Homogeneous Bent Functions

Chengxin Qu, Jennifer Seberry, Josef Pieprzyk

Center for Computer Security Research
School of Information Technology and Computer Science
University of Wollongong
Email: cxq01,jennie,josef@uow.edu.au

Abstract

This paper discusses homogeneous bent functions. The space of homogeneous functions of degree three in six boolean variables was exhaustively searched and thirty bent functions were found. These are found to occur in a single orbit under the action of relabeling of the variables. The homogeneous bent functions identified exhibit interesting combinatorial structures and are, to the best of our knowledge, the first examples of bent functions without quadratic terms. A construction for other homogeneous bent functions of degree three in larger spaces is also given.

Key words: Boolean functions, Bent functions, Homogeneous bent functions, Machine computations, Discrete mathematics in computer science.

1 Introduction

Boolean functions have always been of great interest in many fields of engineering and science. There is already a well established theory of S-boxes which has sprung from cryptography. This theory concentrates on the design and analysis of boolean functions which possess desirable cryptographic properties such as balance, strict avalanche criterion and high nonlinearity. Boolean functions with the highest possible nonlinearity are called bent functions. Bent functions are building blocks for cryptographically strong S-boxes and spread spectrum systems.

In 1970 Rothaus [11] defined boolean bent functions, investigated their properties and gave the first constructions. Kumar, Scholtz and Welch [9] generalized the notion of bent functions over arbitrary fields with arithmetic modulo a prime. MacWilliams and Sloane [7] observed that bent functions are strongly linked with Reed-Muller codes. Berman and Grushko [1] argued that binary bent functions can be equivalently described in the terms of Hadamard codes.

It is well-known that bent functions exist if the degree of boolean function is at least 2. Homogeneous bent functions of degree 2 can be designed very easily using many published constructions. It has been unknown whether or not there are some other homogeneous bent functions of degree three or higher. This work answers the question positively and gives examples of such functions. It is obvious that homogeneous functions are not closed under affine transformations as in general, such transformations will produce quadratic and linear terms. Nevertheless, they seem to have very interesting combinatorial properties.

2 Background

We use the Galois field $V_1 = GF(2)$. A function $f : V_n \to V_1$ takes a n boolean variables and assigns a value from V_1. We treat arguments of the function $f(x) = f(x_1, \ldots, x_n)$ as vectors α of n boolean variables and we use the following assignment:

x	x_n	x_{n-1}	...	x_2	x_1
α_0	0	0	...	0	0
α_1	0	0	...	0	1
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
α_{2^n-2}	1	1	...	1	0
α_{2^n-1}	1	1	...	1	1

Let $\alpha = (a_1, ..., a_n)$ and $x = (x_1, \ldots, x_n)$. The inner product of x and α is defined as $\alpha \cdot x = a_1 x_1 \oplus ... \oplus a_n x_n$. A boolean function $f : V_n \to V_1$ is said to be affine if it can be written as $f(x) = a_1 x_1 \oplus ... \oplus a_n x_n \oplus c$ $(c \in V_1)$. If $c = 0$, the function $f(x)$ is called linear. Any boolean function $f : V_n \to V_1$ can be expressed by the following polynomial

$$f(x) = \bigoplus_{\alpha \in V_n} c_\alpha x^\alpha \tag{1}$$

where $x^\alpha = x_1^{a_1} \cdots x_n^{a_n}$ and $c_\alpha \in GF(2)$. We say that a boolean function $f(x)$ of the form (1) is homogeneous of degree k if $c_\alpha = 0$ whenever α has weight not equal to k ($c_\alpha = 0$ if $wt(\alpha) \neq k$).

The Walsh-Hadamard transform is defined as follows

$$c_f(\lambda) = \frac{1}{2^{n/2}} \sum_{x \in V_n} (-1)^{f(x) \oplus \lambda \cdot x} \text{ where } \lambda \in V_n \tag{2}$$

Definition 2.1 *The function* $f(x)$ *is* bent *if the Walsh-Hadamard transform*

$$c_f(\lambda) = \pm 1, \qquad \textit{for all } \ \lambda \in V_n.$$

3 Homogeneous Bent Functions

The constructions known for bent functions can be divided into two categories. The first one gives a new bent function from scratch. The second uses bent functions on smaller dimension space. More details about constructions and properties of bent functions can be found in [2–5,8–10,12]. The direct constructions appear to always give bent functions with quadratic terms and recursive constructions also seem to preserve these terms; so at present there seem to be no general way to construct bent functions with no quadratic terms.

