INCOMPLETE DRAFT: Classifying bent functions by their Cayley graphs

Paul Leopardi [*]

INCOMPLETE DRAFT: 7 May 2017

Abstract

In 1999 Bernasconi and Codenotti noted that the Cayley graph of a bent function is strongly regular. This paper describes the concept of extended Cayley equivalence of bent functions, discusses some connections between bent functions, designs, and codes, and explores the relationship between extended Cayley equivalence and extended affine equivalence. SageMath scripts and SageMathCloud worksheets are used to compute and display some of these relationships, for bent functions up to dimension 8.

1 Introduction

Binary bent functions are important combinatorial objects. Besides the well-known application of bent functions and their generalizations to cryptography [1] [41, 4.1-4.6], bent functions have well-studied connections to Hadamard difference sets [13], symmetric designs with the symmetric difference property [14, 22], projective two-weight codes [15] 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

[*] University of Melbourne; Australian Government – Bureau of Meteorology mailto:paul.leopardi@gmail.com

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 [23], 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.

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 [27].

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 computational study is conducted into bent functions of dimension at most 8, using SageMath [39] and SageMathCloud [36].

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 computational 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* $f : \mathbb{Z}_2^{2m} \to \mathbb{Z}_2$ *is*

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

Definition 2. *A Boolean function* $f : \mathbb{Z}_2^{2m} \to \mathbb{Z}_2$ *is* bent *if and only if its Walsh Hadamard transform has constant absolute value* 2^m *[13, p. 74] [34, 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 [32, 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* $f : \mathbb{Z}_2^{2m} \to \mathbb{Z}_2$*, the function* $\widetilde{f}$*, defined by*

$$(-1)^{\widetilde{f}(x)} := 2^{-m} W_f(x)$$

is called the dual *of* f *[40].*

Remark: The function $\widetilde{f}$ *is also a bent function on* $\mathbb{Z}_2^{2m}$ *[34, 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 [13, 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 two block designs of a bent function

The first block design of a bent function f on $\mathbb{Z}_2^{2m}$ is obtained by interpreting the adjacency matrix of $\mathrm{Cay}\,(f)$ as the incidence matrix of a block design. In this case we do not need $f(0) = 0$ [14, p. 160].

The second block design of a bent function f involves the *symmetric difference property*, which was first investigated by Kantor [22, Section 5].

Definition 6. *[22, p. 49].*

A symmetric block design $\mathcal{D}$ has the symmetric difference property (SDP) if, for any three blocks, B, C, D of $\mathcal{D}$, the symmetric difference $B \bigtriangleup C \bigtriangleup D$ is either a block or the complement of a block.

This second block design is defined as follows.

Definition 7. *For a bent function f on $\mathbb{Z}_2^{2m}$, define the matrix $M_D(f) \in \mathbb{Z}_2^{2^{2m} \times 2^{2m}}$ where*

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

and use it as the incidence matrix of a symmetric block design, which we call it the SDP design *of f.*

Kantor describes the special case where f is quadratic [22, Section 5], and Dillon and Schatz [14] describe the general case.

Definition 7 is different from but equivalent to the one given by Dillon and Schatz [14, p. 160]:

Lemma 1. *[33, 3.29]*

For any bent function f on $\mathbb{Z}_2^{2m}$, the rows of the incidence matrix $M_D(f)$ are given by the words of minimum weight in the code spanned by the support of f and the Reed-Muller code $RM(1, 2m)$.

The proof of Lemma 1 is deferred to Section 3.

The following properties of SDP designs of bent functions are well known.

Proposition 1. *[14, p. 160] [33, Theorem 3.29]*

For any bent function f on $\mathbb{Z}_2^{2m}$, the SDP design of f has the symmetric difference property.

Proposition 2. *[14, p. 161] [23]*

For bent functions f, g on $\mathbb{Z}_2^{2m}$, the two SDP designs $D(f)$ and $D(g)$ are isomorphic as symmetric block designs if and only if f and g are affine equivalent.

2.4 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 8. *For a Boolean function $f : \mathbb{Z}_2^{2m} \rightarrow \mathbb{Z}_2$, with $f(0) = 0$ we consider the simple undirected* Cayley graph $\operatorname{Cay}(f)$ *[2, 3.1] where the vertex set $V(\operatorname{Cay}(f)) = \mathbb{Z}_2^{2m}$ and for $i, j \in \mathbb{Z}_2^{2m}$, the edge (i, j) is in the edge set $E(\operatorname{Cay}(f))$ 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 8 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 3 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 9. *A simple graph Γ of order v is* strongly regular *[4, 7, 37] 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 3. *The Cayley graph* $\operatorname{Cay}(f)$ *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 $\operatorname{Cay}(f)$ *are [13, Theorem 6.2.10] [18, Theorem 3.2]*

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

2.5 Bent functions, linear codes and strongly regular graphs

Another way to obtain a strongly regular graph from a bent function is via a projective two-weight code.

Projective two-weight binary codes

Definition 10. *[5] [42]*

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.

A projective two-weight binary code with parameters $[n, k, d]$ is thus a two-weight binary with these parameters which is also projective as an $[n, k]$ linear code.

From bent function to linear code.

Definition 11. *[15, 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

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

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

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

Proposition 4. *[15, 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:

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

From linear code to strongly regular graph.

Definition 12. *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

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

Since $C(f)$ is a projective two-weight binary code, $R(f)$ is a strongly regular graph [12, Theorem 2].

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 13. *For bent functions $f, g : \mathbb{Z}_2^{2m} \to \mathbb{Z}_2$, f is extended affine equivalent [41, 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 14. *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 15. *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 16. *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 $\operatorname{Cay}(f) \equiv \operatorname{Cay}(g)$ 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

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

Extended Cayley equivalence.

Definition 17. *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 2. *For a bent function $f : \mathbb{Z}_2^{2m} \to \mathbb{Z}_2$, and $x \in \mathbb{Z}_2^{2m}$,*

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

The proof of Lemma 2 relies on the following lemma about weight classes.

Lemma 3. *For a bent function $f : \mathbb{Z}_2^{2m} \to \mathbb{Z}_2$,*

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

so that

$$\operatorname{wt}(f) = 2^m \operatorname{wc}(f) + 2^{2m-1} - 2^{m-1}.$$

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

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

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

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

□

Proof of Lemma 2. Let $h(y) := y \mapsto f(y) + \langle x, y \rangle$. Then

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

where we have used Lemma 3. □

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 5. *[13, Remark 6.2.7]*
For a bent function $f : \mathbb{Z}_2^{2m} \rightarrow \mathbb{Z}_2$, 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 $\widetilde{g} \equiv g$.

Remark: Functions of the form

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

are self dual bent functions, $f = \widetilde{f}$ [13, Remark 6.3.2]. There are many other self dual bent functions [10, 16].

Secondly, the following proposition displays a relationship between the extended translation class of a bent function f, and that of its dual $\widetilde{f}$.

Proposition 6. *[13, Remark 6.2.7] [9, Proposition 8.7]*
For a bent function f on $\mathbb{Z}_2^{2m}$, 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 an implication for the relationship between the set of bent functions within an extended translation (ET) equivalence class, and the set of their duals. Recall that a bent function is not necessarily extended affine (EA) equivalent to its dual [26]. The following "all or nothing" property holds within an extended translation equivalence class of bent functions.

Corollary 4. *For bent functions f, g on $\mathbb{Z}_2^{2m}$, if f is EA equivalent to $\widetilde{f}$ and g is ET equivalent to f, then $\widetilde{g}$ is EA equivalent to g. Thus, by Theorem 2, the set of isomorphism classes of Cayley graphs of the duals of the bent functions in the ET class of f equals the set of isomorphism classes of Cayley graphs of the bent functions themselves.*

Conversely, for a bent function f on $\mathbb{Z}_2^{2m}$, if there is any bent function g that is ET equivalent to f, such that $\widetilde{g}$ is not EA equivalent to g, then no bent function in the ET class is EA equivalent to its dual, including f itself.

Weight classes and the SDP design matrix. With Lemma 2 in hand, it is easy to prove Lemma 1 on the equivalence of the definitions of the SDP design of a bent function f on Z_2^{2m}.

Proof of Lemma 1. Firstly, it is well known (e.g. [38, 10.5.2]) that the Reed-Muller code $RM(1, 2m)$ consists of the words spanned by the affine functions on Z_2^{2m}, that is, the incidence matrix $M_{RM(1,2m)}$ is defined by

$$M_{RM(1,2m)_{c,x}} := \langle c, x \rangle + d,$$

where $d \in \mathbb{Z}_2$.

