September 2000

Construction of cubic homogeneous boolean bent functions

Jennifer Seberry
University of Wollongong, jennie@uow.edu.au

Tianbing Xia
University of Wollongong, txia@uow.edu.au

J. Pieprzyk
University of Wollongong

Abstract
We prove that cubic homogeneous bent functions f : V2n → GF(2) exist for all n ≥ 3 except for n = 4.

Construction of cubic homogeneous boolean bent functions[1]

Jennifer Seberry, Tianbing Xia, Josef Pieprzyk

Centre for Computer Security Research,
University of Wollongong, NSW 2500, Australia
Email: [j.seberry, tx01, josef] @uow.edu.au

Abstract

We prove that cubic homogeneous bent functions $f : V_{2n} \rightarrow GF(2)$ exist for all $n \geq 3$ except for $n = 4$.

1 Introduction

The theory of S-boxes emerged as a branch of cryptography whose main aim is the design of cryptographically strong Boolean functions or S-boxes. Typically the strength of an S-box is quantified by a collection of cryptographic criteria. There is an intimate relation between cryptographic attacks and this collection of cryptographic criteria. A new criterion is added to the collection every time a new cryptographic attack is invented. If an S-box satisfies the criterion, then the designer may immunise a cryptographic algorithm against the attack by using the S-box. Bent functions are basic algebraic constructions which enable designers of cryptographic algorithms to make them immune against a variety of attacks including the linear cryptanalysis.

We concentrate on homogenous bent functions. Homogeneousity becomes a highly desirable property when efficient evaluation of the function is important. It was argued in [5], that for cryptographic algorithms which are based on the structure of MD4 and MD5 algorithms, homogeneous Boolean functions can be an attractive option; they have the property that they can be evaluated very efficiently by re-using evaluations from previous iterations.

Let us summarise some arguments from [5] which can be used to justify our interest in homogeneous functions. Note that in the MD-type hashing (such as MD4 or MD5 or HAVAL), a single Boolean function is used for a number of rounds (in MD4 and MD5 this number is 16, in HAVAL it is 32). In two consecutive rounds, the same function is evaluated with all variables the same except one. More precisely, in the i-th round the function $f(x)$ is evaluated for $(x_1, ..., x_n)$. In the $(i + 1)$-th round, the same function is evaluated for $f(x_2, ..., x_n, y_1)$ where y_1 is a new variable generated in the i-th round. Note that variables are rotated between two rounds. It can be proved that evaluations from the i-th round can be re-used

[1] Published in Australasian Journal of Combinatorics 22(2000), pp 233-245

if f (x) = f (ROT(x)). These Boolean functions create a class of rotation-symmetric functions. An important property of rotation-symmetric functions is that they can be decomposed into one or more homogeneous parts. To keep a round function f (x) short, one would prefer a homogeneous rotation-symmetric function.

In [4] we proved there do not exist homogeneous bent functions of degree n in $GF(2)^{2n}$ when n > 3. However the construction of high degree homogeneous bent functions has remained an open problem. In this paper we show how to construct cubic homogeneous bent functions in $GF(2)^{2n}$ where $n \geq 3$ and $n \neq 4$.

2 Background

Let $V_n = GF(2)^n$ be the set of all vectors with n binary co-ordinates. V_n contains 2^n different vectors from $\alpha_0 = (0, 0, ..., 0)$ to $\alpha_{2^n-1} = (1, 1, ...,1)$. A boolean function $f : V_n \rightarrow GF(2)$ assigns binary values to vectors from V_n. Let $x = (x_1, \ldots, x_n)$ and $y = (y_1, ..., y_n)$ be two vectors in $GF(2)^n$. Throughout the paper we use the following notations:

- *the inner product* of x and y defined as

  $$\langle x, y \rangle = x \circ y = x_1 y_1 \oplus \cdots \oplus x_n y_n = \sum_{i=1}^{n} x_i y_i ,$$

  where $x = (x_1, ..., x_n)$ and $y = (y_1, ..., y_n)$;
- *the inner addition* of x and y given by

  $$x \oplus y = (x_1 \oplus y_1, \cdots, x_n \oplus y_n) ,$$

  where $x = (x_1, ..., x_n)$ and $y = (y_1, ..., y_n)$. Note that inner addition is equivalent to bit-by-bit XOR addition;
- *the extension* of vector $x \in V_n$ by a vector $y \in V_m$, is defined as

  $x \otimes y = (x_1, ..., x_n, y_1, ..., y_m)$.

