Codes, Graphs and Schemes from Nonlinear Functions

van Dam, E.R.; Fon-der-Flaass, D.

Publication date:
2000

Document Version
Publisher's PDF, also known as Version of record

Link to publication in Tilburg University Research Portal

Citation for published version (APA):
van Dam, E. R., & Fon-der-Flaass, D. (2000). *Codes, Graphs and Schemes from Nonlinear Functions*. (FEW Research Memorandum; Vol. 790). Operations research.

Codes, graphs, and schemes from nonlinear functions

E.R. van Dam
Tilburg University, Dept. Econometrics
PO Box 90153, 5000 LE Tilburg, The Netherlands
email: `Edwin.vanDam@kub.nl`

D. Fon-Der-Flaass *
Institute of Mathematics
Novosibirsk, 90, Russia, 630090
email: `d.g.flaass@writeme.com`

May 19, 2000

1991 Mathematical Subject Classification: 05E30, 05B20, 94B05

Abstract

We consider functions on binary vector spaces which are far from linear functions in different senses. We compare three existing notions: almost perfect nonlinear (APN) functions, almost bent (AB) functions, and crooked (CR) functions. Such functions are of importance in cryptography because of their resistance to linear and differential attacks on certain cryptosystems. We give a new combinatorial characterization of almost bent functions in terms of the number of solutions to a certain system of equations, and a characterization of crooked functions in terms of the Fourier transform. We also show how these functions can be used to construct several combinatorial structures; such as semi-biplanes, difference sets, distance regular graphs, symmetric association schemes, and uniformly packed (BCH and Preparata) codes.

1 Almost perfect nonlinear, almost bent, and crooked functions

We consider functions on binary vector spaces which are far from linear functions in different senses. We compare three existing notions: almost perfect nonlinear (APN) functions, almost bent (AB) functions, and crooked (CR) functions. Such functions are of importance in cryptography because of their resistance to linear and differential attacks on certain cryptosystems (cf. [8], [9], [10, p. 1037]). Furthermore they are of interest in the study of linear feedback shift register sequences with low crosscorrelation (cf. [17, pp. 1795-1810]). Also in the construction of certain combinatorial structures they have proven to be useful; we will give an overview and update on this in Section 2. Furthermore we give a new combinatorial characterization of almost bent functions in terms of the number of solutions to a certain system of equations (similar to such a characterization of APN functions), and a new characterization of crooked functions in terms of the Fourier transform.

First we introduce some notation which will be used throughout the paper. Let V be an n-dimensional space over the field $GF(2)$; and let $N = 2^n = |V|$. By $\langle \cdot, \cdot \rangle$ we shall denote the standard inner product on V. By $|X|$ we denote the size of a finite set X. Let $f : V \to V$ be any function. For $0 \neq a \in V$, we denote by $H_a(f)$, or simply H_a, the set

$$H_a = H_a(f) = \{f(x) + f(x + a) \mid x \in V\}.$$

The Fourier transform (also called Walsh transform) $\mu_f : V \times V \to \mathbb{R}$ of f is defined by the formula

$$\mu_f(a, b) = \sum_{x \in V} (-1)^{\langle a,x \rangle} (-1)^{\langle b,f(x) \rangle}.$$

*Partly supported by the grant 99-01-00581 of the Russian Foundation for Fundamental Research.

Now we introduce the three different classes of "extremely non-linear" functions which we shall consider in this paper.

Definition 1 *A function $f : V \to V$ is called:*
(i) **APN** *(almost perfect nonlinear) if $|H_a(f)| = \frac{1}{2}N$ for all $0 \neq a \in V$;*
(ii) **AB** *(almost bent) if $\mu_f(a,b) = 0, \pm\sqrt{2N}$ for all $(a,b) \neq (0,0)$;*
(iii) **CR** *(crooked) if $f(0) = 0$ and every set $H_a(f)$, $a \neq 0$, is the complement of a hyperplane. We shall denote the class of APN (AB, CR) functions by $\mathcal{APN}$ ($\mathcal{AB}$, $\mathcal{CR}$).*

Note that as a consequence of its definition, an AB function can only exist if the dimension n is odd.

We use here the terminology from the papers [8] and [1]; other authors sometimes use the terms *semiplanar* for APN ([11]), and *maximally nonlinear* for AB functions ([7, 23]). The definition of crooked functions given here is different from, but equivalent to, the one used in [1, 12]:

Definition 1′ *A function $f : V \to V$ is called crooked if it satisfies the following three properties:*
(i) $f(0) = 0$;
(ii) $f(x) + f(y) + f(z) + f(x + y + z) \neq 0$ *when x, y, z are distinct;*
(iii) $f(x) + f(y) + f(z) + f(x + a) + f(y + a) + f(z + a) \neq 0$ *when $a \neq 0$.*

It is also shown in [1] that, for a crooked function f, all sets $H_a(f)$ are distinct, that is, every complement of a hyperplane occurs among them exactly once.

Let us recall some more properties of APN, AB, and CR functions. Most of them are taken from the papers [1, 8].

A function remains APN, AB, or CR after applying any non-degenerate affine transformations to the argument and/or the value of the function (for a crooked function, it is additionally required that the resulting function maps 0 to 0).

