Available online at www.sciencedirect.com
ScienceDirect
Discrete Applied Mathematics 155 (2007) 1066–1070
DISCRETE APPLIED MATHEMATICS
www.elsevier.com/locate/dam

Note

Generalized hyper-bent functions over $GF(p)$

A.M. Youssef

Concordia Institute for Information Systems Engineering, Concordia University, Montreal, QC, H3G 1M8, Canada

Received 19 January 2006; received in revised form 3 October 2006; accepted 26 November 2006
Available online 22 January 2007

Abstract

In this paper, we extend the concept of binary hyper-bent functions introduced by Carlet to functions defined over $GF(p)$. We show that such functions must be quadratic. We also provide the necessary and sufficient conditions on the symmetric coefficient matrix corresponding to the quadratic form of $f : Z_p^n \to Z_p$ that guarantee that f is a hyper-bent function.

Keywords: Cryptography; Hyper-bent functions; Quadratic forms; Finite fields

1. Introduction

Binary bent functions, defined and first analyzed by Rothaus [12], exist for even values of n and achieve the maximum possible nonlinearity [9]. These functions have been the subject of great interest in several areas including cryptography [10]. In fact, the Canadian government block cipher standard (CAST [1]) is designed based on these functions.

Adams and Tavares [2] introduced two subclasses of binary bent functions: the bent-based functions and the linear-based functions. For $f : Z_2^n \to Z_2$, the first ones (resp. the second ones) are the concatenations of 2^{n-2} bent (resp. linear) subfunctions of length 4. Bent-based bent functions are interesting from a cryptographic point of view, since fixing the coordinates of a cryptosystem is a well-known cryptanalysis method.

Carlet noted that there is no reason to prefer the first $(n-2)$ coordinates to the others and, from a cryptanalytic point of view, we need to consider the possibility of fixing less coordinates than $n-2$ [4]. Based on this argument, Carlet introduced a new class of binary bent functions, which he called hyper-bent functions. Binary hyper-bent[1] functions are those Boolean functions with n inputs (n even) such that, for a given even integer k ($2 \leqslant k \leqslant n-2$), any of the Boolean functions obtained by fixing k coordinates of the variable is bent.

The main purpose of this note is to generalize the concept of hyper-bent functions to functions defined over $GF(p)$, $p \geqslant 3$. In particular, we show that such functions must be quadratic. We also provide the necessary and sufficient conditions on the symmetric coefficient matrix corresponding to the quadratic form of $f : Z_p^n \to Z_p$ that guarantee that f is a hyper-bent function.

E-mail address: youssef@ciise.concordia.ca.
[1] This should not be confused with the hyper-bent functions introduced in [13].

0166-218X/$ - see front matter © 2006 Elsevier B.V. All rights reserved.
doi:10.1016/j.dam.2006.11.007

2. Algebraic preliminaries

In this section, we present some definitions and algebraic preliminaries required to prove our result. The reader is referred to [8] for the theory of finite fields.

Definition 1. Let p be a prime and denote the set of integers modulo p by Z_p. Let $u = e^{i(2\pi/p)}$ be the pth root of unity in C, where $i = \sqrt{-1}$. The Fourier transform of a function $f : Z_p^n \to Z_p$ is defined as

$$F(w) = \frac{1}{\sqrt{p^n}} \sum_{x \in Z_p^n} (u)^{f(x) - w \cdot x},$$

where $w \in Z_p^n$ and $w \cdot x$ denotes the dot product between w and x, i.e., $w \cdot x = \sum_{i=1}^{n} w_i x_i \bmod p$.

Definition 2. A function $f : Z_p^n \to Z_p$ is bent if $|F(w)| = 1$ for all $w \in Z_p^n$ [7].

Throughout the rest of this paper, let p denote an odd prime. Unlike binary bent functions which exist for even values of n, p-ary bent functions exist for both even and odd values of n.

Definition 3. A polynomial f over a finite field F is called a difference permutation polynomial [6] (or perfect nonlinear function [11]) if the mapping $x \to f(x+a) - f(x)$ is a permutation of F for each nonzero element a of F.