  The vector $x \otimes y \in V_{n+m}$.
- *the Hadamard product* of vector $a = (a_1, ..., a_n)'$ and vector $b = (b_1, ..., b_n)'$ given by

  $$a * b = (a_1 b_1, ..., a_n b_n)'$$

  where the symbol "'" means transpose of the vector or matrix.

Definition 1 A boolean function $f : V_n \rightarrow GF(2)$ is homogeneous of degree k if it can be represented as

$$f(x) = \bigoplus_{1 \leq i_1 \leq \cdots \leq i_k \leq n} a_{i_1 \cdots i_k} x_{i_1} \ldots x_{i_k} . \tag{1}$$

where $x = (x_1, \ldots, x_n)$. Each term $x_{i_1} \ldots x_{i_k}, a_{i_1 \ldots i_k} \in GF(2)$ *is a product of precisely k co-ordinates.*

Let p_n denote the set of all boolean functions in $GF(2)^n$. For $f \in p_n$ we let deg(f) be the degree of f. Define

$$R(m, n) = \{ f \in p_n : \deg(f) \le m\}.$$

If $f \in p_{2n}$ is a bent function, we call $f + R(1, 2n)$ a bent coset.

Let ~ denote the equivalence relation under the action of linear transformation. We define for any nonsingular $n \times n$ matrix A and vector $\alpha \in GF(n)$,

$$\sigma(f) = f(XA \oplus \alpha), \text{ where } X = (x_1, \ldots, x_n).$$

Let F f denote the Fourier transform of f. Thus F f is defined as

$$Ff(\alpha) = \frac{1}{2^n} \sum_{X \in V_{2n}} (-1)^{f(X) \oplus \langle X, \alpha \rangle} \tag{2}$$

3 The Rank

For $0 \le t \le n$, let S_t^n be the set of all t-subsets of $\{1, ..., n\}$. For any $I \subset S_t^n$, we write $X_I = \prod_{j \in I} x_j$. Let $t_1, t_2 \ge 0$ with $t_1 + t_2 = t$, and f= $\sum_{I \subset S_t^n} a_I X_I \in R(t,n)/R(t-1,n)$, where $a_I \in GF(2)$. We define an $\binom{n}{t_1} \times \binom{n}{t_2}$ matrix $B_{t_1,t_2}^{(t,n)}(f)$ over GF(2) as follows:

1. The rows and columns of $B_{t_1,t_2}^{(t,n)}(f)$ are labelled by the elements of $S_{t_1}^n$ and the elements of $S_{t_2}^n$, respectively.
2. $a_I = 0$ for $I \subset \{1, ..., n\}$ with $\|I\| < t$.

   For $F \in R(t,n)/R(t-1, n)$, $t \ge 1$, let

$$r_t(F) = \text{rank}\left(B_{1,t-1}^{(t,n)}(F)\right). \tag{3}$$

If $F \in R(t, n)$, we define $r_t(F) = r_t(F \oplus R(t-1, n))$.

Theorem 1 (Hou[3]) Let F be a cubic bent function in p_{2n}.

1. If $r_2(F) > 0$, then
$$F \sim P(x_i, .., x_{2n-2}) \oplus x_{2n-1}x_{2n}, \tag{4}$$
   where P is a cubic bent function in P_{2n-2}.
2. If $r_3(F) < n$, then $r_2(F) > 0$.
3. If $r_3(F) = n$ and $r_2(F) = 0$, then
$$F \sim Q(x_1, \ldots, x_n) \oplus \sum_{i=1}^{n} x_i x_{n+i} \tag{5}$$
   for some $Q \in p_n$.

Theorem 2 Let f (x) be a boolean function in $GF(2)^n$ and g(y) be a boolean function in $GF(2)^m$. $f(x) \oplus g(y)$ *is a homogeneous bent function of degree k in* $GF(2)^{n+m}$ *if and only if both f (x) and g(y) are homogeneous bent functions of degree k.*

Proof. If f(x) and g(y) are homogeneous bent functions of degree k, it is easy to see $H(z) = f(x) \oplus g(y)$ is a homogeneous bent function of degree k where $z = x \otimes y$.

On the other hand, if $H(z) = f(x) \oplus g(y)$ is a homogeneous bent function of degree k where $z = x \otimes y$, we know f(x) and g(y) are bent functions, too. Obviously f(x) and g(y) are homogeneous bent functions.

The proof is complete. ❑

4 The Equivalence

Definition 2 Let F(X) and G(X) be two bent functions in $GF(2)^{2n}$. If there exists a matrix T $\in GL(2n, 2)$ *and* $b \in GF(2)^{2n}$, *such that*

$$F(XT) \oplus \langle X, b \rangle = G(X),$$

we say that F equivalent to G, and denote this by F ~ G.

