Available online at www.sciencedirect.com
SCIENCE DIRECT
Discrete Applied Mathematics 154 (2006) 202–218
DISCRETE APPLIED MATHEMATICS
www.elsevier.com/locate/dam

Finding nonnormal bent functions

Anne Canteaut[a], Magnus Daum[b], Hans Dobbertin[b], Gregor Leander[b]

[a] *INRIA-Projet CODES, BP 105, 78153 Le Chesnay Cedex, France*
[b] *Ruhr-University Bochum, Postfach 102148, 44780 Bochum, Germany*

Received 12 September 2003; received in revised form 27 April 2004; accepted 21 March 2005
Available online 21 September 2005

Abstract

The question if there exist nonnormal bent functions was an open question for several years. A Boolean function in n variables is called normal if there exists an affine subspace of dimension $n/2$ on which the function is constant. In this paper we give the first nonnormal bent function and even an example for a nonweakly normal bent function. These examples belong to a class of bent functions found in [J.F. Dillon, H. Dobbertin, New cyclic difference sets with Singer parameters, in: Finite Fields and Applications, to appear], namely the Kasami functions. We furthermore give a construction which extends these examples to higher dimensions. Additionally, we present a very efficient algorithm that was used to verify the nonnormality of these functions.

Keywords: Algorithm; Boolean function; Bent function; Normal function

1. Introduction

In cryptography, Boolean functions are used in many different areas, the probably most important being the design of S-Boxes for symmetric encryption. The main *complexity characteristics* for Boolean functions on $\mathbb{F}_2^n$ which are relevant to cryptography are the algebraic degree and the nonlinearity. But other criteria have also been studied. One of them is the question if there exists a space of dimension $n/2$ such that the restriction of a given function is constant (resp. affine) on this space. We call the functions for which such a space exists normal (resp. weakly normal). The notion of normality has been introduced for the first time in [7]. This notion was used to construct balanced functions with high nonlinearities. This construction relies on the fact that if a bent function f is constant on an $(n/2)$-dimensional affine subspace, then f is balanced on each of the other cosets of this affine subspace [2]. Since that time the question if there exist nonnormal bent functions was open. For arbitrary Boolean functions, an easy counting argument shows that there must exist nonnormal functions of n variables for $n \geqslant 10$. It was even shown in [7] that, for increasing dimension, nearly all functions are nonnormal. Asymptotically, there exist Boolean functions of n variables which are not affine on any $\alpha \log_2(n)$-dimensional affine subspace for every $\alpha > 1$ (see [3]). But the question if there exist nonnormal bent functions was an open problem. For a survey on normal Boolean functions see [4].

The question of normality can be generalized to the following combinatorial problem. Given a set of bent functions $\mathscr{B}$, determine the maximal dimension $d(\mathscr{B})$ such that for all functions $f \in \mathscr{B}$ there exists a affine subspace U of dimension $d(\mathscr{B})$ such that f is constant on U.

E-mail address: gregor.leander@rub.de (G. Leander).

0166-218X/$ - see front matter © 2005 Elsevier B.V. All rights reserved.
doi:10.1016/j.dam.2005.03.027

Throughout the paper $n = 2m$ be an even number. We recall some definitions:

Definition 1. A *flat* of dimension t is a t-dimensional affine subspace.

Definition 2. Given a function $f : \mathbb{F}_2^n \to \mathbb{F}_2$, the function

$$a \in \mathbb{F}_2^n \mapsto f^w(a) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+\langle a,x\rangle}$$

is called the *Walsh transform* of f. Moreover, the $f^w(a)$, $a \in \mathbb{F}_2^n$ are called the Walsh coefficients of f.

Definition 3. A function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is called *bent* if for all $a \in \mathbb{F}_2^n$ with $a \neq 0$ the following equation holds:

$$\sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+f(x+a)} = 0.$$

This property is equivalent to the fact that all the Walsh coefficients are equal to $\pm 2^m$.

Definition 4. The dual function $\tilde{f}$ of a bent function f of $2m$ variables is the Boolean function defined by

$$f^w(a) = (-1)^{\tilde{f}(a)} 2^m.$$

The dual of a bent function is also bent.

Definition 5. A function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is called *normal* if there exists a flat of dimension m such that f is constant on this flat.

As bentness is invariant under addition of affine functions it is natural to consider a generalization of Definition 5.

Definition 6. A function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is called *weakly normal* if there exists a flat of dimension m such that the restriction of f to this flat is affine.

A function f is weakly normal if and only if there exists an element $a \in \mathbb{F}_2^n$ such that $f(x) + \langle a, x\rangle$ is normal.

The Hamming weight of a bent function f is $\sum_{x \in \mathbb{F}_2^n} f(x) = 2^{n-1} - (-1)^{\tilde{f}(0)} 2^{m-1}$. It is known that if a bent function is normal with respect to a flat U then it is balanced on all cosets of U. This implies that, if f is constant on a flat of dimension m, the value of the corresponding constant is $\tilde{f}(0)$.

The following section investigates all known families of bent functions and their normality. We prove that most functions in the main classes of bent functions (the Maiorana–McFarland class, the partial spread class and the class $\mathcal{N}$) are normal. We also prove the normality of some modified Maiorana–McFarland bent functions. In Section 3 we present the first nonnormal bent function and even a nonweakly normal bent function. As normality is defined via the *existence* of a flat fulfilling certain criteria, it is very hard to check this property, both in theory and with an algorithm. In order to decide normality of Boolean functions, we present in Section 4 an algorithm which is much faster than a naive approach would be. Finally, Section 5 contains some further applications for this algorithm.

2. Normality of the known families of bent functions

2.1. Direct constructions

Amongst all known constructions for bent functions, there exist three families which can be directly constructed (i.e., which are not derived from other bent functions): the Maiorana–McFarland class, the partial spread class and the class $\mathcal{N}$ which was introduced by Dobbertin [7].

Maiorana–McFarland functions

Definition 7. Let $\pi : \mathbb{F}_2^m \to \mathbb{F}_2^m$ be a permutation and $h : \mathbb{F}_2^m \to \mathbb{F}_2$ an arbitrary Boolean function. Then $f : \mathbb{F}_2^m \times \mathbb{F}_2^m \to \mathbb{F}_2$ with

$$f(x, y) = \langle x, \pi(y)\rangle + h(y)$$

is called a *Maiorana–McFarland function*. The set of all Maiorana–McFarland functions is denoted by $\mathscr{M}$.

All Maiorana–McFarland functions are bent. Moreover, they are obviously normal, since they are constant on the m-dimensional subspace $\mathbb{F}_2^m \times \{\pi^{-1}(0)\}$.

Partial spreads. The partial spread family, denoted by $\mathscr{PS}$, was introduced by Dillon [5]. It is defined as follows.

Definition 8. Let $\{E_i,\ i = 1, 2, \ldots, N\}$, with $N = 2^{m-1}$ or $N = 2^{m-1} + 1$, be a set of N subspaces of $\mathbb{F}_2^{2m}$ of dimension m such that $E_i \cap E_j = \{0\}$ for all $i \neq j$. The Boolean function f of $2m$ variables defined by

$$\{x \in \mathbb{F}_2^{2m},\ f(x) = 1\} = \bigcup_{i=1}^{N} E_i$$

is called a *partial spread*. Moreover, f is said to be in the class $\mathscr{PS}^+$ if $N = 2^{m-1} + 1$ and in the class $\mathscr{PS}^-$ if $N = 2^{m-1}$.

Dillon proved that all partial spreads are bent [5].

By definition, any function in the class $\mathscr{PS}^+$ is normal since it takes the value 1 on all m-dimensional subspaces E_i. The situation is different for the functions in $\mathscr{PS}^-$: they are not constant on any E_i since they vanish at 0. Determining whether there exist nonnormal and nonweakly normal functions in the class $\mathscr{PS}^-$ is still an open problem. However, this problem can be solved for a subclass of $\mathscr{PS}^-$, called $\mathscr{PS}_{ap}$, defined by Dillon [5, p. 97]. This subclass consists of all the functions of the form

$$f : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_2,$$
$$(x, y) \mapsto g(xy^{2^m-2}),$$

where g is any balanced function from $\mathbb{F}_{2^m}$ into $\mathbb{F}_2$ such that $g(0) = 0$. It is clear that all functions in $\mathscr{PS}_{ap}$ are normal since they vanish on the m-dimensional subspace $\{0\} \times \mathbb{F}_2^m$.

