Boolean-Cayley-graphs: Using Sage and Python software to explore Boolean functions, their Cayley graphs and associated structures

Paul Leopardi

ACCESS-NRI
The Australian National University

For Hadamard 2025

Motivation

Question:

Which strongly regular graphs arise as Cayley graphs of bent Boolean functions?

Bent functions

Definition 1

The Walsh Hadamard transform of a Boolean function $f : \mathbb{F}_2^{2m} \to \mathbb{F}_2$ *is*

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

Definition 2

A Boolean function $f : \mathbb{F}_2^{2m} \to \mathbb{F}_2$ *is bent if and only if its Walsh Hadamard transform has constant absolute value* 2^m.

(Dillon 1974; Rothaus 1976)

The Cayley graph of a Boolean function

Definition 3

The Cayley graph $\mathrm{Cay}\,(f)$ *of a Boolean function*

$$f : \mathbb{F}_2^n \to \mathbb{F}_2 \quad \textit{where} \quad f(0) = 0$$

is an undirected graph with

$$V(\mathrm{Cay}\,(f)) := \mathbb{F}_2^n, \quad (x, y) \in E(\mathrm{Cay}\,(f)) \Leftrightarrow f(x + y) = 1.$$

(Bernasconi and Codenotti 1999)

Strongly regular graphs

Definition 4

A simple graph Γ *of order* v *is strongly regular with parameters* (v, k, λ, μ) *if*

- *each vertex has degree* k,
- *each adjacent pair of vertices has* λ *common neighbours, and*
- *each nonadjacent pair of vertices has* μ *common neighbours.*

(Brouwer, Cohen and Neumaier 1989)

Cayley graphs of bent functions

Proposition 1

(Bernasconi and Codenotti 1999)
The Cayley graph $\operatorname{Cay}(f)$ *of a bent function* f *on* $\mathbb{F}_2^{2m}$ *with* $f(0) = 0$ *is a strongly regular graph with* $\lambda = \mu$.

The parameters of $\operatorname{Cay}(f)$ are

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

(Bernasconi and Codenotti 1999)

Extended affine equivalence

Definition 5

For bent functions $f, g : \mathbb{F}_2^{2m} \to \mathbb{F}_2$*,*
f *is extended affine equivalent to* g *if and only if*

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

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

(Budaghyan, Carlet and Pott 2006)

General linear equivalence

Definition 6

For bent functions $f, g : \mathbb{F}_2^{2m} \to \mathbb{F}_2$, 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 7

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

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

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

Cayley equivalence

Definition 8

For $f, g : \mathbb{F}_2^{2m} \to \mathbb{F}_2$*, 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 $\pi : \mathbb{F}_2^{2m} \to \mathbb{F}_2^{2m}$ *such that*

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

Extended Cayley equivalence

Definition 9

For $f, g : \mathbb{F}_2^{2m} \to \mathbb{F}_2$, 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 $\mathbb{F}_2^{2m}$.

General linear equivalence implies Cayley equivalence

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.

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

$\square$

Extended affine, extended translation, and extended Cayley equivalence (1)

Theorem 2

For $A \in GL(2m, 2)$, $b, c \in \mathbb{F}_2^{2m}$, $\delta \in \mathbb{F}_2$, $f : \mathbb{F}_2^{2m} \to \mathbb{F}_2$, *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 then* $h \cong g$.

Extended affine, extended translation, and extended Cayley equivalence (2)

Therefore, to determine which extended Cayley equivalence classes have members within the extended affine equivalence class of a bent function $f : \mathbb{F}_2^{2m} \to \mathbb{F}_2$ (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 $b, c \in \mathbb{F}_2^{2m}$.

Weights and weight classes

Definition 10

The weight of a binary function is the cardinality of its support.
For f on $\mathbb{F}_2^{2m}$

$$\operatorname{supp}(f) := \{x \in \mathbb{F}_2^{2m} \mid f(x) = 1\}.$$

A bent function f on $\mathbb{F}_2^{2m}$ has weight

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

Quadratic bent functions have two General Linear classes

Theorem 3

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

Quadratic bent functions have two extended Cayley classes

Corollary 4

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

Demo of Boolean-Cayley-graphs

CoCalc: Public worksheets, Sage and Python source code

`http://tinyurl.com/Boolean-Cayley-graphs`

GitHub: Sage and Python source code

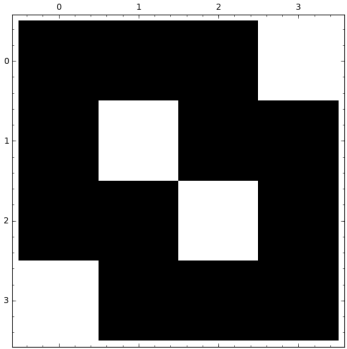
`https://github.com/penguian/Boolean-Cayley-graphs`

SourceForge: Documentation

`https://boolean-cayley-graphs.sourceforge.io/`

For 2 dimensions: ET class $[f_{2,1}]$

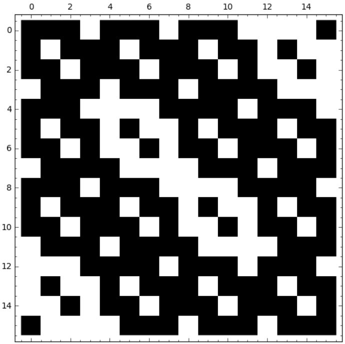
One extended affine class, containing the extended translation class $[f_{2,1}]$, where $f_{2,1}(x) := x_0 x_1$.



