On the normality of Boolean quartics

The 9th International Workshop on Boolean Functions and their Applications dedicated to Claude Carlet's 75th birthday. September 9-13, 2024, Dubrovnik, Croatia

Valérie Gillot, Philippe Langevin and Alexandr Polujan

Université de Toulon, Otto-von-Guericke-Universität

Table of contents

Walk along Claude’s gardens

Boolean function

Claude's favorite universe is made up of an infinite number of gardens $B(1)$, $B(2)$, $B(3)$ ... The flowers of the garden $B(m)$ are Boolean functions often called m-bit functions. With friends, we like to spend time in garden $B(8)$, searching for nice object among 8-bit functions...

115792089237316195423570985008687907853269984665640564039457584007913129639936 flowers...

Rare pearl

What is the minimal linearity of a balanced Boolean function?

Walsh coefficient

spectral amplitude

$$\widehat{f}(a) = \sum_{x \in \mathbb{F}_2^m} (-1)^{f(x)+a.x} \qquad R(f) = \max_{a \in \mathbb{F}_2^m} |\widehat{f}(a)|$$

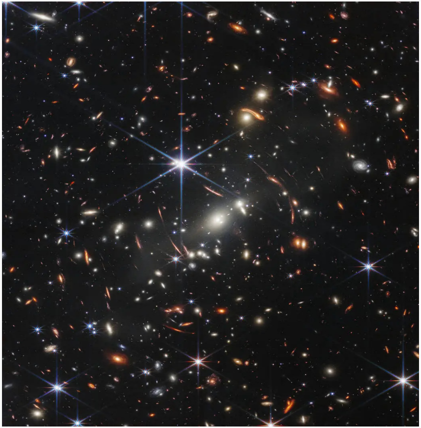
$$\mathrm{R}(m) = \min_{f} R(f) \qquad \mathrm{R_b}(m) = \min_{\widehat{f}(0)=0} R(f)$$

spectral radius

balanced radius

galaxy cluster SMACS 0723 : 2^{32} light years . . .

NASA's James Webb Space Telescope has produced the deepest and sharpest infrared image of the distant universe to date.



The number of atoms in the universe is estimated to 10^{80}

The number of 8-bit functions is $\approx 10^{77}$

Open question regarding garden $B(8)$

All is known for Boolean function spaces in dimension smaller than 7, below is a list of open questions are in dimension 8 :

- normality of bent functions ?
- classification of bent functions ?
- normality of quartics ?
- covering radius of $RM(2, 8)$?
- covering radius of $RM(3, 8)$?
- ~~covering radius of $RM(4, 8)$?~~
- linearity of balanced functions ?
- *What else... Let me know!*

Numerical point of view

For all these questions, in dimension 8, **numerical approaches** based on **classifications under the action of the affine general group** may give results.

Classification in dimension 7 and 8

$\mathrm{AGL}(m,2)$ acts naturally on Reed-Muller codes, RM-spaces :

$$B(s,t,m) := \{ \sum_{s \leq |S| \leq t} a_S X_S \quad \} = RM(t,m)/RM(s-1,m)$$

$\widetilde{B}(s,t,m)$ denotes a system of represensentatives of $B(s,t,m)$

$s \backslash t$	1	2	3	4	5	6	7
0	3	12	**3486**	$10^{13.5}$	$10^{19.8}$	$10^{21.9}$	$10^{22.2}$
1	2	8	1890	$10^{13.1}$	$10^{19.5}$	$10^{21.6}$	$10^{21.9}$
2		4	179	$10^{11.0}$	$10^{17.3}$	$10^{19.5}$	$10^{19.8}$
3			12	68443	$10^{11.0}$	$10^{13.1}$	$10^{13.5}$
4				12	179	1890	**3486**
5					4	8	12
6						2	3
7							2

Class numbers of $B(s,\ t,\ 7)$

$s \backslash t$	1	2	3	4	5	6	7	8
1	2	9	3814830	$10^{27.6}$	$10^{44.5}$	$10^{52.9}$	$10^{55.3}$	$10^{55.6}$
2		5	**20748**	$10^{25.2}$	$10^{42.0}$	$10^{50.5}$	$10^{52.9}$	$10^{53.2}$
3			32	$10^{16.7}$	$10^{33.6}$	$10^{42.0}$	$10^{44.5}$	$10^{44.8}$
4				**999**	$10^{16.7}$	$10^{25.2}$	$10^{27.6}$	$10^{27.9}$
5					32	20748	3814830	7611801
6						5	9	14
7							2	3
8								2

Class numbers of $B(s,\ t,\ 8)$

see our recent works [7] with Valérie Gillot.