Class $\mathscr{N}$. A third family, called class $\mathscr{N}$, was exhibited by Dobbertin [7].

Definition 9. Let g be a balanced function from $\mathbb{F}_{2^m}$ into $\mathbb{F}_2$ and let T_g denote the affine subspace spanned by the support of its Walsh transform. Let ψ be a mapping from $\mathbb{F}_{2^m}$ to itself and ϕ be a permutation of $\mathbb{F}_{2^m}$ such that both ϕ and ψ are affine on all sets $aT,\ a \in \mathbb{F}_{2^m}^*$.

The function f defined by

$$\forall (x, y) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}, \quad f(x, \phi(y)) = \begin{cases} g\left(\dfrac{x + \psi(y)}{y}\right) & \text{if } y \neq 0 \\ 0 & \text{if } y = 0 \end{cases}$$

is said to be in *class* $\mathscr{N}$.

It is shown in [7] that all functions in $\mathscr{N}$ are bent. Moreover, family $\mathscr{N}$ contains both the Maiorana–McFarland class and the $\mathscr{PS}_{ap}$ class as extremal cases. It is obvious that any function in family $\mathscr{N}$ is normal because it vanishes on the m-dimensional space $\mathbb{F}_2^m \times \{\phi(0)\}$.

Since bentness is invariant under addition of an affine function and under right composition by an affine permutation, it is natural to consider the completions of the previous classes under these transformations. We denote by $\overline{\mathscr{B}}$ the completed version of any class $\mathscr{B}$.

Proposition 10. *All functions in* $\overline{\mathscr{PS}^+} \cup \overline{\mathscr{N}}$ *and their duals are weakly normal.*

2.2. Modified Maiorana–McFarland bent functions

Now, we focus on some bent functions derived from the Maiorana–McFarland family by adding an indicator function of a flat E and we prove their normality. In particular we are interested in functions described in [2] and below. These functions are all of the following form:

$$f : \mathbb{F}_2^m \times \mathbb{F}_2^m \to \mathbb{F}_2,$$

$$f(x, y) = \langle x, \pi(y)\rangle + h(x) + \Phi_E(x, y),$$

where $\pi : \mathbb{F}_2^m \to \mathbb{F}_2^m$ is a permutation, $h : \mathbb{F}_2^m \to \mathbb{F}_2$ is an arbitrary function and Φ_E is the characteristic function of E:

$$\Phi_E(x, y) : \mathbb{F}_2^m \times \mathbb{F}_2^m \to \mathbb{F}_2,$$

$$\Phi_E(x, y) = 1 \quad \text{if and only if} \quad (x, y) \in E.$$

For some of these functions we shall show that they are normal, or at least weakly normal.

Carlet's construction. In [2] Carlet considers only the special situation, where E is of the form $\tilde{E} \times \mathbb{F}_2^m$ for a subspace $\tilde{E}$ of $\mathbb{F}_2^m$. We denote the characteristic function $\Phi_{\tilde{E}\times\mathbb{F}_2^m}(x, y)$ just by $\phi_{\tilde{E}}(x)$ to simplify the notation.

The bent functions constructed in [2] are described in the following theorem.

Theorem 11 (*Carlet [2]*). *Let E be any linear subspace of $\mathbb{F}_2^m$, and π be a permutation on $\mathbb{F}_2^m$ such that for any element λ of $\mathbb{F}_2^m$, the set $\pi^{-1}(\lambda + E^\perp)$ is a flat. Then the function*

$$f(x, y) = \langle x, \pi(y)\rangle + \phi_E(x)$$

is bent.

It is obvious that these functions are normal, because f restricted to $\{0\} \times \mathbb{F}_2^m$ equals 1. Therefore, in order to find nonnormal bent one might consider a small appropriate generalization which also involves a function h as the general form of the Maiorana–McFarland-construction requires. It can be proved that this construction leads to bent functions in the same way as Carlet's original result.

Lemma 12. *Let E and π be as in Theorem* 11, *and h be a Boolean function on $\mathbb{F}_2^m$, such that for any element λ of $\mathbb{F}_2^m$, the function h is affine on $\pi^{-1}(\lambda + E^\perp)$. Then*

$$f(x, y) = \langle x, \pi(y)\rangle + h(y) + \phi_E(x)$$

is bent.

The next lemma shows that all these functions are still normal bent functions.

Lemma 13. *All bent functions f defined in Lemma* 12 *are normal.*

Proof. We assume w.l.o.g that $\pi(0) = 0$ and $h(0) = 0$. We first consider the case that h is not constant on $\pi^{-1}(E^\perp)$. Then, we find an element $y_0 \in \pi^{-1}(E^\perp)$, with $h(y_0) = 1$. Define the hyperplane

$$S = \{x \in \mathbb{F}_2^m : \langle x, \pi(y_0)\rangle = 1\},$$

then it is clear that $S \cap E = \emptyset$ since $\pi(y_0) \in E^\perp$. Therefore, the restriction of f to the m-dimensional flat

$$(S \times \{0\}) \cup (S \times \{y_0\})$$

is constant and equal to 0.

If h is constant on the flat $\pi^{-1}(E^\perp)$ then $f(x, y)$ is constant and equal to $1 + h(y)$ on the n-dimensional flat $E \times \pi^{-1}(E^\perp)$. □

Note that the first part of the above proof shows that actually *every* function derived from the Maiorana–McFarland family by adding an indicator function of the form $\Phi_{E\times\mathbb{F}_2^m}$ is weakly normal.

Canteaut's construction. Another class of bent functions can be derived from the Maiorana–McFarland functions by adding the indicator function of a linear subspace E of $\mathbb{F}_2^m \times \mathbb{F}_2^m$ with codimension 2. This construction is based on some properties of the derivatives of the dual function. Recall that the derivative of a Boolean function on $\mathbb{F}_2^n$, f, with respect to any direction $a \in \mathbb{F}_2^n$ is the Boolean function $D_a f : x \mapsto f(x+a) + f(x)$.

Proposition 14 (*Canteaut [1, Theorem 8]*). *Let f be a bent function of $2m$ variables, $m \geqslant 2$. Let a and b be two distinct nonzero elements of $\mathbb{F}_2^{2m}$ and $E = \langle a, b\rangle^\perp$. Then, the function $f + \Phi_E$ is bent if and only if the dual function, $\widetilde{f}$, satisfies $D_a D_b \widetilde{f} = 0$.*

Note that this result can also be deduced from [2, p. 94]. The previous proposition enables us to derive some new bent functions from the Maiorana–McFarland family. From now on, we use an explicit description of the scalar product via the trace mapping: $\mathbb{F}_2^m$ is identified with the finite field of order 2^m, $\mathbb{F}_{2^m}$, and the linear functions are the mappings $y \mapsto \mathrm{Tr}(by)$ on $\mathbb{F}_{2^m}$, where b describes $\mathbb{F}_{2^m}$ and Tr is the trace function from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$. The scalar product of two elements x and y then corresponds to $\mathrm{Tr}(xy)$. As an example, the following corollary exhibits a bent function obtained from the Maiorana–McFarland family by the construction described in Proposition 14.

Corollary 15. *Let $m = gk$ where g is odd and $k > 1$. Let*

$$s = 1 + \sum_{i=0}^{((g-1)/2)-1} (2^k - 1)2^{(2i+1)k}.$$

Let α, β and λ be three nonzero elements in $\mathbb{F}_{2^m}$ such that α has order (2^k-1), $\mathrm{Tr}(\beta^2(\alpha^2+\alpha))=0$ and $\mathrm{Tr}(\lambda(\alpha^2+\alpha))=0$. Let $x, y \in \mathbb{F}_{2^m}$, then the $2m$-variable function

$$g(x, y) = \mathrm{Tr}(xy^s) + \mathrm{Tr}(\lambda y^{3s}) + \mathrm{Tr}(x + \beta y)\,\mathrm{Tr}(\alpha x + \alpha^{2^{k-1}}\beta y)$$

is bent and does not belong to the completed version of the Maiorana–McFarland family.

