Crooked Functions, Bent Functions, and Distance Regular Graphs

T.D. Bending D. Fon-Der-Flaass
School of Mathematical Sciences,
Queen Mary and Westfield College, London E1 4NS, U.K.
T.Bending@mdx.ac.uk d.g.flaass@writeme.com

Submitted: March 25, 1998; Accepted: June 30, 1998.
1991 Mathematical Subject Classification: 05E30, 05B20

Abstract

Let V and W be n-dimensional vector spaces over $GF(2)$. A mapping $Q: V \to W$ is called *crooked* if it satisfies the following three properties:

$Q(0) = 0$;

$Q(x) + Q(y) + Q(z) + Q(x+y+z) \neq 0$ for any three distinct x, y, z;

$Q(x) + Q(y) + Q(z) + Q(x+a) + Q(y+a) + Q(z+a) \neq 0$ if $a \neq 0$ (x, y, z arbitrary).

We show that every crooked function gives rise to a distance regular graph of diameter 3 having $\lambda = 0$ and $\mu = 2$ which is a cover of the complete graph. Our approach is a generalization of a recent construction found by de Caen, Mathon, and Moorhouse. We study graph-theoretical properties of the resulting graphs, including their automorphisms. Also we demonstrate a connection between crooked functions and bent functions.

1 Crooked functions and bent functions

Let V and W be n-dimensional vector spaces over GF(2), and $Q: V \to W$ any mapping. We shall use the notation

$$Q(a_1, a_2, \ldots, a_m) = Q(a_1) + Q(a_2) + \ldots + Q(a_m).$$

Also, for $0 \neq a \in V$, we denote by $H_a(Q)$, or simply H_a, the set

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

We shall denote the size of a finite set X either by $|X|$ or by $\#X$; whichever notation looks better in the context.

DEFINITION 1 *A mapping* $Q : V \to W$ *is called* crooked *if it satisfies the following three properties:*

(1.1) $Q(0) = 0$;

(1.2) $Q(x, y, z, x + y + z) \neq 0$ *for any three distinct* x, y, z;

(1.3) $Q(x, y, z, x + a, y + a, z + a) \neq 0$ *if* $a \neq 0$.

If $Q : V :\to W$ is a crooked function, and $A \in GL(V)$, $B \in GL(W)$ any two automorphisms then the function $Q' = BQA$, $Q'(x) = B(Q(A(x)))$ is also crooked. We shall call such functions Q and Q' *equivalent*. Also, for every $a \in V$, the function $Q''(x) = Q(a, x + a)$ is also crooked. We say that Q'', and every function equivalent to Q'', is *affine equivalent* to Q.

PROPOSITION 2 *If* Q *is a crooked mapping then*

(2.1) Q *is a bijection;*

(2.2) *Every set* $H_a(Q)$ *is the complement of a hyperplane;*

(2.3) *The sets* H_a *are all distinct; in particular, every complement of a hyperplane appears among them exactly once.*

Moreover, every mapping Q *satisfying property* (2.2) *above, and such that* $Q(0) = 0$, *is crooked.*

PROOF. (2.1) follows immediately from property (1.3): if $Q(x) = Q(y)$ for some $x \neq y$, then, setting $a = x + y$, we have $Q(x, x, x, x + a, x + a, x + a) = 0$, contrary to (1.3).

Now we shall prove (2.2) and (2.3).

Condition (1.2) can be reformulated as follows: for $a \neq 0$ and $\{x, x + a\} \neq \{y, y + a\}$ the elements $Q(x) + Q(x + a)$ and $Q(y) + Q(y + a)$ are distinct; or, equivalently, $|H_a| = |V|/2$. Condition (1.3) is equivalent to saying that the sets H_a are sum-free.

Obviously, complements of hyperplanes satisfy both these properties; therefore (2.2) together with $Q(0) = 0$ imply that Q is crooked.

Conversely, let H be a sum-free set of size $|V|/2$, and $K = \{x + y \mid x, y \in H\}$. Fix also any element $h \in H$, and let $K_0 = \{h + x \mid x \in H\}$. H being sum-free means that $H \cap K = \emptyset$, and since $|K| \geq |K_0| = |H| = |V|/2$, we have $|K| = |V|/2$, and $K = K_0 = V \setminus H$. The set K is closed under addition, since $K + K = K_0 + K_0 \subseteq K$, and therefore it is a hyperplane.

