 + x_2x_3x_5 + x_2x_4 + x_3x_7$
$[f_{8,6}]$	$f_{8,6} := x_0x_1x_2 + x_0x_2 + x_0x_3 + x_1x_3x_4 + x_1x_6 + x_2x_3x_5 + x_2x_4 + x_5x_7$
$[f_{8,7}]$	$f_{8,7} := x_0x_1x_2 + x_0x_1 + x_0x_2 + x_0x_3 + x_1x_3x_4 + x_1x_4 + x_1x_5 + x_2x_3x_5 + x_2x_4 + x_6x_7$
$[f_{8,8}]$	$f_{8,8} := x_0x_1x_2 + x_0x_5 + x_1x_3x_4 + x_1x_6 + x_2x_3x_5 + x_2x_4 + x_3x_7$
$[f_{8,9}]$	$f_{8,9} := x_0x_1x_6 + x_0x_3 + x_1x_4 + x_2x_3x_6 + x_2x_5 + x_3x_4 + x_4x_5x_6 + x_6x_7$
$[f_{8,10}]$	$f_{8,10} := x_0x_1x_2 + x_0x_3x_6 + x_0x_4 + x_0x_5 + x_1x_3x_4 + x_1x_6 + x_2x_3x_5 + x_2x_4 + x_3x_7$

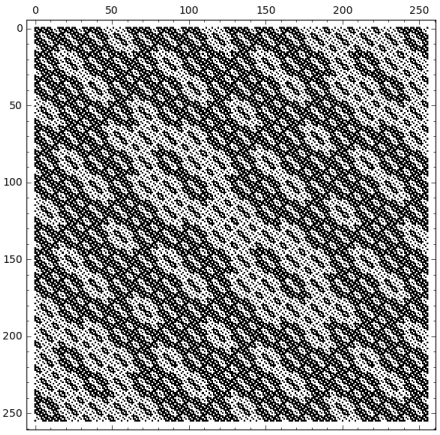

Figure 1: $[f_{8,1}]$: weight classes

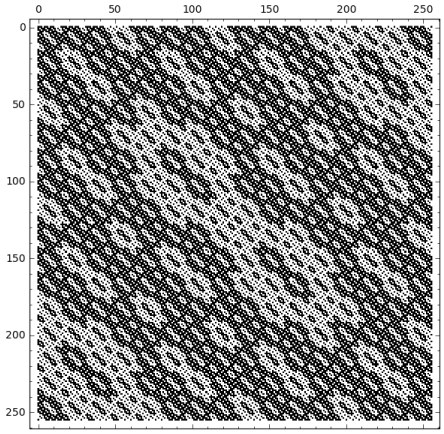

Figure 2: $[f_{8,1}]$: 2 extended Cayley classes

ET class $[f_{8,1}]$.

ET class $[f_{8,2}]$.

ET class $[f_{8,3}]$.

ET class $[f_{8,4}]$**.**

ET class $[f_{8,5}]$**.**

ET class $[f_{8,6}]$**.** The same 9 classes as $[f_{8,5}]$, with the same frequencies!

ET class $[f_{8,7}]$**.**

ET class $[f_{8,8}]$**.**

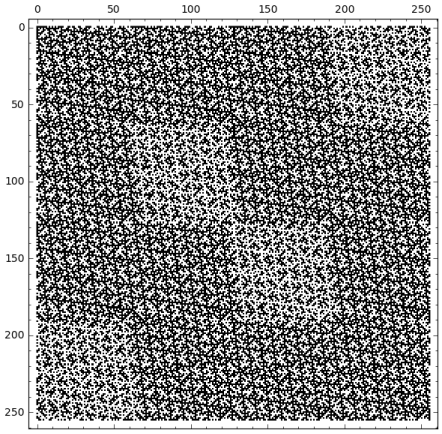

Figure 3: $[f_{8,2}]$: weight classes

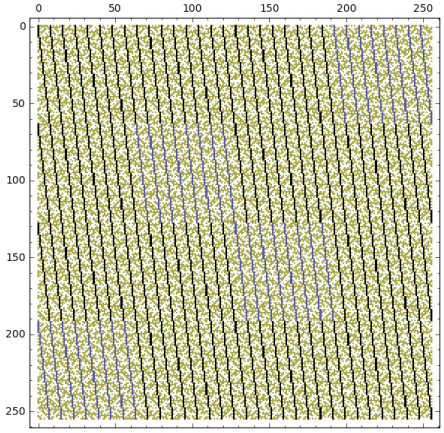

Figure 4: $[f_{8,2}]$: 4 extended Cayley classes

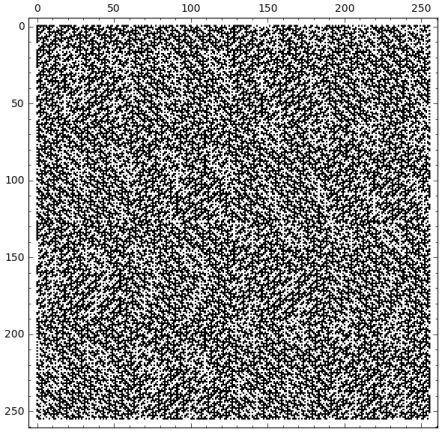

Figure 5: $[f_{8,3}]$: weight classes

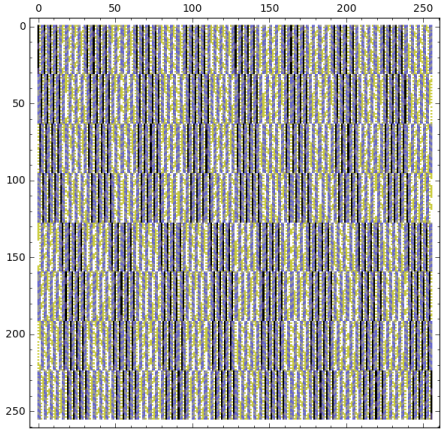

Figure 6: $[f_{8,3}]$: 6 extended Cayley classes

ET class $[f_{8,9}]$**.** 4 of the 8 classes form 2 dual pairs of classes.