If a function f is APN or AB, and bijective, then so is its inverse function f^{-1}. In contrast to this, the inverse of a crooked function need not be crooked. Also, a function remains APN (AB) after adding any linear function to it. Again, this is not true for crooked functions.

There are proper inclusions between the three classes:

$$\mathcal{CR} \subset \mathcal{AB} \subset \mathcal{APN}.$$

In the next section we shall prove both inclusions (note that $\mathcal{CR} \subseteq \mathcal{APN}$ follows from the definition).

Not too many constructions of APN, AB, or CR functions are known; all known such functions are equivalent under the above transformations to certain functions $f : GF(2^n) \to GF(2^n)$ of the form $f(x) = x^k$. In Section 3 we give a complete list of all currently known APN, AB, and CR functions.

1.1 Alternative descriptions of $\mathcal{APN}$, $\mathcal{AB}$, and $\mathcal{CR}$

As is well-known, the definition of APN functions given above can easily be re-formulated in terms of the number of solutions of a certain system of equations.

Lemma 1 *A function f is APN if and only if the system of equations*

$$\begin{cases} x + y &= a \\ f(x) + f(y) &= b \end{cases} \tag{1}$$

has 0 or 2 solutions (x, y) for every $(a, b) \neq (0, 0)$. If so, then the system has 2 solutions precisely when $b \in H_a(f)$.

PROOF. For any function f, if the system (1) has a solution then it has at least two of them. Therefore for every $a \neq 0$ the set $H_a(f)$ has at most $\frac{1}{2}N$ elements, and equality is achieved if and only if the system (1) has 0 or 2 solutions for each b. □

It turns out that AB functions can be characterized in a similar way.

Theorem 1 *A function f is AB if and only if the system of equations*

$$\begin{cases} x + y + z &= a \\ f(x) + f(y) + f(z) &= b \end{cases} \tag{2}$$

has $N-2$ or $3N-2$ solutions (x, y, z) for every (a, b). If so, then the system has $3N-2$ solutions if $b = f(a)$, and $N-2$ solutions otherwise.

PROOF. The proof presented below is a typical application of the Fourier transform. We shall present it in the language of matrices.

First we define several $N \times N$ matrices with real entries whose rows and columns are indexed by vectors from V. Let I be the identity matrix, J the all-one matrix, E the matrix with a single nonzero entry $E_{00} = 1$, $E_{ij} = 0$ for $(i, j) \neq (0, 0)$. The entries of the matrices $X, M, M^{(3)}, F, S$ are as follows:
$X_{ab} = (-1)^{\langle a,b\rangle}$; $M_{ab} = \mu_f(a, b)$; $M^{(3)}_{ab} = \mu_f(a, b)^3$;
$S_{ab} = |\{(x, y, z) \mid x + y + z = a;\ f(x) + f(y) + f(z) = b\}|$;
$F_{ab} = 1$ if $b = f(a)$; otherwise $F_{ab} = 0$.
One can easily check the following equalities:

$$X^2 = NI; \quad M = XFX; \quad XJX = N^2E. \tag{3}$$

In particular, it follows that the matrix X is nonsingular.

The condition that the system (2) has $N-2$ or $3N-2$ solutions is equivalent to the identity

$$S = (N-2)J + 2NF. \tag{4}$$

Indeed, when $b = f(a)$, the system (2) has $3N-2$ "trivial" solutions with one variable equal to a, and the two other variables equal to each other. So, from counting all (x, y, z, a, b) satisfying (2) in two ways it follows that the system has $3N-2$ solutions when $b = f(a)$, and $N-2$ solutions otherwise.

The property that f is AB can also be stated in matrix terms. It is equivalent to the identity

$$M^{(3)} - 2NM = (N^3 - 2N^2)E. \tag{5}$$

Indeed, all values $\mu_f(a, b)$ except $\mu_f(0, 0) = N$ are roots of the cubic equation $x^3 - 2Nx = 0$.

Finally, we have the identity

$$M^{(3)} = XSX. \tag{6}$$

Let us prove it. We have

$$\begin{aligned} \mu_f(a, b)^3 &= \sum_{x,y,z \in V} (-1)^{\langle a, x+y+z\rangle} (-1)^{\langle b, f(x)+f(y)+f(z)\rangle} \\ &= \sum_{p \in V} (-1)^{\langle a,p\rangle} \sum_{x+y+z=p} (-1)^{\langle b, f(x)+f(y)+f(z)\rangle}. \end{aligned}$$

In the inner summation, collect all terms with the same value $q = f(x) + f(y) + f(z)$; for each q there will be S_{pq} of them. So,

$$\begin{aligned}\mu_f(a,b)^3 &= \sum_{p\in V}(-1)^{\langle a,p\rangle}\sum_{q\in V}S_{pq}(-1)^{\langle b,q\rangle}\\ &= \sum_{p,q\in V}X_{ap}S_{pq}X_{qb} = (XSX)_{ab}.\end{aligned}$$

Combining the identities (3) and (6) we get:

$$X(S - 2NF - (N-2)J)X = M^{(3)} - 2NM - (N^3 - 2N^2)E.$$

As X is nonsingular, it follows that the identities (4) and (5) hold simultaneously, and the theorem is proved. □

Remark. The identities $M = XFX$ and $M^{(3)} = XSX$ from the proof represent a special case of the general fact that the Fourier image of the convolution of several functions is the product of their Fourier images.

