Construction of Bent Functions and Balanced Boolean Functions with High Nonlinearity

Hans Dobbertin

German Information Security Agency
P.O. Box 20 10 63, D-53133 Bonn, Germany

dobbertin@skom.rhein.de

Abstract. A general explicit construction of bent functions is described, which unifies well known constructions due to Maiorana-McFarland and Dillon as two opposite extremal cases. Within this framework we also find new ways to generate bent functions. Then it is shown how the constructed bent functions can be modified in order to obtain highly nonlinear balanced Boolean functions. Although their nonlinearity is the best known so far, it remains open whether this bound can still be improved.

1 Introduction

Boolean functions form important components of various practical cryptographic algorithms. One basic criterion for their design is nonlinearity. The significance of this aspect has again been demonstrated by the recent development of linear cryptanalysis by Matsui [5] and others.

Loosely speaking, bent functions are Boolean functions achieving the highest possible nonlinearity uniformly. In view of the Parseval equation this definition implies that they exist only for an even number of variables.

Bent functions were introduced by Rothaus [8] in 1976. They turned out to be rather complicated combinatorical objects. While a concrete description of all bent functions is elusive, there are two well-known explicit constructions of special bent functions due to Maiorana-McFarland [6] and Dillon [4].

In the next section a general construction of normal bent functions is described (triple construction, see Definition 1 and Lemma 2), where we call a Boolean function with $2n$ variables normal if it is constant on a n-dimensional affine subspace. Within the framework of the triple construction we obtain the bent functions of Maiorana-McFarland and of Dillon as the two opposite extremal cases, and we also find new ways to construct bent functions (see Theorem 4).

Depending on the conditions of the concrete application, it has often to be considered as a defect from the cryptographic point of view that bent functions are necessarily non-balanced. In the third section it is shown how normal bent

functions can be modified in order to get highly nonlinear balanced Boolean functions with $2n$ variables (see Proposition 8). We conclude that, in the balanced case, the maximal nonlinearity for $2n$ variables is connected by a certain inequality with the maximal nonlinearity for n variables (see Theorem 9). However, the challenging problem to determine the maximal nonlinearity of balanced Boolean functions precisely remains open.

2 Normal Bent Functions

The **Walsh transformation** of a Boolean function g defined on a finite vector space V over GF(2) with a scalar product is denoted by $g^{\mathcal{W}}$:

$$g^{\mathcal{W}}(a) = \sum_{x \in V} (-1)^{g(x)+(a,x)}.$$

The Walsh transformation is a very powerful tool for analyzing Boolean functions. Note that the set of values occuring as Walsh coefficients is independent of the choice of the scalar product. Recall that a **bent function** f on a $2n$-dimensional vector space V over GF(2) is defined by the property

$$f^{\mathcal{W}}(z) = \pm 2^n \text{ for all } z \in V.$$

We call a Boolean function f with $2n$ variables **normal**, if there is an affine subspace with dimension n, on which f is constant. In the following we shall be concerned with normal bent functions. Starting point of our investigation is the following fact (see Lemma 7, Section 3):

Let f be a normal bent function on a $2n$-dimensional vector space V over GF(2) such that the restriction of f on an affine subspace U of dimension n is constant. Then the restriction of f on each proper co-set of U is balanced.

Thus if one wants to construct a normal bent function then this means essentially that one has to construct a suitable collection $(f_y)_{y \in W \setminus \{y_0\}}$ ($y_0 \in W$ fixed) of balanced Boolean functions on a n-dimensional vector space W over GF(2). The Boolean function on W^2 corresponding to such a collection is defined as

$$f(x,y) = \begin{cases} f_y(x) \text{ for } y \neq y_0 \\ \\ \text{constant, otherwise.} \end{cases}$$

For the following the value, 0 or 1, of the constant is not important. Hence we assume that it is 0. If instead of f we consider its support $T = \operatorname{supp} f$ then the above setting means

$$T = \bigcup_{y \in W \setminus \{y_0\}} S_y \times \{y\},$$

where $\operatorname{supp} f_y = S_y \subseteq W$ und $\#S_y = 2^{n-1}$.

