Des. Codes Cryptogr. (2008) 49:341–346
DOI 10.1007/s10623-008-9196-4

On Boolean functions with the sum of every two of them being bent

Christian Bey · Gohar M. Kyureghyan

Received: 1 June 2007 / Revised: 17 December 2007 / Accepted: 4 January 2008 /
Published online: 28 March 2008

Abstract A set of Boolean functions is called a bent set if the sum of any two distinct members is a bent function. We show that any bent set yields a homogeneous system of linked symmetric designs with the same design parameters as those systems derived from Kerdock sets. Further we observe that there are bent sets of size equal to the square root of the Kerdock set size which consist of Boolean functions with arbitrary degrees.

Keywords Bent function · Kerdock set · System of linked symmetric designs · Association scheme

AMS Classifications 11T71 · 05B05

1 Introduction

A bent function is a Boolean function with an even number of variables which has maximal Hamming distance from the set of all affine Boolean functions. Bent functions were introduced in [11]. See ([6], Ch. 6) for a survey, and the next section for a formal definition.

Let all functions below have n variables, n even. A set of Boolean functions is called a *bent set* if the sum of any two different members of the set is a bent function. A *Kerdock set* is a bent set consisting of 2^{n-1} quadratic forms. Recall that a quadratic form is bent if and only if it is nonsingular. It is easy to show and well known that the size of a Kerdock set is maximal with respect to the other defining properties, cf. ([4], Ch. 12). Whether there are

Dedicated to the memory of Hans Dobbertin.

C. Bey (✉) · G. M. Kyureghyan
Fakultät für Mathematik, Otto-von-Guericke Universität Magdeburg, Universitätsplatz 2,
39106 Magdeburg, Germany
e-mail: christian.bey@mathematik.uni-magdeburg.de

G. M. Kyureghyan
e-mail: gohar.kyureghyan@mathematik.uni-magdeburg.de

bent sets of size 2^{n-1} which consist of non-quadratic functions is an open problem, cf. ([6], Ch. 6.10). In this note we show that there are bent sets consisting of $2^{n/2}$ Boolean functions with *arbitrary* degrees.

In [3] the structure of Kerdock sets is investigated; it is shown that such a set defines a homogeneous system of linked symmetric designs ([2], see the next section for definitions). The only known examples of such systems have design parameters $v = 2^n$, $k = 2^{n-1} \pm 2^{n/2-1}$, $\lambda = 2^{n-2} \pm 2^{n/2-1}$. We show that an arbitrary bent set defines a homogeneous system of linked symmetric designs with these design parameters. In particular, the size of a bent set is upper bounded by 2^{n-1}.

2 Preliminaries

Let $\mathbf{F}_2$ denote the field with two elements and let $\mathcal{L}_n$ be the set of all linear functions $\mathbf{F}_2^n \to \mathbf{F}_2$, i.e. $\mathcal{L}_n = \{\varphi_a : \mathbf{F}_2^n \to \mathbf{F}_2,\ x \mapsto x \cdot a \mid a \in \mathbf{F}_2^n\}$. For a Boolean function $f : \mathbf{F}_2^n \to \mathbf{F}_2$ set

$$wt(f) = \#\{x \in \mathbf{F}_2^n \mid f(x) = 1\},$$

the weight of f. Let n be even. A Boolean function $f : \mathbf{F}_2^n \to \mathbf{F}_2$ is called *bent* if

$$wt(f + \varphi_a) = 2^{n-1} \pm 2^{n/2-1}$$

for all $a \in \mathbf{F}_2^n$. Clearly, if f is bent then so is $f + \varphi$ for any $\varphi \in \mathcal{L}_n$.

The dual function of a bent function f, denoted by $\tilde{f}$, is the Boolean function defined by

$$wt(f + \varphi_a) = 2^{n-1} - (-1)^{\tilde{f}(a)}\, 2^{n/2-1}. \tag{1}$$

The dual of a bent function is again bent, moreover $\tilde{\tilde{f}} = f$ ([11], see also [6], Ch. 6.1). Using (1) we get

$$wt(\tilde{f}) = 2^{n-1} - (-1)^{f(0)} 2^{n/2-1}. \tag{2}$$

If f and g are bent then ([11], see also [6], Ch. 6.1)

$$wt(\tilde{f} + \tilde{g}) = wt(f + g). \tag{3}$$

A *bent set* (called *bent Kerdock set* in [1]) is a set of Boolean functions such that the sum of every two functions in the set is bent.