Theorem 3 Let F(X) be a cubic bent function in $GF(2)^{2n}$ *and G(X) be a homogeneous cubic bent function in* $GF(2)^{2n}$. *If F ~ G, then* $r_2(F) = 0$ *and* $r_3(F) \geq n$.

Proof. Since F ~ G, from the results of the work[3] we know $r_i(F) = r_i(G)$, i = 2, 3. Because G is a homogeneous bent function, we have $r_2(G) = 0$, $r_2(F) = r_2(G) = 0$. From Theorem 1 we know $r_3(F) \geq n$, which completes the proof. ❑

Lemma 1 Let $A = (a_{ij})$ be an n $\times$ *n matrix,* $a_{ij} \in GF(2)$, $1 \leq i, j \leq n$, *and X be a vector in* $GF(2)^n$, *Then* XAX' *is a linear boolean function if and only if* $A = A'$.

Proof. If XAX' is a linear boolean function, then there exists a vector $b \in GF(2)^n$, such that

$$XAX' = \langle X, b \rangle \tag{6}$$

for all $X \in GF(2)^n$. As $b = (b_1, ..., b_n)$, and $X = (x_1, ..., x_n)$, we can rewrite (6) in the following form:

$$\sum_{ij=1}^{n} a_{ij} x_i x_j = \sum_{i=1}^{n} b_i x_i \tag{7}$$

For any fixed i, $1 \leq i \leq n$, let $x_i = 1$ and $x_j = 0$, $j \neq i$, $1 \leq j \leq n$, then from (7) we have

$$a_{ii} = b_i, \ i = 1, \dots, n. \tag{8}$$

For any pair of i, j, $i \neq j$, $1 \leq i, j \leq n$, let $x_i = x_j = 1$, $x_k = 0$, $k \neq i$ and $k \neq j$, $1 \leq k \leq n$, then from (7) we have

$$a_{ii} + a_{jj} + a_{ij} + a_{ji} = b_i + b_j. \tag{9}$$

From (8) and (9) we have

$$a_{ij} = a_{ji} \quad 1 \leq i, \; j \leq n, \tag{10}$$

and $A = A'$.

Assume that $A = A'$. We obtain the following:

$$XAX' = \sum_{ij=1}^{n} a_{ij} x_i x_j$$

$$= \sum_{i=1}^{n} a_{ii} x_i^2 \oplus \sum_{i=1}^{n-1} \sum_{j=i+1}^{n} (a_{ij} \oplus a_{ji}) x_i x_j = \sum_{i=1}^{n} a_{ii} x_i$$

is a linear boolean function. This completes the proof. o

5 The Matrix Representation of Cubic Bent Functions

Let F(X) be a cubic bent function in $GF(2)^{2n}$, $r = r_3(F) \geq n$, $r_2(F) = 0$, then

$$F(X) = \sum_{(i,j,k)\in E} x_i x_j x_k \oplus \sum_{(u,v)\in D} x_u x_v, \tag{11}$$

$i \neq j$, $j \neq k$, $k \neq i$, $u \neq v$. Suppose E is a collection of unordered triples, and further suppose D is a collection of unordered pairs. Since $r = r_3(F)$, the cubic part of F(X) can be represented as

$$f(x_1, ..., x_r) = \sum_{(i,j,k)\in E} x_i x_j x_k. \tag{12}$$

We denote

$$X = (x_1, ..., x_{2n}) = X_{(1)} \otimes X_{(2)},$$

$$X_{(1)} = (x_1, \ldots, x_r), \quad X_{(2)} = (x_{r+1}, ..., x_{2n}). \tag{13}$$

The quadratic part of F(X) can be represented as

$$g(x_1, ..., x_{2n}) = \sum_{(u,v)\in D} x_u x_v = XQX'_{(1)}, \tag{14}$$

where $Q = (Q_{ij})$ is a $2n \times r$ matrix with

$$q_{ij} = \begin{cases} 1, & i > j \text{ and } (i, j) \in D, \\ 0, & \text{otherwise}, \end{cases} \tag{15}$$

where $1 \le i \le 2n$, $1 \le j \le r$. It is known that $r_3(F) = r_3(f)$. We can construct a matrix $B_{1,2}^{(3,r)}(f)$ with r rows and $\frac{r(r-1)}{2}$ columns. The rows of the matrix are ordered (1, 2), …, (1, r), (2, 3), ..., (2, r), …, (r–1, r), and the columns of the matrix are ordered 1, …, r. Then the ith row and (j, k)th column of the matrix is 1, if $(i, j, k) \in E$, or is 0, if $(i, j, k) \notin E$.