Finally, suppose that $H_a = H_b$ for some $a \neq b$, and $K = V \setminus H_a$. Then for every x we have $Q(x) + Q(x+a+b) = Q(x) + Q(x+a) + Q(x+a) + Q(x+a+b) \in H_a + H_b = K$; and therefore $H_{a+b} \subseteq K$, which is impossible. □

Let $Q : V \to W$ be a crooked function, $\dim V = n$. Let $0 \neq a \in V$. We define a linear functional h_a on W, and a mapping $Q_a : V \to \mathrm{GF}(2)$, by the following rules:

$h_a(w) = 1$ if and only if $w \in H_a(Q)$;

$Q_a(v) = h_a(Q(v))$.

PROPOSITION 3 *The dimension of V is odd, $n = 2m+1$.*

For any hyperplane $U \subset V$, and any $0 \neq a \in V$, the set $\{u \in U \mid Q_a(u) = 1\}$ is of size 2^{n-2} if $a \in U$, and of size $2^{n-2} \pm 2^{m-1}$ if $a \notin U$.

PROOF. Suppose first that $a \notin U$. Let the function Q_a on U take the value 1 at x points, and the value 0 at y points, $x + y = 2^{n-1}$. Then on $V \setminus U$ it takes the value 1 at y points, and the value 0 at x points.

For any $v \in V$, by (2.3) we have $|H_v \cap H_a| = |H_v|/2 = 2^{n-2}$. Elements of this intersection correspond to pairs $\{x, x+v\} \subset V$ such that $Q_a(x) = 0$, $Q_a(x+v) = 1$. Summing over all non-zero elements of U we get:

$$2xy = (|U| - 1)|H_v \cap H_a| = (2^{n-1} - 1)2^{n-2}.$$

Now x, y are the roots of the quadratic equation

$$z^2 - 2^{n-1}z + (2^{n-1} - 1)2^{n-3} = 0;$$

$x, y = 2^{n-2} \pm 2^{(n-3)/2}$. Therefore n must be odd, and also the second equality of the proposition is proved. A similar argument proves the first equality. □

As the sizes of the sets in Proposition 3 suggest, crooked functions are closely related to quadrics, or more generally to Rothaus' bent functions [R], which we now explore. We will consider functions $F : V \to \mathrm{GF}(2)$, and will often identify such a function with its support (the set of points on which it takes the value 1), so that we can write $|F|$ (or $\#F$) to mean the size of F's support, for example.

DEFINITION 4 *A mapping $F : V \to \mathrm{GF}(2)$ is called* bent *if for every linear function $L : V \to \mathrm{GF}(2)$ we have $|F + L| = 2^n \pm 2^{n/2}$.*

Clearly if F is a bent function on V then n must be even. As with crooked functions if $A \in GL(V)$ then $F' = FA$ is bent. Also if $a \in V$ then $F''(x) = F(x+a)$ is bent, and if L is linear then $F''' = F + L$ is bent — these three operations all preserve bentness because they map linear functions to linear functions and hence preserve the condition in Definition 4. We say that two bent functions related by any combination of these three operations are equivalent. Note that every non-singular quadratic function is bent, so bent functions exist for all even n.

Extending the summation notation introduced above, we write $F(\bullet, \bullet + a)$ to mean $\{F(x, x+a) \mid x \in V\}$, and so on. The following useful characterisation of bent functions is quite straightforward:

LEMMA 5 *F is bent iff for all non-zero $a \in V$ we have $\#F(\bullet, \bullet + a) = 2^{n-1}$.* □

We can now describe the connection between bent functions and crooked functions.

PROPOSITION 6 *With the above notation, if $0 \neq a \in V$ then for any hyperplane $U \subset V$ not containing a:*

(6.1) *The two functions obtained by restricting Q_a to U and to $V \setminus U$ are complementary, in the sense that we can translate one to the complement of the other.*

(6.2) *The function $Q_a|_U$ is bent.*

PROOF. First, remark that for all $x \in V$ we have $Q(x, x+b) \in H_a$ iff $Q_a(x, x+b) = 1$.

(6.1) For all $x \in V$, $Q(x, x+a)$ is certainly in H_a, so by the above remark $Q_a(x) \neq Q_a(x+a)$ and hence the two restrictions $Q_a|_U$ and $Q_a|_{V \setminus U}$ are complementary via translation through a.

(6.2) Fix a vector $b \in U$. Using (6.1), and the same argument applied to $Q_a(\bullet + b)$,

$$\#Q_a|_U(\bullet, \bullet + b) = \frac{1}{2}\#Q_a(\bullet, \bullet + b).$$

Now by the remark $Q_a(x, x+b) = 1$ iff $Q(x, x+b) \in H_a$, and the number of such x is $2|H_a \cap H_b| = 2^{n-1}$. Hence $\#Q_a|_U(\bullet, \bullet + b) = 2^{n-2}$, but b was arbitrary in U, so by Lemma 5 $Q_a|_U$ is bent. $\square$

We call a function such as Q_a which is composed of a bent function and its complement in this way *quasibent*. Given a quasibent function there is a unique translation (the vector a above) which takes it to its complement, which we call the function's *associated vector*. Translation through any other vector produces a function agreeing with the original one on exactly half the domain, by Lemma 5.