ET class $[f_{8,10}]$**.** 6 of the 10 classes form 3 dual pairs of classes.

Partial spread bent functions. According to Langevin and Hou [20] there are $705767472375941143920 64 \approx 2^{75.9}$ *partial spread* bent functions in dimension 8, contained in 14758 EA classes, of which 14756 classes have degree 4. The EA class representatives are listed at Langevin's web site

`http://langevin.univ-tln.fr/project/spread/psp.html`

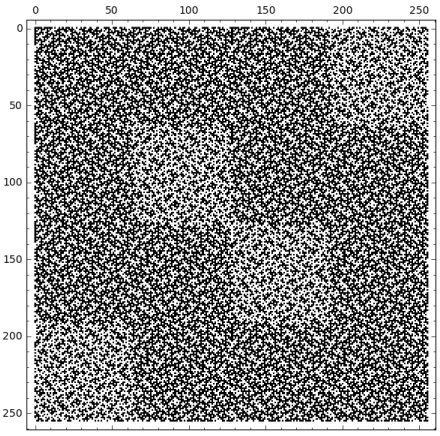

Figure 7: $[f_{8,4}]$: weight classes

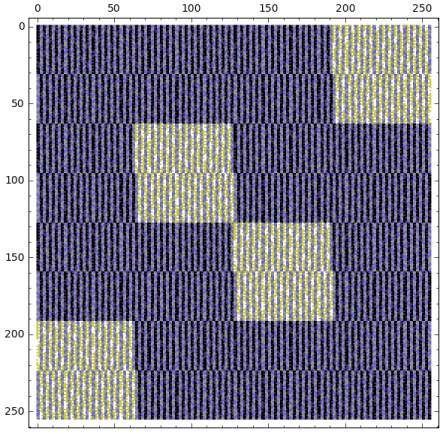

Figure 8: $[f_{8,4}]$: 5 extended Cayley classes

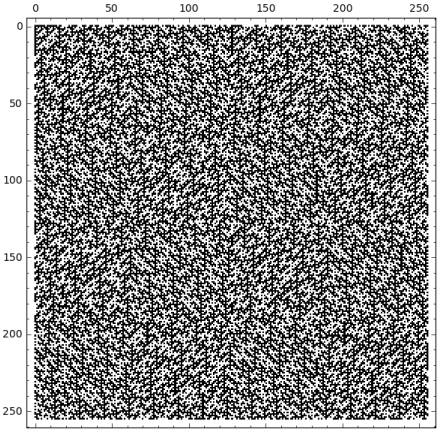

Figure 9: $[f_{8,5}]$: weight classes

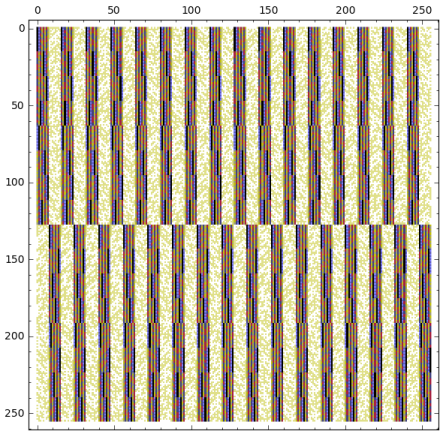

Figure 10: $[f_{8,5}]$: 9 extended Cayley classes

Example partial spread ET class $[psf_{9,5438}]$**.** 6 of the 16 classes form 3 dual pairs of classes.

5 SageMath and SageMathCloud code

Bliss: [16, 17]

Boolean-Cayley-graphs: GitHub repository [24] and SageMathCloud folder [25].