If all bent functions must contain quadratic terms, then all bent functions over V_6 in particular must contain quadratic terms. Since every bent function of dimension $2k$ has the degree at most k, V_6 is the smallest space to possibly accommodate some homogeneous bent functions of degree 3.

We use an exhaustive computer search to test all possible homogeneous boolean functions of degree 3 over space V_6. As there are 20 distinct 3-subsets of a 6-set, there are 20 distinct monomials of degree 3 in 6 variables. Hence there are 2^{20} possible homogeneous functions of degree 3 on V_6.

We use $(i\ j\ k)$ to denote the monomial $x_i x_j x_k$ where $i < j < k$. The monomials of degree 3 are as follows :

$$\begin{array}{lll}
1-(123)-x_1x_2x_3 & 8-(145)-x_1x_4x_5 & 15-(246)-x_2x_4x_6 \\
2-(124)-x_1x_2x_4 & 9-(146)-x_1x_4x_6 & 16-(256)-x_2x_5x_6 \\
3-(125)-x_1x_2x_5 & 10-(156)-x_1x_5x_6 & 17-(345)-x_3x_4x_5 \\
4-(126)-x_1x_2x_6 & 11-(234)-x_2x_3x_4 & 18-(346)-x_3x_4x_6 \\
5-(134)-x_1x_3x_4 & 12-(235)-x_2x_3x_5 & 19-(356)-x_3x_5x_6 \\
6-(135)-x_1x_3x_5 & 13-(236)-x_2x_3x_6 & 20-(456)-x_4x_5x_6 \\
7-(136)-x_1x_3x_6 & 14-(245)-x_2x_4x_5 &
\end{array}$$

For later purposes we number these in order so 1 stands for the monomial (123), 2 stands for (124), and so on. Thus 20 stands for (456).

Our computer search revealed that there are 30 homogeneous bent functions of degree 3 with 16 monomials. A representative of these 30 functions is given as follows

$$123 \oplus 124 \oplus 125 \oplus 126 \oplus 134 \oplus 135 \oplus 146 \oplus 156 \oplus$$
$$234 \oplus 236 \oplus 245 \oplus 256 \oplus 345 \oplus 346 \oplus 356 \oplus 456.$$

The full form of this function is

$$\begin{aligned} f(x) = {} & x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_2x_5 \oplus x_1x_2x_6 \oplus x_1x_3x_4 \oplus \\ & x_1x_3x_5 \oplus x_1x_4x_6 \oplus x_1x_5x_6 \oplus x_2x_3x_4 \oplus x_2x_3x_6 \oplus \\ & x_2x_4x_5 \oplus x_2x_5x_6 \oplus x_3x_4x_5 \oplus x_3x_4x_6 \oplus x_3x_5x_6 \oplus x_4x_5x_6 \\ = {} & (x_1 \oplus x_2)(x_3x_4 \oplus x_5x_6) \oplus (x_3 \oplus x_4)(x_1x_2 \oplus x_5x_6) \oplus \\ & (x_5 \oplus x_6)(x_1x_2 \oplus x_3x_4) \oplus x_1(x_3x_5 \oplus x_4x_6) \oplus x_2(x_3x_6 \oplus x_4x_5) \end{aligned}$$

in our numbering notation this function is the set

$$(1, 2, 3, 4, 5, 6, 9, 10, 11, 13, 14, 16, 17, 18, 19, 10)$$

which can be equivalently represented by its complement $(7, 8, 12, 15)$. The support of $f(x)$ yields the difference set below over $(V_6, \oplus)$.

$$\begin{array}{cccc} (1,0,1,0,0,1) & (1,0,0,1,1,1) & (0,1,0,0,1,1) & (0,1,0,1,0,1) \\ (1,0,1,1,0,0) & (1,1,0,1,1,0) & (1,1,1,0,0,1) & (0,1,1,1,0,1) \\ (1,1,1,0,0,0) & (1,0,0,0,1,1) & (0,1,1,0,0,1) & (0,1,0,1,1,1) \\ (1,1,0,0,0,1) & (1,0,0,1,1,0) & (0,1,1,1,1,0) & (1,0,1,0,1,1) \\ (0,0,1,1,0,1) & (1,1,0,0,1,0) & (0,0,1,0,1,1) & (1,0,1,1,1,0) \\ (0,0,0,1,1,1) & (1,1,0,1,0,0) & (0,0,1,1,1,0) & (1,1,1,0,1,0) \\ (1,0,1,1,0,1) & (0,1,1,1,0,0) & (0,1,1,0,1,0) & (1,1,0,1,0,1) \end{array}$$