It is a natural idea to endow W with a field structure, to choose some fixed subset S of W with $\#S = 2^{n-1}$, and to define the S_y as a permutation of sets of the form

$$yS + c_y.$$

This leads to the following construction of Boolean functions:

Definition 1 (Triple Construction). *Let L be the field* $\mathrm{GF}(2^n)$. *Choose*

$$\sigma : L \longrightarrow \mathrm{GF}(2) \text{ balanced,}$$
$$\phi : L \longrightarrow L \text{ bijective,}$$
$$\psi : L \longrightarrow L \text{ arbitrary.}$$

The Boolean function $f = f_{\sigma,\phi,\psi}$ on L^2 associated to the triple (σ, ϕ, ψ) is defined as follows:

$$f(x, \phi(y)) = \begin{cases} \sigma\left(\frac{x+\psi(y)}{y}\right) \text{ for } y \neq 0 \\ 0 \text{ otherwise.} \end{cases}$$

The support of f is

$$\operatorname{supp} f = \bigcup_{y \in L^*} (yS + \psi(y)) \times \{\phi(y)\},$$

where $S = \operatorname{supp} \sigma$.

We call (σ, ϕ, ψ) a **bent triple** if the associated Boolean function $f_{\sigma,\phi,\psi}$ is a bent function.

In the sequel, with respect to the Walsh coefficients of a Boolean function g, we refer to the scalar product

$$\langle x, y \rangle = \mathrm{Tr}(xy)$$

if g is defined on the field L, and to the scalar product

$$\langle (x, u), (y, v) \rangle = \mathrm{Tr}(xy + uv)$$

if g is defined on L^2.

Lemma 2. *Suppose that σ, ϕ, ψ and $f = f_{\sigma,\phi,\psi}$ are given as specified in the triple construction (Definition 1).*

1. *For all $b \in L$ we have $f^{\mathcal{W}}(0, b) = (-1)^{\mathrm{Tr}(b\phi(0))} 2^n$. For $a, b \in L$, $a \neq 0$ set*

$$\Gamma_{a,b}(x) = \mathrm{Tr}\left(a\psi(x/a) + b\phi(x/a)\right).$$

Then

$$f^{\mathcal{W}}(a, b) = \sum_{x \in L} (-1)^{\Gamma_{a,b}(x)} \sigma^{\mathcal{W}}(x).$$

2. *Let $T_\sigma \subseteq L$ denote the affine subspace generated by* $\operatorname{supp} \sigma^{\mathcal{W}}$. *The following condition implies that (σ, ϕ, ψ) is a bent triple:*

$$\phi \text{ and } \psi \text{ are affine}^1 \text{ on } aT_\sigma \text{ for all } a \in L^*. \tag{1}$$

[1] ϕ is said to be *affine on a affine subspace* T if there is an affine mapping which coincides on T with ϕ, or equivalently if $\phi(u) + \phi(v) + \phi(w) = \phi(u + v + w)$ for all $u, v, w \in T$.

Proof. 1. We have

$$f^{\mathcal{W}}(a,b) = \sum_{x,y\in L} (-1)^{f(x,y)+\langle(a,b),(x,y)\rangle} = \sum_{x,y}(-1)^{f(x,\phi(y))+\mathrm{Tr}(ax+b\phi(y))}$$
$$= \sum_x \sum_{y\neq 0}(-1)^{\sigma\left(\frac{x+\psi(y)}{y}\right)+\mathrm{Tr}(ax+b\phi(y))} + (-1)^{\mathrm{Tr}(b\phi(0))}\sum_x (-1)^{\mathrm{Tr}(ax)}$$

By the substitution $z = (x+\psi(y))/y$ we get

$$\sum_x \sum_{y\neq 0}(-1)^{\sigma\left(\frac{x+\psi(y)}{y}\right)+\mathrm{Tr}(ax+b\phi(y))} = \sum_{y\neq 0}\sum_z (-1)^{\sigma(z)+\mathrm{Tr}(ayz+a\psi(y)+b\phi(y))}$$
$$= \sum_{y\neq 0}(-1)^{\mathrm{Tr}(a\psi(y)+b\phi(y))}\sigma^{\mathcal{W}}(ay)$$

Since σ is balanced it follows that $\sigma^{\mathcal{W}}(0) = 0$. In the above sum over y we therefore can add the case $y = 0$, and for $a = 0$ we conclude

$$f^{\mathcal{W}}(0,b) = (-1)^{\mathrm{Tr}(b\phi(0))}\,2^n.$$

In the following suppose $a \neq 0$. Then $\sum_x (-1)^{\mathrm{Tr}(ax)} = 0$, and it follows that

$$f^{\mathcal{W}}(a,b) = \sum_y (-1)^{\mathrm{Tr}(a\psi(y)+b\phi(y))}\sigma^{\mathcal{W}}(ay)$$
$$= \sum_x (-1)^{\mathrm{Tr}(a\psi(x/a)+b\phi(x/a))}\sigma^{\mathcal{W}}(x).$$

2. Let g and Γ be Boolean functions on L, where Γ is affine. Then obviously

$$\sum_{x\in L}(-1)^{\Gamma(x)}g^{\mathcal{W}}(x) = \pm 2^n.$$

Of course this equation already holds if Γ is affine on T_g, the affine subspace generated by $\mathrm{supp}\, g^{\mathcal{W}}$.