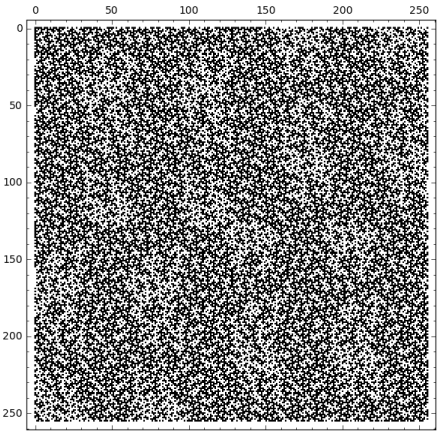

Figure 11: $[f_{8,6}]$: weight classes

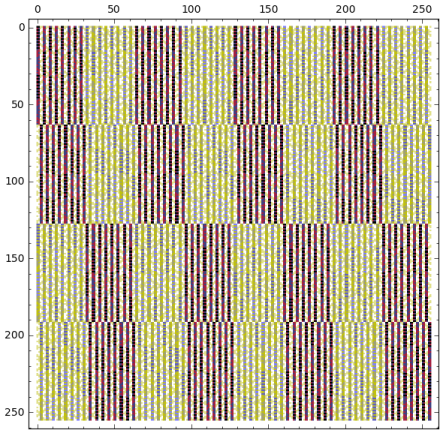

Figure 12: $[f_{8,6}]$: 9 extended Cayley classes

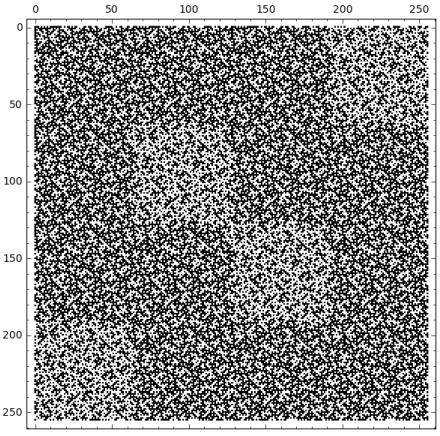

Figure 13: $[f_{8,7}]$: weight classes

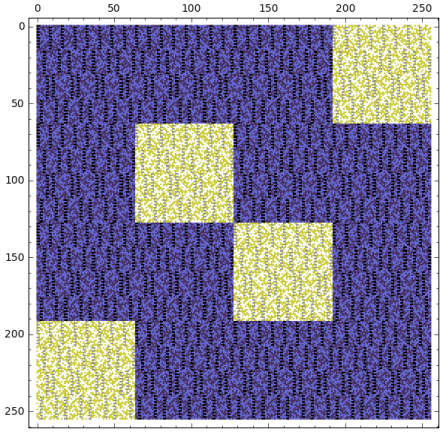

Figure 14: $[f_{8,7}]$: 5 extended Cayley classes

Nauty: [26, 27]
Coding theory and cryptography in Sage: [15]
SageMath: [34]
SageMathCloud: [32].

- 2015-04 to 2015-05 SageMathCloud: Cliques-Automorphisms project starts looking at Cayley classes for bent functions of dimension up to 6, using BooleanFunction and `is_isomorphic()`.
- 2015-12 SageMathCloud: Cliques-Automorphisms project worksheets

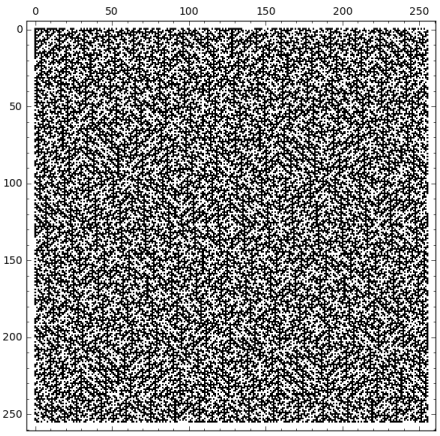

Figure 15: $[f_{8,8}]$: weight classes

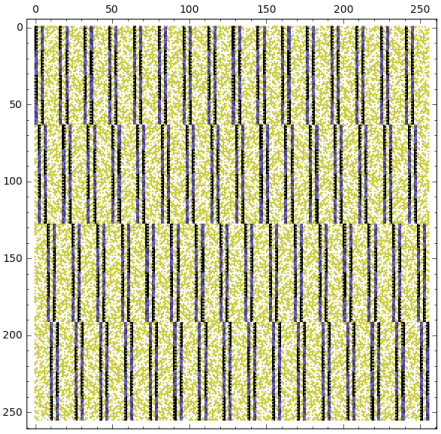

Figure 16: $[f_{8,8}]$: 6 extended Cayley classes

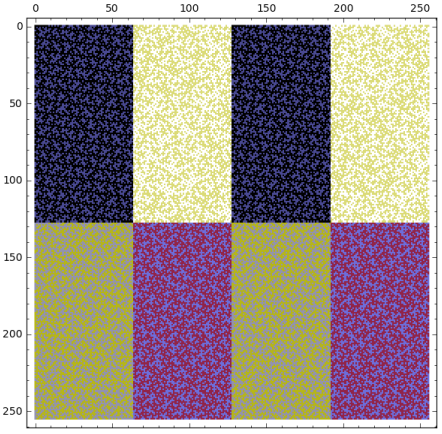

Figure 17: $[f_{8,9}]$: 8 extended Cayley classes

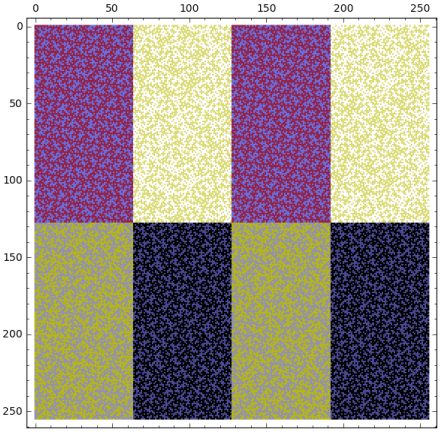

Figure 18: $[f_{8,9}]$: 8 extended Cayley classes of dual bent functions

produced initial results used in the ACCMCC presentation. The worksheets were too slow to effectively tackle bent functions in 8 dimensions.