The characterizations of APN and AB functions given in Lemma 1 and Theorem 1 allow us to give simple proofs of the inclusions $\mathcal{CR} \subseteq \mathcal{AB} \subseteq \mathcal{APN}$.

Proposition 1 *Any crooked function is almost bent, and any almost bent function is almost perfect nonlinear.*

PROOF. For the second assertion, it is enough to notice that if for some $q \neq 0$, $a \neq p \neq a+q$, the equality $f(p) + f(p+q) = f(a) + f(a+q)$ holds (that is, f is not APN), then the system

$$\left\{\begin{array}{rcl} x+y+z &=& a\\ f(x)+f(y)+f(z) &=& f(a)\end{array}\right.,$$

apart from trivial solutions, has the solution $x = p$, $y = p+q$, $z = a+q$, and so f is not AB.

To prove the first assertion, take any crooked function f. It is enough to show that, for every a and every $b \neq 0$, the system

$$\left\{\begin{array}{rcl} x+y+z &=& a\\ f(x)+f(y)+f(z) &=& f(a)+b\end{array}\right.$$

has $N-2$ solutions (when b does equal 0, it follows from Definition 1′ that the system only has $(3N-2)$ trivial solutions). Obviously, every such solution (x,y,z) satisfies $z \neq a$. Let $p = z + a = x + y$. Then $f(x) + f(y) \in H_p$, $f(z) + f(a) \in H_p$, and therefore $b \in V \setminus H_p$, since H_p is the complement of a hyperplane. Every nonzero vector b belongs to $\frac{1}{2}N - 1$ hyperplanes, which gives $\frac{1}{2}N - 1$ choices for p, and hence for z. Once z is determined, the system in x and y has precisely 2 solutions, because of Lemma 1. Hence we get $2(\frac{1}{2}N - 1) = N - 2$ solutions in all. □

In Theorem 1 we characterized AB functions (which are defined in terms of the Fourier transform) in terms of the number of solutions of a certain system of equations. Next, we shall give characterizations of APN functions and CR functions in terms of the Fourier transform. In the case of APN functions this characterization is due to Chabaud and Vaudenay [9]; in fact they used it to prove the inclusion $\mathcal{AB} \subseteq \mathcal{APN}$.

Theorem 2 *Let f be an AB function such that $f(0)=0$. Then f is crooked if and only if the set $\{a \mid \mu_f(a,b)=0\}$ is a hyperplane for every $b \neq 0$. If so, then all these hyperplanes are distinct and $\{a \mid \mu_f(a,b)=0\} = \{a \mid \langle a,c\rangle = 0\}$, where c is such that $H_c(f) = \{x \mid \langle b,x\rangle = 1\}$.*

PROOF. This proof will have a similar flavor as the proof of the characterization of AB functions in Theorem 1. We will make use of the same matrices X and E introduced there. Moreover we introduce the matrices $M^{(2)}$ and T of which the entries are given by $M^{(2)}_{ab} = \mu_f(a,b)^2$ and $T_{ab} = |\{(x,y) \mid x+y=a;\ f(x)+f(y)=b\}|$. It follows that $M^{(2)} = XTX$, which can be proven just like the identity $M^{(3)} = XSX$ was proven in Theorem 1.

The stated assertion that the set $\{a \mid \mu_f(a,b)=0\}$ is a hyperplane for every $b \neq 0$ is equivalent to the existence of a function $c : V \to V$ such that $\{a \mid \mu_f(a,b)=0\} = \{a \mid \langle a, c(b)\rangle = 0\}$ for every $b \neq 0$. Without loss of generality we complete the definition of c by taking $c(0)=0$.

Since f is an AB function the stated assertion is equivalent to $\mu_f(a,b)^2 = N - N(-1)^{\langle a,c(b)\rangle}$ for all a and $b \neq 0$, hence to $M^{(2)} = N(J - XC) + N^2E$, where C is the matrix given by $C_{ab} = 1$ if $a = c(b)$; 0 otherwise. After multiplying both sides of the matrix equation from the left and right by the nonsingular matrix X it follows that the stated assertion is equivalent to the equation $T = E - CX + J$.

Now we use that f is APN: $T_{ax} = 2$ if $x \in H_a(f)$, $T_{00} = N$, and $T_{ax} = 0$ otherwise. Finally, we may conclude that the stated assertion is equivalent to the existence of a function $c : V \to V$, $c(0) = 0$ such that

$$\sum_{b:a=c(b)} (-1)^{\langle b,x\rangle} = \begin{cases} -1 & \text{if } x \in H_a(f) \\ \ \ 1 & \text{otherwise} \end{cases}$$

for all $a \neq 0$.

Now suppose that the stated assertion is true, and the above equations hold. By considering $x = 0$ it follows that for every $a \neq 0$ the number of b such that $a = c(b)$ must be equal to one, hence c is a bijection. Now the equations reduce to $\langle c^{-1}(a), b\rangle = 1$ if and only if $b \in H_a(f)$ for all b and $a \neq 0$. Hence $H_a(f)$ is the complement of a hyperplane for every $a \neq 0$, and we may conclude that f is crooked.