Notation 1 *Let* $T = (t_{ij})$, $1 \le i \le n$, $1 \le j \le p$. We denote the jth column of the matrix by t_j, so $T = (t_1, \ldots, t_p)$. Let

$$T^* = (t_1 * t_2, \ldots t_1 * t_p, t_2 * t_3, \ldots, t_2 * t_p, \ldots, t_{p-1} * t_p). \tag{16}$$

Let $X = (x_1, \ldots, x_n) \in V_n$, we denote

$$X^* = (x_1x_2, x_1x_3, \ldots, x_{n-1}x_n) \tag{17}$$

T* is a matrix with n rows and $\frac{p(p-1)}{2}$ columns. We denote

$$C = C(f) = B_{1,2}^{(3,r)}(f)'. \tag{18}$$

Then

$$f(x_1, \ldots, x_r) = X_{(1)}^* C X_{(1)}', \tag{19}$$

where $X_{(1)}$, C, $X_{(1)}'$ are defined as (13), (18), (17).

From (11), (12), (13), (14), and (19) we have

$$F(X) = X_{(1)}^* C X_{(1)}' \oplus XQX_{(1)}' \tag{20}$$

Example 1 $F(x_1, \ldots, x_6) = x_1x_2x_3 \oplus x_2x_4x_5 \oplus x_1x_2 \oplus x_1x_4 \oplus x_2x_6 \oplus x_3x_5 \oplus x_4x_5$. $r = r_3(F) = 5$. $X_{(1)} = (x_1, x_2, \ldots, x_5)$, and

$$C' = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix},$$

$$Q = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

We have $F(X) = X_{(1)}^* C X_{(1)}' \oplus XQX_{(1)}'$.

Theorem 4 Let F(X) be the cubic bent function in $GF(2)^{2n}$ which is defined by (20). The function F(X) possesses a cubic homogeneous equivalent if and only if there exists a nonsingular $2n \times 2n$ *matrix* $T = T_{(1)} \otimes T_{(2)}$, *and*

$$(T^{*}_{(1)}C \oplus TQ)T'_{(1)} = T_{(1)}\,(T^{*}_{(1)} \oplus TQ)'\ , \qquad (21)$$

where $T_{(1)}$ is a matrix with 2n rows and $r = r_3(F)$ columns. $T_{(1)}$ is defined by (16).

Proof. From formula (12) we have the cubic part of F(X):

$$f(X_{(1)}) = \sum_{(i,j,k)\in E} x_i x_j x_k\ . \qquad (22)$$

We fix $(i, j, k) \in E$, when $Y = XT$, $T = (T_1, \ldots, T_{2n})$, where T_u is the uth column of matrix T, and t_{ui} denote the uth column and ith row of the matrix T, $1 \le u, i \le 2n$. y_i, y_j, y_k become XT_i, XT_j, XT_k.

$$y_i y_j y_k = XT_i XT_j XT_k = \sum_{u,v,w=1}^{2n} x_u t_{ui} x_v t_{vj} x_w t_{wk} = S_1 \oplus S_2, \qquad (23)$$

where

$$S_1 = \sum_{u\neq v, v\neq w, w\neq u} t_{ui} t_{vj} t_{wk} x_u x_v x_w = \delta_{ijk} \qquad (24)$$

is a cubic homogeneous polynomial, and

$$S_2 = \left(\sum_{u=v\neq w} \oplus \sum_{u=w\neq v} \oplus \sum_{u\neq v=w} \oplus \sum_{u=v=w} \right) t_{ui} t_{vj} t_{wk} x_u x_v x_w$$

$$= \left(\Big(\sum_{u=v\neq w} \oplus \sum_{u=v=w}\Big) \oplus \Big(\sum_{u=w\neq v} \oplus \sum_{u=v=w}\Big) \oplus \Big(\sum_{u\neq v=w} \oplus \sum_{u=v=w}\Big) \right) t_{ui} t_{vj} t_{wk} x_u x_v x_w$$

$$= \sum_{u=1}^{2n} t_{ui} t_{uj}\, x_u \sum_{w=1}^{2n} t_{wk}\, x_w \oplus \sum_{u=1}^{2n} t_{ui} t_{uk}\, x_u \sum_{v=1}^{2n} t_{vj}\, x_v \oplus \sum_{v=1}^{2n} t_{vj} t_{vk}\, x_v \sum_{u=1}^{2n} t_{ui}\, x_u$$