$[f_{2,1}]$: 2 extended Cayley classes, 2 General Linear classes

For 4 dimensions: ET class $[f_{4,1}]$

One extended affine class, containing the extended translation class $[f_{4,1}]$, where $f_{4,1}(x) := x_0 x_1 + x_2 x_3$.



$[f_{4,1}]$: 2 extended Cayley classes, 2 General Linear classes

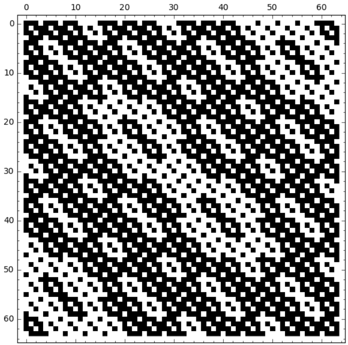
For 6 dimensions: ET classes

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

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

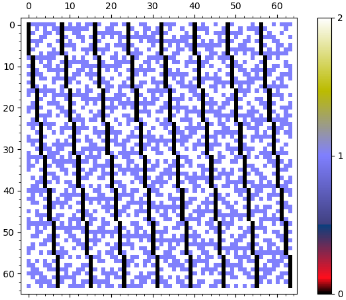
(Rothaus 1976; Tokareva 2015)

ET class $[f_{6,1}]$

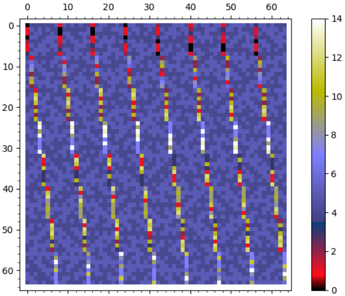


$[f_{6,1}]$: 2 extended Cayley classes,
2 General Linear classes

ET class $[f_{6,2}]$



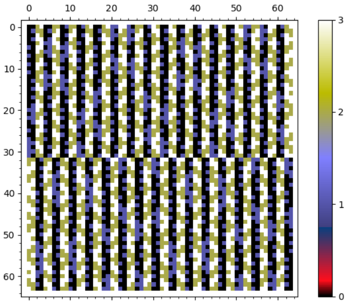
$[f_{6,2}]$: 3 extended Cayley classes



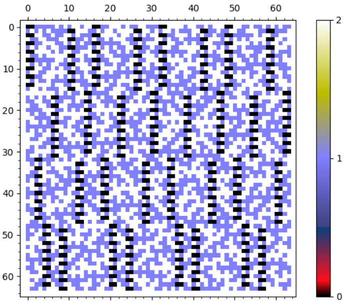
$[f_{6,2}]$: 15 General Linear classes

Since $f_{6,1} \equiv f_{6,2}$, the Cayley graph for extended Cayley class 0 is isomorphic to the Cayley graph for class 0 of $[f_{6,1}]$.

ET classes $[f_{6,3}]$ and $[f_{6,4}]$



$[f_{6,3}]$: 4 extended Cayley classes, 4 General Linear classes



$[f_{6,4}]$: 3 extended Cayley classes, 3 General Linear classes

Preprint, source code and documentation

Preprint: Paul Leopardi, Classifying bent functions by their Cayley graphs, arXiv:1705.04507 [math.CO]. Revised, December, 2023.

CoCalc: Public worksheets, Sage and Python source code

`http://tinyurl.com/Boolean-Cayley-graphs`

GitHub: Sage and Python source code

`https://github.com/penguian/Boolean-Cayley-graphs`

SourceForge: Documentation

`https://boolean-cayley-graphs.sourceforge.io/`

References (1)

1. A. Bernasconi and B. Codenotti. Spectral analysis of Boolean functions as a graph eigenvalue problem. *IEEE Transactions on Computers*, 48(3):345–351, (1999).
2. A. Braeken. *Cryptographic Properties of Boolean Functions and S-Boxes*. PhD thesis, Katholieke Universiteit Leuven, Belgium, (2006).
3. A. Brouwer, A. Cohen, and A. Neumaier. *Distance-Regular Graphs*. Ergebnisse der Mathematik und Ihrer Grenzgebiete, vol. 18. Berlin, Heidelberg, [Germany] : Springer-Verlag, (1989).
4. L. Budaghyan, C. Carlet, and A. Pott. New classes of almost bent and almost perfect nonlinear polynomials. *IEEE Transactions on Information Theory*, 6;52(3):1141-52 (2006).

References (2)

5. J. F. Dillon. *Elementary Hadamard Difference Sets*. PhD thesis, University of Maryland College Park, Ann Arbor, USA, (1974).
6. O. S. Rothaus. On "bent" functions. *Journal of Combinatorial Theory, Series A*, 20(3):300–305, (1976).
7. N. Tokareva. *Bent functions: results and applications to cryptography*. Academic Press, (2015).

Acknowledgements

Robin Bowen, An Braeken, Nathan Clisby, Robert Craigen, Joanne Hall, David Joyner, Philippe Langevin, Matthew Leingang, William Martin, Padraig Ó Catháin, Judy-anne Osborn, Dima Pasechnik, William Stein, Natalia Tokareva, and Sanming Zhou.

Australian National University. University of Newcastle, Australia. University of Melbourne. Australian Government - Bureau of Meteorology. National Computational Infrastructure. ACCESS-NRI.

SageMath, CoCalc, Bliss, Nauty, MPI4py, SQLite3, DB Browser for SQLite, PostgreSQL, Psycopg2.