Thus the incidence matrix of the code spanned by the support of f and $RM(1, 2m)$ is defined by

$$M_{f,RM(1,2m)_{c,x}} := f(x) + \langle c, x \rangle + d.$$

Finally, from Lemma 2 we know that

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

so that

$$\mathrm{wc}\left(x \mapsto f(x) + \langle c, x \rangle + \widetilde{f}(c)\right) = 0.$$

□

The following characterization of the SDP design of a bent function f also relies on Lemma 2 for its proof.

Theorem 3. *For a bent function $f : \mathbb{Z}_2^{2m} \to \mathbb{Z}_2$, define the weight class matrix of f by*

$$M_{wc}(f)_{c,b} := \mathrm{wc}\,(x \mapsto f(x + b) + \langle c, x \rangle + f(b))$$

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

Then the weight class matrix of f equals the incidence matrix of the SDP design of f. Specifically,

$$\begin{aligned} M_{wc}(f)_{c,b} &= f(b) + \langle c, b \rangle + \widetilde{f}(c) \\ &= M_D(f)_{c,b}, \end{aligned}$$

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

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

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

as a consequence of Lemma 2. □

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 given in Appendix A.

3.3 Bent functions, linear codes and strongly regular graphs

The graph $R(f)$ is the Cayley graph of the extended dual. Recall the strongly regular graph $R(f)$ of bent function f as defined by Definition 12.

Theorem 5. *For bent $f : \mathbb{Z}_2^{2m} \to \mathbb{Z}_2$, 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

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

But

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

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

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

and therefore

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

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

If $\operatorname{wc}(f) = 0$ then $\operatorname{wt}(f) = 2^{2m-1} - 2^{m-1}$. 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

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

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

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

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

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

Also, as a consequence of Lemma 2, $\operatorname{wc}(f) = \widetilde{f}(0)$, so if $g(y) := \widetilde{f}(y) + \operatorname{wc}(f)$ then $g(0) = 0$ and therefore the Cayley graph of g is well defined. □

4 Computational results for low dimensions

This section lists some properties of bent functions and their extended translation classes and extended Cayley classes that have been computed for 2, 4, 6 and 8 dimensions. The computations were made using Sage [39] and SageMathCloud [36]. Sage and Python code for these computations are available on GitHub [28] and SageMathCloud [29]. Some SageMathCloud worksheets also illustrate these and related computations [29]. The Sage and Python code is described in more detail in Section 5.

In the tables below, each bent function is defined by its algebraic normal form, and each Cayley class is described by its number within the extended translation class of the bent function (from 0 in the order in which Sage identified non-isomorphic graphs), followed by three properties of the Cayley graph: its parameters as a strongly regular graph, the 2-rank of its adjacency matrix [8], and its clique polynomial [17].

4.1 Bent functions in 2 dimensions

The bent functions on $\mathbb{Z}_2^2$ consist of one extended affine class, containing the extended translation class: $[f_{2,1}]$ where $f_{2,1}(x) := x_0 x_1$ is self dual. The extended translation class contains two extended Cayley classes as per Table 1. Note that the Cayley graph for class 1 is K_4, which is not considered to be strongly regular, by convention.

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

Table 1: $[f_{2,1}]$ extended Cayley classes.

As expected from Theorem 4, the two extended Cayley classes correspond to the two weight classes, as shown in Figures 1 and 2.

4.2 Bent functions in 4 dimensions

The bent functions on $\mathbb{Z}_2^4$ consist of one extended affine class, containing the extended translation class $[f_{4,1}]$ where $f_{4,1}(x) := x_0 x_1 + x_2 x_3$ is self dual. The extended translation class contains two extended Cayley classes as per Table 2.

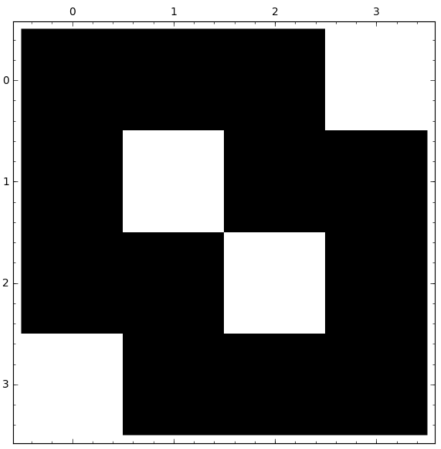

Figure 1: $[f_{2,1}]$: weight classes.

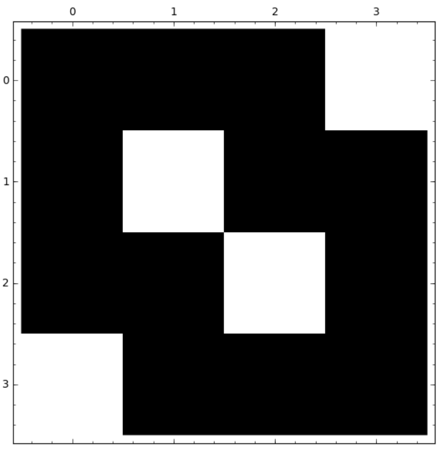

Figure 2: $[f_{2,1}]$: extended Cayley classes.

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	$16t^5 + 120t^4 + 160t^3 + 80t^2 + 16t + 1$

Table 2: $[f_{4,1}]$ extended Cayley classes.

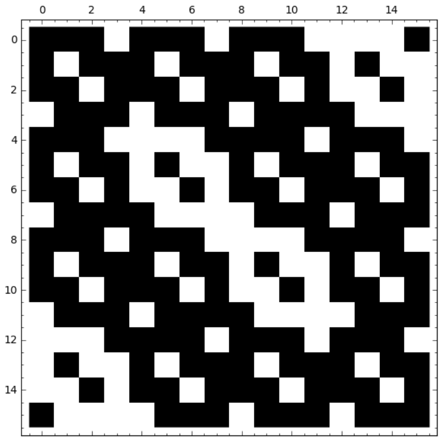

Figure 3: $[f_{4,1}]$: weight classes.

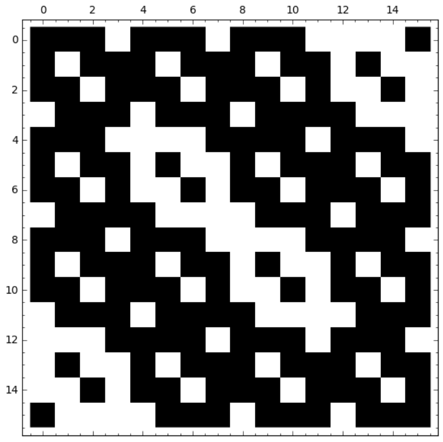

Figure 4: $[f_{4,1}]$: extended Cayley classes.

The two extended Cayley classes correspond to the two weight classes, as shown in Figures 3 and 4.

4.3 Bent functions in 6 dimensions

Extended affine classes. The bent functions on $\mathbb{Z}_2^6$ consist of four extended affine classes, containing the extended translation classes as listed in Table 3 [34, p. 303] [41, Section 7.2].

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

Table 3: 6 dimensions: extended translation 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 [42]. These tables are repeated as Tables 1.155 and 1.156 in Chapter VII.1 of the Handbook of Combinatorial Designs, Second Edition [43], with a different numbering. For each of the codes listed in these two tables, the characteristics of the corresponding strongly regular graph is also listed.

In the classification given below, the Cayley graph of each Cayley class is matched by isomorphism with a strongly regular graph corresponding to one or more of Tonchev's projective two-weight codes, or the complement of such a graph. Tonchev's strongly regular graphs were checked using the function `strongly_regular_from_two_weight_code`, which uses the smaller of the two weights to create the graph [39].

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

The extended translation class contains two extended Cayley classes as per Table 4.

The Cayley graphs for classes 0 and 1 are isomorphic to those those obtained from the Tonchev's projective two-weight codes [43] as per Table 5.

The two extended Cayley classes correspond to the two weight classes, as shown in Figures 5 and 6.

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	$2304t^6 + 13824t^5 + 19200t^4 + 7680t^3 + 1152t^2 + 64t + 1$

Table 4: $[f_{6,1}]$ extended Cayley classes.

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

Table 5: $[f_{6,1}]$ Two-weight projective codes.