A *system of linked symmetric designs* (introduced in [2]) consists of sets $\Omega_1, \Omega_2, \ldots, \Omega_\ell$ and an incidence relation between each pair of sets such that

- each pair $\{\Omega_f, \Omega_h\}$ (of different sets) with its incidence relation is a non-trivial symmetric design, and
- for each triple of different sets $\Omega_f, \Omega_g, \Omega_h$, the number of $z \in V_h$ incident with both $x \in \Omega_f$ and $y \in \Omega_g$ depends only on whether or not x and y are incident.

These two properties are kept if one replaces incidence by non-incidence in a pair $\{\Omega_f, \Omega_h\}$ (i.e. replacing the design by its complement). A system of linked symmetric designs is called *homogeneous* if after suitable such replacements

- all designs $\{\Omega_f, \Omega_h\}$ have the same parameters.

A homogeneous system of linked symmetric designs can be transformed into an imprimitive 3-class association scheme, cf. ([7], Sect. 5.4).

3 Linked symmetric designs from bent sets

For every Boolean function $f : \mathbf{F}_2^n \to \mathbf{F}_2$ let $\Omega_f := f + \mathcal{L}_n = \{f + \varphi \mid \varphi \in \mathcal{L}_n\}$.

Theorem 1 *Let $\mathcal{B}$ be a bent set of functions $\mathbf{F}_2^n \to \mathbf{F}_2$. Then the sets Ω_b, $b \in \mathcal{B}$, and the pairs of complementary incidence relations between any two different such sets defined by*

$$\begin{aligned} \{f, g\} \in R_0 &:\Leftrightarrow wt(f+g) = 2^{n-1} - 2^{n/2-1} \Leftrightarrow \widetilde{f+g}(0) = 0\,, \\ \{f, g\} \in R_1 &:\Leftrightarrow wt(f+g) = 2^{n-1} + 2^{n/2-1} \Leftrightarrow \widetilde{f+g}(0) = 1 \end{aligned}$$

form a homogeneous system of linked symmetric designs. The design parameters are $(2^n, 2^{n-1} \pm 2^{n/2-1}, 2^{n-2} \pm 2^{n/2-1})$.

The proof is given after the following three auxiliary results. Given $f, g : \mathbf{F}_2^n \to \mathbf{F}_2$ and $i, j \in \mathbf{F}_2$ let

$$c_{ij}(f, g) = \#\{x \in \mathbf{F}_2^n \,:\, f(x) = i,\ g(x) = j\}.$$

Claim 1 *For any $f, g : \mathbf{F}_2^n \to \mathbf{F}_2$ holds*

$$\begin{aligned} c_{10}(f, g) &= \frac{1}{2}\left(wt(f) - wt(g) + wt(f+g)\right) \\ c_{01}(f, g) &= \frac{1}{2}\left(-wt(f) + wt(g) + wt(f+g)\right) \\ c_{11}(f, g) &= \frac{1}{2}\left(wt(f) + wt(g) - wt(f+g)\right) \\ c_{00}(f, g) &= 2^n - \frac{1}{2}\left(wt(f) + wt(g) + wt(f+g)\right). \end{aligned}$$

Indeed, the numbers $c_{ij} = c_{ij}(f, g)$ satisfy for $f \neq g$ the following identities:

$$\begin{aligned} c_{10} + c_{11} &= wt(f) \\ c_{01} + c_{11} &= wt(g) \\ c_{01} + c_{10} &= wt(f+g) \\ c_{00} + c_{01} + c_{10} + c_{11} &= 2^n. \end{aligned}$$

Claim 2 *Let $f, g : \mathbf{F}_2^n \to \mathbf{F}_2$ be bent functions such that $f + g$ is also bent. Then it holds*

$$\begin{aligned} c_{10}(\tilde{f}, \tilde{g}) &= 2^{n-2} - \left((-1)^{f(0)} - (-1)^{g(0)} + (-1)^{\widetilde{f+g}(0)}\right) 2^{n/2-2} \\ c_{01}(\tilde{f}, \tilde{g}) &= 2^{n-2} - \left(-(-1)^{f(0)} + (-1)^{g(0)} + (-1)^{\widetilde{f+g}(0)}\right) 2^{n/2-2} \\ c_{11}(\tilde{f}, \tilde{g}) &= 2^{n-2} - \left((-1)^{f(0)} + (-1)^{g(0)} - (-1)^{\widetilde{f+g}(0)}\right) 2^{n/2-2} \\ c_{00}(\tilde{f}, \tilde{g}) &= 2^{n-2} + \left((-1)^{f(0)} + (-1)^{g(0)} + (-1)^{\widetilde{f+g}(0)}\right) 2^{n/2-2}. \end{aligned}$$

Indeed, Claim 1 and Eq. 3 imply

$$c_{10}(\tilde{f}, \tilde{g}) = \frac{1}{2}\left(wt(\tilde{f}) - wt(\tilde{g}) + wt(f+g)\right).$$

Then use (2). The remaining cases are analogous.