Condition (1) assures that all mappings $\Gamma_{a,b}$ are affine on T_σ. From 1. it follows that $f^{\mathcal{W}}(a,b) = \pm 2^n$ for all $a, b \in L$. □

In order to state the main result of this section we need a preparing lemma.

Lemma 3. *Let U be a subspace of the vector space $V = G(2)^n$, and $y_0 \in V$. Then there is an onto linear mapping $\rho : V \longrightarrow U$ such that a one-to-one correspondence between all Boolean functions $\sigma : V \longrightarrow \mathrm{GF}(2)$ with*

$$\mathrm{supp}\,\sigma^{\mathcal{W}} \subseteq y_0 + U$$

and all Boolean functions τ on U is given by setting

$$\sigma(x) = \tau\rho(x) + \langle x, y_0\rangle.$$

Moreover, all σ are balanced if and only if $y_0 \notin U$.

Proof. We have the formula

$$(\sigma A)^{\mathcal{W}}(a) = \sigma^{\mathcal{W}}((A^*)^{-1}(a)),$$

where $A : V \longrightarrow V$ is a bijective linear mapping, and A^* is the adjoint of A, i.e. $\langle A(x), y\rangle = \langle x, A^*(y)\rangle$. On the other hand $(\sigma + \ell_{y_0})^{\mathcal{W}}(a) = \sigma^{\mathcal{W}}(a + y_0)$, for the linear mapping $\ell_{y_0}(x) = \langle x, y_0\rangle$. Thus the first assertion has to be shown only for the case that U is generated by unit vectors and $y_0 = 0$. But this case is easily verified.

The last statement is obvious, since σ is balanced iff $\sigma^{\mathcal{W}}(0) = 0$. □

Maiorana-McFarland and Dillon gave two different constructions of bent functions. We say these bent functions are of *Maiorana-McFarland type (MM-type)* and *Dillon type (D-type)*, respectively. Their definitions can be found in the proof of the following theorem.

Theorem 4. *Let $L = \mathrm{GF}(2^n)$, and let (σ, ϕ, ψ) be given as described in the triple construction.*

1. *If σ is affine then (σ, ϕ, ψ) is a bent triple for arbitrary ϕ, ψ. In this case one obtains precisely the bent functions of MM-type.*
2. *Conversely if ϕ and ψ are affine then (σ, ϕ, ψ) is a bent triple for arbitrary σ. In this case $f_{\sigma,\phi,\psi}$ and $f_{\sigma,\mathsf{id},0}$ are affinely equivalent. The bent functions of D-type are precisely the functions of the form $f_{\sigma,\mathsf{id},0}$.*
3. *Besides the two opposite extremal cases 1. and 2. there are further bent triples:*
   Suppose $\phi(x) = x^d$, $\psi(x) = x^{d'}$ (or $\psi = 0$) for $d, d' < 2^n - 1$, and let a non-trivial subspace U of L and $y_0 \in L \setminus U$ be given such that the following conditions are satisfied:
   (a) ϕ is bijective, i.e. d is relatively prime to $2^n - 1$,
   (b) ϕ and ψ are not affine, i.e. d and d' are not powers of 2,
   (c) ϕ and ψ are affine on $y_0 + U$.
   Define $\sigma : L \longrightarrow \mathrm{GF}(2)$ as a non-affine balanced Boolean function such that the support of $\sigma^{\mathcal{W}}$ is a subset of $y_0 + U$. This means that σ is of the form

$$\sigma(x) = \tau\rho(x) + \mathrm{Tr}(xy_0),$$

   where $\rho : L \longrightarrow U$ is an onto linear mapping chosen according to Lemma 3, and τ is an arbitrary non-affine Boolean functions on U.
   Then (σ, ϕ, ψ) is a bent triple, which is neither of D- nor of MM-type. The explicit definition of the corresponding bent function is

$$f(x, y^d) = \begin{cases} \tau\rho\left(\frac{x}{y} + y^{d'-1}\right) + \mathrm{Tr}\left(\left(\frac{x}{y} + y^{d'-1}\right)y_0\right) & \text{if } y \neq 0, \\ 0 \text{ otherwise.} \end{cases}$$

Two concrete examples are given after the proof of this theorem.