Proof. Let f be the $2m$-variable bent function in the Maiorana–McFarland family defined by

$$f(x, y) = \mathrm{Tr}(xy^s) + \mathrm{Tr}(\lambda y^{3s}).$$

Let $a = (1, \beta)$, $b = (\alpha, \alpha^{2^{k-1}}\beta)$ and $V = \langle a, b\rangle^\perp$. From Proposition 14, we deduce that g is bent if and only if $D_a D_b \widetilde{f} = 0$. Let $x \mapsto x^d$ be the inverse of $x \mapsto x^s$ over $\mathbb{F}_{2^m}$, i.e. $d = 2^{m-1} + 2^{k-1}$. The dual $\widetilde{f}$ of f is given by [5, p. 91]:

$$\widetilde{f}(x, y) = \mathrm{Tr}(x^d y) + \mathrm{Tr}(\lambda (x^d)^{3s}) = \mathrm{Tr}(x^d y) + \mathrm{Tr}(\lambda x^3).$$

By hypothesis, we have

$$D_a D_b\,\mathrm{Tr}(\lambda x^3) = D_1 D_\alpha\,\mathrm{Tr}(\lambda x^3) = \mathrm{Tr}(\lambda(\alpha^2 + \alpha)) = 0.$$

Hence, we obtain

$$\begin{aligned} D_a D_b \widetilde{f}(x, y) = {} & \mathrm{Tr}(y((x+\alpha+1)^d + (x+\alpha)^d + (x+1)^d + x^d)) \\ & + \mathrm{Tr}(\beta((x+\alpha+1)^d + (x+1)^d)) \\ & + \mathrm{Tr}(\alpha^{2^{k-1}}\beta((x+\alpha+1)^d + (x+\alpha)^d)). \end{aligned}$$

The first term in the previous expression vanishes since

$$\begin{aligned} (x+\alpha+1)^d + (x+\alpha)^d + (x+1)^d + x^d &= (\alpha+1)^d + \alpha^d + 1 \\ &= \alpha^{2^{m-1}} + \alpha^{2^{k-1}} \\ &= (\alpha + \alpha^{2^k})^{2^{m-1}} = 0, \end{aligned}$$

because α has order (2^k-1). It follows that

$$\begin{aligned} D_a D_b \widetilde{f}(x,y) &= \mathrm{Tr}(\beta(\alpha^{2^{k-1}} x^{2^{m-1}} + \alpha^{2^{m-1}} x^{2^{k-1}} + \alpha^{2^{m-1}+2^{k-1}} + \alpha^{2^{m-1}} + \alpha^{2^{k-1}})) \\ &\quad + \mathrm{Tr}(\alpha^{2^{k-1}} \beta(x^{2^{m-1}} + x^{2^{k-1}} + \alpha^{2^{m-1}} + \alpha^{2^{k-1}} + 1)) \\ &= \mathrm{Tr}(\beta(\alpha^{2^{m-1}+2^{k-1}} + \alpha^{2^{k-1}})) = \mathrm{Tr}(\beta(\alpha^{2^k} + \alpha^{2^{k-1}})) \\ &= \mathrm{Tr}(\beta^2(\alpha^2+\alpha)) = 0. \end{aligned}$$

Therefore, $D_a D_b \widetilde{f} = 0$, implying that g is bent.

Now, g belongs to $\overline{\mathscr{M}}$ if and only if there exists an m-dimensional subspace $U \subset \mathbb{F}_2^{2m}$ such that $D_u D_v g = 0$ for any $u, v \in U$ [5, p. 102]. We can prove that $U = \mathbb{F}_2^m \times \{0\}$ does not satisfy this condition. Thus, if g belongs to $\overline{\mathscr{M}}$, there exist two nonzero distinct elements $u, v \in \mathbb{F}_2^{2m}$ with $u \notin \mathbb{F}_2^m \times \{0\}$ such that $D_u D_v g = D_u D_v f + D_u D_v \Phi_V = 0$. This implies that $D_u D_v f$ is constant on $\mathbb{F}_2^{2m}$. By computing $D_u D_v f$, we deduce that the function $D_u D_v f$ is constant only if there exist $\mu, \nu \in \mathbb{F}_{2^m}^*$, $\mu \neq \nu$, such that

$$(x+\mu+\nu)^s + (x+\mu)^s + (x+\nu)^s + x^s = 0, \quad \forall x \in \mathbb{F}_{2^m},$$

or if there exist $\mu, \nu \in \mathbb{F}_{2^m}^*$ such that

$$x \mapsto \mathrm{Tr}(\mu((x+\nu)^s + x^s))$$

is constant on $\mathbb{F}_{2^m}$. Using the expression for s, we can then prove that none of these conditions is satisfied (see e.g. [1, Corollary 6]). □

However, we can prove that any function derived from the Maiorana–McFarland family by adding the indicator function of a linear subspace of codimension 2, as described in Proposition 14, is normal.

Lemma 16. *Let π be a permutation on $\mathbb{F}_2^m$ and ξ_i be arbitrary Boolean functions on $\mathbb{F}_2^m$. For any nonzero α and β in $\mathbb{F}_{2^m}$, $\alpha \neq \beta$, the function*

$$g(x,y) = \mathrm{Tr}(x\pi(y)) + \mathrm{Tr}(\alpha x)\,\mathrm{Tr}(\beta x) + \xi_1(y)\,\mathrm{Tr}(\alpha x) + \xi_2(y)\,\mathrm{Tr}(\beta x) + \xi_3(y)$$

is normal.

Proof. Let

$$E = \{x \in \mathbb{F}_{2^m} : \ \mathrm{Tr}(x) = \mathrm{Tr}(\alpha x) = 0\} = \langle 1, \alpha \rangle^{\perp}.$$

The function g restricted to $y \in \pi^{-1}(E^{\perp})$ can be represented as

$$g(x,y)_{|\mathbb{F}_2^m \times \pi^{-1}(E^{\perp})} = \mathrm{Tr}(\alpha x)\,\mathrm{Tr}(\beta x) + \xi_1(y)\,\mathrm{Tr}(\alpha x) + \xi_2(y)\,\mathrm{Tr}(\beta x) + \xi_3(y)$$

by changing the functions ξ_i appropriately.

For a fixed $y \in \pi^{-1}(E^{\perp})$ we denote $g_y(x) := g(x,y)$. The support of g_y is either a coset of E or the complement of a coset of E. We have

$$E^{\perp} = \{0, \alpha, \beta, \alpha+\beta\}.$$

Thus, there are four possibilities to choose y. At least for two different values y_0 and y_1 the supports of g_{y_0} and of g_{y_1} have the same size. W.l.o.g we assume that the size of the support of g_{y_0} and g_{y_1} is $\#E$. Now, it follows that $g_{y_0}(x) = g_{y_1}(x) = 0$ for x in the affine hyperplane $(c_0 + E) \cup (c_1 + E)$, where the $c_i + E$, $i = 0, 1$ are different cosets of E. Hence g is constant on the m-dimensional flat

$$\{(c_0 + E) \cup (c_1 + E)\} \times \{y_0, y_1\}. \qquad \square$$

Theorem 17. *Let π be a permutation of $\mathbb{F}_2^m$ and h be an arbitrary Boolean function on $\mathbb{F}_2^m$. Let E be a linear subspace of $\mathbb{F}_2^m \times \mathbb{F}_2^m$ of codimension 2 such that*

$$f(x, y) = \mathrm{Tr}(x\pi(y)) + h(y) + \Phi_E(x, y)$$

is bent. Then f is normal.

Proof. Let $E = \langle(\alpha_1, \alpha_2), (\beta_1, \beta_2)\rangle^{\perp}$. If $\dim\langle\alpha_1, \beta_1\rangle < 2$, then f belongs to the Maiorana–McFarland class, implying that it is normal. Actually, a bent function f of $2m$ variables belongs to $\overline{\mathscr{M}}$ if and only if there exists an m-dimensional subspace $V \subset \mathbb{F}_2^{2m}$ such that $D_a D_b f = 0$ for any $(a, b) \in V$ [5, p. 102]. Here, we obviously have that $D_a D_b f = 0$ for any $a, b \in \mathbb{F}_2^m \times \{0\}$.