Claim 3 *Let $f, g : \mathbf{F}_2^n \to \mathbf{F}_2$ be bent functions with $0 \neq f + g \in \mathcal{L}_n$. Then it holds*

$$\begin{aligned} c_{10}(\tilde{f}, \tilde{g}) &= 2^{n-2} \\ c_{01}(\tilde{f}, \tilde{g}) &= 2^{n-2} \\ c_{11}(\tilde{f}, \tilde{g}) &= 2^{n-2} - (-1)^{f(0)} 2^{n/2-1} \\ c_{00}(\tilde{f}, \tilde{g}) &= 2^{n-2} + (-1)^{f(0)} 2^{n/2-1}. \end{aligned}$$

Indeed, these formulas are implied by Claim 1 and the Eqs. 2, 3 and $f(0) = g(0)$.

Proof of Theorem 1 Let $\Omega = \bigcup_{b \in \mathcal{B}} \Omega_b$. This is clearly a disjoint union. Consider $f, g, h \in \Omega$ with $\Omega_h \neq \Omega_f$ and $\Omega_h \neq \Omega_g$. Define for $i, j \in \{0, 1\}$

$$p_{ij} := p_{ij}(f, g, \Omega_h) = \#\left\{h' \in \Omega_h \mid \{f, h'\} \in R_i, \{g, h'\} \in R_j\right\}.$$

Note that

$$\begin{aligned} p_{ij} &= \#\left\{\varphi_a \in \mathcal{L}_n \mid \widetilde{f+h}(a) = i\,, \widetilde{g+h}(a) = j\right\} \\ &= c_{ij}(\widetilde{f+h}, \widetilde{g+h}). \end{aligned}$$

Now the proof follows from the following three facts.
(i) Let $\Omega_f \neq \Omega_g$. Then Claim 2 yields

$$\begin{aligned} p_{10} &= 2^{n-2} - \left((-1)^{f+h(0)} - (-1)^{g+h(0)} + (-1)^{\widetilde{f+g}(0)}\right) 2^{n/2-2} \\ p_{01} &= 2^{n-2} - \left((-1)^{g+h(0)} - (-1)^{f+h(0)} + (-1)^{\widetilde{f+g}(0)}\right) 2^{n/2-2} \\ p_{11} &= 2^{n-2} - \left((-1)^{f+h(0)} + (-1)^{g+h(0)} - (-1)^{\widetilde{f+g}(0)}\right) 2^{n/2-2} \\ p_{00} &= 2^{n-2} + \left((-1)^{f+h(0)} + (-1)^{g+h(0)} + (-1)^{\widetilde{f+g}(0)}\right) 2^{n/2-2}, \end{aligned}$$

and these numbers depend only on $\Omega_f, \Omega_g, \Omega_h$ (even only on $\Omega_f + \Omega_h, \Omega_g + \Omega_h$) and the relation in which $\{f, g\}$ lies.
(ii) Let $f \neq g$ and $\Omega_f = \Omega_g$. Then Claim 3 yields

$$\begin{aligned} p_{10} &= p_{01} = 2^{n-2} \\ p_{11} &= 2^{n-2} - (-1)^{f+h(0)} 2^{n/2-1} \\ p_{00} &= 2^{n-2} + (-1)^{f+h(0)} 2^{n/2-1}, \end{aligned}$$

and these numbers depend only on $\Omega_f (= \Omega_g)$ and Ω_h (even only on $\Omega_f + \Omega_h$).
(iii) Let $f = g$. Then Eq. 2 yields

$$\begin{aligned} p_{11} &= wt(\widetilde{f+h}) = 2^{n-1} - (-1)^{f+h(0)} 2^{n/2-1} \\ p_{00} &= 2^n - wt(\widetilde{f+h}) = 2^{n-1} + (-1)^{f+h(0)} 2^{n/2-1}, \end{aligned}$$

and again these numbers depend only on $\Omega_f (= \Omega_g)$ and Ω_h (even only on $\Omega_f + \Omega_h$).