Proof. 1. Obviously σ is affine if and only if $T_\sigma = \operatorname{supp} \sigma^{\mathcal{W}}$ is a singleton. Thus the first claim follows immediately by Lemma 2.2.

We identify L with $\mathrm{GF}(2)^n$. A bent function $g : L^2 \longrightarrow \mathrm{GF}(2)$ is of **MM-type** if it is of the form

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

where π is a bijection on L, h is an arbitrary Boolean function on L and $\langle \cdot, \cdot \rangle$ is the canonical scalar product on $\mathrm{GF}(2)^n$. W.l.o.g. we can assume $\pi(0) = 0$ and $h(0) = 0$.

Let $\varrho : L \longrightarrow L$ be the bijective linear mapping defined by the equation

$$\langle x, y \rangle = \mathrm{Tr}(x\varrho(y))$$

for all $x, y \in L$. Now define ϕ such that the equation

$$\phi^{-1}(y) = \frac{1}{\varrho\pi(y)} \quad (y \in L^*)$$

holds, and choose ψ with the property

$$\mathrm{Tr}\left(\frac{\psi(y)}{y}\right) = h\phi(y) \quad (y \in L^*).$$

Then as desired we have

$$g = f_{\mathrm{Tr},\phi,\psi}.$$

Similarly we see that every $f_{\sigma,\phi,\psi}$ with linear σ is of MM-type.

2. Again the first assertion follows immediately from Lemma 2.2. If ϕ and ψ are affine then $f_{\sigma,\mathsf{id},0}\, \Lambda = f_{\sigma,\phi,\psi}$ for the bijective affine mapping

$$\Lambda : (x, y) \longmapsto \left(x + \psi\phi^{-1}(y), \phi^{-1}(y)\right).$$

It remains to verify that the bent functions of D-type are precisely the $f_{\sigma,\mathsf{id},0}$:

Let $E = \mathrm{GF}(2^{2n})$. We consider E as field extension of $L = \mathrm{GF}(2^n)$. Choose an $\alpha \in E$ with $E = L[\alpha]$. We set

$$\overline{x} = x^{2^n} \quad (x \in E),$$

for the Frobenius automorphism of $E : L$. The mapping

$$h : \begin{cases} x \longmapsto \overline{x}/x \\ \\ E^* \longrightarrow E^* \end{cases}$$

is a multiplicative homomorphism with image

$$H = \{z \in E^* \,:\, z\overline{z} = 1\}.$$

The kernel of h is L^*. Therefore H is a representation system for the elements of the factor group E^*/L^*, i.e. the sets of the form xL^* $(x \in E^*)$. In view of $H \cong E^*/L^*$ we have

$$\#H = 2^n + 1.$$

Set $H_1 = H \setminus \{1\}$. The bent functions of **D-type** are precisely the characteristic functions of sets of the form

$$D(Z) = \bigcup_{z \in Z} zL^*,$$

where $Z \subseteq H_1$ has exactly 2^{n-1} elements. (The condition $\#Z = 2^{n-1}$ assures that $\chi_{D(Z)}$ is a bent function.)

A bijection between H_1 and L is defined by

$$\Upsilon : z \longmapsto \frac{\overline{\alpha} z + \alpha \overline{z}}{z + \overline{z}}.$$

If we identify L^2 and E by setting $(x, y) = x + y\alpha$ then for $S = \Upsilon[Z]$

$$D(Z) = \bigcup_{z \in Z} zL^* = \bigcup_{y \in L^*} yS \times \{y\} = \operatorname{supp} f_{\sigma, \mathsf{id}, 0}, \tag{2}$$

where σ is the characteristic function of S.

Remark. As we have seen there is an interesting analogy between the field extensions $E : L$ and $\mathbb{C} : \mathbb{R}$. For instance, (2) can be interpreted as the change from the representation of D in "polar coordinates" to the representation in "cartesian coordinates."

3. If the power functions ϕ and ψ are affine on T_σ, the affine subspace generated by the support of $\sigma^{\mathcal{W}}$, then of course they are affine on aT_σ for all $a \in L^*$. Thus (σ, ϕ, ψ) is a bent triple by Lemma 2.2 if the conditions (a) – (c) are satisfied. □

We want to give two concrete examples how the exponents d, d' and the affine subspace $y_0 + U$ can be choosen such that the conditions (a) – (c) in Theorem 4.3 are satisfied.