Definition 4. A quadratic form [8] in n indeterminates over $GF(p)$ is a homogeneous polynomial in $F_p(x_1, \ldots, x_n)$ of degree 2 or the zero polynomial. Since $2^{-1} \bmod p$ always exists, we can write the mixed terms $b_{ij} x_i x_j$ as $\frac{1}{2} b_{ij} x_i x_j + \frac{1}{2} b_{ij} x_j x_i$, and this leads to the representation

$$f(x_1, \ldots, x_n) = \sum_{i,j=1}^{n} a_{ij} x_i x_j,$$

with $a_{ij} = a_{ji}$ for any quadratic form over $GF(p)$. The symmetric $n \times n$ matrix A whose (i, j) entry is a_{ij} is called the coefficient matrix of f.

Example 1. Consider the quadratic form $f(x_1, x_2) = 3x_1^2 + 4x_2^2 + 5x_1 x_2$ over $GF(7)$. Then the associated coefficient matrix is given by

$$A = \begin{pmatrix} a_{11} & 2^{-1} a_{12} \\ 2^{-1} a_{12} & a_{22} \end{pmatrix} = \begin{pmatrix} 3 & 6 \\ 6 & 4 \end{pmatrix},$$

and we have

$$(x_1 x_2) \begin{pmatrix} 3 & 6 \\ 6 & 4 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = 3x_1^2 + 4x_2^2 + 5x_1 x_2 = f(x_1, x_2).$$

3. Results

Here, we generalize the concept of hyper-bent functions to functions defined over $GF(p)$.

Definition 5. A function $f : Z_p^n \to Z_p$ is said to be hyper-bent if any of the functions obtained by fixing $k < n$ coordinates of the input variables is bent.

Note that, unlike binary hyper-bent functions, for $p \geqslant 3$, both n and k can be even or odd integers.

Lemma 1. *Let* $f : Z_p \to Z_p$ *be given by*

$$f(x) = a_0 + a_1 x + \cdots + a_t x^t \bmod p, \quad a_t \neq 0.$$

Then f is bent implies that $t = 2$, i.e., for $n = 1$, only quadratic functions can be bent.

Proof. A perfect nonlinear function is bent and the converse is also true over $GF(p)$ [11]. The lemma follows by noting that difference permutation polynomials over $GF(p)$ are only quadratic [6]. □

Lemma 2. *Let A denote the coefficient matrix corresponding to the quadratic form of f. Then f is bent if and only if* $rank(A) = n$.

Proof. Every quadratic form over $GF(p)$ is equivalent (under a linear transformation) to a diagonal quadratic form [8, Theorem 6.21]. Thus, if $rank(A) = n$, then f is in the same linear equivalence class as

$$g(x) = \sum_{i=1}^{n} a_{ii} x_i^2, \quad a_{ii} \neq 0.$$

The rest of the proof follows by noting that $g(x) - g(x + w)$ is an affine balanced function and hence g is perfect nonlinear. On the other hand, if $rank(A) = r < n$, then f is in the same linear equivalence class as the degenerate function

$$d(x) = \sum_{i=1}^{n} a_{ii} x_i^2,$$

where $a_{ii} = 0$ for $n - r$ values of i. Since we can choose $w = (0 \cdots w_j \cdots 0)$, $w_j \neq 0$, $j \in \{i | a_{ii} \neq 0\}$ to obtain $d(x) - d(x + w) = 0$. Thus $d(x)$ is not perfect nonlinear and hence f is not bent since it belongs to the same linear equivalence class of g. □

From Lemma 2 and by noting that the nonlinearity of f does not change by adding any affine function to it, we have:

Corollary 1. *The number of quadratic bent functions over* $GF(p)$ *is equal to* $p^{n+1} \times$ *the number of nonsingular symmetric matrices over* $GF(p)$.

The number of nonsingular symmetric matrices over $GF(p)$ is already determined in [3,5].

Let $T_{i_1}(A)$ denote the matrix obtained by deleting the i_1th row and i_1th column from A. Consequently, $(T_{i_2 i_1}(A)) = T_{i_2}(T_{i_1}(A))$ denote the matrix obtained by deleting the i_2th row and i_2th column from $T_{i_1}(A)$ and so on.

Theorem 1. *Let A denote the coefficient matrix corresponding to the quadratic form of the function*

$$f(x) = \sum_{i,j=1}^{n} a_{i,j} x_i x_j.$$

Let $h(x)$ *denote any affine function over* $GF(p)$, *then* $g(x) = f(x) + h(x)$ *is a hyper-bent function over* $GF(p)$ *if and only if* $rank(A) = n$ *and* $rank(T_{i_k \cdots i_1}(A)) = n - k$, $1 \leqslant k \leqslant n - 1$, $1 \leqslant i_j \leqslant n - j + 1$.