In Proposition 6 we had a choice of the hyperplane U, and different choices lead to different bent functions $Q_a|_U$. However, note that the bent functions corresponding to the various choices differ by linear functions, so are equivalent.

DEFINITION 7 *A set of 2^{n-1} quadratic forms $V \to \mathrm{GF}(2)$ is called a* Kerdock set *if the sum of every two of them is non-singular.*

By considering bilinear forms corresponding to the quadratic functions in a Kerdock set it is easy to show that such a set is maximal.

We write RM_k to denote the kth order Reed-Muller code, consisting of the supports of all functions $V \to \mathrm{GF}(2)$ of degree at most k. A Kerdock set $\mathcal{K}$ induces a Kerdock code consisting of the cosets of the RM_1 represented by the functions in $\mathcal{K}$. A Kerdock code is a subcode of RM_2, and with the above assumption it contains RM_1. It has (length, size, minimum distance) parameters $(2^n, 2^{2n}, 2^{n-1} - 2^{n/2-1})$ — see [CvL, Chapter 12], for example.

However, if we wish to construct a code with these parameters as the union of various cosets of RM_1, it is not necessary for the differences between the representative functions to be non-singular quadratics — by Definition 4 it is enough that they are bent.

Thus we call a set of functions a *bent Kerdock set* if the sum of every two of them is bent. As before without loss of generality we may assume that the constant-0 function is in the set and hence that all the other functions are themselves bent. Similarly we can define a *quasibent Kerdock set* — note that in such a set all the quasibent functions have different associated vectors, for if two functions have the same associated vector their sum is fixed by translation through that vector, so isn't quasibent, so must be the constant-0 function.

The point is that a true Kerdock code has maximal size given its length and minimum distance, among codes in RM_2 which contain RM_1. However, a bent Kerdock set allows us to go outside RM_2. Since the bilinear forms argument does not apply we may be able to find such a set with more than 2^{n-1} functions, and hence obtain a larger code than we can obtain from a true Kerdock set.

DEFINITION 8 (8.1) *A set of functions is called* closed *if the sum of every two functions in the set is also in the set.*

(8.2) *A set of functions* $V \to \mathrm{GF}(2)$ *is called* normal *if every function maps* $0 \in V$ *to* $0 \in \mathrm{GF}(2)$.

If we add the constant-1 function to a quasibent function it remains quasibent, so by doing this where necessary we can make a quasibent Kerdock set normal. By considering the values the functions take on 0 it is clear that this normalisation will preserve closure.

Now, setting $Q_0 \equiv 0$, we have

PROPOSITION 9 $\{Q_a\}_{a\in V}$ *is a closed normal quasibent Kerdock set.*

PROOF. Closure: Pick $a, b \neq 0$. $(Q_a + Q_b)(x) = 1$ iff $Q(x)$ is in exactly one of H_a, H_b. These sets are complements of hyperplanes, so their symmetric difference is also the complement of a hyperplane, and by (2.3) it is some H_c. Thus $(Q_a + Q_b)(x) = 1$ iff $Q(x) \in H_c$ iff $Q_c(x) = 1$, so that $Q_a + Q_b = Q_c$.

Normality: Pick $a \neq 0$. H_a is a hyperplane complement so $Q(0) = 0 \neq H_a$ so $Q_a(0) = 0$. □

It turns out that the converse is true as well:

PROPOSITION 10 *If* $\mathcal{K}$ *is a closed normal quasibent Kerdock set then there exists a crooked function* Q *which induces* $\mathcal{K}$ *via Proposition 9.*

PROOF. $\mathcal{K}$ is closed under addition, and contains 2^n functions, so is an n-dimensional subspace of the space of functions $V \to \mathrm{GF}(2)$. Label the functions in $\mathcal{K}$ with the points of V by picking a basis $\{e_1, \ldots, e_n\}$ for V and a corresponding basis $\{Q_{e_1}, \ldots, Q_{e_n}\}$ for $\mathcal{K}$, and then extending linearly. Similarly, let H_{e_i} denote the hyperplane complement consisting of vectors in V whose dot product with e_i is 1, and then extend this labelling linearly to every hyperplane complement H_v.