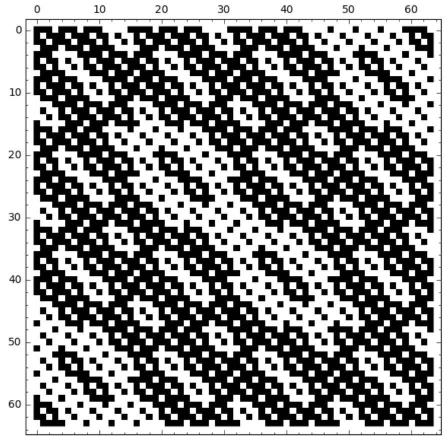

Figure 5: $[f_{6,1}]$: weight classes.

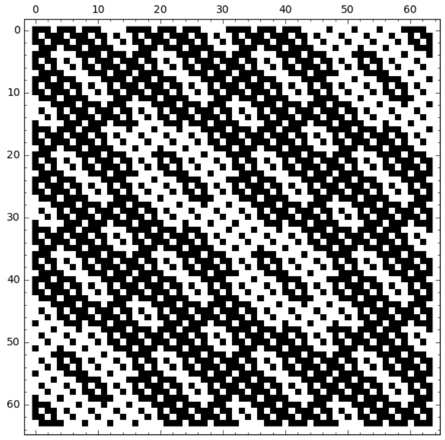

Figure 6: $[f_{6,1}]$: extended Cayley classes.

Remark: The sequence of Figures 1, 3, and 5 displays a fractal-like self-similar quality.

ET class $[f_{6,2}]$**.** This is the extended translation class of the bent function $f_{6,2}(x) := x_0x_1x_2 + x_0x_3 + x_1x_4 + x_2x_5$.

The extended translation class contains three extended Cayley classes as per Table 6.

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	$192t^8 + 1536t^7 + 8960t^6 + 19968t^5 + 20224t^4 + 7680t^3 + 1152t^2 + 64t + 1$

Table 6: $[f_{6,2}]$ extended Cayley classes.

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 [35]. This reflects the fact that $f_{6,0} \equiv f_{6,1}$, even though these two functions are not extended affine equivalent.

The Cayley graphs for classes 0 to 2 are isomorphic to those those obtained from the Tonchev's projective two-weight codes [43] as per Table 7.

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

Table 7: $[f_{6,2}]$ Two-weight projective codes.

The three extended Cayley classes are distributed between the two weight classes, as shown in Figures 7 and 8.

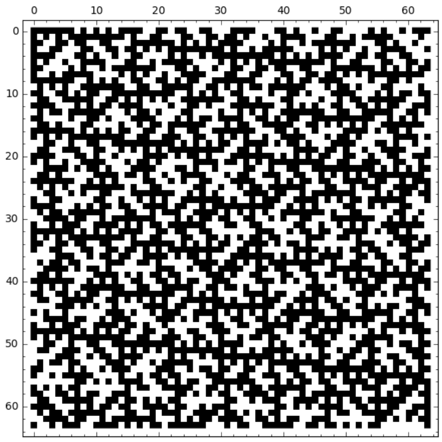

Figure 7: $[f_{6,2}]$: weight classes.

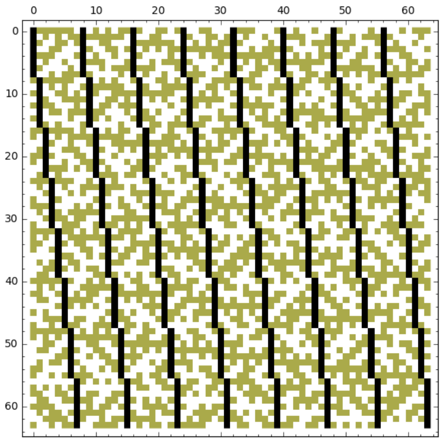

Figure 8: $[f_{6,2}]$: extended Cayley classes.

ET class $[f_{6,3}]$**.** This is the extended translation class of the bent function

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

The extended translation class contains four extended Cayley classes as per Table 8.

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	$160t^8 + 1664t^7 + 9792t^6 + 21504t^5 + 20480t^4 + 7680t^3 + 1152t^2 + 64t + 1$

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

The Cayley graphs for classes 0 to 3 are isomorphic to those those obtained from the Tonchev's projective two-weight codes [43] as per Table 9.

The four extended Cayley classes are distributed between the two weight classes, as shown in Figures 9 and 10.

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

Table 9: $[f_{6,3}]$ Two-weight projective codes.

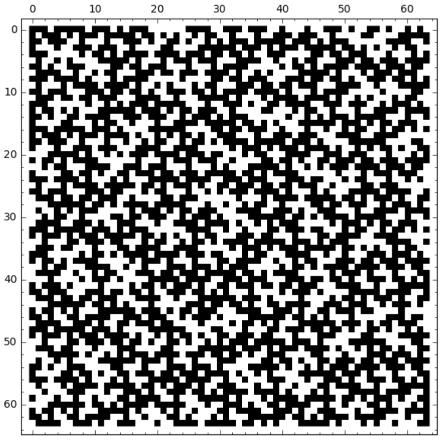

Figure 9: $[f_{6,3}]$: weight classes.

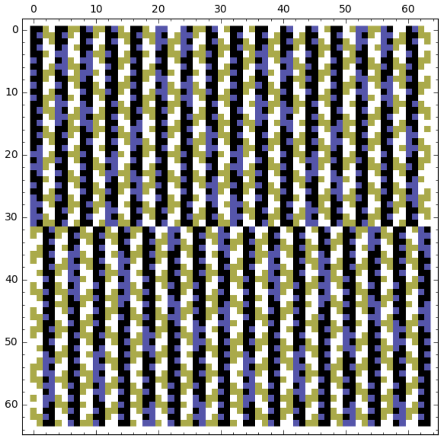

Figure 10: $[f_{6,3}]$: extended Cayley classes.

ET class $[f_{6,4}]$. This is the extended translation class of the bent function

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

The extended translation class contains three extended Cayley classes as per Table 10.

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	$176t^8 + 1408t^7 + 9664t^6 + 22272t^5 + 20608t^4 + 7680t^3 + 1152t^2 + 64t + 1$

Table 10: $[f_{6,4}]$ extended Cayley classes.

The Cayley graphs for classes 0 to 2 are isomorphic to those those obtained from the Tonchev's projective two-weight codes [43] as per Table 7.

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

Table 11: $[f_{6,4}]$ Two-weight projective codes.

The three extended Cayley classes are distributed between the two weight classes, as shown in Figures 11 and 12.

4.4 Bent functions in 8 dimensions

There are 99270589265934370305785861242880 $\approx 2^{106}$ bent functions in 8 dimensions, according to Langevin and Leander [25]. The number of extended affine classes has not yet been published, let alone a list of representative bent functions. The lists of extended affine classes of bent functions that

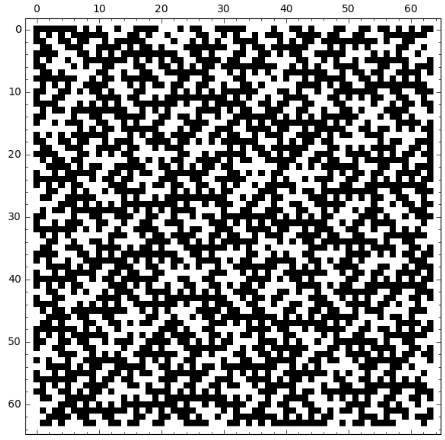

Figure 11: $[f_{6,4}]$: weight classes.

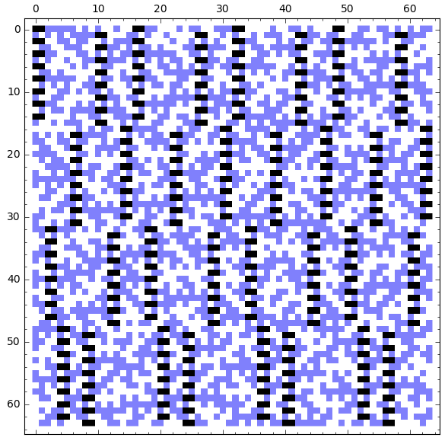

Figure 12: $[f_{6,4}]$: extended Cayley classes.

have so far been published include those for the bent functions up to degree 3 [6, Section 5.5.2] [41, Section 7.3], the partial spread bent functions [24] [TBD], and the bent functions used in the S-boxes of the CAST-128 encryption algorithm [1] [TBD].