Now, if α_1 and β_1 are two nonzero distinct elements of $\mathbb{F}_2^m$, f corresponds to the sum of $\mathrm{Tr}(x\pi(y))+\mathrm{Tr}(\alpha_1 x)\,\mathrm{Tr}(\beta_1 x)+\xi_1(y)\,\mathrm{Tr}(\alpha_1 x) + \xi_2(y)\,\mathrm{Tr}(\beta_1 x) + \xi_3(y)$ and a linear mapping. From the previous lemma, we deduce that f is normal. □

3. Nonnormal bent functions

Here, we exhibit some examples of nonnormal and even nonweakly normal bent functions. One set of functions that turns out to include nonnormal functions is the class of the Kasami functions. This class of bent functions was found by Dobbertin and Dillon in [6] and some of the functions in this class seemed to be good candidates for nonnormal bent functions.

The Kasami functions are defined as follows:

Definition 18. Let $d=2^{2k}-2^k+1$ with $\gcd(k, n)=1$ and $\alpha \in \mathbb{F}_{2^n}$. Then, we call $f_{\alpha,k} : \mathbb{F}_{2^n} \to \mathbb{F}_2$ with $f_{\alpha,k}(x)=\mathrm{Tr}(\alpha x^d)$ a Kasami function.

Under some conditions these functions are bent.

Theorem 19 (*Dillon and Dobbertin [6]*). *Let k and $f_{\alpha,k}$ be as in Definition* 18. *If n is not divisible by* 3 *and $\alpha \notin \{x^3 \mid x \in \mathbb{F}_{2^n}\}$ then $f_{\alpha,k}$ is bent.*

For some values of n it is possible to show that the Kasami functions are always normal.

Lemma 20. *Let $n = 2m$ with m even. The Kasami power functions*

$$f : \mathbb{F}_{2^n} \to \mathbb{F}_2$$

$$x \mapsto \mathrm{Tr}(\alpha x^d)$$

are normal.

Proof. First note that $\gcd(d, 2^n - 1) = 3$, i.e.,

$$U = \{x^d \mid x \in \mathbb{F}_{2^n}^*\} = \{x^3 \mid x \in \mathbb{F}_{2^n}^*\}$$

and there exist $\lambda_1, \lambda_2 \notin U$ such that

$$\mathbb{F}_{2^n}^* = U \cup \lambda_1 U \cup \lambda_2 U.$$

In the case where $4 \mid n$, we will show that λ_1, λ_2 can be chosen in $\mathbb{F}_{2^m}$. It is sufficient to show that there exists $x \in \mathbb{F}_{2^m}$ such that $x \notin U$. Let g be a generator of $\mathbb{F}_{2^m}$. g is in U if and only if $g^{(2^n-1)/3} = 1$. But

$$\begin{aligned} g^{(2^n-1)/3} &= g^{(2^m-1)(2^m+1)/3} \\ &= g^{(2^m+1)((2^m-1)/3)} \neq 1 \end{aligned}$$

as 2^m+1 is not divisible by 3 if m is even. So we can choose $\lambda_1 = g$ and $\lambda_2 = g^2$. Note that if $\alpha' = \alpha c^d$ for some $c \in \mathbb{F}_{2^n}^*$ then $f_{\alpha,k}(cx) = f_{\alpha',k}(x)$ for all $x \in \mathbb{F}_{2^n}$. Thus, we can assume that α is in $\{1, g, g^2\} \subset \mathbb{F}_{2^m}$. So for $x \in \mathbb{F}_{2^m}$ we get

$$\begin{aligned} f_{\alpha,k}(x) &= \mathrm{Tr}(\alpha x^d) \\ &= \mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_2}(\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^m}}(\alpha x^d)) \\ &= \mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_2}(\alpha x^d \,\mathrm{Tr}_{\mathbb{F}_{2^n}/\mathbb{F}_{2^m}}(1)) \\ &= 0. \end{aligned}$$

This proves the lemma. □

So we can only hope to get nonnormal Kasami functions for m odd. Furthermore, as all quadratic bent functions are normal, only the case $k \neq 1$ is interesting. As it is known that all bent functions on $\mathbb{F}_2^6$ are normal, the first possibility for a Kasami function to be nonnormal is $n = 10$.

We found out that for $n = 10$ all the Kasami functions are normal but by addition of a linear function they can be modified into nonnormal functions.

Fact 21. *Let $\alpha \in \mathbb{F}_4 \backslash \mathbb{F}_2 \subset \mathbb{F}_{2^{10}}$. Then there exists $\beta \in \mathbb{F}_{2^{10}}$ such that the function $f : \mathbb{F}_{2^{10}} \to \mathbb{F}_2$ with*

$$f(x) = \mathrm{Tr}(\alpha x^{57} + \beta x)$$

is nonnormal.

Verification. This can be verified using the algorithm described in Section 4. □

Furthermore, we found that for $n = 14$ and $k = 3$ the corresponding Kasami functions are nonweakly normal.

Fact 22. *Let $\alpha \in \mathbb{F}_4 \backslash \mathbb{F}_2 \subset \mathbb{F}_{2^{14}}$. The function $f : \mathbb{F}_{2^{14}} \to \mathbb{F}_2$ with*

$$f(x) = \mathrm{Tr}(\alpha x^{57})$$

is nonweakly normal.

Verification. By using the algorithm described in Section 4. □

These results are verified with a computer algorithm, proving these results theoretically is still an open problem. We state the following conjecture.

Conjecture 23. *All nonquadratic Kasami functions on $\mathbb{F}_{2^{2m}}$ with m odd and $m \geqslant 7$ are nonweakly normal.*

Corollary 24. *The Kasami bent function $f : \mathbb{F}_{2^{14}} \to \mathbb{F}_2$ defined by*

$$f(x) = \mathrm{Tr}(\alpha x^{57})$$

with $\alpha \in \mathbb{F}_4 \backslash \mathbb{F}_2 \subset \mathbb{F}_{2^{14}}$ and its dual do not belong to

$$\overline{\mathscr{PS}} \cup \overline{\mathscr{N}}.$$

Proof. We know from Proposition 10 that all functions in $\overline{\mathscr{PS}^+} \cup \overline{\mathscr{N}}$ are weakly normal. Thus, the only remaining case is family $\mathscr{PS}^-$. But, any function in $\mathscr{PS}^-$ of $2m$ variables has degree m since its restrictions to some m-dimensional subspaces have an odd weight. It follows that f does not belong to the completed class $\mathscr{PS}^-$ because its algebraic degree is equal to 4. The same argument is valid for the dual function since the dual of a bent function of $2m$ variables of degree m has degree m [5, p. 80]. □

Now, we show how to construct nonweakly normal bent functions of n variables for all even $n \geqslant 14$. The following lemma is a generalization of Theorem 4.5 of [8].

Lemma 25. *Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a Boolean function. The following properties are equivalent*:

(1) *f is (weakly) normal.*
(2) *The function*

$$g : \mathbb{F}_2^n \times \mathbb{F}_2 \times \mathbb{F}_2 \to \mathbb{F}_2$$
$$(x, y, z) \mapsto f(x) + yz$$

is (weakly) normal.

Proof. (1) $\Rightarrow$ (2): We assume that f is normal, i.e., there exists a $n/2$ dimensional flat E, such that $f|_E$ is constant. We define

$$E' = (E \times \{0\} \times \{0\}) \cup (E \times \{1\} \times \{0\})$$

which is a $(n+2)/2$ dimensional flat. It is easy to see that $g|_{E'}$ is constant, i.e., g is normal. Furthermore, if f is affine on E then g is affine on E'.

(1) $\Leftarrow$ (2): Now, we assume that g is weakly normal, i.e., there exists a $(n+2)/2$ dimensional flat E, $\gamma \in \mathbb{F}_2^n$ and $\alpha, \beta \in \mathbb{F}_2$ such that

$$h(x, y, z) = g(x, y, z) + \alpha y + \beta z + \langle \gamma, x \rangle$$

takes the same value, c, on E. We claim that $f(x) + \langle \gamma, x \rangle$ is normal.