Example 1. Assume that n is not prime and not a power of 2, i.e. $n = mr$ with $r > 1$ and odd $m > 1$. Let $d = 2^r + 1$, $U = K = \mathrm{GF}(2^r)$, and $y_0 \in L \setminus U$. Then for all $x \in y_0 + U$ we have

$$\begin{aligned} x^d &= ((x + y_0) + y_0)^{2^r+1} \\ &= (x + y_0)^2 + (x + y_0)y_0 + (x + y_0){y_0}^{2^r} + {y_0}^d \\ &= x^2 + \left(y_0 + {y_0}^{2^r}\right) x, \end{aligned}$$

i.e. ϕ is linear on $y_0 + U$. It remains to show that $2^r + 1$ and $2^n - 1$ are relatively prime. In fact

$$(2^r + 1)(2^{(m-1)r-1} - 2^{(m-2)r-1} + \ldots - 2^{r-1} + 2^{n-1}) \equiv 1 \pmod{2^n - 1}.$$

Note that the surjective linear mapping ρ from L onto $U = K$ can here be taken as the orthogonal[2] projection $\rho = \mathrm{Tr}_{L:K}$, that is

$$\sigma(x) = \tau \mathrm{Tr}_{L:K}(x) + \mathrm{Tr}(xy_0),$$

[2] That is $\mathrm{Tr}((x + \rho(x))u) = 0$ for all $x \in L$, $u \in U$.

where τ is any non-affine mapping on K. To complete the definition of the bent triples set $\psi = 0$.

Example 2. Assume that $n = 2r > 2$ is even. Set

$$d = (2^r + 2)(1 + 2^2 + 2^4 + ... + 2^{2s}) + 1.$$

Then

$$d \equiv 2^{2(s+1)} \pmod{2^r - 1},$$

and consequently the restriction of $\phi(x) = x^d$ onto $K = \mathrm{GF}(2^r)$ is linear. Similarly set

$$d' = (2^r + 2)(1 + 2^2 + 2^4 + ... + 2^{2s'}) + 1.$$

Now let U be any hyperplane of K and $y_0 \in K \setminus U$. Then the conditions (b) and (c) of Theorem 4.3 are fulfilled. We do not know when in general ϕ is bijective. But at least for $s = 0$ this is always the case, since

$$(2^r + 3)(3 \cdot 2^{n-3} - 2^{r-3}) \equiv 1 \pmod{2^n - 1}.$$

To describe the surjection from L onto U for a concrete example, suppose that

$$U = \ker \mathrm{Tr}_K$$

and r is odd. Then again the orthogonal projection can be taken as ρ, i.e. $\rho(x) = \mathrm{Tr}_{L:K}(x) + \mathrm{Tr}(x)$, and consequently

$$\sigma(x) = \tau(\mathrm{Tr}_{L:K}(x) + \mathrm{Tr}(x)) + \mathrm{Tr}(xy_0).$$

It is easy to find further similar examples of bent triples, where ϕ and ψ are power functions.

According to Theorem 4.3 we have found a new construction of bent functions. But of course this does not mean that the resulting bent functions are really new in the sense that they cannot be derived from already known ones using simple modifications. For instance, the following constructions alter a given bent function f on $V = \mathrm{GF}(2)^{2n}$ into another bent function g on V:

1. "affine modification," i.e. $g = f\Lambda$, where $\Lambda : V \longrightarrow V$ is bijective and affine,
2. "affine addition," i.e. $g = f + \ell$, where $\ell : V \longrightarrow \mathrm{GF}(2)$ is affine,
3. "dualizing," i.e. $g = f^*$, where the *dual* bent function f^* associated to f is defined by the equation
$$f^{\mathcal{W}} = 2^n (-1)^{f^*},$$

Also, the direct sum of bent functions is again a bent function. Another kind of modifications are those which require certain conditions to guarantee that the resulting function is bent again. A lot of them are known in the literature, the most simple is

4. "skipping," i.e. setting $g = f + \chi_U$, where f is bent function with $2n$ variables, and U is an affine subspace with dimension n such that f is constant on U.

Note that skipping can be applied precisely to normal bent functions.

Let $\mathcal{D}$, $\mathcal{M}$ and $\mathcal{N}$ denote the class of all bent functions of D-type, MM-type and the type constructed in Theorem 4.3, respectively. For any class $\mathcal{B}$ of bent functions let $\widetilde{\mathcal{B}}$ denote its completion under *equivalence* (i.e. modifications of type 1. and 2.), and let $\overline{\mathcal{B}}$ denote its completion under forming direct sums, the above modifications 1. – 3. and known "conditional" modifications such as for instance 4.