$$= X(T_i * T_j).XT_k \oplus X(T_i * T_k).XT_j\ X(T_j * T_k).XT_i. \qquad (25)$$

So,

$$f(XT_{(1)}) = \sum_{(i,j,k)\in E} XT_i XT_j XT_k = \sum_{(i,j,k)\in E} \delta_{ijk}$$

$$\oplus \sum_{(i,j,k)\in E} (X(T_i * T_j).XT_k \oplus X(T_i * T_k).XT_j \oplus X(T_j * T_k).XT_i)$$

$$= \sum_{(i,j,k)\in E} \delta_{ijk} \oplus \sum_{i=1}^{r} \left(\sum_{(j,k)\in E_i} X(T_j * T_k) \right) XT_i$$

$$= \sum_{(i,j,k)\in E} \delta_{ijk} \oplus XT^{*}_{(1)} C (XT_{(1)})'\ . \qquad (26)$$

We define

$$H(X) = \sum_{(i,j,k)\in E} \delta_{ijk}. \qquad (27)$$

Now we have

$$F(XT) = f(XT_{(1)}) \oplus XTQ(XT_{(1)})' = H(X) \oplus X(T^*_{(1)}\,C \oplus TQ)T'_{(1)}X'. \qquad (28)$$

So the necessary and sufficient condition for $F(X) \sim H(X)$ is that there exists a nonsingular matrix T that makes $X(T^*_{(1)}C \oplus TQ)T'_{(1)}X'$ be a linear function of X.

From Lemma 1, $T^*_{(1)}C \oplus TQ)T'_{(1)}$ must be a symmetric matrix. The proof is now completed. ❑

6 Cubic Homogeneous Bent Functions

Lemma 2 (Rothaus[1]) Let $f(x_1, \ldots, x_n)$ be a boolean function in $GF(2)^n$. Then

$$F(x_1, ..., x_{2n}) = f(x_1, ..., x_n) \oplus \sum_{i=1}^{n} x_i x_{i+n} \qquad (29)$$

is a bent function in $GF(2)^{2n}$.

Lemma 3 For any $n \geq 3$, there exist cubic bent functions with $r_3 = n$ in $GF(2)^{2n}$.

Proof. According to Lemma 2 we can easily construct cubic bent functions in $GF(2)^{2k}$ with $r_3(F) = n$. ❑

Theorem 5 Let F(X) be a cubic bent function given by (29). We construct a nonsingular $2n \times 2n$ *matrix T which has the following structure*:

$$T = \begin{pmatrix} I & 0 \\ A & M \end{pmatrix}, \qquad (30)$$

where I is a $n \times n$ *identity matrix*, 0 is a $n \times n$ *zero matrix*, M is a $n \times n$ *nonsingular matrix*, $A = (a_{ij})$, $a_{ij} \in GF(2)$, i, j = 1, ..., n. Then F(XT) is a cubic homogeneous bent function if and only if

$$A^*C = M, \qquad (31)$$

where C is defined in (18), and A^* is defined as (16).

Proof. For an arbitrary cubic bent function F(X), it probably can be represented in the form (20). When C and Q are uniquely defined, according to theorem 4, there exists a matrix $T_{(1)}$ of the form (21). We define Q and $T_{(1)}$ as

$$Q = \begin{pmatrix} 0 \\ I \end{pmatrix}, \quad T_1 = \begin{pmatrix} I \\ A \end{pmatrix}, \qquad (32)$$

then

$$T_{(1)}^{*} = \begin{pmatrix} I \\ A \end{pmatrix}^{*} = \begin{pmatrix} 0 \\ A^{*} \end{pmatrix}, \quad TQ = \begin{pmatrix} 0 \\ M \end{pmatrix}. \qquad (33)$$

F(X) ~ H(X) where H(X) is a cubic homogeneous function if and only if formula (21) holds. Now

$$\begin{aligned}(T_{(1)}^{*}C \oplus TQ)T_{(1)}' &= \begin{pmatrix} 0 \\ A^{*}C \oplus M \end{pmatrix}(I, A') \\ &= \begin{pmatrix} 0 & 0 \\ A^{*}C \oplus M & A^{*}CA' \oplus MA' \end{pmatrix} \qquad (34)\end{aligned}$$

The resulting matrix is symmetric iff $A^{*}C \oplus M = 0$. The proof is completed. ❑

Theorem 6 Let $F(X) = f(x_1, \ldots, x_n) \oplus \sum_{i=1}^{n} x_i x_{i+n}$ be a bent function in $GF(2)^{2n}$ where f is a homogeneous cubic function of $(x_i, \ldots, x_n)$ and $r_3(f) = n$. Then there exists a nonsingular matrix T such that F(XT) is a cubic homogeneous bent function.