Using Rothaus' [11] characterization of bent functions on 6 variables we see from the automorphism group of the difference set that 3-homogeneous bent function is equivalent to the bent function

$$x_1x_2x_3 \oplus x_1x_4 \oplus x_2x_5 \oplus x_3x_6$$

We now show that the cubic homogeneous bent function on V_6 are related in a very special way. Let π be a permutation on $\{1,2,3,4,5,6\}$, and let x^π denote the vector $(x_{\pi(1)}, x_{\pi(2)}, x_{\pi(3)}, x_{\pi(4)}, x_{\pi(5)}, x_{\pi(6)})$. Let f be the degree 3 homogeneous bent function given above. Then $f^\pi(x) = f(x^\pi)$ is also a degree 3 homogeneous bent function on variable $x_1, x_2, x_3, x_4, x_5, x_6$. We will show that all six variable degree 3 homogeneous bent functions are of the form f^π where π is a permutation on $\{1,2,3,4,5,6\}$.

Let H denote the group of permutations such that f^π is the same boolean function as f. Now consider the matrix

$$B = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}$$

which encodes the degree 3 terms which do not appear in f. Let B^π denote the matrix obtained by permuting the rows of B according to π. (So if $\pi = (1,2)$, then B^π would equal to the matrix obtained by interchanging the first row and second row of B.) Notice that $\pi \in H$ if and only if the set of columns in the matrix B^π equals to the set of columns in B.

Since the columns of B are distinct, every $\pi \in H$ induces a permutation of the set $\{1,2,3,4\}$: namely the permutation needed to be applied to the columns of B^π in order to change B^π back to B. Let K be the subgroup of H whose elements induce the identity permutation on $\{1,2,3,4\}$. Any element ϕ of K must fix the sets $\{1,3,5\}$, $\{1,4,6\}$, $\{2,3,6\}$ and $\{2,4,5\}$ setwise. so $\phi(1) \in \{1,3,5\} \cap \{1,4,6\} = \{1\}$. That is $\phi(1) = 1$. Similarly, we can show that $\phi(i) = i$ for $i = 2,3,4,5,6$. Hence K is trivial, and H can have at most one element for each element in S_4. On the other hand, each row of B corresponds to one of the six pairs of elements in $\{1,2,3,4\}$. The first row corresponds to the pair $\{1,2\}$, the second row to the pair $\{3,4\}$, and so on. So it is easy to construct a row permutation which induces any prescribed permutation of the columns. Hence H contains exactly $4! = 24$ elements. Since S_6 has 720 elements it follows that exactly $30 = 720/24$ distinct boolean function are of the form f^π where $\pi \in S_6$. Since this is the total number of bent functions by our exhaustion, every homogeneous degree 3 bent function on six variable can be obtained from f by applying a permutation to the indices of its variables.

The incidence matrix of f is [1]

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

and its adjacency matrix is of the following form

$$C = AA^t = \begin{bmatrix}
8&4&3&3&3&3\\
&8&3&3&3&3\\
&&8&4&3&3\\
&&&8&3&3\\
&&&&8&4\\
&&&&&8
\end{bmatrix}$$

For the matrix A, any row permutation does not affect the values in the diagonal of matrix C. Since there are 6 rows in matrix A, the row permutations give 6! different matrices A. However the matrix C has only 15 different matrices corresponding to the all row permutations of A. Every matrix C corresponds to 2 bent functions. The diagonal entries of C indicate the frequency of each variable appearing in the function and the other entries specify the frequency of each pair occurring in the function. From a combinatorial point of view, every homogeneous bent function found in our search, has the following properties:

(1) its covering is 2-$(6, 3, 3)$ and its packing is 2-$(6, 3, 4)$;
(2) each variable occurs the same number of times,
(3) three disjoint pairs of variables occur 4 times and the other pairs happen 3 times.