On the other hand, if f is crooked then the function given by $c(b) = a$ where a is the unique vector such that $H_a(f) = \{x \mid \langle b,x\rangle = 1\}$ satisfies the required equations. Note that in this case c is a bijective function so the sets $\{a \mid \mu_f(a,b)=0\}$, $b \neq 0$ comprise all hyperplanes. $\square$

Proposition 2 *[9] Let $f : V \to V$ be any function. Then*

$$\sum_{a,b} \mu_f(a,b)^4 \geq 3N^4 - 2N^3$$

with equality if and only if f is APN.

PROOF. Again, we use the matrix methods (and matrices) of Theorems 1 and 2. For the function f we have that

$$\sum_{a,b} \mu_f(a,b)^4 = \sum_{a,b} (M^{(2)}_{ab})^2 = \mathrm{tr}(M^{(2)} M^{(2)T}) = \mathrm{tr}(XTXXT^TX) = N\mathrm{tr}(XTT^TX) =$$

$$N\mathrm{tr}(TT^TXX) = N^2\mathrm{tr}(TT^T) = N^2 \sum_{a,b} (T_{ab})^2 = N^4 + N^2 \sum_{a\neq 0} \sum_b (T_{ab})^2.$$

As is noticed in the proof of Lemma 1, T_{ab} is equal to zero or at least two. This means that $\sum_{a\neq 0}\sum_b (T_{ab})^2 \geq \sum_{a\neq 0}\sum_b 2T_{ab}$ with equality if and only if T_{ab} equals 0 or 2 for all b and $a \neq 0$, i.e. if and only if f is APN. We finish our proof by observing that $\sum_{a\neq 0}\sum_b 2T_{ab} = 2(N^2 - N)$. $\square$

To sum things up: APN functions can be defined in terms of the number of solutions of a certain system of equations, in terms of the Fourier transform, or in terms of the sets $H_a(f)$; AB functions — in terms of the Fourier transform, or in terms of the number of solutions of a certain system of equations; and CR functions — in terms of $H_a(f)$ or in terms of the Fourier transform. It would also be interesting to find a characterization of AB functions in terms of the sets $H_a(f)$.

1.2 Algebraic degree

First we recall the definition and some standard properties of the algebraic degree of a function. Consider our space V as the standard vector space of row vectors $(x_1, \ldots, x_n)$, $x_i \in GF(2)$. Any function $f : V \to V$ can be represented as a polynomial in the variables $x_1, \ldots, x_n$ with coefficients in V. Further, all monomials of this polynomial can be chosen to have degree at most 1 in each variable, since the elements of $GF(2)$ satisfy the identity $x^2 = x$. With such a choice of monomials, the polynomial representation of f becomes unique; and it can be found by expanding the representation

$$f(x_1, \ldots, x_n) = \sum_{(a_1,\ldots,a_n)\in V} f(a_1, \ldots, a_n) \cdot (x_1 + a_1 + 1) \ldots (x_n + a_n + 1).$$

The degree of the resulting polynomial is called *the algebraic degree* of f. The algebraic degree does not depend on the choice of a basis for V. This follows from the following characterization:

Lemma 2 *The algebraic degree of f is equal to the maximum dimension k for which there is an affine k-subspace U of V such that $\sum_{u\in U} f(u) \neq 0$.*

This lemma follows from standard properties of Reed–Muller codes (cf. for instance [6, Chapter 12], in particular (12.3) and (12.5)).

It is proved in [8] that the algebraic degree of an AB function does not exceed $\frac{1}{2}(n+1)$. We shall prove a better bound for crooked functions.

Theorem 3 *Let $f : V \to V$ be a crooked function,* $\dim V = n = 2m+1 \geq 5$. *Then the algebraic degree of f is at most $m = \frac{1}{2}(n-1)$.*

To prove it, we need the following easy combinatorial lemma.

Lemma 3 *Let $X \subseteq V$, $l < n$, $k > 0$. If for every affine l-subspace U of V the number $|X \cap U|$ is divisible by 2^k then for every affine $(l-1)$-subspace W of V the number $|X \cap W|$ is divisible by 2^{k-1}.*

PROOF. Let W_1 be any affine $(l-1)$-subspace of V. Let W_2, W_3 be two translates of W_1 such that all the W_i are distinct. Let $x_i = |X \cap W_i|$, $i = 1, 2, 3$.

All sets $W_i \cup W_j$ are affine l-subspaces of V. Thus, we have the system of equations $x_1 + x_2 = a$, $x_2 + x_3 = b$, $x_3 + x_1 = c$, where a, b, c are multiples of 2^k. Solving this system, we find that every x_i is a multiple of 2^{k-1}, and the lemma is proved. $\square$

PROOF of Theorem 3. Instead of f we shall consider Boolean functions $f_h : V \to GF(2)$, $f_h(v) = h(f(v))$, for arbitrary non-zero linear functionals $h : V \to GF(2)$. Let

$$X_h = \{v \in V \mid h(f(v)) = 1\}.$$

We only need to show that, for every affine $(m+1)$-subspace U of V, the number $|X_h \cap U|$ is even. Indeed, as h was arbitrary, this would imply that $\sum_{v \in U} f(v) = 0$, and the theorem would then follow from Lemma 2.