Proof. Let C be the $n \times \frac{n}{2}$ matrix defined as in (18). Since rank(C) = n, there are n rows of C, say, $(j_1, k_1), \ldots, (j_n, k_n)$, such that the matrix M which consists of these n rows is a nonsingular matrix. We define $A = (a_{ij})_{1 \le i, j \le n}$ as follows:

$$a_{ij} = \begin{cases} 1, & \text{if } j = j_i \text{ or } j = k_i, \\ 0, & \text{otherwise} \end{cases} \quad i = 1, \ldots, n. \qquad (35)$$

Let $T = \begin{pmatrix} I & 0 \\ A & M \end{pmatrix}$, where I is the $n \times n$ identity matrix, 0 is the $n \times n$ zero matrix.

Obviously, T is a nonsingular matrix. For any fixed i, $1 \le i \le n$, in the ith row of A*, $a_{i1}a_{i2}, \ldots, a_{i1}a_{in}, \ldots, a_{in-1}a_{in}$, only one component $a_{ij_i} a_{ik_i} = 1$ and others are all 0. So the matrix product of the ith row of A* with C gives the (j_i, k_i)-th row of C. That is $A^{*}C = M$, so (31) holds and F(XT) is a cubic homogeneous bent function. The theorem is proven. ❑

Let E be an unordered triple set: $E = \{(i, j, k) : 1 \le i, j, k \le r\}$, write $E_i = \{(j, k) : (i, j, k) \in E\}$, $1 \le i \le n$.

Definition 3 (Regular unordered triplet set) The unordered triplet set E is called regular if $E_i / (\cup_{j \ne i} E_j) \ne 0$, $1 \le i, j \le r$.

Theorem 7 Let $F(X) = \sum_{(i,j,k) \in E} x_i x_j x_k + \sum_{i=1}^{n} x_i x_{i+n}$, $r_3(F) = n$ be a boolean function in $GF(2)^{2n}$. If E is a regular unordered triple set, then there exists a square matrix A which satisfies the equation (31) with M = I, and F(XT) is a cubic homogeneous bent function.

Proof. We expand the left side of (31). Hence we have

$$\left(\sum_{(j,k)\in E_1} a_j * a_k, \ldots, \sum_{(j,k)\in E_n} a_j * a_k \right) = M, \tag{36}$$

in which a_i, $1 \le i \le n$ is the ith column of matrix A. Since E is regular, $E_i / \left(\cup_{j=1}^{n} E_j\right) \neq 0$, so there exists at least one unordered pair $(j,k) \in E_i / \left(\cup_{j=1}^{n} E_j\right)$ which makes

$$a_{ik} = a_{ij} = 1, \ a_{il} = 0, \ j \neq l \neq k, \ 1 \le l \le n.$$

In this case, only $a_{ij}a_{ik} = 1$, and if $(u, v) \neq (j, k)$, $a_{iu}a_{iv} = 0$. Now the ith row of the left side of (36) becomes $\overbrace{0,\ldots,0}^{i-1}, 1, \overbrace{0,\ldots,0}^{n-i}$, and this is identical with the ith row of right side of (36). Hence equation (36) holds. Consequently, F(XT) is a cubic homogeneous bent function. The proof is completed. ❑

Theorem 8 **For all n** ≥ 3 and $n \neq 4$, there exist cubic homogeneous bent functions in $GF(2)^{2n}$.

Proof. There are three cases:

1. $n \equiv 0 \pmod 3$, we can write n = 3m for some positive integer m. Let

$$F(X) = \sum_{i=1}^{m} x_{3i-2}x_{3i-1}x_{3i} \oplus \sum_{i=1}^{3m} x_i x_{i+3m}. \tag{37}$$

From Lemma 2 and we know that F(X) is a bent function. Now

$$E = \{(3i-2, 3i-1, 3i) : 1 \le i \le m\}$$

is the regular un-ordered triple set and F(X) has the form of (29). Hence from Theorem 5 we know that there exists a $2n \times 2n$ nonsingular matrix T with the form of (30) which makes (31) hold. So F(XT) is cubic homogeneous bent function.