We note that taking the block complements of the functions as 30 blocks on 20 elements, the repetition number is 6 and with the association scheme that elements are first associates if they appear together in a block, third associates if they are complementary (for example $x_1x_2x_3$ is complementary to

[1] for definitions of incidence and adjacency (coincidence) matrices see [13] [14]

$x_4x_5x_6$ so we say 1 is complementary to 20 and k is complementary to $21-k$), and second associates otherwise, we have a $PBIBD(v,b,r,k;\lambda_1,\lambda_2,\lambda_3)$ design $PBIBD(20,30,6,4;2,0,0)$.

Finally, we note that using the well known fact that $f(x,y) = g(x) \oplus h(y)$ is bent whenever g and h are. We can now construct homogeneous bent functions of degree 3 in large space V_{6k} $(k = 1, 2, \cdots)$. We know that there are 30 bent functions for V_6. The following result gives a lower bound on the number of homogeneous bent functions of degree 3 in V_{6k}.

Corollary 3.1 *Given space V_{6k}, the number of all homogeneous bent functions of degree 3 in the space is greater than or equal to*

$$30^k \binom{6k}{6}.$$

Proof : We know that the number of bent functions is 30 when $k = 1$. The space V_{6k} can be looked at as a collection of k disjoint subspaces V_6. In other words, there are $6k$ boolean variables which can be arranged into $\binom{6k}{6}$ combinations. For each combination, there are 30^k distinct bent functions. In total, there are at least $\binom{6k}{6} 30^k$ homogeneous bent functions. □

Acknowledgement

The authors wish to thank Dr Xian-mo Zhang, Dr Chris Charnes, Mr Tianbing Xia, Dr R McFarland and attendees at the CCCS'98 Conference in Lethbridge, Canada for their helpful conversations and suggestions while we were undertaking this study. We would also like to thank the referee for rewriting substantial parts of this paper.

References

[1] S. D. Berman and I. I. Grushko, *B-functions encountered in modular codes*, Problemy Perdachi Informatsii, 17: 10-18, 1981.

[2] C. Carlet, J. Seberry and X. M. Zhang, *Comments on "Generating and counting binary bent sequences"*, IEEE Transactions on Information Theory, 40.2: 600-600, 1994.

[3] C. Carlet, *A transformation on boolean functions, its consequences on some problems related to Reed-Muller codes*, Eurocode'90, 42-50, 1990.

[4] Claude Carlet, *Partially-bent functions*, Designs, Codes and Cryptography, 3:135-145, 1993.

[5] Claude Carlet, *Two new classes of bent functions*, Advances in Cryptology - EUROCRYPT'93, Lecture Notes in Computer Science 765, Springer-Verlag, Berlin, Heidelberg, New York, 77-101, 1994,

[6] J. F. Dillon, *Elementary Hadamard Difference Sets*, PhD Dissertation, University of Maryland, 1976.

[7] F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, 1978.

[8] Kaisa Nyberg, *Construction of bent functions and difference sets*, In I.B. Damgård, editor, Advances in Cryptology - EUROCRYPT'90 473, Lecture Notes in Computer Science, Springer-Verlag, Berlin, Heidelberg, New York, 151-160, 1991,

[9] P. V. Kumar, R. A. Scholtz and L. R. Welch, *Generalised bent functions and their properties*, Journal of Combinatorial Theory (A), 40:90-107, 1985.

[10] Josef Pieprzyk, *Bent permutations*, In G. Mullen and P. Shiue, editors, Proceedings of First International Conference on Finite Fields, Coding Theory and Advances in Communication and Computing, Lecture Notes in Pure and Applied Mathematics 141, Las Vegas, 1991,1992.

[11] O. S. Rothaus, *On "bent" functions*, Journal of Combinatorial Theory (A), 20:300-305 1976.

[12] Claude Carlet, *Partially-bent functions*, Advances in Cryptology - CRYPTO'92, Lecture Notes in Computer Science 740, Springer-Verlag, Berlin, Heidelberg, New York, 280-291, 1993.

[13] Anne Penfold Street and Deborah J. Street, *Combinatorics of Experimental Design*, Oxford Science Publications, 1987.

[14] Charles J. Colbourn and Jeffrey H. Dinitz *The CRC Handbook of Combinatorial Designs*, CRC Press, Boca Raton, Fla, 1996.