The set $\{v \in V \mid h(v) = 1\}$ is the complement of a hyperplane; therefore it coincides with the set $H_a(f)$ for some $a \in V$. It is proved in [1, Proposition 3] that, for any hyperplane $V' \subset V$, the set $X_h \cap V' = \{v \in V' \mid h(f(v)) = 1\}$ is of size 2^{n-2} if $a \in V'$, and of size $2^{n-2} \pm 2^{m-1}$ if $a \notin V'$. Note also that $|X_h| = 2^{n-1}$, since f is a bijection.

Take an arbitrary linear subspace $W_0 \subset V$ of codimension 2; let W_1, W_2, W_3 be the affine subspaces parallel to it.

The sets $W_0 \cup W_i$, $i = 1, 2, 3$, are the three hyperplanes containing W_0. So we can easily find the numbers $|X_h \cap W_i|$: if $a \in W_0$ then they all are equal to 2^{n-3}; otherwise two of them are equal to 2^{n-3}, and two others to $2^{n-3} \pm 2^{m-1}$. In any case, as $n \geq 5$, these numbers are divisible by 2^{m-1}.

Thus, $|X_h \cap W|$ is divisible by 2^{m-1} for every affine subspace $W \subset V$ of dimension $n-2$. Now Lemma 3 applied $m-2$ times gives the desired result. □

In the class of functions of algebraic degree 2 (quadratic functions) the three classes $\mathcal{APN}$, $\mathcal{AB}$, and $\mathcal{CR}$ essentially coincide. More precisely, it is proved in [8, Theorem 8] that every quadratic APN function of odd dimension is AB. Now we shall briefly demonstrate that every quadratic APN function which is bijective, and maps 0 to 0, is crooked. It is convenient to use Definition 1′. The property (ii) there is equivalent to the function being APN. Take any $x, y, z \in V$, $0 \neq a \in V$. We need to check that the sum

$$s = f(x) + f(y) + f(z) + f(x+a) + f(y+a) + f(z+a)$$

is not equal to 0. If any two of the six terms coincide, this follows from the bijectivity of f. If not, then the set

$$\{x, y, z, x+a, y+a, z+a, x+y+z, x+y+z+a\}$$

is an affine 3-subspace. As f is quadratic, the sum of its values over this subspace is equal to 0, and therefore $s = f(x+y+z) + f(x+y+z+a)$, and $s \neq 0$, again by bijectivity.

We note finally that all known examples of crooked functions have algebraic degree 2.

2 Combinatorial structures

In this section we will construct several combinatorial structures, such as semi-biplanes, difference sets, distance-regular graphs, association schemes, and uniformly packed (BCH and Preparata) codes, all by using APN, AB, or CR functions. For some background on distance-regular graphs and association schemes we refer the reader to [2]; for background on codes to [20].

2.1 APN functions and semi-biplanes

A *semi-biplane* $sbp(v, k)$ is a connected incidence structure of v points and v blocks, each incident with k points, such that any 2 points are incident with 0 or 2 blocks, and any two blocks are incident with 0 or 2 points. Coulter and Henderson [11] construct a semi-biplane from an almost perfect nonlinear function f in the following way.

Construction 1 Let f be an APN funtion. Then the incidence structure with point set and block set $V \times V$, where a point (x, a) is incident with a block (y, b) if and only if $a + b = f(x + y)$ is a semi-biplane $sbp(N^2, N)$ if the incidence structure is connected, or else it consists of two disjoint $sbp(\frac{1}{2}N^2, N)$.

Coulter and Henderson [11] also construct certain 2-class association schemes from the crooked (Gold) functions $f(x) = x^{2^k+1}, (k, n) = 1$ (here V is identified with $GF(2^n)$). These association schemes are fusions of the schemes constructed in Section 2.3.

2.2 AB functions, Kasami codes, and Kasami graphs

A *uniformly packed e-error-correcting code* is a code with minimum distance $d = 2e + 1$ and the property that the number of codewords at distance $e + 1$ from a word which is at distance e from the code is constant, and the number of codewords at distance $e + 1$ from a word which is at distance $e + 1$ or more from the code is also constant (cf. [20]). Carlet, Charpin, and Zinoviev [8] found the following.

Construction 2 Let f be an AB function with $f(0) = 0$ (and $n > 3$). Then the code C of characteristic vectors of all subsets S of $V \setminus \{0\}$ such that $\sum_{r \in S} r = 0$ and $\sum_{r \in S} f(r) = 0$ is a double-error-correcting binary linear uniformly packed code of length $N - 1$ and dimension $N - 1 - 2n$.

The code C generalizes the double error-correcting BCH codes, and are also called Kasami codes (note that these codes are extremal in the sense that no linear code of this length and minimum distance can have more codewords). The essence of the proof of this result given in [8] lies in the fact that the dual code has 3 nonzero weights, which follows from the definition of almost bent functions in terms of the Fourier transform.

In [12] the present authors gave a combinatorial proof of the above result for crooked functions. Their proof is easily adjusted (and simplified!) for almost bent functions, by using the combinatorial characterization of almost bent functions in Section 1.1.

Carlet, Charpin, and Zinoviev [8] also show that in order to prove that the above code has dimension $N - 1 - 2n$ and minimum distance 5 (hence that the code is extremal) it suffices that f is almost perfect nonlinear (with $f(0) = 0$).