By (ii) and (iii) the design parameters of $\{\Omega_f, \Omega_h\}$ are $(2^n, 2^{n-1} \pm 2^{n/2-1}, 2^{n-2} \pm 2^{n/2-1})$, depending on $\Omega_f + \Omega_h$. □

Recall from the introduction that the size of a Kerdock set is upper bounded by 2^{n-1}. We observe that the same bound holds also for bent sets:

Theorem 2 *Let $\mathcal{B}$ be a bent set of Boolean functions on $\mathbf{F}_2^n$. Then $|\mathcal{B}| \leq 2^{n-1}$*

This follows for instance from a result of Delsarte which we state in Theorem 3 below. When applying it to the bent set $\mathcal{B}$ we may assume that $b(0) = 0$ holds for all $b \in \mathcal{B}$. Indeed, replacing every $b \in \mathcal{B}$ for which $b(0) = 1$ by the Boolean function $b + 1$ yields again a bent set of size $|\mathcal{B}|$. Now consider $\Omega = \bigcup_{b\in\mathcal{B}} \Omega_b$ as a binary code $\mathcal{C}$ of length 2^{n-1}, by evaluating every $f \in \Omega$ on all $0 \neq a \in \mathbf{F}_2^n$. Then $\mathcal{C}$ has size $2^n|\mathcal{B}|$, and every pair of distinct codewords has Hamming distance from the set $\{2^{n-1} - 2^{n/2-1}, 2^{n-1} + 2^{n/2-1}, 2^{n-1}\}$.

Theorem 3 ([8], Example 2 on p. 82) *Let m be an even square. If $\mathcal{C} \subseteq \{0, 1\}^{m-1}$ is a code such that the Hamming distance between distinct codewords only assumes one of the three values $m/2 - \sqrt{m}/2$, $m/2 + \sqrt{m}/2$ and $m/2$, then $|\mathcal{C}| \leq m^2/2$.*

Alternatively, Theorem 2 follows from Theorem 1 and the following result of Noda.

Theorem 4 ([10], Corollary 3) *Let $\Omega_1 \ldots \Omega_l$ be a homogeneous system of linked symmetric designs with designs parameters $\left(m, m/2 \pm \sqrt{m}/2, m/4 \pm \sqrt{m}/2\right)$ (with m being an even square). Then $l \leq m/2$.*

See also [9] for another proof of Theorem 4.

4 Non-quadratic bent sets

The algebraic normal form of a Boolean function $f : \mathbf{F}_2^n \to \mathbf{F}_2$ is its n-variable polynomial representation from $\mathbf{F}_2[x_1, \ldots, x_n]/\prod_{i=1}^n (x_i^2 + x_i)$. The algebraic degree of a Boolean function is the degree of its algebraic normal form. If the vector space $\mathbf{F}_2^n$ is endowed with the structure of the field $\mathbf{F}_{2^n}$, then the algebraic degree of a Boolean function is the binary weight of the degree of its univariate polynomial representation from $\mathbf{F}_{2^n}[x]/(x^{2^n} + x)$, cf. ([6], Ch. 2.1). The algebraic degree of a bent function is upper bounded by $n/2$ [11]. Moreover, for any $2 \leq d \leq n/2$ there are bent functions of algebraic degree d. A Kerdock set is a bent set consisting of 2^{n-1} quadratic functions. In this section we show that there are bent sets of size $2^{n/2}$ which contain functions with arbitrary algebraic degrees.

Let $x \cdot y$ denote the standard inner product of two elements of $\mathbf{F}_2^k$. A vectorial bent function is a function $F : \mathbf{F}_2^n \to \mathbf{F}_2^k$ such that for every nonzero $v \in \mathbf{F}_2^k$ the Boolean function $F_v : \mathbf{F}_2^n \to \mathbf{F}_2, \quad x \mapsto v \cdot F(x)$ is bent, cf. [5]. Vectorial bent functions exist if and only if $1 \leq k \leq n/2$. The following result is now immediate:

Proposition 1 *Let $F : \mathbf{F}_2^n \to \mathbf{F}_2^k$ be a vectorial bent function. Then*

$$\left\{F_v : \mathbf{F}_2^n \to \mathbf{F}_2\,,\ x \mapsto v \cdot F(x) \mid v \in \mathbf{F}_2^k\right\}$$

is a bent set. Moreover, this set is closed under addition.

Taking $k = n/2$ in Proposition 1 we get a bent set of size $2^{n/2}$.