The class of all explicitly known bent functions so far can now be written as

$$\overline{\mathcal{D} \cup \mathcal{M}}.$$

Thus if we want to show that the bent functions of Theorem 4.3 are *new* in the strongest sense of the word then we would have to establish that $\mathcal{N}$ is not included in $\overline{\mathcal{D} \cup \mathcal{M}}$. However, this seems to be a very difficult problem. The weaker statement $\mathcal{N} \not\subseteq \widetilde{\mathcal{D}} \cup \widetilde{\mathcal{M}}$ is a desirable first step. The probably easier half of this statement is shown next. To this end we have proven by computation of explicit examples:

Lemma 5. *The class $\mathcal{N}$ contains bent functions with non-degenerated second derivation.*

Proposition 6. *The class $\mathcal{N}$ is not contained in $\widetilde{\mathcal{M}}$.*

Proof. To seperate $\mathcal{D}$ from $\widetilde{\mathcal{M}}$, Dillon [4] showed that the bent functions of MM-type have a degenerated second derivation, while this in general is not true for bent functions of D-type. In view of Lemma 5 we can argue in the same way. □

Remark. Carlet [2] has shown that a generalized form of skipping applied to bent functions of MM-type leads out of $\widetilde{\mathcal{PS}} \cup \widetilde{\mathcal{M}}$, where $\mathcal{PS}$ denotes the class of all bent functions, which are "partial spreads." ($\mathcal{PS}$ includes $\mathcal{D}$ as the subclass of its concretely known examples.)

3 Balanced Boolean Functions

The **spectral radius** of a Boolean function $f : \mathrm{GF}(2)^m \longrightarrow \mathrm{GF}(2)$ is

$$R_f = \max\{\, |f^W(a)| : a \in \mathrm{GF}(2)^m \}.$$

R_f can be considered as a measure for the linearity of f. Thus if we are interested in Boolean functions with high nonlinearity then we have to look for f's with small R_f.

The **Parseval equation** states that the square sum over the Walsh coefficients of a Boolean function with m variables equals to 2^{2m}. Hence we have

$$R_f \geq 2^{m/2},$$

and in the even case $m = 2n$ this lower bound is achieved by bent functions, which can be characterized by the property that their Walsh spectrum consists only of the values $\pm 2^n$. (The odd case is known to be difficult; see [7].)

However, bent functions are not balanced. Thus if we ask for balanced functions with high nonlinearity then it is a natural idea to obtain them by "making a bent function balanced," where the spectral radius is increased as less as possible. In the following it will be shown that this idea works for all *normal* bent functions. In this way we can construct balanced functions with almost the same nonlinearity as bent functions.

First we prove the following lemma (cf. [2], Lemma 1):

Lemma 7. *Let $W = \mathrm{GF}(2)^n$ and $V = W^2$. Let f be a normal bent function on V. That is w.l.o.g. $f(x,0) = 0$ for all $x \in W$. Then*[3] *$f^{\mathcal{W}}(0,b) = 2^n$ for all $b \in W$. Moreover for each fixed $y \in W \setminus \{0\}$ the function*

$$f_y : \begin{cases} W \longrightarrow \mathrm{GF}(2) \\ x \longmapsto f(x,y) \end{cases}$$

is balanced.

Proof. Set for $y \in W$

$$F(y) = \begin{cases} {f_y}^{\mathcal{W}}(0) = \sum_x (-1)^{f(x,y)} \text{ for } y \neq 0 \\ 0 \text{ otherwise.} \end{cases}$$

We compute

$$\begin{aligned} \sum_b f^{\mathcal{W}}(0,b) &= \sum_{b,x,y} (-1)^{f(x,y)+\langle b,y\rangle} \\ &= \sum_{b,x} (-1)^{f(x,0)+\langle b,0\rangle} + \sum_{y\neq 0} F(y) \left(\sum_b (-1)^{\langle b,y\rangle} \right) \\ &= 2^{2n} + 0 = 2^{2n}. \end{aligned}$$

In view of $f^{\mathcal{W}}(0,b) = \pm 2^n$ we conclude $f^{\mathcal{W}}(0,b) = 2^n$. Hence

$$2^n = f^{\mathcal{W}}(0,b) = 2^n + \sum_{y\neq 0} F(y)(-1)^{\langle b,y\rangle},$$

and therefore $\widehat{F}(b) = \sum_y F(y)(-1)^{\langle b,y\rangle} = 0$ for all $b \in W$. Consequently $F = 2^{-n}\,\widehat{\widehat{F}} = 0$. □

[3] We use the canonical scalar product to define the Walsh coefficients.

Remark. Lemma 7 shows that if f is a normal bent function then also its dual f^* is normal.