A *distance-regular graph* (with parameters $\{b_0, b_1, ..., b_d; c_0, c_1, ..., c_d\}$) is a connected regular graph such that for an arbitrary pair of vertices $\{x, y\}$ at distance i, the number of vertices adjacent to x and at distance $i - 1$ (respectively i, and $i + 1$) from y is a constant c_i (respectively a_i, and b_i) depending only on i (cf. [2]). It follows from the work of Delsarte (cf. [2, Chapter 11]) that the coset graph of the uniformly packed Kasami code as described above is distance-regular with diameter three. An alternative description of this coset graph, like the one given in [4] is the following:

Construction 3 Let f be an AB function with $f(0) = 0$. Then the graph with vertex set $V \times V$, where two distinct vertices (x, a) and (y, b) are adjacent if $a + b = f(x + y)$ is a distance-regular graph with parameters $\{N - 1, N - 2, \frac{1}{2}N + 1; 1, 2, \frac{1}{2}N - 1\}$.

A direct proof that this is indeed a distance-regular Kasami graph is given in [12] for crooked functions. Again, this proof can be adjusted for almost bent functions using the combinatorial characterization of such functions in Section 1.1.

Note by the way the resemblance between the construction of the distance-regular graph and the construction of the semi-biplane in Section 2.1. If in the above definition of the graph we would allow an almost perfect nonlinear function we would obtain an $(N-1)$-regular graph without triangles, such that any two vertices at distance two have two common neighbours, Such a graph, when connected, is called a *rectagraph*. Note that a more general connection between semi-biplanes, binary linear codes of minimum distance at least 5, and rectagraphs has been observed; cf. [2, Section 1.13].

2.3 AB functions, accomplices, CR functions, Preparata codes and graphs

In [1] crooked functions were introduced to generalize the antipodal distance-regular graphs constructed by de Caen, Mathon, and Moorhouse [5]. In [12] the present authors used crooked functions to generalize 5-class association schemes constructed in [4], and Preparata codes. Note that the above mentioned antipodal distance-regular graphs are strongly related to the 5-class association schemes and the Preparata codes, hence they will be called Preparata graphs in the following.

Here we will further generalize the construction of these combinatorial structures by using an almost bent function f (with $f(0)=0$) with a so-called accomplice g, instead of a crooked function.

Definition 2 *Let $f: V \to V$ be a function. A function $g: V \to V$ is called an accomplice of f if $(H_a(f)+H_a(f)) \cap H_a(g) = \emptyset$ for all $a \neq 0$.*

A crooked function is an accomplice of itself, since if f is crooked, then $H_a(f)$ is the complement of a hyperplane, which implies that the sum of any two of its elements lies in the complementary hyperplane. In fact, any function $g_{c,d}$ given by $g_{c,d}(x) = f(x+c)+d$ is an accomplice of f.

For AB functions that are not crooked it seems hard to find accomplices. In low dimensions it seems typical that in this case the sets $H_a(f)+H_a(f)$ are equal to the entire space V (at least for some a). Nevertheless, we challenge the reader to construct such accomplices, or new crooked functions, since this would give some interesting new codes and graphs by the following constructions.

A *nearly perfect e-error-correcting code* is a code with minimum distance $d=2e+1$ such that each word at distance at least e from the code has distance e or $e+1$ to exactly $\lfloor \frac{L}{e+1} \rfloor$ codewords, where L is the length of the code (clearly such a code is also uniformly packed).

Construction 4 Let f be an AB function with $f(0)=0$, and with an accomplice g. Then the code P consisting of characteristic vectors of pairs (S,T) with $S \subseteq V \setminus \{0\}, T \subseteq V$, such that $|T|$ is even, $\sum_{s \in S} s = \sum_{t \in T} t$, and $\sum_{s \in S} f(s) = \sum_{t \in T} f(t) + g(\sum_{t \in T} t)$ is a double-error-correcting nearly perfect code of size $2^{2N-2-2n}$ and length $L = 2N-1$, i.e. it has the same parameters as the Preparata code.

The proof of this result is essentially given in [12].

As was briefly mentioned in [12] (end of Section 3) linear accomplices would be of particular interest since it looked like new Kerdock codes could be constructed from them. However, it is shown by Brouwer and Tolhuizen [3] that no linear code with the same parameters as the Preparata code exists. This implies that the accomplice g cannot be linear, since such a function would give rise to a linear Preparata code by the above construction, as is easily checked.

Corollary 1 *An almost bent function does not have a linear accomplice.*

A *d-class association scheme* is a partition of the edge set of the complete graph into regular spanning subgraphs $G_1, G_2, ..., G_d$ such that, for any edge $\{x,y\}$ in G_h, the number of vertices z such that $\{x,z\}$ is in G_i and $\{z,y\}$ is in G_j equals a constant p^h_{ij} depending only on h, i, j.