Next we recall the Maiorana–McFarland construction for vectorial bent functions, cf. [5]. Identify $\mathbf{F}_2^{n/2}$ with the field $\mathbf{F}_{2^{n/2}}$ and $\mathbf{F}_2^n$ with $\mathbf{F}_{2^{n/2}} \times \mathbf{F}_{2^{n/2}}$. The inner product in $\mathbf{F}_{2^{n/2}}$ is given by $x \cdot y := Tr_{n/2}(xy) = xy + (xy)^2 + \cdots + (xy)^{2^{n/2-1}}$. Let $\pi : \mathbf{F}_{2^{n/2}} \to \mathbf{F}_{2^{n/2}}$ be a permutation and $h : \mathbf{F}_{2^{n/2}} \to \mathbf{F}_{2^{n/2}}$ be arbitrary. Then the function $F : \mathbf{F}_{2^{n/2}} \times \mathbf{F}_{2^{n/2}} \to \mathbf{F}_{2^{n/2}}$ given by

$$F(x, y) = \pi(x)\, y + h(x)$$

is a vectorial bent function of Maiorana–McFarland type. In [3], a bent set of quadratic functions is obtained by taking $\pi(x) = x$ and $h(x) = 0$.

Now we use a similar construction to define bent sets of size $2^{n/2}$ which consist of functions with arbitrary given degrees. Let again $\pi : \mathbf{F}_{2^{n/2}} \to \mathbf{F}_{2^{n/2}}$ be a permutation, and for each nonzero $v \in \mathbf{F}_{2^{n/2}}$ let $h_v : \mathbf{F}_{2^{n/2}} \to \mathbf{F}_{2^{n/2}}$ be an arbitrary function. Put $h_0 := 0$. Then

$$\left\{F_v : \mathbf{F}_{2^{n/2}} \times \mathbf{F}_{2^{n/2}} \to \mathbf{F}_2\,,\ (x, y) \mapsto Tr_{n/2}\left(v\,\pi(x)\,y + h_v(x)\right)\ \middle|\ v \in \mathbf{F}_{2^{n/2}}\right\} \tag{4}$$

is a bent set.

Theorem 5 *Given integers $d_1, \ldots, d_{2^{n/2}-1}$ with $2 \le d_i \le n/2$, there exists a bent set $\{0, b_1, \ldots, b_{2^{n/2}-1}\}$ of size $2^{n/2}$ such that the algebraic degree of b_i is d_i.*

Proof Let $0, v_1, \ldots, v_{2^{n/2}-1}$ be the elements of the field $\mathbf{F}_{2^{n/2}}$. In (4) let $\pi(x) = x$. Consider

$$b_i(x, y) := Tr_{n/2}\left(v_i\,x\,y + h_{v_i}(x)\right) = Tr_{n/2}(v_i\,x\,y) + Tr_{n/2}(h_{v_i}(x))$$

where h_{v_i} is choosen such that the algebraic degree of $Tr_{n/2}(h_{v_i}(x))$ equals d_i. The degree of b_i is d_i since the algebraic degree of $Tr_{n/2}(v_i\,x\,y)$ is two.

Acknowledgments The authors thank Pascale Charpin for helpful discussions on Kerdock sets, and Alex Pott for indicating the connection of our original construction with the notion of vectorial bent functions.

References

1. Bending T.D., Fon-Der-Flaas D.: Crooked functions, bent functions, and distance regular graphs. Electron. J. Combin. **5** (1998) Research Paper 34, 14 pp (electronic).
2. Cameron P.J.: On groups with several doubly-transitive permutation representations. Math. Z. **128**, 1–14 (1972).
3. Cameron P.J., Seidel J.J.: Quadratic forms over $GF(2)$. Indag. Math. **35**, 1–8 (1973).
4. Cameron P.J., van Lint J.H.: Designs, Graphs, Codes and Their Links. Cambridge University Press, Cambridge (1991).
5. Carlet C.: Vectorial Boolean functions for cryptography. In: Crama Y., Hammer P. (eds.) Boolean Methods and Models. Cambridge University Press (to appear).
6. Carlet C.: Boolean functions for cryptography and error correcting codes. In: Crama Y., Hammer P. (eds.) Boolean Methods and Models. Cambridge University Press (to appear).
7. van Dam E.R.: Three-class association schemes. J. Alg. Combin. **10**, 69–107 (1999).
8. Delsarte P.: An algebraic approach to the association schemes of coding theory. Phillips Res. Repts. Suppl. **10** (1973).
9. Mathon R.: The systems of linked $2-(16,\ 6,\ 2)$ designs. Ars Combin. **11**, 131–148 (1981).
10. Noda R.: On homogeneous systems of linked symmetric designs. Math. Z. **138**, 15–20 (1974).
11. Rothaus O.S.: On "bent" functions. J. Combin. Theory Ser. A **20**, 300–305 (1976).