For $a, b \in \mathbb{F}_2$ we define $E_{ab} = \{x \in \mathbb{F}_2^n \mid (x, a, b) \in E\}$. Then $f(x) + \langle \gamma, x \rangle$ is constant on all flats E_{ab}. If one of the flats E_{ab} has dimension $\geqslant n/2$ we are done. If this is not true, all the flats E_{ab} have dimension $(n/2) - 1$. Furthermore, since the union of all E_{ab} is a flat, all E_{ab} are cosets of the same subspace U: $E_{ab} = U + x_{ab}$. Moreover, $x_{\alpha\bar{\beta}} \neq x_{\bar{\alpha}\beta}$. Otherwise, for any element $(x, \bar{\alpha}, \beta)$ in E, $(x, \alpha, \bar{\beta})$ belongs to E. Then, if we consider two elements $(x, \bar{\alpha}, \beta)$ and (x', α, β) in E, we obtain that

$$(x, \bar{\alpha}, \beta) + (x, \alpha, \bar{\beta}) + (x', \alpha, \beta) = (x', \bar{\alpha}, \bar{\beta})$$

belongs to E. Thus, both (x', α, β) and $(x', \bar{\alpha}, \bar{\beta})$ lie in E, implying that $h(x', \alpha, \beta) = h(x', \bar{\alpha}, \bar{\beta})$. But,

$$\begin{aligned} h(x', \bar{\alpha}, \bar{\beta}) &= f(x') + \bar{\alpha}\bar{\beta} + \alpha\bar{\alpha} + \beta\bar{\beta} + \langle \gamma, x' \rangle \\ &= f(x') + \alpha\beta + \alpha + \beta + 1 + \langle \gamma, x' \rangle = h(x', \alpha, \beta) + 1, \end{aligned}$$

which leads to a contradiction. Therefore, since $x_{\alpha\bar{\beta}} \neq x_{\bar{\alpha}\beta}$, the set $E_{\alpha\bar{\beta}} \cup E_{\bar{\alpha}\beta}$ is a flat of dimension $n/2$. Moreover, we have

$$\forall x \in E_{\alpha\bar{\beta}}, \quad f(x) + \langle \gamma, x \rangle = c + \alpha\bar{\beta} + \alpha + \beta\bar{\beta} = c + \alpha\beta,$$

$$\forall x \in E_{\bar{\alpha}\beta}, \quad f(x) + \langle \gamma, x \rangle = c + \bar{\alpha}\beta + \alpha\bar{\alpha} + \beta = c + \alpha\beta,$$

implying that $f(x) + \langle \gamma, x \rangle$ is constant on $E_{\alpha\bar{\beta}} \cup E_{\bar{\alpha}\beta}$. The special case $\gamma = 0$ and $\alpha = \beta = 0$ shows that if g is normal then f is normal as well. □

Thus, given a nonnormal function f with n variables Lemma 25 can be used to construct a nonnormal function with $n + 2$ variables.

According to this procedure applied recursively, if f is a Boolean function on $\mathbb{F}_2^n$ and if f' is a quadratic bent function on $\mathbb{F}_2^{n'}$, then f is (weakly) normal if and only if $g(x, y) = f(x) + f'(y)$ is (weakly) normal. The question if this is true for any normal bent function f' is still open. An important observation from our point of view is that, if the function f in the above lemma is bent, then g is also bent.

With Facts 21 and 22 we get:

Fact 26. *There exist nonnormal bent functions of n variables for all even $n \geqslant 10$ and nonweakly normal bent functions for all even $n \geqslant 14$.*

From Corollary 24, we deduce that for any even $n \geqslant 14$, the bent functions of n variables obtained by recursively applying Lemma 25 to the Kasami function of 14 variables (and their duals) do not belong to $\overline{\mathscr{PS}} \cup \overline{\mathscr{N}}$.

4. Checking normality efficiently

Checking (weak) normality of a function usually needs one to take into account all flats of dimension m to check whether f is constant (affine) on one of them. One possible but rather complex way of doing this would be to do an exhaustive search on all flats of dimension m.

In this section we present an algorithm, which, given a Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$, is able to compute a list of all flats of dimension m of $\mathbb{F}_2^n$ on which f is affine in much less time than needed for an exhaustive search.

Additionally, besides checking normality this algorithm can also be used to check whether a given bent function is a Maiorana–McFarland or a partial-spread bent function, as it is described in Section 5.

4.1. General idea

The main idea of the algorithm presented here is to make use of the fact that a Boolean function which is affine on a flat A is also affine on all flats contained in A.

Even more the function is either constant on A and hence constant on all flats contained in A or we can find two flats $A_0, A_1 \subset A$ with $\dim(A_0) = \dim(A_1) = \dim(A) - 1$ and $A = A_0 \cup A_1$ such that the function is 0 on A_0 and 1 on A_1. In the latter case, of course, the function is also constant on all flats of A_0 and A_1, respectively.

Hence, it suffices for a given Boolean function, first to determine the flats of a "small" dimension t_0 on which the function is constant and then to combine these spaces to get those flats of dimension m on which the function is affine.

Therefore, the general structure of the algorithm can be described as follows:

Algorithm 1.

Input: *a Boolean function* $f : \mathbb{F}_2^n \to \mathbb{F}_2$, *a starting dimension* t_0
Output: *a list of all flats of dimension* m *on which* f *is affine*
For all *subspaces* U *of* $\mathbb{F}_2^n$ *with* $\dim(U) = t_0$ **do**

Determine *all flats* $a + U$ *with* $f|_{a+U} = 0$ *and* $f|_{a+U} = 1$ *resp.*
Combine *pairs* $(a_1 + U, a_2 + U)$
with $f|_{a_1+U} = f|_{a_2+U} = 0$ (*resp. with* $f|_{a_1+U} = f|_{a_2+U} = 1$)
to get flats $a_1 + \tilde{U} = a_1 + \langle U, a_1 + a_2 \rangle$ *of dimension* $t_0 + 1$
such that $f|_{a_1+\tilde{U}} = 0$ (*resp.* $f|_{a_1+\tilde{U}} = 1$)
Repeat *the last step for new flats with equal* $\tilde{U}$ *up to dimension* $m - 1$
Combine *pairs of flats* $(a_1 + \hat{U}, a_2 + \hat{U})$ *with* $\dim(\hat{U}) = m - 1$
(*independent of whether* $f|_{a_i+\hat{U}}$ *is* 0 *or* 1)
to get those flats of dimension m *on which* f *is affine*
Output *these flats of dimension* m

To implement this algorithm efficiently and prove the correctness of the optimized version, we first have to make some definitions.

4.2. Definitions and notation

In this section we represent vectors $u \in \mathbb{F}_2^n$ as n-tuples $u = (u_1, \ldots, u_n)$, $u_i \in \mathbb{F}_2$, we denote the index of the leftmost 1 in this representation by

$$v(u) := \max\{i \in \{1, \ldots, n+1\} \mid u_j = 0 \text{ for } 1 \leqslant j < i\}$$

and for a vector space $U \subseteq \mathbb{F}_2^n$ we define $\Upsilon(U) := \{v(u) \mid u \in U \backslash \{0\}\}$.

By using the standard lexicographical ordering $<$ on $\mathbb{F}_2^n$, i.e.

$$u > v \quad \Leftrightarrow \quad \begin{array}{l} v(u) < v(v) \quad \text{or} \\ (v(u) = v(v) \quad \text{and} \quad ((u_{v(u)+1}, \ldots, u_n) > (v_{v(v)+1}, \ldots, v_n)) \end{array}$$

we can define a unique representation of subspaces $U \subseteq \mathbb{F}_2^n$:

Definition 27. An ordered basis $u_1, \ldots, u_k \in \mathbb{F}_2^n$ of U is called a Gauss–Jordan basis (GJB) if

$$u_1 > \cdots > u_k \quad \text{and} \quad (u_j)_{v(u_i)} = 0 \quad \forall i \neq j.$$

Lemma 28. *For each vector space $U \subseteq \mathbb{F}_2^n$ there is one unique GJB.*

Using the lexicographical ordering is also very efficient for implementations as it corresponds directly to the natural ordering on the integers that we get by considering $(u_1, \ldots, u_n)$ as the binary representation of $\sum_{i=1}^n u_i \cdot 2^{n-i}$.

With the notation of $v(u)$ we can also define the complement $\bar{U}$ of a vector space U as

$$\bar{U} := \{a \in \mathbb{F}_2^n \mid a_i = 0 \ \forall i \in \Upsilon(U)\}$$

and it is obvious that $U \cap \bar{U} = \{0\}$ and thus $U \oplus \bar{U} = \mathbb{F}_2^n$ because of dimensional reasons. So all flats of the form $a + U$ can be uniquely represented as $\bar{a} + U$ with $\bar{a} \in \bar{U}$.