Construction 5 Let f be an AB function f with $f(0) = 0$, and with an accomplice g. Take as vertex set $V \times V$, and let G_1 be the Kasami graph as described in Section 2.2, i.e. distinct vertices (x, a) and (y, b) are adjacent if $a + b = f(x + y)$. The graph G_2 is an isomorphic copy of G_1, and is defined by the equation $a + b = f(x + y) + g(x) + g(y)$. The graphs G_3 and G_4 are the distance-two graphs of G_1 and G_2, respectively. The final graph G_5 is the remainder, and is given by the equations $x = y, a \neq b$. Then the graphs $G_1, G_2, ..., G_5$ form a 5-class association scheme.

For crooked functions this is proven in [12], and this proof is easily adjusted to almost bent functions with an accomplice. This association scheme is of particular interest since it has many fusion schemes (that is, association schemes that are obtained from the original one by uniting some of the graphs) (cf. [4]). For example, the association scheme $\{G_1, G_3, G_2 \cup G_4 \cup G_5\}$ is the 3-class association scheme of the distance 1, 2, and 3 graphs of the distance-regular Kasami graph of the previous section. Further fusion gives the association scheme $\{G_1 \cup G_3, G_2 \cup G_4 \cup G_5\}$ with the same parameters as the 2-class association scheme mentioned by Coulter and Henderson [11], see Section 2.1 (note that these two fusion schemes can be obtained for almost bent functions without an accomplice). Another interesting fusion scheme is $\{G_1 \cup G_2, G_3 \cup G_4, G_5\}$, since it is a so-called quotient of the association scheme of an antipodal distance-regular graph with the same parameters as the Preparata graphs constructed by de Caen, Mathon, and Moorhouse [5]. This means that the following construction generalizes the Preparata graphs.

Construction 6 Let f be an AB function with $f(0) = 0$, and with an accomplice g. Consider the graph with vertex set $V \times V \times GF(2)$, where two distinct vertices (x, a, i) and (y, b, j) are adjacent if $a + b = f(x + y) + (i + j)(g(x) + g(y))$. This graph is a distance-regular graph with parameters $\{2N - 1, 2N - 2, 1; 1, 2, 2N - 1\}$.

Note that the Preparata graphs just like the Kasami graphs are rectagraphs.

If the code P we constructed earlier were linear, then its coset graph would have the same parameters as these antipodal distance-regular graphs. Still, it is possible to indicate the relation between the (nonlinear) code P and the antipodal distance-regular graphs, in the spirit of [5].

2.4 AB functions, CR functions, Hadamard difference sets, and bent functions

An *elementary Hadamard difference set* is a $(2^{2n}, 2^{2n-1} - 2^{n-1}, 2^{2n-2} - 2^{n-1})$ difference set on $GF(2)^{2n}$, i.e. a subset of $GF(2)^{2n}$ of size $2^{2n-1} - 2^{n-1}$, such that any nonzero element of $GF(2)^{2n}$ occurs $2^{2n-2} - 2^{n-1}$ times as a difference of distinct elements of the subset (note that the complement of the difference set is a difference set with parameters $(2^{2n}, 2^{2n-1}+2^{n-1}, 2^{2n-2}+2^{n-1})$, and this is also called a Hadamard difference set). Xiang [23] constructed an elementary Hadamard difference set as follows.

Construction 7 Let f be an AB function. Then the set $\{(x, y) \mid y \in H_x(f), x \neq 0\} = \{(x, f(z) + f(x + z)) \mid x, z \in V, x \neq 0\}$ is an elementary Hadamard difference set on $V \times V$.

It is well-known (essentially already by Turyn [22]) that the characteristic function of an elementary Hadamard difference set is another highly nonlinear function called a *bent function*, i.e a function from $GF(2)^{2n}$ to $GF(2)$ that is at Hamming distance $2^{2n-1} \pm 2^{n-1}$ to all linear functions from $GF(2)^{2n}$ to $GF(2)$. The bent functions corresponding to the difference set of Construction 2 have also been constructed by Carlet, Charpin, and Zinoviev [8].

Another class of Hadamard difference sets and corresponding bent functions can be constructed from crooked functions (cf. [1]).

Construction 8 Let f be a CR function, U a hyperplane in V, and $a \notin U$. Then the set $\{v \in U \mid f(v) \in H_a(f)\}$ is a Hadamard difference set on U with parameters $(2^{n-1}, 2^{n-2} \pm 2^{(n-3)/2}, 2^{n-3} \pm 2^{(n-3)/2})$.

3 Known nonlinear functions

We conlude with the list of all, up to equivalence, known APN, AB, an CR functions. As was mentioned earlier, all known such functions are equivalent to certain power functions $f : GF(2^n) \to GF(2^n)$, $f(x) = x^k$. In Table 1 we give the values of exponents k for odd values of n, $n = 2m + 1$, with the indication to which of the three classes the function belongs. In Table 2 we give those values of k for even n, $n = 2m$, which give APN functions. Note that the inverse of an APN (AB) function is also APN (AB), but this need not be so for CR functions. In particular, the inverses to known CR functions are AB but not CR.