Now define $Q(x) = (Q_{e_1}, \ldots, Q_{e_n})$ with respect to our chosen basis for V. By normality $Q(0) = 0$. Now if we pick $a, b \in V$ and write $b = \sum_i \lambda_i e_i$ then

$$\begin{array}{rcl} & Q(v, v+a) & \in H_b \\ \iff & \sum_i Q_{e_i}(v, v+a) e_i & \in \sum_j \lambda_j H_j \\ \iff & \sum_i \sum_{\{j : e_i \in H_j\}} Q_{e_i}(v, v+a) \lambda_j & = 1 \\ \iff & \sum_i Q_{e_i}(v, v+a) \lambda_i & = 1 \\ \iff & Q_b(v, v+a) & = 1 \end{array}$$

If $b = a$ then this last equality is true for all v because Q_a is quasibent, so $\{Q(\bullet, \bullet + a)\} \subseteq H_a$. Otherwise the last equality is true for exactly half the possible values of v, hence so is the first equality. Each value of $Q(v, v+a)$ occurs for two choices of v, so

$$\#\{Q(\bullet, \bullet + a) \cap H_b\} = 2^{n-2} = \frac{1}{2}|H_b|$$

Since this is true for all $b \neq a$ the set $\{Q(\bullet, \bullet + a)\}$ must be the whole of H_a. Thus Q is crooked as required, and it's a straightforward check that Q induces the original set $\mathcal{K}$. $\square$

Note that if we compose Q with a linear map A we obtain a crooked function AQ which induces the same family of quasibent functions as Q, so this reconstruction cannot be unique. In fact it is not even clear whether the reconstruction is unique up to such a composition.

We might hope to use a quasibent Kerdock set to construct a bent Kerdock set. Consider an odd-dimensional space V embedded as a subspace of codimension 1 in a space W. If we have a quasibent function Q_a on V we can extend it to a bent function on W, as follows. Suppose Q_a has associated vector a, and as before pick a hyperplane U in V not containing a. U has two cosets U and $U + a$ in V, and another two cosets $U + b$ and $U + a + b$, say, in $W \setminus V$. Define a function

$$\widehat{Q_a}(x) = \begin{cases} Q_a(x) & \text{if } x \in U \text{ or } x \in U + a \\ Q_a(x + b) & \text{if } x \in U + b \\ Q_a(x + a + b) & \text{if } x \in U + a + b. \end{cases}$$

Thus $\widehat{Q_a}$ consists of four copies of the bent function $Q_a|_U$, except that the copy on $U + a$ has been inverted (recall that $Q|_U$ and $Q|_{U+a}$ are complementary). Then $\widehat{Q_a}$ is a bent function on W — see [R], for example.

So given a crooked function Q we can construct a closed quasibent Kerdock set $\{Q_a\}$, and we'd like to extend these functions to form a closed bent Kerdock set

$\{\widehat{Q_a}\}$. The simplest way to ensure closure of $\{\widehat{Q_a}\}$ after the extension from V to W is to pick the hyperplanes U such that for all distinct a, b, c we have

$$Q_a + Q_b = Q_c \quad \Rightarrow \quad \widehat{Q_a} + \widehat{Q_b} = \widehat{Q_c}.$$

If we write U_a for the hyperplane used to extend Q_a then from the definition of $\widehat{Q_a}$ it's enough to ensure that

$$Q_a + Q_b = Q_c \quad \Rightarrow \quad \overline{U_a} + \overline{U_b} = \overline{U_c}.$$

However, recall that associated with a crooked function Q we already have an indexed set of hyperplane complements $\{H_a\}$ such that

$$H_a + H_b = H_c \quad \Rightarrow \quad Q_a + Q_b = Q_c.$$

Thus we are looking for an indexed set of hyperplane complements $\{\overline{U_a}\}$ such that $a \in \overline{U_a}$ for all a and for all distinct a, b, c we have

$$H_a + H_b = H_c \quad \Rightarrow \quad \overline{U_a} + \overline{U_b} = \overline{U_c}.$$

If we define a map $\varphi : H_a \mapsto \overline{U_a}$ then it is a straightforward check that this last condition is satisfied iff φ is linear. But in this case $\{\varphi H_a\}$ is just the set of H_as associated with the crooked function φQ. Thus finding a suitable set of $\overline{U_a}$s corresponds to finding a linear image of the original Q such that $a \in H_a$ for all a.

We now need some examples of crooked functions to work with.

PROPOSITION 11 *Let $* : V \times V \to V$ be a bilinear multiplication satisfying*

(i) $x * x \neq y * y$ for $x \neq y$; and

(ii) $x * y \neq y * x$ for x, y linearly independent.

Then $Q(x) = x * x$ is crooked.