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

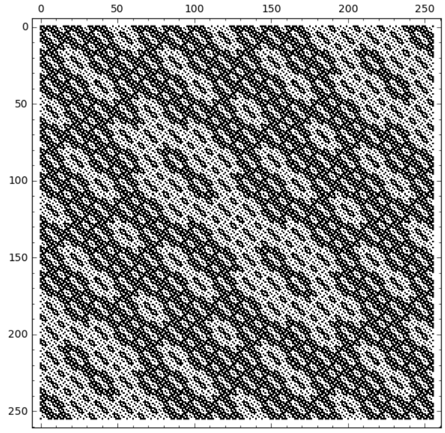

Figure 13: $[f_{8,1}]$: weight classes.

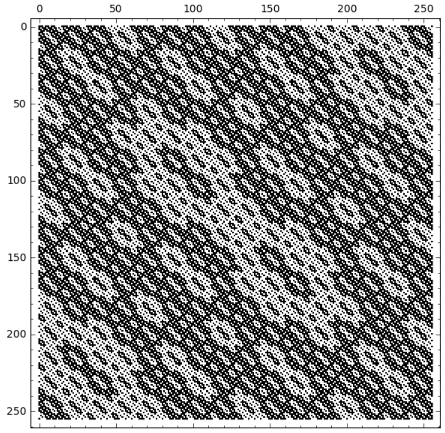

Figure 14: $[f_{8,1}]$: extended Cayley classes.

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

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

Table 12: 8 dimensions: extended translation classes.

Class	Parameters	2-rank	Clique polynomial
0	$(256, 120, 56, 56)$	10	$245760t^9 + 3317760t^8 + 8847360t^7 + 10321920t^6 + 6193152t^5 + 2007040t^4 + 286720t^3 + 15360t^2 + 256t + 1$
1	$(256, 136, 72, 72)$	10	$417792t^8 + 3342336t^7 + 11698176t^6 + 11698176t^5 + 3760128t^4 + 417792t^3 + 17408t^2 + 256t + 1$

Table 13: $[f_{8,1}]$ extended Cayley classes.

ET class $[f_{8,2}]$**.** This is the extended translation class of the bent function

$$f_{8,2} = \ x_0x_1x_2 + x_0x_3 + x_1x_4 + x_2x_5 + x_6x_7.$$

The extended translation class contains four extended Cayley classes as per Table 14.

Class	Parameters	2-rank	Clique polynomial
0	$(256, 120, 56, 56)$	10	$245760t^9 + 3317760t^8 + 8847360t^7 + 10321920t^6 + 6193152t^5 + 2007040t^4 + 286720t^3 + 15360t^2 + 256t + 1$
1	$(256, 120, 56, 56)$	10	$49152t^9 + 663552t^8 + 2555904t^7 + 5079040t^6 + 4620288t^5 + 1875968t^4 + 286720t^3 + 15360t^2 + 256t + 1$
2	$(256, 136, 72, 72)$	10	$327680t^9 + 4055040t^8 + 13828096t^7 + 22183936t^6 + 14319616t^5 + 3891200t^4 + 417792t^3 + 17408t^2 + 256t + 1$
3	$(256, 136, 72, 72)$	10	$417792t^8 + 3342336t^7 + 11698176t^6 + 11698176t^5 + 3760128t^4 + 417792t^3 + 17408t^2 + 256t + 1$

Table 14: $[f_{8,2}]$ extended Cayley classes.

The four extended Cayley classes are distributed between the two weight classes, as shown in Figures 15 and 16.

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

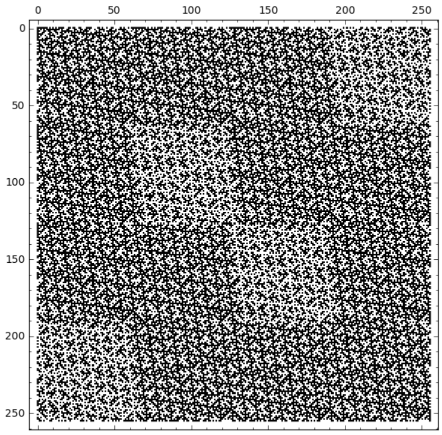

Figure 15: $[f_{8,2}]$: weight classes.

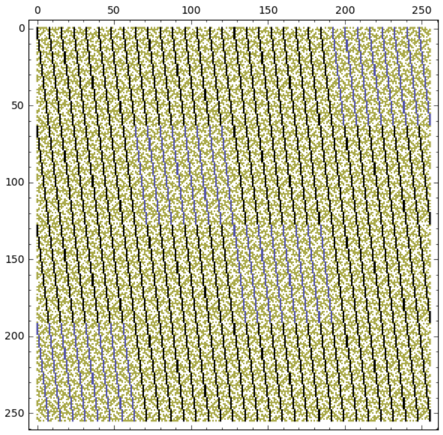

Figure 16: $[f_{8,2}]$: extended Cayley classes.

Class	Parameters	2-rank	Clique polynomial
0	$(256, 120, 56, 56)$	12	$81920t^9 + 1368064t^8 + 4653056t^7 + 7176192t^6 + 5406720t^5 + 1941504t^4 + 286720t^3 + 15360t^2 + 256t + 1$
1	$(256, 136, 72, 72)$	12	$294912t^9 + 6299648t^8 + 21692416t^7 + 27951104t^6 + 15630336t^5 + 3956736t^4 + 417792t^3 + 17408t^2 + 256t + 1$
2	$(256, 120, 56, 56)$	12	$16384t^9 + 221184t^8 + 1277952t^7 + 3768320t^6 + 4227072t^5 + 1843200t^4 + 286720t^3 + 15360t^2 + 256t + 1$
3	$(256, 136, 72, 72)$	12	$262144t^9 + 4399104t^8 + 16220160t^7 + 24281088t^6 + 14974976t^5 + 3923968t^4 + 417792t^3 + 17408t^2 + 256t + 1$
4	$(256, 120, 56, 56)$	12	$49152t^9 + 729088t^8 + 2686976t^7 + 5079040t^6 + 4620288t^5 + 1875968t^4 + 286720t^3 + 15360t^2 + 256t + 1$
5	$(256, 136, 72, 72)$	12	$196608t^9 + 3399680t^8 + 13172736t^7 + 21659648t^6 + 14319616t^5 + 3891200t^4 + 417792t^3 + 17408t^2 + 256t + 1$

Table 15: $[f_{8,3}]$ extended Cayley classes.

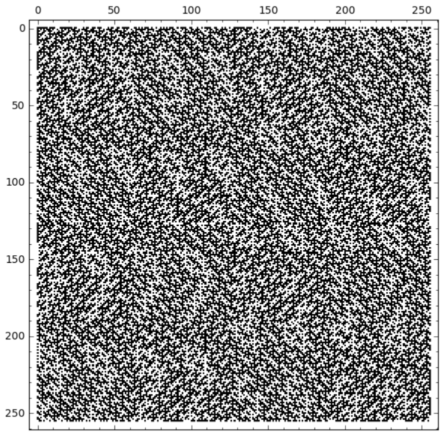

Figure 17: $[f_{8,3}]$: weight classes.

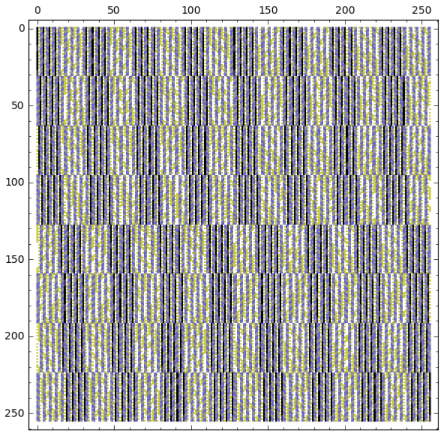

Figure 18: $[f_{8,3}]$: extended Cayley classes.