- 2016-07 SageMath: Downloaded Sage and began refactoring worksheets into Sage code.
- 2016-08 GitHub: Uploaded refactored Sage code to new Boolean-Cayley-graphs project.
- 2016-08 SageMath: Began using canonical labels rather than directly testing for isomorphism between Cayley graphs. Canonical labelling

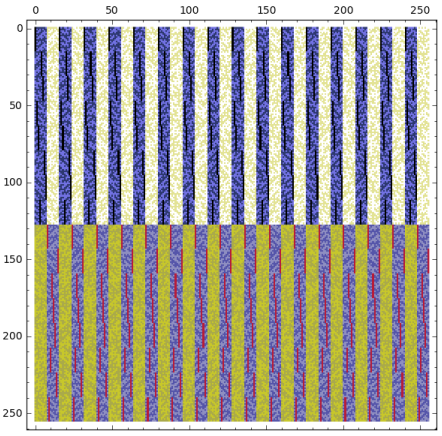

Figure 19: $[f_{8,10}]$: 10 extended Cayley classes

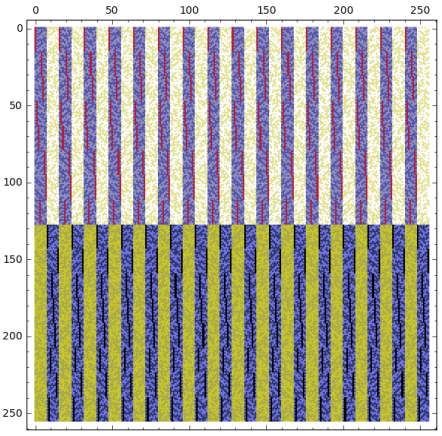

Figure 20: $[f_{8,10}]$: 10 extended Cayley classes of dual bent functions

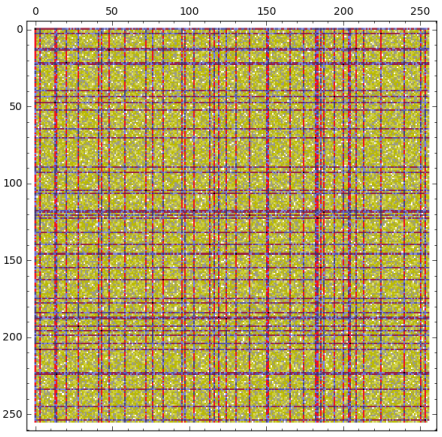

Figure 21: $[psf_{9,5438}]$: 16 extended Cayley classes

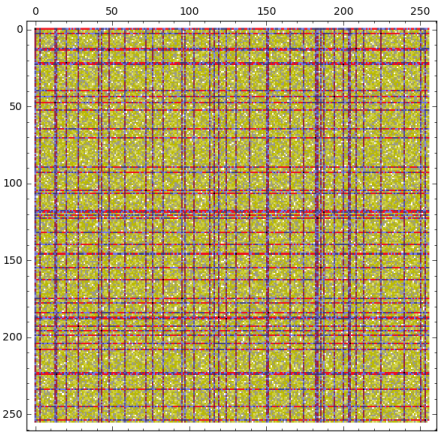

Figure 22: $[psf_{9,5438}]$: 16 extended Cayley classes of dual bent functions

uses the Bliss algorithm, speeding up computation in comparison to the default Sage algorithm, and allows comparison between graphs using equality of canonically labelled graphs rather than isomorphism, also giving a speed boost. This finally made it feasible to check bent functions in 8 dimensions up to degree 3.

- 2016-09 SageMath: Changed many Sage code files into Python modules. Introduced a BentFunction class.
- 2016-11 SageMath: `check_graphs_using_gap`

6 Discussion

The following questions have been settled only for $m \leqslant 3$:

1. How many EC classes are there for each m? Are there "Exponential numbers" of classes [19]?
2. Are there any ET classes that contain the maximum number, 16^m, different EC classes?
3. Which EC classes overlap more than one ET class?
4. Which bent functions are Cayley equivalent to their dual?

Also, what are the remaining EA and EC classes for $m = 4$, i.e. the EA and EC classes of binary bent functions of dimension 8 and degree 4 [21]?

A Proof of Theorem 4

The proof of Theorem 4 relies on a number of supporting lemmas, which are stated and proved here.

Lemma 3. *Let* $q(x) := x^T L x$ *where* $L \in \mathbb{Z}_2^{2m \times 2m}$,

$$L := \begin{bmatrix} 0 & I \\ 0 & 0 \end{bmatrix},$$

so that

$$q(x) = \sum_{k=0}^{m-1} x_k x_{m+k}.$$

Let $f(x) := q(x+b) + \langle c, x \rangle + q(b)$. *Then there exists* $c' \in \mathbb{Z}_2^{2m}$ *such that*

$$f(x) = q(x) + \langle c', x \rangle.$$

Proof.

$$\begin{aligned} q(x) = x^T L x, \quad \text{so } q(x+b) &= (x^T + b^T)L(x+b) \\ &= q(x) + x^T L b + b^T L x + q(b) \\ &= q(x) + \langle (L + L^T)b, x \rangle + q(b), \end{aligned}$$

and therefore

$$q(x+b) + \langle c, x \rangle + q(b) = q(x) + \langle (L + L^T)b + c, x \rangle.$$