Proposition 8. *Let $W = \mathrm{GF}(2)^n$ and $V = W^2$. Let f be a normal bent function on V. That is w.l.o.g. $f(x,0) = 0$ for all $x \in W$. Furthermore let a balanced function $\theta : W \longrightarrow \mathrm{GF}(2)$ be given. Set for $x, y \in W$*

$$\Theta(x,y) = \begin{cases} f(x,y), & \text{if } y \neq 0 \\ \theta(x), & \text{otherwise.} \end{cases}$$

Then Θ is balanced and we have

$$\Theta^{\mathcal{W}}(a,b) = \begin{cases} f^{\mathcal{W}}(a,b) + \theta^{\mathcal{W}}(a), & \text{if } a \neq 0 \\ 0, & \text{otherwise.} \end{cases}$$

In particular it follows that

$$R_\Theta = 2^n + R_\theta.$$

Proof. We have

$$\begin{aligned} \Theta^{\mathcal{W}}(a,b) &= \sum_{x,y} (-1)^{\Theta(x,y)+\langle a,x\rangle+\langle b,y\rangle} \\ &= \sum_{x} (-1)^{\theta(x)+\langle a,x\rangle} + \sum_{x,y} (-1)^{f(x,y)+\langle a,x\rangle+\langle b,y\rangle} - \sum_{x} (-1)^{\langle a,x\rangle} \\ &= \theta^{\mathcal{W}}(a) + f^{\mathcal{W}}(a,b) - \sum_{x} (-1)^{\langle a,x\rangle}. \end{aligned}$$

This proves the first assertion, since $f^{\mathcal{W}}(0,b) = 2^n$ by Lemma 7.

If we apply Lemma 7 to the dual bent function of f then in particular we see that for each fixed $a \in W \setminus \{0\}$ both values 2^n and -2^n are attained by $f^{\mathcal{W}}(a,b)$. This implies $R_\Theta = 2^n + R_\theta$. □

In order to discuss the implications of Proposition 8 we introduce the notations

$$\begin{aligned} \mathsf{R}(m) &= \min\{R_f \mid f : \mathrm{GF}(2)^m \longrightarrow \mathrm{GF}(2)\}, \\ \mathsf{RB}(m) &= \min\{R_f \mid f : \mathrm{GF}(2)^m \longrightarrow \mathrm{GF}(2) \text{ balanced}\}. \end{aligned}$$

Theorem 9. $\mathsf{RB}(2n) \leq 2^n + \mathsf{RB}(n)$.

Proof. Use Proposition 8 with some θ such that $R_\theta = \mathsf{RB}(n)$. □

For even $m = 2^s u$, u odd, one concludes by an inductive application of Theorem 9:

Corollary 10. $\mathsf{RB}(m) \leq 2^{m/2} + 2^{m/4} + 2^{m/8} + \ldots + 2^u + \mathsf{RB}(u)$.

On the other hand one easily verifies that

$$\mathsf{RB}(u) \leq 2^{\frac{u+1}{2}}.$$

Using this fact and a lower bound basically derived from the Parseval equation we obtain for $m \geq 4$

$$2^{m/2} + 4 \leq \mathsf{RB}(m) \leq 2^{m/2} + 2^{m/4} + 2^{m/8} + \ldots + 2^u + 2^{\frac{u+1}{2}}. \tag{3}$$

Independently the upper bound of (3) has been found by Seberry, Zhang and Zheng (see Theorem 1 of [9]). For instance it yields

$$132 \leq \mathsf{RB}(14) \leq 144. \tag{4}$$

For $u = 1, 3, 5$ and 7 it is known that $\mathsf{R}(u) = \mathsf{RB}(u) = 2^{(u+1)/2}$. But in 1983 Patterson and Wiedemann [7] showed that

$$\mathsf{R}(15) \leq 216 = \frac{27}{32} 2^{\frac{15+1}{2}}. \tag{5}$$

We can derive from this fact a similar result for balanced Boolean functions (cf. Theorem 2 of [9]). In fact note that for the spectral radius of the direct sum of Boolean functions f and g we have the formula $R_{f \oplus g} = R_f R_g$. Hence

$$\mathsf{RB}(n+m) \leq \mathsf{RB}(n)\,\mathsf{R}(m) \tag{6}$$

for all n and m, since $f \oplus g$ is balanced if f is balanced. Thus by (4), (5) and (6)

$$\mathsf{RB}(29) \leq \mathsf{RB}(14)\,\mathsf{R}(15) \leq 144 \cdot 216 = \frac{243}{256} 2^{\frac{29+1}{2}}.$$