Proof. Let g denote the function obtained from the quadratic form f defined above by fixing the input variable x_i. Then g belongs to the affine equivalence class whose associated coefficient matrix is obtained from A by deleting the ith row and ith column. The rest of the proof follows directly from Lemmas 1, 2 and the definition of hyper-bent functions. □

Example 2. Consider the quadratic form $f(x_1, x_2, x_3) = x_1^2 + x_2^2 + x_3^2 + 6x_1x_2 + x_1x_3 + 3x_2x_3$ over $GF(7)$. The coefficient matrix

$$A = \begin{pmatrix} 1 & 3 & 4 \\ 3 & 1 & 5 \\ 4 & 5 & 1 \end{pmatrix} \quad \text{and} \quad T_1(A) = \begin{pmatrix} 1 & 5 \\ 5 & 1 \end{pmatrix}, \quad T_2(A) = \begin{pmatrix} 1 & 4 \\ 4 & 1 \end{pmatrix}, \quad T_3(A) = \begin{pmatrix} 1 & 3 \\ 3 & 1 \end{pmatrix}.$$

It is easy to verify that $Rank(A) = 3$, $Rank(T_{i_1}(A)) = 2$, $Rank(T_{i_1 i_2}(A)) = 1$. Hence f is a hyper-bent function.

Example 3. Let $f(x_1, x_2, x_3, x_4) = x_1^2 + x_2^2 + x_3^2 + 6x_4^2 + 5x_1x_2 + x_1x_3 + 3x_1x_4 + 3x_2x_3 + 5x_2x_4 + 3x_3x_4$ over $GF(7)$. Then

$$A = \begin{pmatrix} 1 & 6 & 4 & 5 \\ 6 & 1 & 5 & 6 \\ 4 & 5 & 1 & 5 \\ 5 & 6 & 5 & 6 \end{pmatrix},$$

$$T_1(A) = \begin{pmatrix} 1 & 5 & 6 \\ 5 & 1 & 5 \\ 6 & 5 & 6 \end{pmatrix}, \quad T_2(A) = \begin{pmatrix} 1 & 4 & 5 \\ 4 & 1 & 5 \\ 5 & 5 & 6 \end{pmatrix}, \quad T_3(A) = \begin{pmatrix} 1 & 6 & 5 \\ 6 & 1 & 6 \\ 5 & 6 & 6 \end{pmatrix}, \quad T_4(A) = \begin{pmatrix} 1 & 6 & 4 \\ 6 & 1 & 5 \\ 4 & 5 & 1 \end{pmatrix}.$$

Thus we have $det(A) = 6$, $det(T_1(A)) = 4$, $det(T_2(A)) = 4$, $det(T_3(A)) = 5$, $det(T_4(A)) = 5$ and hence all functions obtained by fixing one input variable of f is bent. However, we have $det(T_{34}(A)) = 0$ and hence f is not a hyper-bent function. This is easy to verify; by fixing $x_3 = 0$, $x_4 = 0$ we get $g(x_1, x_2) = x_1^2 + x_2^2 + 5x_1x_2$, which is not bent since its associated coefficient matrix $\begin{pmatrix} 1 & 6 \\ 6 & 1 \end{pmatrix}$ is singular over $GF(7)$.

Theorem 2. *The above set of functions* (*defined in Theorem* 1) *constitutes the whole class of hyper-bent functions over* $GF(p)$.

Proof. Any function $f : Z_p^n \to Z_p$ can be written as

$$f(x_1, x_2, \ldots, x_n) = \sum_{i_1, \ldots, i_n = 1}^{n} a_{i_1, \ldots, i_n} x_1^{i_1} \ldots x_n^{i_n}.$$

If f is a hyper-bent function, then all functions obtained by fixing $n - 1$ variables must be bent (and hence quadratic). Thus, we must have $a_{i_1 \cdots i_n} = 0$ for all $i_j > 2$, $1 \leqslant j \leqslant n$, and $a_{i_1 \cdots i_n} \neq 0$ for $(i_1 \cdots i_n) = \pi_n(2, 0, \ldots, 0)$, where π_n is any permutation of the enclosed n elements. This completes the proof for $n < 3$.