The converse also holds: if $*$ is a bilinear multiplication such that $Q(x) = x * x$ is crooked then this multiplication satisfies (i) and (ii).

PROOF. In one direction: let $*$ satisfy (i) and (ii).

Condition (1.1) is trivially satisfied.

Condition (1.2): the elements $x + y$ and $x + z$ are linearly independent, therefore

$$x*x+y*y+z*z+(x+y+z)*(x+y+z) = (x+y)*(x+z)+(x+z)*(x+y) \neq 0,$$

by (ii).

Condition (1.3):

$$x * x + y * y + z * z + (x + a) * (x + a) + (y + a) * (y + a) + (z + a) * (z + a)$$

$$= (x + y + z) * (x + y + z) + (x + y + z + a) * (x + y + z + a) \neq 0,$$

by (i).

In the opposite direction: suppose that $Q(x) = x * x$ is crooked. The condition (i) follows from (2.1). Take any two distinct non-zero vectors x, y. We have

$$x * y + y * x = Q(0, x, y, x + y) \neq 0$$

by (1.2), thus proving the condition (ii). $\square$

Examples of such a multiplication can be constructed as follows: take $V = \mathrm{GF}(2^n)$, n odd, take k coprime to n, and let $x * y = x \cdot y^{2^k}$. Thus we get the examples constructed by de Caen et al. in [dCMM]. Actually, these are the only examples of crooked functions known at present. In particular, it is unknown if there exist crooked functions which don't come from a bilinear multiplication.

Unfortunately, given any crooked function Q with $n \leq 9$ constructed by Proposition 11 there is no linear image of Q satisfying $a \in H_a$ for all a, so in these cases we cannot construct a closed bent Kerdock set as suggested above.

We conclude this section with a characterization of crooked functions constructed by Proposition 11.

PROPOSITION 12 *A crooked function Q comes from a bilinear multiplication if and only if*

$(*)$ *for every 3-dimensional affine subspace $U \subseteq V$*

$$Q(U) = \sum_{u \in U} Q(u) = 0.$$

PROOF. Let $\dim V = \dim W = n$. Let $\mathcal{C}$ be the set of all functions $Q : V \to W$ satisfying both $(*)$ and the condition (1.1) of Definition 1, which is simply $Q(0) = 0$. Let also $\mathcal{M}$ be the set of all bilinear maps $f : V \times V \to W$, and $\mathcal{M}_0 = \{f \in \mathcal{M} \mid f(x, x) = 0 \text{ for all } x \in V\}$. The sets $\mathcal{C}$, $\mathcal{M}$, and $\mathcal{M}_0$ are vector spaces over GF(2). It is easy to check that for every $f \in \mathcal{M}$, the function $Q(x) = f(x, x)$ is in $\mathcal{C}$. Two functions $f_1, f_2 \in \mathcal{M}$ give the same function from $\mathcal{C}$ if and only if they are in the same coset of $\mathcal{M}_0$. So, to prove the theorem, we only need to check that $\dim \mathcal{C} = \dim \mathcal{M} - \dim \mathcal{M}_0$.

A function $f \in \mathcal{M}$ is uniquely determined by its n^2 values $f(e_i, e_j)$ on basis vectors; therefore $\dim \mathcal{M} = n^3$.

A function $f \in \mathcal{M}$ belongs to $\mathcal{M}_0$ if and only if for all x, y, $f(x, y) = f(y, x)$, and $f(e_i, e_i) = 0$ for all basis vectors. Indeed, if $f(x, x) \equiv 0$ then for all x, y we have

$$f(x, y) + f(y, x) = f(x + y, x + y) + f(x, x) + f(y, y) = 0.$$

Conversely, if for all x, y we have $f(x, y) = f(y, x)$ then the same equality implies that the function $f(x, x)$ is linear; and if it is zero on the basis vectors then it is identically zero. Therefore an element $f \in \mathcal{M}_0$ is uniquely determined by the values $f(e_i, e_j)$ for $i < j$, and it follows that $\dim \mathcal{M}_0 = n\binom{n}{2}$.

Finally, the characteristic vectors of affine subspaces of dimension 3 generate the Reed-Muller code $\mathrm{RM}(n, n-3)$ the dimension of which is equal to

$$\binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{n-3} = 2^n - 1 - n - \binom{n}{2}$$

(see, for example, [CvL, Chapter 12]). A function $Q \in \mathcal{C}$ is uniquely determined by n functions $Q_i : V \to \mathrm{GF}(2)$, the coordinates of the values with respect to a basis of W. Each Q_i is orthogonal to $\mathrm{RM}(n, n-3)$ and, in addition, $Q_i(0) = 0$. Therefore $\dim \mathcal{C} = n(n + \binom{n}{2})$. Now comparing the dimensions gives us the theorem. □

2 Crooked functions and rectagraphs

A *rectagraph* is a graph without triangles in which every pair of vertices at distance 2 lies in a unique 4-cycle. There are not too many constructions of rectagraphs known; especially rectagraphs of small diameter. In this section we show that every crooked function gives rise to a distance regular rectagraph of diameter 3.