Name	Exponent k	Type	ref.
Gold's functions	$2^i + 1$ with $(i, n) = 1$, $1 \le i \le m$	CR	[16, 1]
Kasami's functions	$2^{2i} - 2^i + 1$ with $(i, n) = 1$, $2 \le i \le m$	AB	[19]
Field inverse	$2^n - 2$	APN	[21]
Welch's function	$2^m + 3$	AB	[7, 18]
Niho's function	$2^m + 2^{m/2} - 1$ (even m) $2^m + 2^{(3m+1)/2} - 1$ (odd m)	AB	[18]
Dobbertin's function	$2^{4i} + 2^{3i} + 2^{2i} + 2^i - 1$ if $n = 5i$	APN	[15]

Table 1: Known APN, AB, and CR functions x^k on $GF(2^n)$, $n = 2m + 1$

Name	Exponent k	Type	ref.
Gold's functions	$2^i + 1$ with $(i, n) = 1$, $1 \le i < m$	APN	[16]
Kasami's functions	$2^{2i} - 2^i + 1$ with $(i, n) = 1$, $2 \le i < m$	APN	[19]
Dobbertin's function	$2^{4i} + 2^{3i} + 2^{2i} + 2^i - 1$ if $n = 5i$	APN	[15]

Table 2: Known APN functions x^k on $GF(2^n)$, $n = 2m$

Acknowledgement. The authors would like to thank Dom de Caen for several stimulating discussions on nonlinear functions, and for his hospitality during the final stage of preparing this paper.

References

[1] T. Bending, D. Fon-Der-Flaass. Crooked functions, bent functions, and distance regular graphs. *Electronic Journal of Combinatorics* **5**, (1998), R34, 14 pp.

[2] A.E. Brouwer, A.M. Cohen, A. Neumaier. *Distance-Regular Graphs*, Springer-Verlag, 1989.

[3] A.E. Brouwer, L.M.G.M. Tolhuizen. A sharpening of the Johnson bound for binary linear codes and the nonexistence of linear codes with Preparata parameters. *Designs, Codes and Cryptography* **3** (1993), 95-98.

[4] D. de Caen, E.R. van Dam. Association schemes related to Kasami codes and Kerdock sets. *Designs, Codes and Cryptography* **18** (1999), 89-102.

[5] D. de Caen, R. Mathon, G.E. Moorhouse. A family of antipodal distance-regular graphs related to the classical Preparata codes. *Journal of Algebraic Combinatorics* **4** (1995), 317–327.

[6] P.J. Cameron, J.H. van Lint. *Designs, Graphs, Codes and their Links*, Cambridge University Press, Cambridge, 1991.

[7] A. Canteaut, P. Charpin, H. Dobbertin. Binary m-sequences with three-valued crosscorrelation: a proof of Welch's conjecture. *IEEE Trans. Inform. Theory* **46** (2000) 4-8.

[8] C. Carlet, P. Charpin, V. Zinoviev. Codes, bent functions and permutations suitable for DES-like cryptosystems. *Designs, Codes and Cryptography* **15** (1998), 125-156.

[9] F. Chabaud, S Vaudenay. Links between differential and linear cryptanalysis. pp. 356-365 in :*Advances in Cryptology, EUROCRYPT '94, Lecture Notes in Computer Science.* Springer, New York, 1995.

[10] P. Charpin. Open problems on cyclic codes. pp. 963-1063 in: V.S. Pless, W.C. Huffman, eds. *Handbook of Coding Theory.* Elsevier, Amsterdam, 1998.

[11] R.S. Coulter, M. Henderson. A class of functions and their application in constructing semi-biplanes and association schemes. *Discrete Math.* **202** (1999), 21-31.

[12] E.R. van Dam, D. Fon-Der-Flaass. Uniformly packed codes and more distance regular graphs from crooked functions. *J. Algebraic Combinatorics*, to appear (2000).

[13] H. Dobbertin. Almost perfect nonlinear power functions on $GF(2^n)$: the Niho case. *Inform. and Comput.* **151** (1999), 57-72.

[14] H. Dobbertin. Almost perfect nonlinear power functions on $GF(2^n)$: the Welch case. *IEEE Trans. Inform. Theory* **45** (1999), 1271-1275.

[15] H. Dobbertin. Almost perfect nonlinear power functions on $GF(2^n)$: a new case for n divisible by 5. Preprint, 1999.

[16] R. Gold. Maximal recursive sequences with 3-valued recursive crosscorrelation functions. *IEEE Trans. Inform. Theory* **14** (1968), 154-156.

[17] T. Helleseth, P.V. Kumar. Sequences with low correlation. pp. 1765-1853 in: V.S. Pless, W.C. Huffman, eds. *Handbook of Coding Theory.* Elsevier, Amsterdam, 1998.

[18] H.D.L. Hollmann, Q. Xiang. A proof of the Welch and Niho conjectures on crosscorrelations of binary m-sequences. Preprint, 1999.

[19] T. Kasami. The weight enumerators for several classes of subcodes of the second order binary Reed–Muller codes. *Inform. and Control* **18** (1971), 369-394.

[20] J.H. van Lint. *Introduction to Coding Theory* (third edition), Springer-Verlag, 1998.

[21] K. Nyberg. Differentially uniform mappings for cryptography. pp. 55-64 in: *Advances in Cryptology, EUROCRYPT '93, Lecture Notes in Computer Science.* Springer, New York, 1994.

[22] R.J. Turyn. Character sums and difference sets. *Pacific J. Math.* **15** (1965), 319-346.

[23] Q. Xiang. Maximally nonlinear functions and bent functions. *Designs, Codes and Cryptography* **17** (1999), 211-218.