Normality, relative degree

Normality, weak normality

The notion of normality was introduced by Hans Dobbertin (1994) in order to produce the inequality :

$$\mathrm{R_b}(2t) \leq 2^t + \mathrm{R_b}(t) \Longrightarrow \mathrm{R_b}(8) \leq 24$$

Pascale Charpin **(2004)**

A Boolean function $f \in B(m)$ is said to be **normal** if there exists a subspace V of $\mathbb{F}_2^m$ with middle dimension $\lceil m/2 \rceil$ such that f is constant on some translate $a + V$ with $a \in \mathbb{F}_2^m$.

It is convenient to use the notation

$$f_{a,V} : v \mapsto f(v+a), \quad f_{a,V} \in B(V) \sim B(\dim V)$$

weak normality

A non normal f is **weakly normal** when $f_{a,V}$ is affine for some $a + V$ with middle dimension.

relative degree

The degree of $f_{a,V}$ is called the **relative degree** of f on $a + V$:

$$\deg_{a+V}(f) := \deg(f_{a,V}), \qquad \text{(by convention} \geq 0)$$

Definition

The r-**degree** of f is the minimal relative degree of f for all affine spaces $a + V$, where $\dim(V) = r$.

$$0 \leq \deg_r(f) = \min\{\deg_{a+V}(f) \mid \dim V = r \quad \text{and} \quad a \in \mathbb{F}_2^m\}.$$

Notions of normality translate:

$$\deg_{\lceil m/2 \rceil}(f) = \begin{cases} 0, & f \text{ is normal;} \\ 1, & f \text{ is weakly normal;} \\ \geq 2, & f \text{ is abnormal.} \end{cases}$$

combinatorial parameters

For integers $r \leq m$ and $k \leq m$, we explore :

$$D_r(k, m) = \max\{\deg_r(f) \mid \deg(f) \leq k\}.$$

In a recent note (August 2024), Jan Kristian Haugland studies :

$$g(m, r) = \max_f \deg_r(f) = \max_k D_r(k, m)$$

Theorem

If $r > t \geq 0$ *and* $m \geq 2^{r-1} + r - \lfloor 2^{t-1} \rfloor$ *then* $g(m, r) \leq t$

Conjecture (Haugland)