Let $Q : V \to W$ be a crooked function. For $a, b \in V$, $i, j \in \mathrm{GF}(2)$ define

$$D(a, i; b, j) = Q(a + b) + (i + j + 1)Q(a, b).$$

Let $G = G_Q$ be the graph on the vertex set $V \times \mathrm{GF}(2) \times W = \{(a, i, \alpha)\}$; vertices (a, i, α) and (b, j, β) are adjacent if and only if they are distinct, and

$$\alpha + \beta = D(a, i; b, j).$$

PROPOSITION 13 *The graph G_Q is distance regular with intersection array*

$$(2^{n+1} - 1, 2^{n+1} - 2, 1;\ 1, 2, 2^{n+1} - 1)$$

— a distance regular 2^n-cover of the complete graph $K_{2^{n+1}}$.

PROOF. The sets $F_{a,i} = \{(a, i, \alpha) \mid \alpha \in W\}$ will be the fibres of the cover. They are independent sets, since $D(a, i; a, i) = Q(a + a) = 0$ by (1.1). Any two fibres are joined by a 1-factor; therefore vertices in every fibre are at mutual distances three or more. We only need to show that G has parameters $\lambda = 0$ and $\mu = 2$ — distance regularity will then follow by a simple counting argument. Add a loop at each vertex of G — this can be done by dropping the condition $(a, i, \alpha) \neq (b, j, \beta)$ in the definition of G_Q. We need to show that in the resulting graph we have $\lambda = \mu = 2$; or, that when $(a, i) \neq (b, j)$, the multiset

$$\{D(a, i; x, k) + D(b, j; x, k) \mid x \in V,\ k \in \mathrm{GF}(2)\}$$

is the whole W taken with multiplicity 2.

Case 1. $i \neq j$. We shall show that $\{D(a,i;x,i)+D(b,j;x,i) \mid x \in V\} = W$ — this will suffice. It is enough to check that

$$D(a,i;x,i)+D(b,j;x,i)+D(a,i;y,i)+D(b,j;y,i) \neq 0$$

for $x \neq y$. The sum in question is equal to

$$Q(a,x,a+x,b+x,a,y,a+y,b+y)$$

$$= Q(x,x+(x+y),a+x,a+x+(x+y),b+x,b+x+(x+y)) \neq 0$$

by (1.3).

Case 2. $i = j$. In this case $a \neq b$. Let $k = i+1$. We shall show that

$$\{D(a,i;x,i)+D(b,i;x,i)\} \cap \{D(a,i;x,k)+D(b,i;x,k)\} = \emptyset, \quad (i)$$

and that in both these multisets every element occurs twice — (ii) and (iii).

(i) $Q(a,x,a+x,b,x,b+x,a+y,b+y) = Q(a,a+(a+b),a+x,a+x+(a+b),a+y,a+y+(a+b)) \neq 0$ by (1.3).

(ii) Let $Q(a,x,a+x,b,x,b+x) = Q(a,y,a+y,b,y,b+y)$; then $Q(a+x,b+x,a+y,(a+x)+(b+x)+(a+y)) = 0$. By (1.2), this happens in exactly two cases: when $x = y$, and when $x = y+(a+b)$.

(iii) The same as (ii): $Q(a+x,b+x,a+y,b+y) = 0$ iff either $x = y$ or $x = y+(a+b)$.

The proposition is proved. $\square$

We call graphs obtained from a crooked function by the above construction *crooked graphs*. Now we shall study structural properties of crooked graphs. We shall follow the lines of [dCMM] as far as possible; many of the arguments from that paper can be applied to our more general situation almost unchanged.

It is evident that equivalent crooked functions give rise to isomorphic graphs; linear transformations of V and W result only in renaming the fibres, and vertices in fibres.

Let $G = G_Q$ be a crooked graph. Obviously, the parition of vertices into fibres is uniquely determined. Following [dCMM], call a set of four fibres a *quad* iff their union contains a subgraph isomorphic to the 3-cube. As the graph induced on any four quads has valency 3, the 3-cube must be one of its connected components.