For $n \geqslant 3$, the rest of the proof follows by showing that $a_{i_1 \cdots i_n} = 0$ for $\sum_{j=1}^n i_j > 2$, $0 \leqslant i_j \leqslant 1$. Assume that $a_{i_1 \cdots i_n} \neq 0$ for $\sum_{j=1}^n i_j > 2$, $0 \leqslant i_j \leqslant 1$. Then we can fix $n - 3$ variables and choose one of the remaining three variables such that the rank of the coefficient matrix corresponding to the quadratic form of the remaining two variables is less than 2 which contradicts the assumption that f is a hyper-bent function. To illustrate this last point, suppose w.l.o.g. that $f(x_1, x_2, x_3, 0 \cdots 0) = a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + 2x_1x_2x_3$, then we can fix one of the three variables so that at least one of the following matrices

$$A_{12} = \begin{pmatrix} a_1 & x_3' \\ x_3' & a_2 \end{pmatrix}, \quad A_{13} = \begin{pmatrix} a_1 & x_2' \\ x_2' & a_3 \end{pmatrix}, \quad A_{23} = \begin{pmatrix} a_2 & x_1' \\ x_1' & a_3 \end{pmatrix}$$

is singular. Ignoring the constant term, we note that A_{12} is the coefficient matrix corresponding to $f(x_1, x_2, x_3', 0 \cdots 0)$, $x_3' \in GF(p)$. Similarly, A_{13} and A_{23} are the coefficient matrices corresponding to $f(x_1, x_2', x_3, 0 \cdots 0)$ and $f(x_1', x_2, x_3, 0 \cdots 0)$, respectively. If ${x_3'}^2 = a_1a_2 \bmod p$ has no solution, then either a_1 or a_2 is a quadratic non-residue but not both; similarly for the other two equations (Note that $a_i \times a_j$ is a quadratic non-residue if and only if either a_i or a_j is a quadratic non-residue but not both). Hence we can always find x_1', x_2' or x_3' such that at least one of the above three matrices is singular over $GF(p)$. □

Open problem: Providing an exact count for the number of hyper-bent functions over $GF(p)$ is an interesting combinatorial problem.

Acknowledgments

The author would like to thank the anonymous reviewers for fixing some typographical errors in the original manuscript. This work was partially supported by the Natural Sciences and Engineering Research Council of Canada (NSERC) Grant N00930.

References

[1] C. Adams, Constructing symmetric ciphers using the CAST design procedure, Designs, Codes Cryptog. 12 (3) (1997) 283–316.
[2] C.M. Adams, S.E. Tavares, Generating and counting binary bent sequences, IEEE Trans. Inf. Theory 36 (5) (1990).
[3] R.P. Brent, B.D. McKay, On determinants of random symmetric matrices over Z_m, Ars Combin. 26A (1988) 57–64.
[4] C. Carlet, Hyper-bent functions, Proceedings of Pragocrypt'96, Czech Technical University Publishing House, Prague, 1996, pp. 145–155.
[5] L. Carlitz, Representation by quadratic forms in a finite field, Duke Math. J. 21 (1954) 123–137.
[6] D. Gluck, A note on permutation polynomials and finite geometeries, Discrete Math. 80 (1990) 97–100.
[7] P.V. Kumar, R.A. Scholtz, L.R. Welch, Generalized bent functions and their properties, J. Combin. Theory Ser. A 40 (1985) 90–107.
[8] R. Lidel, H. Niederreiter, Finite fields, Encyclopaedia of Mathematics and Its Applications, Addison-Wesley, Reading, MA, 1983.
[9] W. Meier, O. Staffelbach, Nonlinearity criteria for cryptographic functions, Proceedings of Eurocrypt '89, Lecture Notes in Computer Science, vol. 434, Springer, Berlin, 1990, pp. 549–562.
[10] A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, Handbook of Applied Cryptography, CRC Press, Boca Raton, 1996.
[11] K. Nyberg, Construction of bent functions and difference sets, Proceedings of Eurocrypt'90, Lecture Notes in Computer Science, vols. 2045, 473, Springer, Berlin, 1991, pp. 151–160.
[12] O.S. Rothaus, On bent functions, J. Combin. Theory 20 (A) (1976) 300–305.
[13] A.M. Youssef, G. Gong, Hyper-bent functions, Proceedings of Eurocrypt' 2001, Lecture Notes in Computer Science, vol. 2045, Springer, Berlin, 2001, pp. 406–419.