If $r \geq 2$ *then*

$$g(r+2, r) = r - 2$$

$$
\begin{gathered}
f(x) = x_8x_7x_5 \oplus x_8x_6x_5 \oplus x_8x_4 \oplus x_8x_6x_4 \oplus x_7x_6x_4 \oplus x_8x_7x_6x_4 \oplus x_8x_5x_4 \oplus x_7x_5x_4 \oplus \\
x_8x_7x_5x_4 \oplus x_8x_6x_5x_4 \oplus x_8x_7x_6x_5x_4 \oplus x_7x_3 \oplus x_8x_7x_3 \oplus x_8x_7x_6x_3 \oplus x_7x_5x_3 \oplus x_6x_5x_3 \oplus \\
x_8x_6x_5x_3 \oplus x_7x_6x_5x_3 \oplus x_8x_7x_6x_5x_3 \oplus x_7x_4x_3 \oplus x_6x_4x_3 \oplus x_7x_6x_4x_3 \oplus x_8x_7x_6x_4x_3 \oplus \\
x_8x_5x_4x_3 \oplus x_7x_5x_4x_3 \oplus x_8x_7x_5x_4x_3 \oplus x_8x_6x_5x_4x_3 \oplus x_7x_6x_5x_4x_3 \oplus x_8x_7x_6x_5x_4x_3 \oplus x_8x_7x_2 \oplus \\
x_6x_2 \oplus x_8x_6x_2 \oplus x_7x_6x_2 \oplus x_8x_7x_6x_2 \oplus x_8x_7x_5x_2 \oplus x_7x_6x_5x_2 \oplus x_8x_7x_6x_5x_2 \oplus x_8x_4x_2 \oplus x_6x_4x_2 \oplus \\
x_5x_4x_2 \oplus x_7x_5x_4x_2 \oplus x_8x_7x_5x_4x_2 \oplus x_6x_5x_4x_2 \oplus x_7x_6x_5x_4x_2 \oplus x_8x_3x_2 \oplus x_8x_7x_3x_2 \oplus x_6x_3x_2 \oplus \\
x_8x_7x_6x_3x_2 \oplus x_5x_3x_2 \oplus x_8x_5x_3x_2 \oplus x_8x_7x_5x_3x_2 \oplus x_6x_5x_3x_2 \oplus x_8x_6x_5x_3x_2 \oplus x_7x_6x_5x_3x_2 \oplus \\
x_8x_7x_6x_5x_3x_2 \oplus x_8x_4x_3x_2 \oplus x_7x_4x_3x_2 \oplus x_8x_7x_4x_3x_2 \oplus x_6x_4x_3x_2 \oplus x_7x_6x_4x_3x_2 \oplus x_8x_5x_4x_3x_2 \oplus \\
x_7x_5x_4x_3x_2 \oplus x_8x_7x_5x_4x_3x_2 \oplus x_6x_5x_4x_3x_2 \oplus x_7x_6x_5x_4x_3x_2 \oplus x_8x_6x_1 \oplus x_7x_6x_1 \oplus x_5x_1 \oplus \\
x_7x_5x_1 \oplus x_8x_7x_5x_1 \oplus x_6x_5x_1 \oplus x_8x_6x_5x_1 \oplus x_7x_6x_5x_1 \oplus x_8x_7x_6x_5x_1 \oplus x_8x_4x_1 \oplus x_8x_7x_4x_1 \oplus \\
x_7x_6x_4x_1 \oplus x_8x_7x_6x_4x_1 \oplus x_8x_7x_5x_4x_1 \oplus x_6x_5x_4x_1 \oplus x_8x_6x_5x_4x_1 \oplus x_7x_6x_5x_4x_1 \oplus \\
x_8x_7x_6x_5x_4x_1 \oplus x_8x_3x_1 \oplus x_7x_3x_1 \oplus x_8x_7x_3x_1 \oplus x_8x_6x_3x_1 \oplus x_8x_7x_6x_3x_1 \oplus x_5x_3x_1 \oplus \\
x_8x_6x_5x_3x_1 \oplus x_4x_3x_1 \oplus x_8x_4x_3x_1 \oplus x_8x_7x_4x_3x_1 \oplus x_6x_4x_3x_1 \oplus x_8x_6x_4x_3x_1 \oplus x_7x_6x_4x_3x_1 \oplus \\
x_8x_7x_6x_4x_3x_1 \oplus x_5x_4x_3x_1 \oplus x_8x_5x_4x_3x_1 \oplus x_6x_5x_4x_3x_1 \oplus x_8x_6x_5x_4x_3x_1 \oplus x_7x_2x_1 \oplus \\
x_8x_6x_2x_1 \oplus x_7x_6x_2x_1 \oplus x_8x_7x_6x_2x_1 \oplus x_5x_2x_1 \oplus x_8x_5x_2x_1 \oplus x_8x_7x_5x_2x_1 \oplus x_8x_6x_5x_2x_1 \oplus \\
x_7x_6x_5x_2x_1 \oplus x_8x_7x_6x_5x_2x_1 \oplus x_4x_2x_1 \oplus x_8x_4x_2x_1 \oplus x_7x_4x_2x_1 \oplus x_8x_7x_4x_2x_1 \oplus x_7x_6x_4x_2x_1 \oplus \\
x_5x_4x_2x_1 \oplus x_8x_5x_4x_2x_1 \oplus x_7x_5x_4x_2x_1 \oplus x_8x_7x_5x_4x_2x_1 \oplus x_6x_5x_4x_2x_1 \oplus x_7x_6x_5x_4x_2x_1 \oplus \\
x_7x_3x_2x_1 \oplus x_8x_7x_3x_2x_1 \oplus x_6x_3x_2x_1 \oplus x_8x_6x_3x_2x_1 \oplus x_7x_6x_3x_2x_1 \oplus x_8x_7x_6x_3x_2x_1 \oplus \\
x_5x_3x_2x_1 \oplus x_8x_5x_3x_2x_1 \oplus x_6x_5x_3x_2x_1 \oplus x_8x_6x_5x_3x_2x_1 \oplus x_8x_4x_3x_2x_1 \oplus x_7x_4x_3x_2x_1 \oplus \\
x_8x_7x_4x_3x_2x_1 \oplus x_6x_4x_3x_2x_1 \oplus x_7x_6x_4x_3x_2x_1 \oplus x_5x_4x_3x_2x_1 \oplus x_8x_5x_4x_3x_2x_1 \oplus x_6x_5x_4x_3x_2x_1
\end{gathered}
$$

In her PhD thesis, Sylvie Dubuc presented the first example of a **non-normal** function in $B(8)$. It has degree 6 comprising 140 monomials.