4.3. Details of the algorithm

The main data structure of the presented algorithm is the list of all flats of the form $a + U$ (for a given U) on which the given function f is constant:

Definition 29. Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$, $u_1, \ldots, u_k \in \mathbb{F}_2^n$ and $c \in \{0, 1\}$. If $(u_1, \ldots, u_k)$ is a GJB of U then let

$$\mathscr{C}_c^{u_1,\ldots,u_k}(f) := \{a \in \bar{U} \mid f|_{a+U} = c\}$$

and $\mathscr{C}_c^{u_1,\ldots,u_k}(f) := \emptyset$ otherwise.

Using the ideas of Section 4.1 and the notation of a GJB in order to get each flat only once, we obtain the following relation between lists belonging to different dimensional spaces:

Lemma 30. *For $f, u_1, \ldots, u_k, c$ as in Definition* 29 *and for all $a, b \in \mathbb{F}_2^n$ the following equivalence holds*:

$$\left.\begin{array}{l} a, b \in \mathscr{C}_c^{u_1,\ldots,u_k}(f) \\ a < b, \quad a + b < u_k \\ u_{i,v(a+b)} = 0 \quad \textit{for } 1 \leqslant i \leqslant k \end{array}\right\} \iff a \in \mathscr{C}_c^{u_1,\ldots,u_k,a+b}(f).$$

As for every $a \in \mathscr{C}_c^{u_1,\ldots,u_{k+1}}(f)$ we can write $b = a + u_{k+1}$ with $a \in \mathscr{C}_c^{u_1,\ldots,u_k,a+b}(f)$, this lemma gives a criterion on how to determine all $\mathscr{C}_c^{u_1,\ldots,u_{k+1}}(f)$ for different u_{k+1} if we know $\mathscr{C}_c^{u_1,\ldots,u_k}(f)$.

This can be done even more efficiently by using the following two ideas.

We can avoid the $a < b$ checks and many $a + b < u_k$ checks by storing the elements of $\mathscr{C}$ in a sorted list. Checking $u_{i,v(a+b)} = 0$ can be done more efficiently if we once evaluate $\hat{u} := \bigvee_{i=1}^k u_i$ (where $\vee$ means the componentwise OR of the vectors u_i, i.e. $\hat{u}_j = \max_{i=1}^k ((u_i)_j)$) and then only check if $\hat{u}_{v(a+b)} = 0$.

Another useful criterion to make the computation more efficient is given by the following corollary:

Corollary 31. *For $f : \mathbb{F}_2^n \to \mathbb{F}_2$, $u_1, \ldots, u_k \in \mathbb{F}_2^n$, $c \in \{0, 1\}$ and $l \in \{1, \ldots, k-1\}$ it holds that*

$$|\mathscr{C}_c^{u_1,\ldots,u_{k-l}}(f)| \geqslant 2^l \cdot |\mathscr{C}_c^{u_1,\ldots,u_k}(f)|.$$

Proof. We show that $|\mathscr{C}_c^{u_1,\ldots,u_{k-1}}(f)| \geqslant 2 \cdot |\mathscr{C}_c^{u_1,\ldots,u_k}(f)|$ (then the claim follows at once). Let $\mathscr{C}_c^{u_1,\ldots,u_k}(f) = \{a_1, \ldots, a_r\}$.

Define $b_i := a_i + u_k$ and by Lemma 30 it follows that $a_i, b_i \in \mathscr{C}_c^{u_1,\ldots,u_{k-1}}(f)$ and that all $a_1, \ldots, a_r, b_1, \ldots, b_r$ are distinct as otherwise we get one of the following contradictions:

$$b_i = b_j \;\Rightarrow\; a_i = b_i + u_k = b_j + u_k = a_j$$

$$a_i = b_j \;\Rightarrow\; u_k = a_j + b_j = a_j + a_i \in \bar{U}. \qquad \square$$

Similarly to Lemma 30 we get the following relations between the flats of dimension m on which f is affine and the lists $\mathscr{C}_c^{u_1,\ldots,u_{m-1}}(f)$ corresponding to dimension $m-1$:

Lemma 32. *Let $a + U \subset \mathbb{F}_2^n$ be a flat of dimension m. Then the following statements are equivalent*:

(1) $f|_{a+U}$ *is affine*
(2) $f|_{a+U}$ *is constant or*

$$\left.\begin{array}{l}\exists \text{ subspace } U' \subset U : \dim(U') = m-1\\ \exists\, \tilde{u} \in U \backslash U' : U = U' \dot\cup (\tilde{u} + U')\\ \exists\, c \in \{0,1\}\end{array}\right\} \text{ such that } \left\{\begin{array}{l} f|_{a+U'} = c\\ f|_{a+\tilde{u}+U'} = 1-c\end{array}\right.$$

(3) $\exists$subspace $U' \subset U : \dim(U') = m-1$ with GJB $u_1, \ldots, u_{m-1}$

$$\exists a' \in a + U', b' \in (a+U)\backslash(a+U')$$

such that $a', b' \in \cup_{c\in\{0,1\}} \mathscr{C}_c^{u_1,\ldots,u_{m-1}}(f)$

Proof. "(1) $\Rightarrow$ (2)" Assume that $f|_{a+U}$ is not constant. Then with a basis $u_1, \ldots, u_m$ of U we have $f(a + \sum_i \lambda_i u_i) = \sum_i \lambda_i \mu_i + c$ with some $\mu \in \mathbb{F}_2^m \backslash \{0\}$ and $c \in \mathbb{F}_2$ and (2) is fulfilled with $U' := \{\sum_i \lambda_i u_i \mid \lambda \cdot \mu = 0\}$.

"(2) $\Rightarrow$ (3)" If $f|_{a+U}$ is constant and equal to c, choose $U' \subset U$ with dimension $m-1$ and $\tilde{u} \in U \backslash U'$. Then we have $U = U' \dot\cup (\tilde{u} + U')$ and $f|_{a+U'} = f|_{a+\tilde{u}+U'} = c$.

In any case (3) follows by choosing $a' := a + \sum a_{v(u_i)} u_i$ and $b' := a + \tilde{u} + \sum (a+\tilde{u})_{v(u_i)} u_i$ where $(u_1, \ldots, u_{m-1})$ is the GJB of U'.

"(3) $\Rightarrow$ (1)" Let $a' \in \mathscr{C}_{c_a}^{u_1,\ldots,u_{m-1}}(f)$ and $b' \in \mathscr{C}_{c_b}^{u_1,\ldots,u_{m-1}}(f)$. Then $U = \langle u_1, \ldots, u_{m-1}, a' + b' \rangle$ and with $x = a + \sum_i \lambda_i u_i + \lambda_m (a' + b')$ if follows that

$$f(x) = \left\{\begin{array}{ll} c_a & \text{if } \lambda_m = 0\\ c_b & \text{if } \lambda_m = 1\end{array}\right\} = (1-\lambda_m)\cdot c_a + \lambda_m \cdot c_b = \lambda_m \cdot (c_b - c_a) + 1$$

is affine. $\square$

This lemma shows that, in order to find all flats on which f is affine, it suffices to compute the lists $\mathscr{C}_c^{u_1,\ldots,u_{m-1}}$ for GJBes of all subspaces of dimension $m-1$.

Together with Corollary 31 we can conclude that having computed $\mathscr{C}_c^{u_1,\ldots,u_k}(f)$, $c \in \{0,1\}$, we only have to consider pairs of elements of these lists if

$$|\mathscr{C}_c^{u_1,\ldots,u_k}(f)| \geqslant 2^{m-k}$$

or

$$(|\mathscr{C}_c^{u_1,\ldots,u_k}(f)| \geqslant 2^{m-k-1} \text{ and } |\mathscr{C}_{1-c}^{u_1,\ldots,u_k}(f)| \geqslant 2^{m-k-1}),$$

otherwise there is no chance to find a flat on which f is affine by considering lists of the form $\mathscr{C}_c^{u_1,\ldots,u_k,\tilde{u}_{k+1},\ldots,\tilde{u}_{m-1}}(f)$.

As described in Section 4.1 the main idea of the algorithm is to begin with a starting dimension t_0 and to compute the lists $\mathscr{C}_c^{u_1,\ldots,u_{t_0}}(f)$ which we need just by enumerating all corresponding flats and checking directly. Then the lists corresponding to higher dimensions can be generated recursively as described in Lemma 30.