2. $n \equiv 1 \pmod 3$, write n = 3m + 1 for some positive integer m. Because $n \neq 4$, $m \ge 2$. Let

$$F(X) = \sum_{i=1}^{m} x_{3i-2}x_{3i-1}x_{3i} \oplus x_1x_4x_{3m+1} \oplus \sum_{i=1}^{3m+1} x_i x_{i+3m+1} \tag{38}$$

By Lemma 2 and we know it is a bent function. In this case, we have

$$E = \{(3i-2, 3i-1, 3i) : 1 \le i \le m\} \cup \{(1, 4, 3m+1)\}, \tag{39}$$

which is regular and F(X) has the form of (29), the conclusion of Theorem 8 is also valid.

3. n ≡ 2 (mod 3), write n = 3m + 2 for some m. Let

$$F(X) = \sum_{i=1}^{m} x_{3i-2}x_{3i-1}x_{3i} \oplus x_1x_{3m+1}x_{3m+2} \oplus \sum_{i=1}^{3m+2} x_i x_{i+3m+2} \qquad (40)$$

and we have

$$E = \{(3i-2, 3i-1, 3i) : 1 \le i \le m\} \cup \{(1, 3m+1, 3m+2)\}. \qquad (41)$$

The proof of this case is the same as before.

Hence the statement of the theorem is true and the proof is completed. ❑

Example 2 **Let F**(X) = $x_1x_2x_3 \oplus \sum_{i=1}^{3} x_ix_{i+3}$ be a cubic bent function in $GF(2)^6$.

We have $C' = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$ and set A = (a_1, a_2, a_3) = $\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$. We calculate A*C = I and get

$$A = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}.$$

So

$$T = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix},$$

and

$$F(XT) = x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_2x_5 \oplus x_1x_3x_4 \oplus x_1x_3x_6 \oplus x_1x_4x_5 \oplus x_1x_4x_6 \oplus x_1x_5x_6 \oplus x_2x_3x_5 \oplus x_2x_3x_6 \oplus x_2x_4x_5 \oplus x_2x_4x_6 \oplus x_2x_5x_6 \oplus x_3x_4x_5 \oplus x_3x_4x_6 \oplus x_3x_5x_6,$$

is a cubic homogeneous bent function.

7 The Fourier Transform of Homogeneous Bent Functions

Lemma 4 **Let Z** = X ⊗ *Y*, where X = (x_1, … , x_n) ∈ $GF(2)^n$, Y = (y_1, …, y_n) ∈ $GF(2)^n$, T is a 2n × 2n matrix and T = $\begin{pmatrix} L & 0 \\ A & M \end{pmatrix}$, where L, A, M are n × *n matrix and* L^{-1} and M^{-1} exist. f(Z) = P(X) ⊕ (X, Y) and g(Z) = f(ZT) are bent functions in $GF(2)^{2n}$. The Fourier transform of g(Z) is:

. $\hat{g}(Z) = P((Y \oplus X(AL^{-1})')M'^{-1} \oplus \langle (Y \oplus X(AL^{-1})')M'^{-1}, XL'^{-1}\rangle.$ (42)

Proof. Let $W = U \otimes V$, $U = (w_1, \ldots, w_n)$, $V = (w_{n+1}, \ldots, w_{2n})$. From the Fourier transform definition, we have

$$
\begin{aligned}
Fg(Z) &= 2^{-n} \sum_{W \in GF(2)^{2n}} (-1)^{g(W) \oplus \langle W,Z \rangle} \\
&= 2^{-n} \sum_{U,V \in GF(2)^n} (-1)^{f(UL \oplus VA) \oplus \langle VL \oplus VA, VM \rangle \oplus \langle U,X \rangle \oplus \langle V,Y \rangle} \\
&= 2^{-n} \sum_{V \in GF(2)^n} (-1)^{\langle V,Y \rangle \oplus \langle VA, XL'^{-1} \rangle} \\
&\quad \Theta \sum_{U \in GF(2)^n} (-1)^{f(VL, \oplus VA) \oplus \langle VL \oplus VA, VM \rangle \oplus \langle VL \oplus VA, XL'^{-1} \rangle} \\
&= 2^{-n} \sum_{V \in GF(2)^n} (-1)^{\langle V, Y \oplus XL'^{-1} A'} \sum_{S \in GF(2)^n} (-1)^{f(S) \oplus \langle S, VM \oplus XL'^{-1} \rangle} \\
&= 2^{-n} \sum_{S \in GF(2)^n} (-1)^{f(S) \oplus \langle S, XL'^{-1} \rangle} \sum_{V \in GF(2)^n} (-1)^{\langle V, Y \oplus XL'^{-1} A' \oplus SM' \rangle} \\
&= (-1)^{f((Y \oplus X(AL^{-1})')M'^{-1}) \oplus \langle (Y \oplus X(AL^{-1})')M'^{-1}, XL'^{-1} \rangle} \qquad (43)
\end{aligned}
$$

❑

Lemma 5 **Let f**(X) be a homogeneous function of degree 3 in $GF(2)^n$. $g(Z) = f(X \oplus YA) \oplus (X \oplus YA, Y)$ is a cubic homogeneous bent function, where A is a $n \times n$ *nonsingular matrix*. When $A = A'$, $g(Z)$ is a cubic homogeneous bent function, too.