□

Lemma 4. *Let $Z \in \mathbb{Z}_2^{2m \times 2m}$ be symmetric with zero diagonal. In other words, $Z = Z^T$, $\operatorname{diag}(Z) = 0$. Then for any $M \in \mathbb{Z}_2^{2m \times 2m}$,*

$$x^T(M + Z)x = x^T M x$$

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

Proof. Let Z, x be as above. Then

$$\begin{aligned} x^T Z x &= \sum_{i=0}^{2m-1} \sum_{j=0}^{2m-1} x_i Z_{i,j} x_j \\ &= \sum_{i=0}^{2m-1} \sum_{j<i} x_i Z_{i,j} x_j + \sum_{i=0}^{2m-1} x_i Z_{i,i} x_i + \sum_{i=0}^{2m-1} \sum_{j>i} x_i Z_{i,j} x_j \\ &= \sum_{i=0}^{2m-1} \sum_{j<i} x_i (Z_{i,j} + Z_{j,i}) = 0. \end{aligned}$$

Therefore

$$x^T(M + Z)x = x^T M x + x^T Z x = x^T M x.$$

□

Lemma 5. *Let q be defined as per Lemma 3. Then for all $c \in Z_2^{2m}$ with $q(c) = 0$, there exists $A \in GL(2m, 2)$ such that*

$$q(Ax) = q(x) + \langle c, x \rangle.$$

Proof. Let $C \in \mathbb{Z}_2^{2m\times 2m}$ be such that $C_{i,j} = \delta_{i,j}c_i$, where δ is the *Dirac delta*: $\delta_{i,j} = 1$ if $i = j$ and 0 otherwise. In other words $\operatorname{diag}(C) = c$. Then

$$\begin{aligned}\langle c, x\rangle &= \sum_{i=0}^{2m-1} c_i x_i \\ &= \sum_{i=0}^{2m-1} x_i c_i x_i = x^T C x.\end{aligned}$$

Therefore, by Lemma 4,

$$q(x) + \langle c, x\rangle = x^T(L + Z + C)x,$$

where $Z \in \mathbb{Z}_2^{2m\times 2m}$ is symmetric with zero diagonal.

For such Z, let $S := Z + C$. We want to find $A \in \mathbb{Z}_2^{2m\times 2m}$ such that $q(Ax) = q(x) + \langle c, x\rangle$. In other words,

$$q(Ax) = (Ax)^T L(Ax) = x^T A^T LAx = x^T(L + S)x.$$

This will be true if $A^T LA = L + S$.

Let

$$A := \begin{bmatrix} A_{0,0} & A_{0,1} \\ A_{1,0} & A_{1,1} \end{bmatrix}, \quad S := \begin{bmatrix} S_{0,0} & S_{0,1} \\ S_{0,1}^T & S_{1,1} \end{bmatrix} =: \begin{bmatrix} Z_{0,0} + C_{0,0} & Z_{0,1} \\ Z_{0,1}^T & Z_{1,1} + C_{1,1} \end{bmatrix}.$$

Since

$$LA = \begin{bmatrix} 0 & I \\ 0 & 0 \end{bmatrix} \begin{bmatrix} A_{0,0} & A_{0,1} \\ A_{1,0} & A_{1,1} \end{bmatrix} = \begin{bmatrix} A_{1,0} & A_{1,1} \\ 0 & 0 \end{bmatrix},$$

we require that

$$\begin{aligned} A^T LA &= \begin{bmatrix} A_{0,0} & A_{1,0} \\ A_{0,1} & A_{1,1} \end{bmatrix} \begin{bmatrix} A_{1,0} & A_{1,1} \\ 0 & 0 \end{bmatrix} \\ &= \begin{bmatrix} A_{0,0}^T A_{1,0} & A_{0,0}^T A_{1,1} \\ A_{0,1}^T A_{1,0} & A_{0,1}^T A_{1,1} \end{bmatrix} \\ &= L + S = \begin{bmatrix} S_{0,0} & I + S_{0,1} \\ S_{0,1}^T & S_{1,1} \end{bmatrix}, \end{aligned}$$

and therefore

$$\begin{aligned} A_{0,0}^T A_{1,0} &= S_{0,0}, \quad & A_{0,0}^T A_{1,1} &= I + S_{0,1}, \\ A_{0,1}^T A_{1,0} &= S_{0,1}^T, \quad & A_{0,1}^T A_{1,1} &= S_{1,1}. \end{aligned}$$

If $S_{0,1} = 0$ and $A_{0,0} = I$ then $A_{1,0} = S_{0,0}$, $A_{1,1} = I$ and $A_{0,1} = S_{1,1}$. In this case, we have $A_{0,1}^T A_{1,0} = S_{0,1}^T = 0$, i.e. $S_{1,1}S_{0,0} = 0$, and

$$A = \begin{bmatrix} I & S_{1,1} \\ S_{0,0} & I \end{bmatrix},$$

so that

$$\begin{aligned} A^T L A &= \begin{bmatrix} I & S_{0,0} \\ S_{1,1} & I \end{bmatrix} \begin{bmatrix} S_{0,0} & I \\ 0 & 0 \end{bmatrix} \\ &= \begin{bmatrix} S_{0,0} & I \\ 0 & S_{1,1} \end{bmatrix} \\ &= L + S. \end{aligned}$$

Also

$$S = \begin{bmatrix} Z_{0,0} + C_{0,0} & 0 \\ 0 & Z_{1,1} + C_{1,1} \end{bmatrix}.$$