So what we need to complete the algorithm is an efficient way to enumerate all initial parts $u_1, \ldots, u_{t_0}$ of GJBes of subspaces of dimension $m-1$.

Table 1
Enumerating all GJBes

		1	$\dots$	v_1	$\dots$	v_2	$\dots$	v_3	$\dots$	v_{t_0}	$\dots n$
u_1	$=$	0	$\dots$	1	$\langle z_{1,1}\rangle_2$	0	$\langle z_{1,2}\rangle_2$	0	$\dots$	0	$\langle z_{1,t_0}\rangle_2$
u_2	$=$	0	$\dots$		$\dots$	1	$\langle z_{2,2}\rangle_2$	0	$\dots$	0	$\langle z_{2,t_0}\rangle_2$
u_3	$=$	0	$\dots$				$\dots$	1	$\dots$	0	$\langle z_{3,t_0}\rangle_2$
									$\ddots$	$\vdots$	$\vdots$
u_{t_0}	$=$	0	$\dots$						$\dots$	1	$\langle z_{t_0,t_0}\rangle_2$

If we take a look at the definition of a GJB it is obvious that this can easily be done by looping over all increasing sequences

$$1 \leqslant v_1 < v_2 < \cdots < v_{t_0} \leqslant m + 1 + t_0$$

and all integers $z_{i,j} \in \{0, \dots, 2^{v_{j+1}-v_j-1} - 1\}$ with $1 \leqslant i \leqslant t_0$, $i \leqslant j \leqslant t_0$ and defining

$$(u_i)_j = \begin{cases} 0 & \text{if } j < v_i \text{ or } j \in \{v_{i+1}, \dots, v_{t_0}\} \\ 1 & \text{if } j = v_i \end{cases}$$

and filling in the gaps with the binary representations $\langle z_{i,j}\rangle_2$ of the integers $z_{i,j}$ as shown in Table 1 .

Additionally, we only have to consider such sets $u_1, \dots, u_{t_0}$ for which

$$\left| \left\{ j > v_{t_0} \;\middle|\; \max_{i=1}^{t_0} (u_i)_j = 1 \right\} \right| \leqslant m - v_{t_0} + 1 + t_0,$$

as otherwise it cannot be completed to a GJB of dimension $m - 1$.

Finally, we just have to enumerate all $a \in \bar{U}$ for $U = \langle u_1, \dots, u_{t_0}\rangle$. This can be done similarly to the enumeration of the u_i themselves just by setting $a_{v_i} = 0$ for $i = 1, \dots, t_0$ and filling in the gaps with all possible binary representations of integers.

So the whole algorithm can be described as follows (some of the ideas described above to make the algorithm even more efficient—e.g. storing the $\mathscr{C}$s in sorted order—are omitted in order to make this description more readable, but they are easily implemented into this algorithm):

Algorithm 2.

Input: *a Boolean function* $f : \mathbb{F}_2^n \to \mathbb{F}_2$, *a starting dimension* t_0
Output: *a list of all flats on which* f *is affine*
For all *GJBes* $u_1, \dots, u_{t_0}$

with $|\{j > v_{t_0} | \max_{i=1}^{t_0} (u_i)_j = 1\}| \leqslant m - v_{t_0} + 1 + t_0$ **do**
For all $a \in \overline{\langle u_1, \dots, u_{t_0}\rangle}$ **do**
If $f(a + \sum \lambda_i \cdot u_i) = c \forall\ \lambda \in \mathbb{F}_2^{t_0}$ **Then** *append* a *to* $\mathscr{C}_c^{u_1,\dots,u_{t_0}}$
Combine$(\mathscr{C}_0^{u_1,\dots,u_{t_0}}, \mathscr{C}_1^{u_1,\dots,u_{t_0}}, (u_1, \dots, u_{t_0}), t_0)$
using the recursive subroutine

Combine$(\mathscr{C}_0, \mathscr{C}_1, (u_1, \dots, u_k), k)$:

If $(k < m - 1)$
Then
If $(|\mathscr{C}_0| < 2^{m-k-1}$ *or* $(|\mathscr{C}_0| < 2^{m-k}$ *and* $|\mathscr{C}_1| < 2^{m-k-1}))$ **Then** $\mathscr{C}_0 := \emptyset$

If $(|\mathscr{C}_1| < 2^{m-k-1}$ *or* $(|\mathscr{C}_1| < 2^{m-k}$ *and* $|\mathscr{C}_0| < 2^{m-k-1}))$ **Then** $\mathscr{C}_1 := \emptyset$
If $(\mathscr{C}_0 = \emptyset$ *and* $\mathscr{C}_1 = \emptyset)$ **Then** *exit combine*
$\hat{u} := \bigvee_{i=1}^{k} u_i$
For all $c \in \{0, 1\}, \quad a, b \in \mathscr{C}_c : a < b$ **do**
If $(\hat{u}_{v(a+b)} = 0$ *and* $a + b < u_k)$ **Then** *append* a *to* $\mathscr{C}_c^{u_1,\ldots,u_k,a+b}$
For all $u_{k+1} \in \mathbb{F}_2^n : u_{k+1} < u_k$ **do**
Combine $(\mathscr{C}_0^{u_1,\ldots,u_{k+1}}, \mathscr{C}_1^{u_1,\ldots,u_{k+1}}, (u_1, \ldots, u_{k+1}), k + 1)$
Else
For all $a, b \in \mathscr{C}_0 \cup \mathscr{C}_1 : a < b$ **do**
Output "f *is affine on* $a + \langle u_1, \ldots, u_k, a + b\rangle$"

In order to choose an optimal starting dimension t_0 we have to take a closer look at some complexity evaluations.

4.4. Complexity evaluations

In this section we will evaluate the complexity of the described algorithm, and, in particular, its dependence on the chosen starting dimension t_0. This will then lead to a suggestion on how to optimally choose t_0.

In order to be able to make a proper complexity evaluation we have to assume that f is a random Boolean function. We will then evaluate the *expected* complexity of the algorithm.

The time complexity evaluations will be split into two parts, the complexity of the "exhaustive search" part in the main loop and the recursive "combining" part:

Exhaustive search. The number of subspaces of dimension t_0 in $\mathbb{F}_2^n$ is

$$\prod_{i=0}^{t_0-1} \frac{2^{n-i} - 1}{2^{t_0-i} - 1} \approx 2^{(n-t_0)t_0+1},$$

and thus the number of flats of this dimension is about

$$2^{(n-t_0)t_0+1} \cdot 2^{n-t_0} = 2^{(n-t_0)(t_0+1)+1}.$$

As checking whether a function is constant on a given subset needs at most two comparisons and three evaluations of f on average, we expect a complexity of about $2^{(n-t_0)(t_0+1)+2}$ steps in the "exhaustive search" part.

For example, for $n = 14$ and $n = 16$ this estimation gives the following concrete complexities:

$n = 14$:	t_0	1	2	3	4	5	6	7
	$\log_2$(compl.)	28	38	46	52	56	58	58

$n = 16$:	t_0	1	2	3	4	5	6	7	8
	$\log_2$(compl.)	32	44	54	62	68	72	74	74

From these tables we can see that it is not feasible to check normality by pure "exhaustive search" for these choices of n as this obviously corresponds to using the above described algorithm with $t_0 = m$ and that has an expected complexity of about 2^{58} and 2^{74} steps, respectively.

Combining. Let $\mathscr{T}_t$ be the combined expected complexity of all calls of *Combine*$(\ldots, t)$ concerning some dimension t. Then for $t < m - 1$ this complexity $\mathscr{T}_t$ mainly depends—besides the complexity $\mathscr{T}_{t+1}$ of further recursive calls of *Combine*—on the average size $\mathscr{S}$ of the input lists $\mathscr{C}_0$ and $\mathscr{C}_1$. As the main part of *Combine* is a loop over all unordered pairs of $\mathscr{C}_0$ and $\mathscr{C}_1$, respectively, in which mainly two comparisons are performed, the complexity can be estimated as

$$2 \cdot \binom{\mathscr{S}}{2} \cdot 2 \approx 2 \cdot \mathscr{S}^2.$$

As f is supposed to be random, the expected size $\mathscr{S}_t$ of $\mathscr{C}_c^{u_1,\ldots,u_t}(f)$ (i.e. a list corresponding to a subspace of dimension t) is $\mathscr{S}_t = 2^{-2^t} \cdot 2^{n-t}$, since the probability that $f(x) = c$ for all 2^t elements x in one of the corresponding flats is 2^{-2^t} for a random function f and there are 2^{n-t} flats corresponding to the subspace $\langle u_1, \ldots, u_t\rangle$.