Proof. Since $A = A'$, from Lemma 4 we have

$$g(Z) = f(Y \oplus XA) \oplus \langle Y \oplus XA, X \rangle. \qquad (44)$$

Since g(Z) is homogeneous bent function. The Fourier transform of g(Z) is also a bent function. We have

$$g(Z) = f(x \oplus YA) \oplus \langle X \oplus YA, Y \rangle = \bigoplus_{1 \le i_1 < i_2 < i_3 \le i_n} a_{i_1 i_2 i_3} z_{i_1} z_{i_2} z_{i_3},$$

where $a_{i_1 i_2 i_3} z_{i_1} z_{i_2} z_{i_3} \in GF(2)$.

Because $Z = X \otimes Y$, z_{i_j} is either x_k or y_ℓ, $1 \le j \le 3$, $1 \le k$, $\ell \le n$. We define $x_i \to y_i$, $y_i \to x_i$, $1 \le i \le n$, then $Z = Y \otimes X$, g(Z) is cubic homogeneous bent function. Then

$$g(Z) = f(Y \oplus XA) \oplus \langle Y \oplus XA, X \rangle = g(Y \otimes X)$$

is a cubic homogeneous bent function. The proof is completed. ❑

Lemma 6 **There exist cubic homogeneous bent functions g**(X) in $GF(2)^{2n}$ when $n \ge 3$, $n \ne 4$, and their Fourier transforms are also cubic homogeneous bent functions.

8 Remark

Example 3 When $n = 5$, we define the function $F(X) = x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_3x_5 \oplus \sum_{i=1}^{5} x_i x_{i+5}$, which is a cubic bent function in $GF(2)^{10}$. $r_3(F) = 5$, $r_2(F) = 0$. Set $E = \{(1, 2, 3), (1, 2, 4), (1, 3, 5)\}$, $E_1 = \{(2, 3), (2, 4), (3, 5)\}$, $E_2 = \{(1, 3), (1, 4)\}$, $E_3 = \{(1, 2), (1, 5)\}$, $E_4 = \{(1, 2)\}$, $E_5 = \{(1, 3)\}$. We define

$$\hat{E}_i = E_i/(\cup_{j\neq i} E_j), \text{ where } 1 \le i,\ j \le 5,$$

and have $\hat{E}_1 = E_1$, $\hat{E}_2 = \{(1, 4)\}$, $\hat{E}_3 = \{(1, 5)\}$, $\hat{E}_4 = \hat{E}_5 = 0$. So E is not a regular triple set. But there exists $n \times n$ nonsingular matrix

$$A = \begin{pmatrix} 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \end{pmatrix}$$

that makes $A^*C = I$. So E regular is not a necessary condition for $A^*C = I$.

References

[1] O.S.Rothaus, On "bent" functions, Journal of Combinatorial Theory, Ser. A, 20, (1976), pp. 300-305.

[2] Chengxin Qu, Jennifer Seberry, Josef Pieprzyk, On the symmetric property of homogeneous boolean functions, Information Security and Privacy, ACISP'99, Lecture Notes in Computer Science, vol. 1587, Springer-Verlag Berlin, Heidelberg, New York, Barcelona, Hong Kong, London, Milan, Paris, Singapore, Tokyo, 1999. pp. 26-35.

[3] Xiang-dong Hou, Cubic bent functions, Discrete Mathematics, 189, (1998), pp. 149-161.

[4] Tianbing Xia, Jennifer Seberry, Josef Pieprzyk, and Chris Charnes. A new upper bound on the degree of homogeneous boolean bent functions. (Submitted).

[5] Josef Pieprzyk, Chenxin Qu, Rotate symmetric functions and fast hashing, Information Security and Privacy, ACISP'98, Lecture Notes in Computer Science, vol. 1438, Springer-Verlag Berlin, Heidelberg, New York, Barcelona, Hong Kong, London, Milan, Paris, Singapore, Tokyo, 1998. pp. 169-180.