More generally this implies

$$\mathsf{RB}(u) < 2^{\frac{u+1}{2}} \text{ for all odd } u \geq 29,$$

since $\mathsf{RB}(u+2) \leq \mathsf{RB}(u)\mathsf{R}(2) = 2\,\mathsf{RB}(u)$. Note that therefore Corollary 10 is stronger than the upper bound of (3). We close our investigation with two conjectures:

Conjecture A. *The recursive inequality given in Theorem 9 is sharp:*

$$\mathsf{RB}(2n) = 2^n + \mathsf{RB}(n).$$

Conjecture B. *For odd m we have the asymptotic formulas*

$$\mathsf{RB}(m) \approx \mathsf{R}(m) \approx 2^{m/2}.$$

4 Applications

Theorem 4 unifies and extends the known constructions of bent functions. Proposition 8 describes how we can get balanced Boolean functions with highest nonlinearity known so far. On the other hand, the generation of bent functions with $2n$ variables by Theorem 4 requires a balanced Boolean function σ with n variables. If n is even, one can choose σ highly nonlinear according to Proposition 8, and then use Theorem 4.2. That is, *applications of Theorem 4 and Proposition 8 can be linked together inductively.*

Adding also the forming of direct sums, affine modifications, affine addition, dualizing and (generalized) skipping as ingredients, all this can be considered as a cooking book for both, the generation of bent functions and of highly nonlinear balanced Boolean functions with an even number of variables.

Concluding Remarks

1. There are certainly more ways to construct "non-standard" bent triples (σ, ϕ, ψ) than those given in Theorem 4.3. The smaller the support of the Walsh transformation of σ becomes, the more freedom we get for ϕ and ψ. We have restricted ourselves to power functions, because this seems to be the simplest non-trivial case.
2. Another class of explicitly constructable bent functions has recently been found by Carlet [3]. This class can also be derived from a slightly modified version of the triple construction, as will be shown in a forthcoming paper.
3. Simon Blackburn [1] mentioned a simple counting argument showing that there are non-normal Boolean functions with $2n$ variables for $n \geq 6$. In fact, for each affine subspace S of dimension n there are precisely

$$b_n = 2 \cdot 2^{2^{2n}-2^n}$$

Boolean functions, which are constant on S. On the other hand it is well-known that there are exactly

$$s_n = \prod_{i=0}^{n-1} \frac{2^{2n}-2^i}{2^n-2^i} \approx 2^{n^2}$$

subspaces of dimension n, i.e. the number of affine subspaces of dimension n is $a_n = 2^n s_n$. Thus an upper bound for the number of normal Boolean functions on $\mathrm{GF}(2)^{2n}$ is given by

$$u_n = a_n b_n = 2^{2^{2n}-2^n+n+1} s_n \approx 2^{2^{2n}-2^n+n^2+n+1}.$$

However, as one easily verifies, u_n is smaller than $2^{2^{2n}}$, the number of all Boolean functions on $\mathrm{GF}(2)^{2n}$, for $n \geq 6$. It remains open whether there are non-normal bent functions.

References

1. Blackburn, S.: private communication, 1995.
2. Carlet, C.: Two new classes of bent functions. Advances in Cryptology, Eurocrypt '93, Lecture Notes in Computer Science 765, Springer–Verlag 1994, pp. 77–101.
3. Carlet, C.: Generalized partial spreads. IEEE Transactions on Information Theory (to appear).
4. Dillon, J. F.: Elementary Hadamard difference sets. Proceedings of the Sixth Southeastern Conference on Combinatorics, Graph Theory and Computing, Boca Raton, Florida, Congressus Numerantium No. XIV, Utilitas Math., Winnipeg, Manitoba, 1975, pp. 237 – 249.
5. Matsui, M.: Linear cryptanalysis method for DES cipher. Advances in Cryptology, Eurocrypt '93, Lecture Notes in Computer Science 765, Springer–Verlag 1994, pp. 386 – 397.
6. McFarland, R. L.: A family difference sets in non-cyclic groups. J. Combinatorical Theory, Ser. A, **15** (1973), pp. 1 – 10.
7. Patterson, N. J., Wiedemann, D. H.: The covering radius of the $(2^{15}, 16)$ Reed-Muller code is at least 16276. IEEE Transactions on Information Theory **29** (1983), pp. 354 – 356.
8. Rothaus, O. S.: On "bent" functions. J. Combinatorical Theory, Ser. A, **20** (1976), pp. 300 – 305.
9. Seberry, J., Zhang, X., Zheng, Y.: Nonlinearity and propagation characteristics of balanced Boolean functions. Information & Computation (to appear).