Since $q(c) = 0$ we have

$$q(c) = \sum_{k=0}^{m-1} c_k c_{m+k} = 0.$$

Let $K := \{k \mid c_k c_{m+k} = 1\}$. Then we must have $|K| = 2r$ for some integer $r \geqslant 0$, i.e. $|K|$ is even. We therefore arbitrarily group the elements of K into pairs (i_p, j_p) for $p = 0, \ldots, r-1$, and define the matrix $T \in \mathbb{Z}_2^{m \times m}$ by

$$T_{i,j} := \sum_{p=0}^{r-1} (\delta_{i,i_p}\delta_{j,j_p} + \delta_{i,j_p}\delta_{j,i_p}),$$

so that

$$\begin{cases} T_{i_p,j_p} = T_{j_p,i_p} = 1 & \text{for } p \in \{0, \ldots, r-1\}, \\ T_{i,j} = 0 & \text{otherwise.} \end{cases}$$

Since the r pairs (i_p, j_p) partition the set K, the matrix T has at most one non-zero in each row and column.

Recalling that

$$(T^2)_{i,j} = \sum_{k=0}^{m-1} T_{i,k} T_{k,j},$$

we see that the general term $T_{i,k}T_{k,j}$ of this sum is non-zero only if either

$$\begin{cases} i = j = i_p, & \text{and } k = j_p, \text{ or} \\ i = j = j_p, & \text{and } k = i_p, \end{cases}$$

for some $p \in \{0, \ldots, r-1\}$, with all $2r$ of these cases being mutually exclusive. So T^2 is diagonal with $2r$ non-zeros at the elements of K.

But $C_{1,1}C_{0,0}$ is diagonal, and $(C_{1,1}C_{0,0})_{i,i} = c_{m+i}c_i$. Therefore

$$T^2 = C_{1,1}C_{0,0}. \tag{2}$$

Now, let $Z_{0,0} = Z_{1,1} = T$. Then $S_{0,0} = T + C_{0,0}$, $S_{1,1} = T + C_{1,1}$, and

$$\begin{aligned} S_{1,1}S_{0,0} &= (T + C_{1,1})(T + C_{0,0}) = T^2 + TC_{0,0} + C_{1,1}T + C_{1,1}C_{0,0} \\ &= TC_{0,0} + C_{1,1}T, \end{aligned}$$

where in the last step, we have used (2).

Now,

$$\begin{aligned} (TC_{0,0} + C_{1,1}T)_{i,j} &= \sum_{k=0}^{m-1} T_{i,k}(C_{0,0})_{k,j} + (C_{1,1})_{i,k}T_{k,j} \\ &= T_{i,j}(C_{0,0})_{j,j} + (C_{1,1})_{i,i}T_{i,j} \\ &= T_{i,j}\left(c_j + c_{m+i}\right). \end{aligned}$$

As above, $T_{i,j}$ is non-zero only when $(i,j) = (i_p, j_p)$ or $(i,j) = (j_p, i_p)$ for some $p \in \{0, \ldots, r-1\}$, but in all those cases $c_j = c_{m+j} = 1$.

Therefore

$$S_{1,1}S_{0,0} = TC_{0,0} + C_{1,1}T = 0.$$

Similarly, $S_{0,0}S_{1,1} = 0$, and therefore

$$\begin{aligned} A^2 &= \begin{bmatrix} I & S_{1,1} \\ S_{0,0} & I \end{bmatrix} \begin{bmatrix} I & S_{1,1} \\ S_{0,0} & I \end{bmatrix} \\ &= \begin{bmatrix} I + S_{1,1}S_{0,0} & S_{1,1} + S_{1,1} \\ S_{0,0} + S_{0,0} & I + S_{0,0}S_{1,1} \end{bmatrix} = \begin{bmatrix} I & 0 \\ 0 & I \end{bmatrix}. \end{aligned}$$

We have therefore shown that

$$A := \begin{bmatrix} I & T + C_{1,1} \\ T + C_{0,0} & I \end{bmatrix}, \quad S := \begin{bmatrix} T + C_{0,0} & 0 \\ 0 & T + C_{1,1} \end{bmatrix} \tag{3}$$

is a solution to $A^T L A = L + S$ with $A \in GL(2m, 2)$.

Finally, given c with $q(c) = 0$, the matrix A as defined by (3) is such that $q(Ax) = q(x) + \langle c, x \rangle$. □

Lemma 6. *For $k \in \{0, \ldots, m-1\}$ define $e^{(k)}$ by*

$$e_i^{(k)} := \delta_{i,k} + \delta_{i,m+k} \tag{4}$$

for $i \in \{0, \ldots, 2m-1\}$.

Let $h(x) := q(x) + \langle e^{(0)}, x\rangle$, where q is defined as per Lemma 3. Then for any c' such that $q(c') = 1$, there exists $B \in GL(2m, 2)$ such that

$$h(Bx) = q(x) + \langle c', x\rangle. \tag{5}$$

Proof. Let $K' = \{k \mid c'_k c'_{m+k} = 1\}$. Since $q(c') = 1$, $|K'|$ is odd. Choose any $\ell \in K'$, and let $c := c' + e^{(\ell)}$. Then $c_\ell = c_{m+\ell} = 0$ and $q(c) = 0$.