Also, by *pairs* we mean the sets $P_a = F_{a,0} \cup F_{a,1}$ for $a \in V$, and by *halves* the sets $H_i = \cup_{a\in V} F_{a,i}$ for $i = 0,1$. The last two definitions, unlike the definition of a quad, depend on the presentation of G as a crooked graph; but we shall show that pairs and halves can be recovered from the graph structure only.

PROPOSITION 14 *The quads are the sets of the form*

(i) $\{F_{a,i}, F_{b,i}, F_{c,i}, F_{a+b+c,i}\}$ *where* $a,b,c \in V$ *are distinct, and* $i \in \{0,1\}$*; and*

(ii) $\{F_{a,0}, F_{b,0}, F_{a,1}, F_{b,1}\}$ *where* $a,b \in V$ *are distinct.*

A set S of two fibres is a pair if and only if S together with an arbitrary third fibre is contained in a unique quad.

A set S of 2^n fibres is a half if and only if any three fibres in S are contained in a unique quad in S.

PROOF. Take a quad, and denote the vertices forming a cube by symbols $[ijk]$, $i, j, k \in \{0, 1\}$, in the usual way. Each fibre contains two opposite vertices of the cube. Suppose, without loss of generality, that

$[000] = (a, 0, \alpha)$,

$[011] = (b, 0, \beta)$.

Then

$[111] = (a, 0, \beta + Q(a, b, a + b))$,

$[100] = (b, 0, \alpha + Q(a, b, a + b))$.

The other two fibres are those containing the two common neighbours of [000] and [011]; from the proof of Proposition 13, case 2, it follows that they are in the same half. Again, we need to consider two cases.

Case 1. $\alpha + \beta = Q(a + x, b + x)$ for some $x \in V$. Let $y = x + a + b$. Then we also have $\alpha + \beta = Q(a + y, b + y)$.

The coordinates of the remaining vertices now are:

$[001] = (x, 1, \alpha + Q(a + x))$,

$[010] = (y, 1, \alpha + Q(a + y))$,

$[110] = (x, 1, \beta + Q(a, b, a + b, a + x))$,

$[101] = (y, 1, \beta + Q(a, b, a + b, a + y))$.

They form the remaining two edges of the cube if and only if

$$Q(x, y, x + y) = \alpha + \beta + Q(a, b, a + b, a + x, a + y)$$

which is equivalent to

$$Q(x, x + a + b, a, b) = 0.$$

By (1.2), this holds if and only if $\{x, y\} = \{a, b\}$, and we get the quads of type (ii).

Case 2. $\alpha + \beta = Q(a, b, a + x, b + x)$ for some $x \in V$. Then we also have $\alpha + \beta = Q(a, b, a+y, b+y)$ for $y = x+a+b$, and the four fibres are $\{(a, 0), (b, 0), (x, 0), (y, 0)\}$. An easy calculation shows that they indeed form a quad of type (i).

The last two claims of the proposition are taken unchanged from [dCMM, Lemma 2.6]. $\square$

Note that the quads inside a half determine on the fibres in this half the structure of an affine space; and the affine structures determined in this way on the two halves are identical, which means that we can consider them as a single affine structure on the set of pairs.

Let $A = \mathrm{Aut}G$.

The mappings $s_\gamma : (a, i, \alpha) \to (a, i, \alpha + \gamma)$, $\gamma \in W$, are automorphisms of G, and comprise the whole kernel of the action of A on the fibres (see [GH, Lemma 7.3]); so the affine structure on each fibre is also uniquely determined. Let $F = \langle s_\gamma \mid \gamma \in W \rangle$.

The automorphism $z : (a, i, \alpha) \to (a, i+1, \alpha)$ is the unique automorphism interchanging the fibres inside each pair which has the additional property that every vertex v is adjacent to $z(v)$. Therefore, z lies in the centre of A. The group $P = \langle F, z\rangle$ is the kernel of the action of A on the pairs.

PROPOSITION 15 *Let $G = G_Q = \{(a, i, \alpha)\}$ be a crooked graph constructed from a crooked mapping $Q : V \to W$, and $c \in V$. The following are equivalent:*

(i) there exists another crooked labelling, $[a, i, \alpha]$, of G in which $[0, 0, 0] = (c, 0, 0)$;

(ii) there exists another crooked labelling, $[a, i, \alpha]$, of G in which $[0, 0, 0] = (c, i, \gamma)$;

(iii) For every 3-dimensional affine subspace $U \subseteq V$ parallel to c

$$Q(U) = \sum_{u \in U} Q(u) = 0.$$

Moreover, then the crooked function corresponding to the new labelling is affine equivalent to Q.

PROOF. (i) and (ii) are clearly equivalent, since by the above remarks all vertices in the pair P_c are equivalent under the automorphism group.