Class	Parameters	2-rank	Clique polynomial
0	$(256, 120, 56, 56)$	14	$69632t^9 + 1099776t^8 + 3784704t^7 + 6160384t^6 + 5013504t^5 + 1908736t^4 + 286720t^3 + 15360t^2 + 256t + 1$
1	$(256, 136, 72, 72)$	14	$225280t^9 + 4319232t^8 + 16203776t^7 + 24313856t^6 + 14974976t^5 + 3923968t^4 + 417792t^3 + 17408t^2 + 256t + 1$
2	$(256, 120, 56, 56)$	14	$1536t^{10} + 15360t^9 + 209920t^8 + 1280000t^7 + 3751936t^6 + 4227072t^5 + 1843200t^4 + 286720t^3 + 15360t^2 + 256t + 1$
3	$(256, 136, 72, 72)$	14	$7680t^{10} + 230400t^9 + 4228096t^8 + 16058368t^7 + 24166400t^6 + 14974976t^5 + 3923968t^4 + 417792t^3 + 17408t^2 + 256t + 1$
4	$(256, 136, 72, 72)$	14	$110592t^9 + 2344960t^8 + 10305536t^7 + 18939904t^6 + 13664256t^5 + 3858432t^4 + 417792t^3 + 17408t^2 + 256t + 1$
5	$(256, 120, 56, 56)$	14	$20480t^9 + 337920t^8 + 1556480t^7 + 3932160t^6 + 4227072t^5 + 1843200t^4 + 286720t^3 + 15360t^2 + 256t + 1$

Table 16: $[f_{8,4}]$ extended Cayley classes.

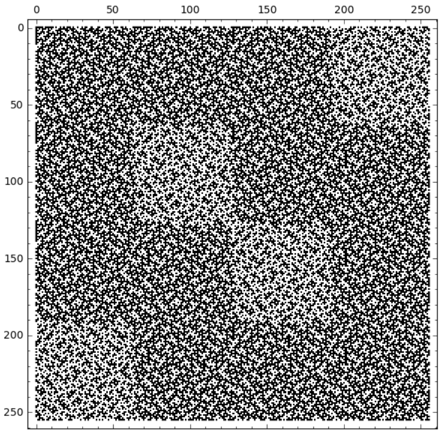

Figure 19: $[f_{8,4}]$: weight classes.

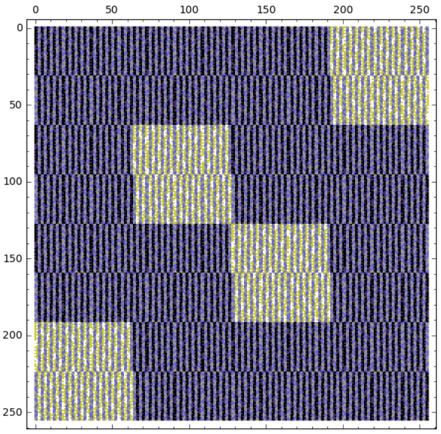

Figure 20: $[f_{8,4}]$: extended Cayley classes.

Class	Parameters	2-rank	Clique polynomial
0	$(256, 120, 56, 56)$	14	$32768t^9 + 731136t^8 + 3096576t^7 + 5767168t^6 + 5013504t^5 + 1908736t^4 + 286720t^3 + 15360t^2 + 256t + 1$
1	$(256, 120, 56, 56)$	14	$28672t^9 + 534528t^8 + 2211840t^7 + 4718592t^6 + 4620288t^5 + 1875968t^4 + 286720t^3 + 15360t^2 + 256t + 1$
2	$(256, 136, 72, 72)$	14	$159744t^9 + 4753408t^8 + 19021824t^7 + 26804224t^6 + 15630336t^5 + 3956736t^4 + 417792t^3 + 17408t^2 + 256t + 1$
3	$(256, 120, 56, 56)$	14	$24576t^9 + 526336t^8 + 2342912t^7 + 4849664t^6 + 4620288t^5 + 1875968t^4 + 286720t^3 + 15360t^2 + 256t + 1$
4	$(256, 136, 72, 72)$	14	$90112t^9 + 2795520t^8 + 12402688t^7 + 21168128t^6 + 14319616t^5 + 3891200t^4 + 417792t^3 + 17408t^2 + 256t + 1$

Table 17: $[f_{8,5}]$ extended Cayley classes (part 1).

Class	Parameters	2-rank	Clique polynomial
5	$(256, 120, 56, 56)$	14	$16384t^9 + 284672t^8 + 1392640t^7 + 3735552t^6 + 4227072t^5 + 1843200t^4 + 286720t^3 + 15360t^2 + 256t + 1$
6	$(256, 136, 72, 72)$	14	$131072t^9 + 3577856t^8 + 15319040t^7 + 23855104t^6 + 14974976t^5 + 3923968t^4 + 417792t^3 + 17408t^2 + 256t + 1$
7	$(256, 120, 56, 56)$	14	$1536t^{10} + 19456t^9 + 279552t^8 + 1394688t^7 + 3751936t^6 + 4227072t^5 + 1843200t^4 + 286720t^3 + 15360t^2 + 256t + 1$
8	$(256, 136, 72, 72)$	14	$5632t^{10} + 148480t^9 + 3621888t^8 + 15206400t^7 + 23773184t^6 + 14974976t^5 + 3923968t^4 + 417792t^3 + 17408t^2 + 256t + 1$

Table 18: $[f_{8,5}]$ extended Cayley classes (part 2).

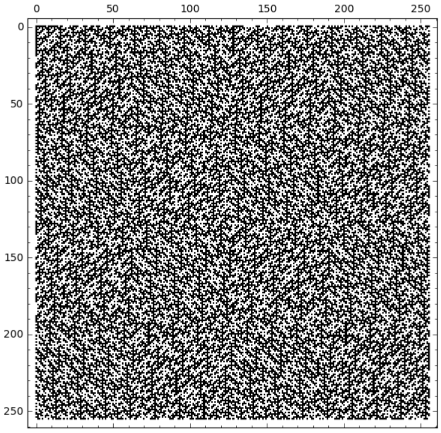

Figure 21: $[f_{8,5}]$: weight classes.

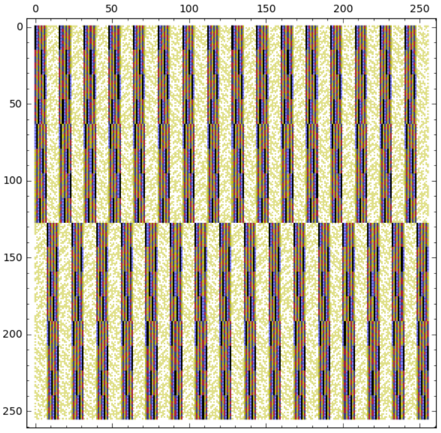

Figure 22: $[f_{8,5}]$: extended Cayley classes.

Class	Parameters	2-rank	Clique polynomial
0	$(256, 120, 56, 56)$	14	$32768t^9 + 731136t^8 + 3096576t^7 + 5767168t^6 + 5013504t^5 + 1908736t^4 + 286720t^3 + 15360t^2 + 256t + 1$
1	$(256, 120, 56, 56)$	14	$28672t^9 + 534528t^8 + 2211840t^7 + 4718592t^6 + 4620288t^5 + 1875968t^4 + 286720t^3 + 15360t^2 + 256t + 1$
2	$(256, 136, 72, 72)$	14	$159744t^9 + 4753408t^8 + 19021824t^7 + 26804224t^6 + 15630336t^5 + 3956736t^4 + 417792t^3 + 17408t^2 + 256t + 1$
3	$(256, 120, 56, 56)$	14	$1536t^{10} + 19456t^9 + 279552t^8 + 1394688t^7 + 3751936t^6 + 4227072t^5 + 1843200t^4 + 286720t^3 + 15360t^2 + 256t + 1$
4	$(256, 136, 72, 72)$	14	$5632t^{10} + 148480t^9 + 3621888t^8 + 15206400t^7 + 23773184t^6 + 14974976t^5 + 3923968t^4 + 417792t^3 + 17408t^2 + 256t + 1$

Table 19: $[f_{8,6}]$ extended Cayley classes (part 1).

Class	Parameters	2-rank	Clique polynomial
5	$(256, 120, 56, 56)$	14	$24576t^9 + 526336t^8 + 2342912t^7 + 4849664t^6 + 4620288t^5 + 1875968t^4 + 286720t^3 + 15360t^2 + 256t + 1$
6	$(256, 120, 56, 56)$	14	$16384t^9 + 284672t^8 + 1392640t^7 + 3735552t^6 + 4227072t^5 + 1843200t^4 + 286720t^3 + 15360t^2 + 256t + 1$
7	$(256, 136, 72, 72)$	14	$131072t^9 + 3577856t^8 + 15319040t^7 + 23855104t^6 + 14974976t^5 + 3923968t^4 + 417792t^3 + 17408t^2 + 256t + 1$
8	$(256, 136, 72, 72)$	14	$90112t^9 + 2795520t^8 + 12402688t^7 + 21168128t^6 + 14319616t^5 + 3891200t^4 + 417792t^3 + 17408t^2 + 256t + 1$

Table 20: $[f_{8,6}]$ extended Cayley classes (part 2).