We checked

it is **weakly normal**!

$$bcdegh + bcdeh + bcdgh + bcdf + bcef + bcdh + bdfh + begh + abc + cde + bef + bdg + cdg + deh + cfh + cgh + bc + be + ce + df + bg + ch + gh + a + b$$

Haugland table

r \ m	1	2	3	4	5	6	7	8	9	10	11	12
1	1	0	0	0	0	0	0	0	0	0	0	0
2		2	1	0	0	0	0	0	0	0	0	0
3			3	2	1	0	0	0	0	0	0	0
4				4	3	2	2	≥ 1	≥ 0	≥ 0	0 or 1	0
5					5	4	3	3	≥ 2	≥ 2	≥ 0	≥ 0
6						6	5	≥ 4	≥ 3	≥ 3	≥ 3	≥ 2

$$g(m, r) = \max_{f \in B(m)} \deg_r(f)$$

Question 1

Does there exist a Boolean function $B(8)$ with 4-relative degree 2?

Does there exist a non normal bent function in $B(m)$?

Asked by Hans Dobbertin 1994...

Sylvie Dubuc

All members of $B(6)$ are normal!

(2001)

Anne Canteaut, Magnus Daum, Hans Dobbertin, Gregor Leander

Some Kasami power functions are 14-bit abnormal bent functions.

(2006)

Gary McGuire, Gregor Leander

Applying magic tricks to Kasami functions, provided 10-bit and 12-bit abnormal bent.

(2009)

Normality of bent functions in $B(8)$

Sylvie Dubuc **(2001)**

All bent cubics of $B(8)$ are normal!

Pascale Charpin **(2004)**

Does it exist non-normal bent functions of 8 variables and degree 4?

Last BFA conference, Luca Mariot, Stjepan Picek and Alexandr Polujan, exhibited example of (non normal) weakly normal function in $B(8)$ coming from the partial spread class.

Question 2

Are there any abnormal 8-bit bent functions?

Numerical facts on relative degree

$D_r^\ddagger(k, 6)$ illustration of Dubuc's result

$r \backslash k$	1	2	3	4	5	6
5	0	2	3	4	3	4
4	0	2	2	2	2	2
3	0	0	0	0	0	0
2	0	0	0	0	0	0

Maximal r-relative degree of functions of degree k of $B(6)$.

Sylvie Dubuc

All flowers of $B(6)$ are normal!

Remark

If $f \in B(7)$ *or* $f \in B(8)$ *then* $\deg_4(f) \leq 2$.

4-relative degree in $B(7)$?

The following member of $RM(6,7)$ has 4-relative degree 2 :

$$cd+abcd+ce+ade+acde+bcde+abcde+abf+adf+bdf+cdf+abdef$$
$$+cdef+acdef+ag+abg+cg+acdg+eg+aceg+bceg+deg+adeg$$
$$+abdeg+cdeg+abcdeg+fg+afg+abfg+adfg+bdfg+abcdfg+befg+bcefg$$

So,

$$D_4(7)=2$$

See Jan Kristian Haugland note on arXiv.

$D_r^\dagger(k,7)$

$r\backslash k$	1	2	3	4	5	6	7
6	0	2	3	≥ 4	≥ 4	5	≥ 4
5	0	2	3	≥ 3	≥ 3	≥ 3	≥ 3
4	0	1	1	≥ 1	≥ 1	2	≥ 1
3	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0

Maximal r-relative degree of functions of degree k of $B(7)$.

Numerical fact using the 3486 members of $\widetilde{B}(0,3,7)$

All cubics in $B(7)$ are normal or weakly normal.

The minoration in the right part of the table $D_r^\dagger(k,7)$ were obtained at random, by adding a random cubic to the 3486 members of $\widetilde{B}(4,7,7)$.

Conjecture

All the quartics of $B(7)$ are normal or weakly normal.

Numerical facts on 8-bit functions

8-bit cubics

Numerical fact

All the cubics in $B(8)$ are normal or weakly normal.

Proof.

For $f \in RM(3,8)$ and for any hyperplane $H \subset \mathbb{F}_2^8$, the restriction of f to H is a cubic in $B(H) \sim B(7)$. $\square$

Alternatively, it is a numerical fact using the 20748 members of $\widetilde{B}(2,3,8)$.