Now let $h^{(\ell)}(x) := q(x) + \langle e^{(\ell)}, x\rangle$. We calculate

$$\begin{aligned} h^{(\ell)}(Ax) &= q(Ax) + \langle e^{(\ell)}, Ax\rangle = q(x) + \langle c, x\rangle + \langle A^T e^{(\ell)}, x\rangle \\ &= q(x) + \langle c + A^T e^{(\ell)}, x\rangle \end{aligned}$$

for A given by the proof of Lemma 5.

If we let $K := \{k \mid c_k c_{m+k} = 1\}$, we see that $K = K' \setminus \{\ell\}$. Applying the other definitions and techniques used in the proof of Lemma 5, we see that since $c_\ell = c_{m+\ell} = 0$ and K does not contain ℓ, column ℓ of each of $S_{0,0} := T + C_{0,0}$ and $S_{1,1} := T + C_{1,1}$ is 0, and therefore columns ℓ and $m + \ell$ of

$$A^T + I := \begin{bmatrix} I & T + C_{0,0} \\ T + C_{1,1} & I \end{bmatrix}$$

are both 0. Therefore $A^T e^{(\ell)} = e^{(\ell)}$, and therefore

$$h^{(\ell)}(Ax) = q(x) + \langle c', x\rangle.$$

□

Lemma 7. *For distinct $k, \ell \in \{0, \ldots, m-1\}$ let $e^{(k)}, e^{(\ell)}$ be defined as per Lemma 6. Let $h(x) := q(x) + \langle e^{(k)}, x\rangle$, where q is defined as per Lemma 3. Then there exists $A \in GL(2m, 2)$ such that*

$$h(Ax) = q(x) + \langle e^{(\ell)}, x\rangle. \tag{6}$$

Proof. The matrix A is the permutation matrix for the the permutation $(k\ \ell)(m+k\ m+\ell)$ (defined using cycle notation.) □

Lemma 8. *Let q be defined as per Lemma 3. Then for all $c, c' \in Z_2^{2m}$ with $q(c) = q(c') = 1$, there exists $A \in GL(2m, 2)$ such that if $h(x) := q(x) + \langle c, x\rangle$, then*

$$h(Ax) = q(x) + \langle c', x\rangle.$$

Proof. This is a consequence of Lemmas 6 and 7. □

Proof of Theorem 4. It is well known that all quadratic bent functions are contained in one Extended Affine equivalence class. As a consequence of Theorem 2, without loss of generality, we need only examine the Extended Translation equivalence class of the quadratic function q as defined in Lemma 3.

As a result of Lemma 3, we actually need only examine functions of the form $f(x) = q(x) + \langle c, x\rangle$ for some $c \in \mathbb{Z}_2^{2m}$. Lemma 5 implies that all such functions for which $q(c) = 0$ are Cayley equivalent to q. Lemma 8 implies that any two such functions $q(x) + \langle c, x\rangle$ and $q(x) + \langle c', x\rangle$ with $q(c) = q(c') = 1$ are Cayley equivalent to each other.

The functions where $q(c) = 0$ are not Cayley equivalent to the functions where $q(c) = 1$ because Lemma 1 implies that

$$\mathrm{wc}\left(x \mapsto q(x) + \langle c, x\rangle\right) = \widetilde{q}(c) = q(c),$$

since q is self-dual. □

Acknowledgements. 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, and concluded while the author was a Visiting Fellow and a Casual Academic at the University of Newcastle, Australia.

References

[1] C. M. Adams. Constructing symmetric ciphers using the cast design procedure. In E. Kranakis and P. Van Oorschot, editors, *Selected Areas in Cryptography*, 71–104, Boston, MA, (1997). Springer US.

[2] A. Bernasconi and B. Codenotti. Spectral analysis of Boolean functions as a graph eigenvalue problem. *IEEE Transactions on Computers*, 48(3):345–351, (1999).

[3] A. Bernasconi, B. Codenotti, and J. M. VanderKam. A characterization of bent functions in terms of strongly regular graphs. *IEEE Transactions on Computers*, 50(9):984–985, (2001).

[4] R. C. Bose. Strongly regular graphs, partial geometries and partially balanced designs. *Pacific J. Math*, 13(2):389–419, (1963).

[5] I. Bouyukliev, V. Fack, W. Willems, and J. Winne. Projective two-weight codes with small parameters and their corresponding graphs. *Designs, Codes and Cryptography*, 41(1):59–78, (2006).

[6] 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).

[7] C. Carlet. Boolean functions for cryptography and error correcting codes. In *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, volume 2, 257–397. Cambridge University Press, (2010).

[8] C. Carlet, L. E. Danielsen, M. G. Parker, and P. Solé. Self-dual bent functions. *International Journal of Information and Coding Theory*, 1(4):384–399, (2010).

[9] P. Delsarte. Weights of linear codes and strongly regular normed spaces. *Discrete Mathematics*, 3(1-3):47–64, (1972).

[10] J. F. Dillon. *Elementary Hadamard Difference Sets*. PhD thesis, University of Maryland College Park, Ann Arbor, USA, (1974).

[11] J. F. Dillon and J. R. Schatz. Block designs with the symmetric difference property. In *Proceedings of the NSA Mathematical Sciences Meetings*, 159–164. US Govt. Printing Office Washington, DC, (1987).

[12] K. Ding and C. Ding. A class of two-weight and three-weight codes and their applications in secret sharing. *IEEE Transactions on Information Theory*, 61(11):5835–5842, (2015).