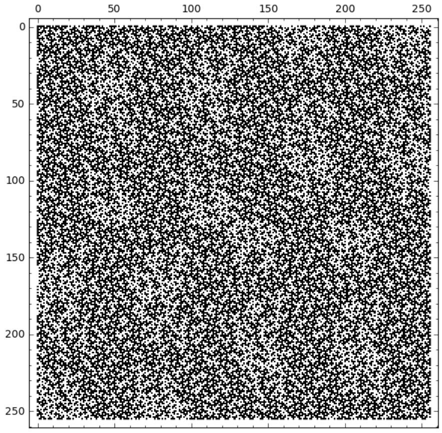

Figure 23: $[f_{8,6}]$: weight classes.

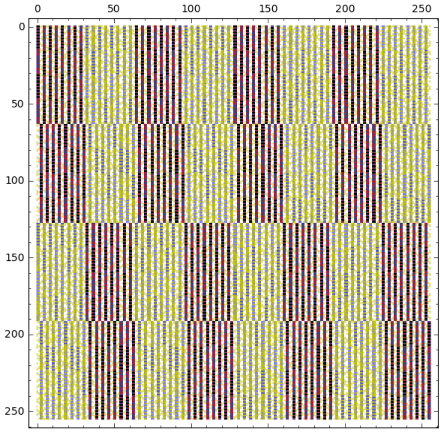

Figure 24: $[f_{8,6}]$: extended Cayley classes.

Class	Parameters	2-rank	Clique polynomial
0	$(256, 120, 56, 56)$	16	$29696t^9 + 655360t^8 + 2789376t^7 + 5332992t^6 + 4816896t^5 + 1892352t^4 + 286720t^3 + 15360t^2 + 256t + 1$
1	$(256, 120, 56, 56)$	16	$20480t^9 + 409600t^8 + 1837056t^7 + 4235264t^6 + 4423680t^5 + 1859584t^4 + 286720t^3 + 15360t^2 + 256t + 1$
2	$(256, 136, 72, 72)$	16	$143360t^9 + 3981312t^8 + 16697344t^7 + 25108480t^6 + 15302656t^5 + 3940352t^4 + 417792t^3 + 17408t^2 + 256t + 1$
3	$(256, 136, 72, 72)$	16	$64512t^9 + 2316288t^8 + 10932224t^7 + 19783680t^6 + 13991936t^5 + 3874816t^4 + 417792t^3 + 17408t^2 + 256t + 1$
4	$(256, 136, 72, 72)$	16	$92160t^9 + 2979840t^8 + 13608960t^7 + 22388736t^6 + 14647296t^5 + 3907584t^4 + 417792t^3 + 17408t^2 + 256t + 1$
5	$(256, 120, 56, 56)$	16	$6144t^9 + 124928t^8 + 944128t^7 + 3219456t^6 + 4030464t^5 + 1826816t^4 + 286720t^3 + 15360t^2 + 256t + 1$

Table 21: $[f_{8,7}]$ extended Cayley classes.

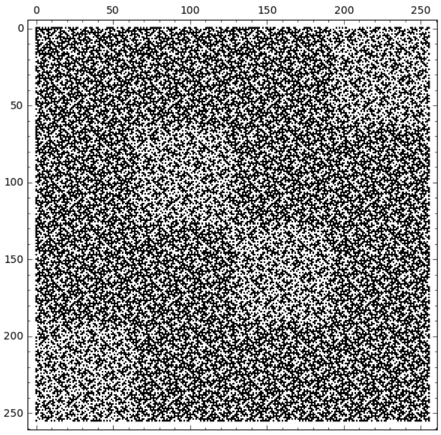

Figure 25: $[f_{8,7}]$: weight classes.

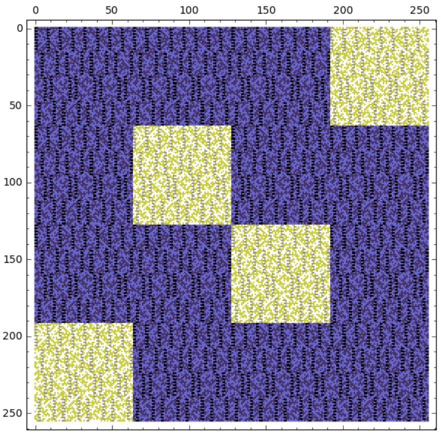

Figure 26: $[f_{8,7}]$: extended Cayley classes.

Class	Parameters	2-rank	Clique polynomial
0	$(256, 120, 56, 56)$	14	$32768t^9 + 712704t^8 + 3014656t^7 + 5734400t^6 + 5013504t^5 + 1908736t^4 + 286720t^3 + 15360t^2 + 256t + 1$
1	$(256, 120, 56, 56)$	14	$24576t^9 + 466944t^8 + 2064384t^7 + 4685824t^6 + 4620288t^5 + 1875968t^4 + 286720t^3 + 15360t^2 + 256t + 1$
2	$(256, 136, 72, 72)$	14	$172032t^9 + 5332992t^8 + 20283392t^7 + 27295744t^6 + 15630336t^5 + 3956736t^4 + 417792t^3 + 17408t^2 + 256t + 1$
3	$(256, 136, 72, 72)$	14	$147456t^9 + 3858432t^8 + 15990784t^7 + 24150016t^6 + 14974976t^5 + 3923968t^4 + 417792t^3 + 17408t^2 + 256t + 1$
4	$(256, 120, 56, 56)$	14	$16384t^9 + 270336t^8 + 1376256t^7 + 3768320t^6 + 4227072t^5 + 1843200t^4 + 286720t^3 + 15360t^2 + 256t + 1$
5	$(256, 136, 72, 72)$	14	$163840t^9 + 3858432t^8 + 15532032t^7 + 23887872t^6 + 14974976t^5 + 3923968t^4 + 417792t^3 + 17408t^2 + 256t + 1$

Table 22: $[f_{8,8}]$ extended Cayley classes.

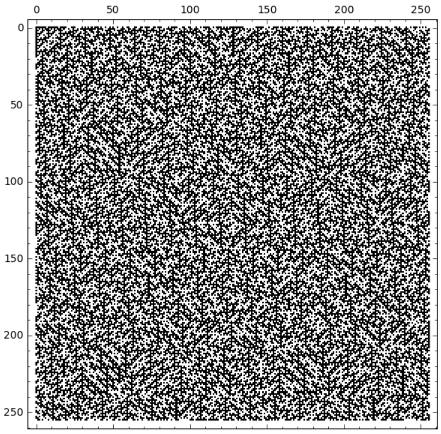

Figure 27: $[f_{8,8}]$: weight classes.

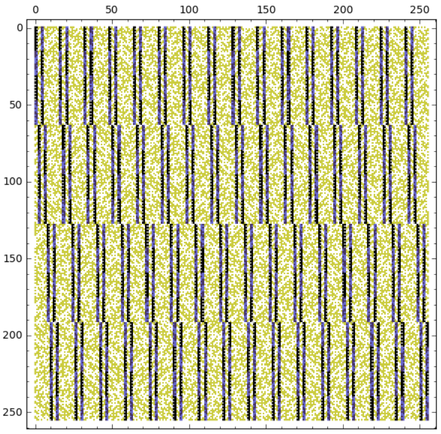

Figure 28: $[f_{8,8}]$: extended Cayley classes.