$r \backslash \deg_r$	0	1	2	3
7	10	0	53	20 712
6	130	21	1 910	18 714
5	5 504	5 227	10 044	0
4	20 748	0	0	0

Distribution of relative degrees of 20748 cubics of $\widetilde{B}(2,3,8)$

Question 2

Are there any abnormal 8-bit bent functions?

possible approaches :

- harmonic analysis folklore
- classification of bent functions

Xiang-Dong Hou condition

The ANF of an 8-bit bent function

$$f = \sum_{2 \leq |S| \leq 4} a_s X_S = h + c + q = \begin{cases} h, \text{quartic;} \\ c, \text{cubic;} \\ q, \text{quadric.} \end{cases}$$

satisfies a system of 36 quadratic equations parametrized by subset $W \subseteq \{1, 2, \ldots, 8\}$ of cardinality 8, 7 and 6 :

$$\sum_{\substack{\{S, S'\} \\ S \cup S' = W}} a_S a_{S'} = 0$$

Given h, the cubic part depends on a linear system of 56 unknowns and 8 equations and one use the <u>stabilizer</u> of h to build a part of cover set.

cover set

Adapting the counting method presented with Gregor Leander in 2011, we obtain a **cover-set** of 8-bit of the set of bent functions of degree 4 :

- size $355\,073\,617 \approx 2^{28.52}$;
- approx 100 cores during 2-3 months (night-time).

Data and bent functions are available :

langevin.univ-tln.fr/project/

It is an easy task to check the weak normality of all these functions.

Numerical fact using the 999 members of $\widetilde{B}(4,4,8)$

All 8-bit **bent** functions are normal or weakly normal.

Conclusion

Practice $\rightsquigarrow$ theory

Now, thanks to our numerical approach, we know that it is true that all 8-bit bent functions are normal...

Il est plus facile de démontrer une conjecture lorsqu'on sait d'une manière ou d'une autre qu'elle est vraie.

It's easier to prove a conjecture when you know one way or another that it's true.

to be continued!

Jacques Hadamard

Summary

Main result

The construction of a **small** cover set of 8-bit bent functions

[forthcoming classification soon]

Milestone for $B(8)$

All 8-bit **bent** functions are normal or weakly normal.

Conjecture

All 7-bit **quartics** *are normal or weakly normal.*

Conjecture

All 8-bit **quartics** *are normal or weakly normal.*

References

A. Canteaut, M. Daum, H. Dobbertin, and G. Leander.
Finding nonnormal bent functions.
Discret. Appl. Math., 154(2):202–218, 2006.

P. Charpin.
Normal Boolean functions.
Journal of Complexity, 20(2):245–265, 2004.
Festschrift for Harald Niederreiter, Special Issue on Coding and Cryptography.

H. Dobbertin.
Construction of bent functions and balanced Boolean functions with high nonlinearity.
In B. Preneel, editor, *Fast Software Encryption*, pages 61–74, Berlin, Heidelberg, 1995. Springer Berlin Heidelberg.

S. Dubuc.
Etude des propriétés de dégénérescence et de normalité des fonctions booléennes et construction de fonctions q-aires parfaitement non-linéaires.
PhD thesis, University of Caen, 2001.

V. Gillot and P. Langevin.
Classification of 8-bit bent functions.
https://langevin.univ-tln.fr/project/genbent/genbent.html.

V. Gillot and P. Langevin.
Classification of $B(s, t, m)$.
http://langevin.univ-tln.fr/data/bst/.

V. Gillot and P. Langevin.
Classification of some cosets of Reed-Muller codes.
Cryptography and Communications, 15:1129–1137, 2023.
doi:10.1007/s12095-023-00652-4.

J. K. Haugland.
On the max min of the algebraic degree and the nonlinearity of a boolean function on an affine subspace.
2408.01477, 2024.

X.-D. Hou and P. Langevin.
Results on bent functions.
Journal of Combinatorial Theory (A), 80(2):232–246, 1997.

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

G. Leander and G. McGuire.
Construction of bent functions from near-bent functions.
J. Combin. Theory Ser. A, 116(4):960–970, 2009.

A. Polujan, L. Mariot, and S. Picek.
Normality of Boolean bent functions in eight variables, revisited.
In *The 8th International Workshop on Boolean Functions and their Applications*, pages 79–83, 2023.

A. Polujan, L. Mariot, and S. Picek.
On two open problems on the normality of bent functions.
Accepted in Discrete Applied Mathematics, 2024.

Hidden motivation

Hidden motivation

We recently construct millions of CCZ class of quadric APN in dimension 8 considering extensions of a $(8,4)$-bent vectorial functions.

Let β be the bent indicator of $F\colon \mathbb{F}_2^m \longrightarrow \mathbb{F}_2^m$,

$$\forall b \in \mathbb{F}_2^m, \quad \beta(b) = 1 \iff \text{component } b.F \text{ is bent.}$$

Conjecture (kind)

The bent indicator of a quadratic APN in 8 variables is normal.

In the space of homogeneous quadratic forms of 8 variables, a space of dimension 28, the indicator of the set of bent functions is a **quartic**...