[13] T. Feulner, L. Sok, P. Solé, and A. Wassermann. Towards the classification of self-dual bent functions in eight variables. *Designs, Codes and Cryptography*, 68(1):395–406, (2013).

[14] T. Huang and K.-H. You. Strongly regular graphs associated with bent functions. In *7th International Symposium on Parallel Architectures, Algorithms and Networks, 2004. Proceedings.*, 380–383, May 2004.

[15] D. Joyner, O. Geil, C. Thomsen, C. Munuera, I. Márquez-Corbella, E. Martínez-Moro, M. Bras-Amorós, R. Jurrius, and R. Pellikaan. Sage:

A basic overview for coding theory and cryptography. In *Algebraic Geometry Modeling in Information Theory*, volume 8 of *Series on Coding Theory and Cryptology*, 1–45. World Scientific Publishing Company, (2013).

[16] T. Junttila and P. Kaski. Engineering an efficient canonical labeling tool for large and sparse graphs. In D. Applegate, G. S. Brodal, D. Panario, and R. Sedgewick, editors, *Proceedings of the Ninth Workshop on Algorithm Engineering and Experiments and the Fourth Workshop on Analytic Algorithms and Combinatorics*, 135–149, New Orleans, LA, (2007). Society for Industrial and Applied Mathematics.

[17] T. Junttila and P. Kaski. Conflict propagation and component recursion for canonical labeling. In *Theory and Practice of Algorithms in (Computer) Systems*, 151–162. Springer, (2011).

[18] W. M. Kantor. Symplectic groups, symmetric designs, and line ovals. *Journal of Algebra*, 33(1):43–58, (1975).

[19] W. M. Kantor. Exponential numbers of two-weight codes, difference sets and symmetric designs. *Discrete Mathematics*, 46(1):95–98, (1983).

[20] P. Langevin and X.-D. Hou. Counting partial spread functions in eight variables. *IEEE Transactions on Information Theory*, 57(4):2263–2269, (2011).

[21] P. Langevin and G. Leander. Counting all bent functions in dimension eight 99270589265934370305785861242880. *Designs, Codes and Cryptography*, 59(1-3):193–205, (2011).

[22] P. Langevin, G. Leander, and G. McGuire. Kasami bent functions are not equivalent to their duals. In G. Mullen, D. Panario, and I. Shparlinski, editors, *Finite Fields and Applications: Eighth International Conference on Finite Fields and Applications, July 9-13, 2007, Melbourne, Australia*, Contemporary mathematics, 187–198. American Mathematical Society, (2008).

[23] P. Leopardi. Twin bent functions, strongly regular Cayley graphs, and Hurwitz-Radon theory. Submitted October 2016 to Journal of Algebra Combinatorics Discrete Structures and Applications, Preprint: arXiv:1504.02827 [math.CO].

[24] P. Leopardi. Boolean-cayley-graphs, (2016). https://github.com/penguian/Boolean-Cayley-graphs GitHub repository. Last accessed 11 March 2017.

[25] P. Leopardi. Boolean-cayley-graphs, (2016). http://tinyurl.com/Boolean-Cayley-graphs SageMathCloud public folder. Last accessed 16 April 2017.

[26] B. D. McKay and A. Piperno. *Nauty and Traces users guide (Version 2.5)*. Computer Science Department, Australian National University, Canberra, Australia, (2013).

[27] B. D. McKay and A. Piperno. Practical graph isomorphism, ii. *Journal of Symbolic Computation*, 60:94–112, (2014).

[28] W. Meier and O. Staffelbach. Nonlinearity criteria for cryptographic functions. In J.-J. Quisquater and J. Vandewalle, editors, *Advances in Cryptology — EUROCRYPT '89: Workshop on the Theory and Application of Cryptographic Techniques*, volume 434 of *Lecture Notes in Computer Science*, 549–562, Berlin, Heidelberg, (1990). Springer Berlin Heidelberg.

[29] T. Neumann. *Bent functions*. PhD thesis, University of Kaiserslautern, (2006).

[30] O. S. Rothaus. On "bent" functions. *Journal of Combinatorial Theory, Series A*, 20(3):300–305, (1976).

[31] G. F. Royle. A normal non-cayley-invariant graph for the elementary abelian group of order 64. *Journal of the Australian Mathematical Society*, 85(03):347–351, (2008).

[32] SageMath, Inc. *SageMathCloud Online Computational Mathematics*, (2016). https://cloud.sagemath.com/.

[33] J. J. Seidel. Strongly regular graphs. In *Surveys in combinatorics (Proc. Seventh British Combinatorial Conf., Cambridge, 1979)*, volume 38 of *London Mathematical Society Lecture Note Series*, 157–180, Cambridge-New York, (1979). Cambridge Univ. Press.

[34] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 7.5)*, (2017). http://www.sagemath.org.

[35] 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).

[36] N. Tokareva. *Bent functions: results and applications to cryptography.* Academic Press, (2015).

[37] V. D. Tonchev. The uniformly packed binary [27, 21, 3] and [35, 29, 3] codes. *Discrete Mathematics*, 149(1-3):283–288, (1996).

[38] V. D. Tonchev. Codes. In C. Colbourne and J. Dinitz, editors, *Handbook of combinatorial designs*, chapter VII.1, 677–701. CRC press, second edition, (2007).