As described in the previous sections due to the extra conditions the subroutine *Combine*$(\ldots, (u_1, \ldots, u_t), t)$ is only called once for each subspace $\langle u_1, \ldots, u_t\rangle$ and as we have a number of $\prod_{i=0}^{t-1}(2^{n-i} - 1)/(2^{t-i} - 1)$ subspaces of dimension t the expected total complexity for all calls of *Combine*$(\ldots, t)$ concerning some dimension $t < m - 1$ is about

$$\mathscr{T}_t = \mathscr{T}_{t+1} + 2 \cdot \mathscr{S}_t^2 \cdot \prod_{i=0}^{t-1} \frac{2^{n-i} - 1}{2^{t-i} - 1}$$
$$\Rightarrow \mathscr{T}_t - \mathscr{T}_{t+1} \approx \mathscr{S}_t^2 2^{(n-t)t+2} = 2^{-2^{t+1}+(n-t)(t+2)+2}.$$

The expected complexity of one call of *Combine*$(\ldots, m - 1)$ should also be about $2 \cdot \mathscr{S}^2$, as in this case we loop over all unordered pairs of $\mathscr{C}_0 \cup \mathscr{C}_1$, which is a set of size $2\mathscr{S}$, but we perform only 1 operation per pair. Thus, for dimension $m - 1$ we get

$$\mathscr{T}_{m-1} \approx 2^{-2^m+(n-m+1)(m+1)+2}.$$

Finally, we can say that the expected total complexity $\mathscr{T}_{t_0}$ of all calls of *Combine* in the main loop of the algorithm can be written as

$$\mathscr{T}_{t_0} = \sum_{t=t_0}^{m-2} (\mathscr{T}_t - \mathscr{T}_{t+1}) + \mathscr{T}_{m-1} \approx \sum_{t=t_0}^{m-1} 2^{-2^{t+1}+(n-t)(t+2)+2}.$$

As before for the "exhaustive search" part, for the "combining" part we get the following exemplary complexities for $n = 14$, $n = 16$:

$n = 14$:	t_0	1	2	3	4	5
	$\log_2(\mathscr{T}_{t_0})$	43	43	41	30	1

$n = 16$:	t_0	1	2	3	4	5
	$\log_2(\mathscr{T}_{t_0})$	52	52	51	42	15

Combined with the table of the complexities for the "exhaustive search" part this table shows that for $n = 14$ and $n = 16$ a proper choice for the starting dimension seems to be $t_0 = 2$ or $t_0 = 3$.

Obviously, in the complexity evaluation described so far, we have not taken into account the restrictions on the Hamming weights of the vectors in the GJBes in the main loop and the if-statements concerning $|\mathscr{C}_c|$, which are very hard to analyze exactly. But these tweaks on the algorithm should have not much influence on the choice of t_0 and, of course, they only decrease the complexity of the algorithm such that the above described complexities can be seen as estimations of "upper bounds" on the complexity of the algorithm.

An actual implementation of the algorithm which we made on a Pentium IV with 1.5 GHz in C++, needed about 50 h for $n = 14$ and $t_0 = 3$.

5. Further applications

Besides the application of checking (weak) normality, which is quite straightforward with the above described algorithm, there are some other applications for this algorithm.

5.1. Maiorana–McFarland functions

The second application of the algorithm we want to describe here is the problem to decide whether a given bent function is a Maiorana–McFarland bent function. Recall that we denote the class of all functions which are equivalent to a Maiorana–McFarland function under affine transformations by $\overline{\mathcal{M}}$.

Due to the following lemma it is possible to use the above described algorithm to determine whether a function is in $\overline{\mathcal{M}}$ or not.

Lemma 33. *Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a bent function. The following properties are equivalent*:

(i) *f is in $\overline{\mathcal{M}}$.*
(ii) *There exists a subspace U of dimension m such that the function f is affine on every coset of U.*

The proof of this Lemma is obvious since the second property is invariant under addition of an affine function and under right composition by an affine permutation. As the algorithm described in this paper outputs every coset of dimension m on which f is affine, this property can be checked easily.

In practice this means that for $n = 8$ we can decide whether a bent function is in $\overline{\mathcal{M}}$ in less than a second, for $n = 10$ in less than a minute and even for $n = 14$ in a few days.

The possibility to determine if a given function is in $\overline{\mathcal{M}}$ can be used to compute an experimental bound on the number of bent functions for $n = 8$ as follows.

By generating "random" bent functions and checking whether they are in $\overline{\mathcal{M}}$ as previously described, the ratio q of the number of bent functions in $\overline{\mathcal{M}}$ to the number of all bent functions can be estimated. Then, if μ_8 is the number of functions in $\overline{\mathcal{M}}$ in eight variables, the number of all bent functions can be estimated as $(1/q)\mu_8$.

But we are unable to estimate this number until we have solved the following two problems.

First the number μ_8 of functions in $\overline{\mathcal{M}}$ for $n = 8$ is not known exactly. The functions in $\overline{\mathcal{M}}$ are all affinely equivalent to $\langle x, \pi(y)\rangle + h(y)$, where π is a permutation and h an arbitrary Boolean function. The number of functions of this form is $2^{2^m}(2^m!)$. The problem is to determine the length of the orbit under the action of the group $AL(n)$ of all affine transformations. This length is equal to $\#AL(n)$ if and only if there are no $A \in AL(n)$ such that $f \circ A = f$. We computed the length of the orbit for randomly chosen functions in $\overline{\mathcal{M}}$ and all of them had orbit length $\#AL(n)$, but it would be much more satisfying to have a theoretical result, so it remains an open problem to determine $\#\overline{\mathcal{M}}$ for $n \geqslant 8$.

The second problem is that the generation of bent functions for $n = 8$ usually uses hill-climbing algorithms and these algorithms mightt find functions in $\overline{\mathcal{M}}$ more or less often than they should. A first step to check this can be to determine the above ratio for $n = 6$ and compare it with the proper ratio, which in this case is known (see [10]).

5.2. Other classes of bent functions

For some other classes of bent function it is also possible to use the algorithm presented in Section 4 to decide if a given bent function is in a specific class of bent functions. Examples are the classes $\mathcal{PS}^+$ and $\mathcal{PS}^-$ introduced in [5]. As the support of bent functions in these classes is defined via the union of subspaces of dimension $n/2$, the algorithm can be used easily to check if a function belongs to one of these classes.

References

[1] A. Canteaut, P. Charpin, Decomposing bent functions, IEEE Trans. Inform. Theory 49 (8) (2003) 2004–2019.
[2] C. Carlet, Two new classes of bent functions, in: Advances in Cryptology—EUROCRYPT'93, Lecture Notes in Computer Science, vol. 765, Springer, Berlin, 1994, pp. 77–101.
[3] C. Carlet, On cryptographic complexity of Boolean functions, in: Finite Fields with Applications to Coding Theory, Cryptography and Related Areas (Proceedings of Fq6), Springer, Berlin, 2002, pp. 53–69.
[4] P. Charpin, Normal Boolean functions, J. Complexity 20 (2004) 245–265 (special issue) ("Complexity Issues in Cryptography and Coding Theory", dedicated to Prof. Harald Niederreiter on the occasion of his 60th birthday.)
[5] J.F. Dillon, Elementary hadamard difference sets, Ph.D. Thesis, University of Maryland, USA, 1974.

[6] J.F. Dillon, H. Dobbertin, New cyclic difference sets with Singer parameters, Finite Fields Appl. 10 (2004) 342–389.
[7] H. Dobbertin, Construction of bent functions and balanced Boolean functions with high nonlinearity, in: Fast Software Encryption—FSE'94, Lecture Notes in Computer Science, vol. 1008, Springer, Berlin, 1995, pp. 61–74.
[8] S. Dubuc-Camus, Etude des fonctions booléennes dégénérées et sans corrélation, Ph.D. Thesis, Université de Caen, France, 1998.
[10] B. Preneel, Analysis and design of cryptographic hash functions, Ph.D. Thesis, Katholieke Universiteit Leuven, Belgium, 1993.