Class	Parameters	2-rank	Clique polynomial
0	$(256, 120, 56, 56)$	16	$45056t^9 + 780288t^8 + 2998272t^7 + 5505024t^6 + 4816896t^5 + 1892352t^4 + 286720t^3 + 15360t^2 + 256t + 1$
1	$(256, 120, 56, 56)$	16	$45056t^9 + 780288t^8 + 2998272t^7 + 5505024t^6 + 4816896t^5 + 1892352t^4 + 286720t^3 + 15360t^2 + 256t + 1$
2	$(256, 136, 72, 72)$	16	$184320t^9 + 3852288t^8 + 14893056t^7 + 23003136t^6 + 14647296t^5 + 3907584t^4 + 417792t^3 + 17408t^2 + 256t + 1$
3	$(256, 136, 72, 72)$	16	$184320t^9 + 3852288t^8 + 14893056t^7 + 23003136t^6 + 14647296t^5 + 3907584t^4 + 417792t^3 + 17408t^2 + 256t + 1$
4	$(256, 120, 56, 56)$	16	$105984t^8 + 976896t^7 + 3440640t^6 + 4128768t^5 + 1835008t^4 + 286720t^3 + 15360t^2 + 256t + 1$

Table 23: $[f_{8,9}]$ extended Cayley classes (part 1).

Class	Parameters	2-rank	Clique polynomial
5	$(256, 136, 72, 72)$	16	$9216t^{10} + 264192t^9 + 4468224t^8 + 16803840t^7 + 24772608t^6 + 15138816t^5 + 3932160t^4 + 417792t^3 + 17408t^2 + 256t + 1$
6	$(256, 120, 56, 56)$	16	$9216t^9 + 124416t^8 + 976896t^7 + 3440640t^6 + 4128768t^5 + 1835008t^4 + 286720t^3 + 15360t^2 + 256t + 1$
7	$(256, 136, 72, 72)$	16	$193536t^9 + 4449792t^8 + 16803840t^7 + 24772608t^6 + 15138816t^5 + 3932160t^4 + 417792t^3 + 17408t^2 + 256t + 1$

Table 24: $[f_{8,9}]$ extended Cayley classes (part 2).

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

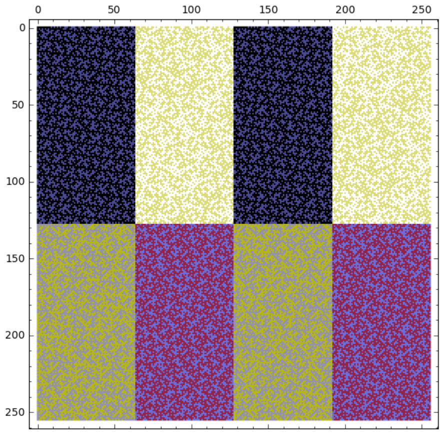

Figure 29: $[f_{8,9}]$: 8 extended Cayley classes

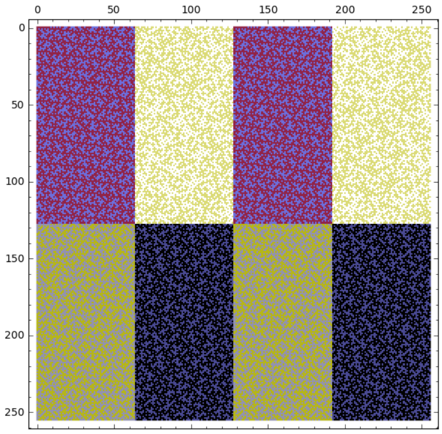

Figure 30: $[f_{8,9}]$: 8 extended Cayley classes of dual bent functions

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 [24] there are 70576747237594114392064 $\approx 2^{75.9}$ *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`

Class	Parameters	2-rank	Clique polynomial
0	$(256, 120, 56, 56)$	16	$16384t^9 + 464896t^8 + 2310144t^7 + 5046272t^6 + 4816896t^5 + 1892352t^4 + 286720t^3 + 15360t^2 + 256t + 1$
1	$(256, 120, 56, 56)$	16	$16384t^9 + 464896t^8 + 2310144t^7 + 5046272t^6 + 4816896t^5 + 1892352t^4 + 286720t^3 + 15360t^2 + 256t + 1$
2	$(256, 120, 56, 56)$	16	$12288t^9 + 301056t^8 + 1589248t^7 + 4128768t^6 + 4423680t^5 + 1859584t^4 + 286720t^3 + 15360t^2 + 256t + 1$
3	$(256, 120, 56, 56)$	16	$12288t^9 + 301056t^8 + 1589248t^7 + 4128768t^6 + 4423680t^5 + 1859584t^4 + 286720t^3 + 15360t^2 + 256t + 1$
4	$(256, 136, 72, 72)$	16	$110592t^9 + 4159488t^8 + 17285120t^7 + 25296896t^6 + 15302656t^5 + 3940352t^4 + 417792t^3 + 17408t^2 + 256t + 1$

Table 25: $[f_{8,10}]$ extended Cayley classes (part 1).

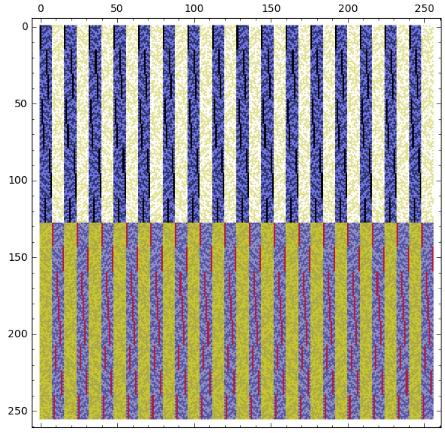

Figure 31: $[f_{8,10}]$: extended Cayley classes.

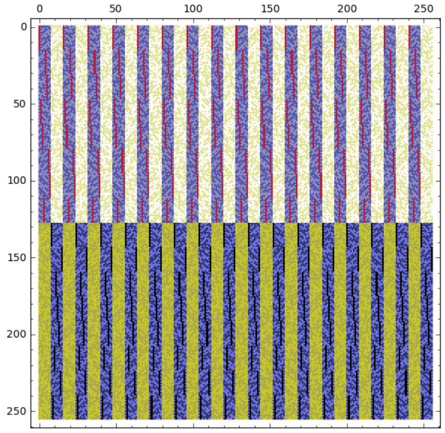

Figure 32: $[f_{8,10}]$: extended Cayley classes of dual bent functions.

Class	Parameters	2-rank	Clique polynomial
5	$(256, 136, 72, 72)$	16	$110592t^9 + 4159488t^8 + 17285120t^7 + 25296896t^6 + 15302656t^5 + 3940352t^4 + 417792t^3 + 17408t^2 + 256t + 1$
6	$(256, 120, 56, 56)$	16	$2048t^9 + 167424t^8 + 1091584t^7 + 3440640t^6 + 4128768t^5 + 1835008t^4 + 286720t^3 + 15360t^2 + 256t + 1$
7	$(256, 136, 72, 72)$	16	$7168t^{10} + 143360t^9 + 3804672t^8 + 15886336t^7 + 24313856t^6 + 15138816t^5 + 3932160t^4 + 417792t^3 + 17408t^2 + 256t + 1$
8	$(256, 120, 56, 56)$	16	$9216t^9 + 181760t^8 + 1091584t^7 + 3440640t^6 + 4128768t^5 + 1835008t^4 + 286720t^3 + 15360t^2 + 256t + 1$
9	$(256, 136, 72, 72)$	16	$107520t^9 + 3790336t^8 + 15886336t^7 + 24313856t^6 + 15138816t^5 + 3932160t^4 + 417792t^3 + 17408t^2 + 256t + 1$

Table 26: $[f_{8,10}]$ extended Cayley classes (part 2).

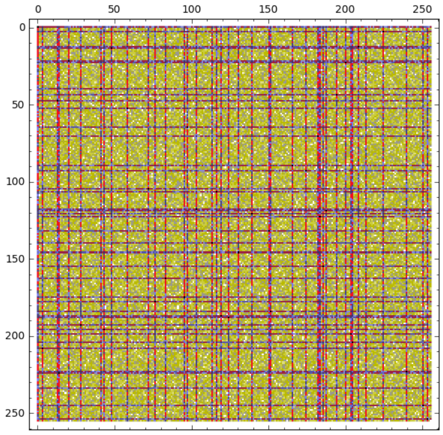

Figure 33: $[psf_{9,5439}]$: extended Cayley classes

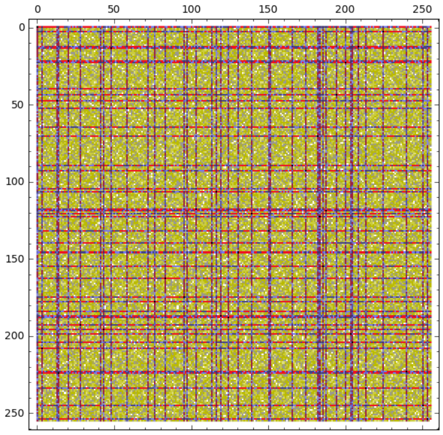

Figure 34: $[psf_{9,5439}]$: extended Cayley classes of dual bent functions

Example partial spread ET class $[psf_{9,5439}]$. 6 of the 16 classes form 3 dual pairs of classes.