Now, let $[a, i, \alpha]$ be a crooked labelling with the crooked function R, such that $[0, 0, 0] = (c, 0, 0)$. Since the affine structure in fibres is invariant, me can assume without loss of generality that $[0, 0, \beta] = (c, 0, \beta)$ for all $\beta \in W$. Since pairs are also invariant, we have $[0, 1, \beta] = (c, 1, \beta)$ ($[0, 1, \beta]$ being the unique neighbour of $[0, 0, \beta]$ inside the pair).

Similarly, invariance of the affine structure on the set of pairs enables us to assume that, for every $x \in V$, $\beta \in W$, $[x, i, \beta] = (x + c, i, \gamma)$ for some $\gamma = \gamma(x, \beta) \in W$.

To find γ, note that the vertices $[0, i, \beta] = (c, i, \beta)$ and $[x, i, \beta] = (x + c, i, \gamma)$ are adjacent. Therefore, $\beta + \gamma = Q(x, c, x + c)$.

Now we know the new labels for all vertices:

$$[x, i, \beta] = (x + c, i, \beta + Q(x, c, x + c)).$$

The vertices $[a, i, \alpha]$ and $[b, i, \beta]$ are adjacent, on one side, if and only if $\alpha + \beta = R(a, b, a + b)$. On the other side, these vertices are $(a + c, i, \alpha + Q(a, c, a + c))$ and $(b+c, i, \beta+Q(b, c, b+c))$, and so are adjacent if and only if (after a simple calculation) $\alpha + \beta = Q(a, b, a + b)$. Therefore

$R(a, b, a + b) = Q(a, b, a + b).$ $(*)$

Considering in the same manner the vertices $[x, i, \alpha]$ and $[a + x, j, \beta]$ for $i \neq j$, we obtain

$R(a) = Q(a) + Q(x, x + c, x + a, x + a + c).$ $(**)$

Thus, for any a the value $Q(x, x+c, x+a, x+a+c) = Q(a)+R(a)$ is independent of x. Setting $x = 0$, we get $R(a) = Q(c, a + c)$, so R is affine equivalent to Q.

To finish the proof, note that $(**)$ implies the assertion (iii) of the proposition; and (iii) together with $R(a) = Q(c, a + c)$ imply both $(*)$ and $(**)$. □

3 Dimension 3

PROPOSITION 16 *The crooked function of dimension 3 is unique up to equivalence. The corresponding crooked graph is vertex transitive.*

PROOF. Note that Proposition 11 gives us at least one crooked function of dimension 3. Let $Q : V \to W$ be a crooked function of dimension 3. We shall denote elements of the spaces V and W by symbols (ijk) and $[ijk]$, respectively $(i, j, k \in \{0, 1\})$. We have:

$$Q((000)) = [000].$$

The elements $Q((001))$, $Q((010))$, $Q((011))$ are non-zero, and have a non-zero sum. Therefore they are linearly independent, and without loss of generality we can assume that

$$Q((001)) = [001],$$
$$Q((010)) = [010],$$
$$Q((011)) = [100].$$

(Any other situation can be reduced to this one by a suitable linear transformation of W.) Similarly, applying a suitable transformation of V, we can ensure that

$$Q((100)) = [110].$$

Now we are left with only 6 possibilities, and it is no problem to check that, up to equivalence, we have only one crooked function:

$$Q((101)) = [011],$$
$$Q((110)) = [101],$$
$$Q((111)) = [111].$$

Let G be the corresponding crooked graph. The property (iii) from Proposition 15 is trivially satisfied; therefore, choosing any vertex of G as $(0, 0, 0)$, we arrive at a crooked labelling. As this new labelling is equivalent to the initial one, we conclude that the automorphism group of G is vertex-transitive. □

The automorphism group turns out to be isomorphic to $2 \times 2^3.L(3, 2)$, the extension being non-split ([dCMM]).

A final remark. The authors have not been able to find examples of crooked functions other than those found by de Caen et al. (described here after Proposition 11). Nevertheless, neither the conditions of Definition 1 nor those of Proposition 11 seem too restrictive. We hope that many other crooked functions (and crooked graphs) can be found.

References

[dCMM] 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.

[CvL] P.J.Cameron, J.H.van Lint. Designs, Graphs, Codes and their Links. LMS Student Texts, 22, Cambridge, 1991.

[GH] C.D. Godsil, A.D. Hensel. Distance Regular Covers of the Complete Graph. *Journal of Combin. Th. Ser. B 56 (1992)*, 205–238.

[R] O.S. Rothaus. On "Bent" Functions, *Journal of Combin. Th. Ser. A 20 (1976)*, 300–305.