Example CAST-128 S-Box ET class $[cast128_{1,0}]$ The CAST-128 encryption algorithm is used in PGP and elsewhere [1]. The algorithm uses 8 S-boxes, each of which consists of 32 binary bent functions in 8 dimensions, with degree 4. CAST-128, including the S-boxes, is specified by IETF RFC 2144:

`https://www.ietf.org/rfc/rfc2144.txt`

Dual bent functions yield another 65 536 extended Cayley classes!

5 SageMath and SageMathCloud code

As mentioned in the previous section, the computational results listed there were obtained by the use of code written in Sage [19] [39] and Python. This code base is called `Boolean-Cayley-graphs` and it is available both as a GitHub repository [28] and as a public SageMathCloud [36] folder [29].

For an introduction to other aspects of coding theory and cryptography in Sage, see the article by Joyner et al. [19].

Description of the Sage code. This section contains a brief description of some of the code included in `Boolean-Cayley-graphs`. More detailed documentation is being developed and this is intended to be included as part of the code base. The code itself is subject to review and revision, and may

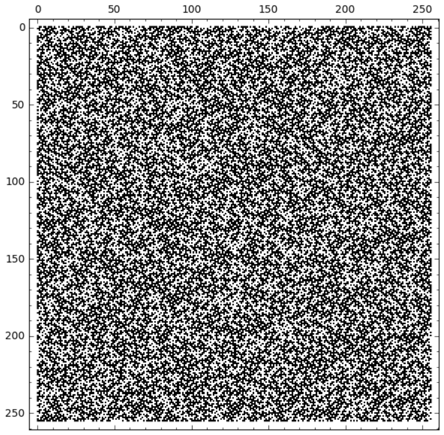

Figure 35: [$cast128_{1,0}$]: weight classes

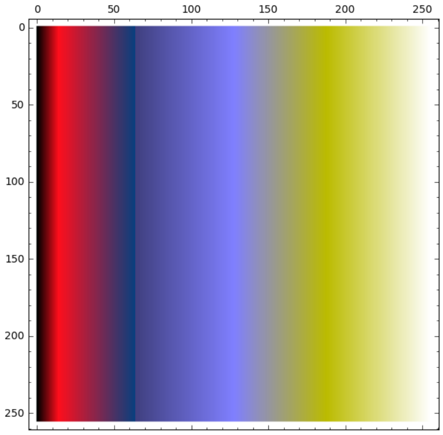

Figure 36: [$cast128_{1,0}$]: 65 536 extended Cayley classes

change as a result of the advice of those more experienced with Sage code. The description in this section applies to the code base as it exists in May 2017.

The code base is structured as a set of Sage script files. These in turn use Python scripts, found in a subdirectory called `Boolean_Cayley_graphs`.

The Python code is used to define a number of useful Python classes. The key class is `BentFunctionCayleyGraphClassification`. This class is used to store the classification of Cayley graphs within the extended translation class of a given bent function f, as well as the classification of Cayley graphs of the duals of each function in the extended translation class.

The class therefore contains the algebraic normal form of the given bent function a list of graphs stored as strings obtained via the `graph6_string` [30] method of the `Graph` class, and two matrices, used to store the list indices corresponding to the Cayley graph for each bent function in the extended translation class, and the dual of each bent function, respectively. The class also contains the weight class matrix corresponding to the given bent function.

The class is initialized by enumerating the bent functions of the form $x \mapsto f(x+b) + \langle c, x \rangle + f(b)$, and determining the Cayley graph of each. For each Cayley graph, the `Graph` method `canonical_label` is used to invoke the Bliss package [20, 21] to calculate the canonical label of the graph, and then `graph6_string` is used to obtain a string. Each new graph is compared for isomorphism to each of the graphs in the current list, by simply comparing the string against each of the existing strings. If the new graph is not isomorphic to any existing graph, it is added to the list. Each list of non-isomorphic graphs can be checked by a function called `check_graph_class_list` which uses the Nauty package to check the non-isomorphism [30, 31].

For an 8 dimensional bent function, the initialization of its Cayley graph classification can take more than 24 hours on an Intel®Core™i7 CPU 870 running at 2.93GHz. For this reason, each computed classification is saved, and a class method (`load_mangled`) is provided to load existing saved classifications.

History of the Sage code. The Sage code originated in 2015 as a series of worksheets on SageMathCloud. While these were useful for investigating extended Cayley classes for bent functions in up to 6 dimensions, they were too slow to use for bent functions in 8 dimensions.

The `Boolean-Cayley-graphs` GitHub project and public SageMathCloud folder was begun in 2016 with the intention of refactoring the code to make it fast enough to use for bent functions in 8 dimensions up to degree 3. The use of canonical labelling via the Bliss algorithm is what made this possible.

Further improvements were made in 2017 to enable the classification of any bent function in up to 8 dimensions to be computed.

6 Discussion

The investigation of the extended Cayley classes of bent functions is just beginning, and there are many open questions. This section lists some of these questions.

The following questions have been settled only for dimensions 2, 4 and 6.

1. How many extended Cayley classes are there for each dimension? Are there "Exponential numbers" of classes [23]?

2. In n dimensions, which extended translation classes contain the maximum number, 4^n, of different extended Cayley classes?

3. Which extended Cayley classes overlap more than one extended translation class?

4. Which bent functions are Cayley equivalent to their dual?

5. Which bent functions are extended affine equivalent to their dual?

Also, what are the extended affine and extended Cayley classes of bent functions of dimension 8 and degree 4 [25]?

Finally, how does the concept of extended Cayley classes of bent functions generalize to bent functions over number fields of prime order $p \neq 2$ [11]?

A Proof of Theorem 4

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

Lemma 5. *Let $q(x) := x^T Lx$ 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.

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

and therefore

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

□

Lemma 6. *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 $M \in \mathbb{Z}_2^{2m\times 2m}$,*

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

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

Proof. Let Z, x be as above. Then

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

Therefore

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

□

Lemma 7. *Let q be defined as per Lemma 5. 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

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

Therefore, by Lemma 6,

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

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,

$$q(Ax) = (Ax)^TL(Ax) = x^TA^TLAx = x^T(L+S)x.$$

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

Let

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

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

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

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 $p \in \{0, \dots, r-1\}$, 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 $p \in \{0, \dots, r-1\}$, 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 8. *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 5. 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 7.

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 7, 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 9. *For distinct $k, \ell \in \{0, \ldots, m-1\}$ let $e^{(k)}, e^{(\ell)}$ be defined as per Lemma 8. Let $h(x) := q(x) + \langle e^{(k)}, x \rangle$, where q is defined as per Lemma 5. 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 10. *Let q be defined as per Lemma 5. 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 8 and 9. □

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 5.

As a result of Lemma 5, 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 7 implies that all such functions for which $q(c) = 0$ are Cayley equivalent to q. Lemma 10 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 2 implies that

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

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. Braeken. *Cryptographic Properties of Boolean Functions and S-Boxes.* Phd thesis, Katholieke Universiteit Leuven, Leuven-Heverlee, Belgium, (2006).

[7] 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).

[8] A. E. Brouwer and C. A. Van Eijl. On the p-rank of the adjacency matrices of strongly regular graphs. *Journal of Algebraic Combinatorics*, 1(4):329–346, (1992).

[9] 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).

[10] 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).

[11] Y. M. Chee, Y. Tan, and X. D. Zhang. Strongly regular graphs constructed from p-ary bent functions. *Journal of Algebraic Combinatorics*, 34(2):251–266, (2011).

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

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

[14] 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).

[15] 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).

[16] 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).

[17] C. Hoede and X. Li. Clique polynomials and independent set polynomials of graphs. *Discrete Mathematics*, 125(1):219 – 228, (1994).

[18] 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.

[19] 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).

[20] 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.

[21] 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).

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

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

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

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

[26] 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).

[27] 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].

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

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

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

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

[32] 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.

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

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

[35] 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).

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

[37] 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.

[38] D. R. Stinson. *Combinatorial designs: constructions and analysis.* Springer Science & Business Media, (2007).

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

[40] 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).

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

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

[43] 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).