CHARACTERIZATION OF MDS MAPPINGS

S. M. DEHNAVI*, A. MAHMOODI RISHAKANI, M. R. MIRZAEE SHAMSABAD

Abstract. MDS codes and matrices are closely related to combinatorial objects like orthogonal arrays and multipermutations. Conventional MDS codes and matrices were defined on finite fields, but several generalizations of this concept has been done up to now. In this note, we give a criterion for verifying whether a map is MDS or not.

1. Introduction

MDS (Maximum Distance Separable) codes and MDS matrices [7, 6] are closely related to combinatorial objects like orthogonal arrays [11] and multipermutations [12]. MDS matrices have also applications in cryptography [3, 10, 4]. Conventional MDS codes and matrices were defined on finite fields, but several generalizations of this concept has been done up to now [1, 9, 2, 8]. In [5] some types of MDS mappings were investigated. In this note, we give a criterion for verifying whether a map is MDS or not.

2. MDS mappings

Definition 2.1. Let A be a nonempty finite set and n be a natural number. For two vectors $a, b \in A^n$ with

$$a = (a_1, a_2, \ldots, a_n),$$

$$b = (b_1, b_2, \ldots, b_n),$$

we define the distance between them as

$$\mathrm{dist}(a, b) = |\{i \mid a_i \neq b_i, 1 \leq i \leq n\}|.$$

Keywords: MDS map, MDS matrix, MDS code, Multipermutation.

* std_dehnavism@khu.ac.ir

Definition 2.2. Let A be a nonempty finite set and k and n be two natural numbers. The (differential) branch number of a map

$$f : A^k \to A^n,$$

is defined as

$$Br(f) = \min\{dist((a, f(a)), (b, f(b))) \mid a, b \in A^k, a \neq b\}.$$

Definition 2.3. Let A be a nonempty finite set and k and n be two natural numbers. We call a map

$$f : A^k \to A^n,$$

(k, n, A)-MDS iff $Br(f) = n + 1$.

Note 2.4. It is not hard to see that we can construct an $(n + k, |A|^k, n + 1)$-code over A which is an MDS code.

Definition 2.5. Let A and B be two nonempty finite sets, r be a natural number and $f : A^r \to B$ be a map. Suppose that $(x_1, x_2, \ldots, x_r) \in A^r$ is the input of f and let $I \subseteq \{1, 2, \ldots, r\}$ be a nonempty subset. We call the arguments of input indexed in I "input variables" and the rest of arguments "parameters". We denote the map f with this separation on input by f_I and we say that f_I is a "parametric map".

Definition 2.6. Let A be a nonempty finite set and k and n be two natural numbers. A map $f : A^k \to A^n$ can be represented as a vector $(f_1, f_2, \ldots, f_n)$ of functions. Here, $f_i : A^k \to A$, $1 \leq i \leq n$, is called the i-th component (projection) function of f.

Definition 2.7. Let A and B be two nonempty finite sets, r be a natural number and $f : A^r \to B$ be a map. Suppose that $I \subseteq \{1, 2, \ldots, r\}$ is a nonempty subset. According to Definition 2.5, we say that f_I is parametric invertible iff it is invertible for any permissible values of the parameters.

Definition 2.8. Let A be a nonempty finite set and k and n be two natural numbers. Let $f : A^k \to A^n$ be a map. For every $1 \leq t \leq \min\{k, n\}$ and for any set $I = \{i_1, i_2, \ldots, i_t \mid 1 \leq i_1 < i_2 < \cdots < i_t \leq k\}$ and $J = \{j_1, j_2, \ldots, j_t \mid 1 \leq j_1 < j_2 < \cdots < j_t \leq n\}$ we define the parametric map

$$f_I^J : A^k \to A^t,$$

$$x \mapsto ((f_{j_1})_I(x), (f_{j_2})_I(x), \ldots, (f_{j_t})_I(x)).$$

We call these parametric functions "square sub-functions" of f.

Theorem 2.9. Let A be a nonempty finite set and k and n be two natural numbers. A map $f : A^k \to A^n$ is (k, n, A)-MDS iff all of its square sub-functions are parametric invertible.

Proof. At first we suppose that every square sub-function of f is parametric invertible. Suppose that f is not a (k, n, A)-MDS map. So, we have $Br(f) \leq n$. Therefore, there exist vectors $X = (a, f(a))$ and $Y = (b, f(b))$ with

$$a = \{a_1, a_2, \ldots, a_n\},$$

$$b = \{b_1, b_2, \ldots, b_n\},$$

and $dist(X, Y) \leq n$. Since

$$dist(X, Y) = dist(a, b) + dist(f(a), f(b)),$$

if $dist(a, b) = t$, then $dist(f(a), f(b)) \leq n - t$. Let $I = \{i | a_i \neq b_i\}$ and $J' = \{j | f_j(a) = f_j(b)\}$. There exists $J \subseteq J'$ with $|J| = t$. So the square sub-function f_I^J is not parametric invertible, due to the existance of a and b. This is a contradiction.

Conversely, suppose that f is a (k, n, A)-MDS map; for any $1 \leq t \leq \min\{k, n\}$ and nonempty subsets $I \subseteq \{1, 2, \ldots, k\}$ and $J \subseteq \{1, 2, \ldots, n\}$ with $|I| = |J| = t$, suppose that the square sub-function f_I^J is not parametric invertible. Then, there exist $a, b \in A$ with $f_I^J(a) = f_I^J(b)$ and $a_i = b_i$, $i \notin I$. This means that

$$dist(a, b) \leq t,$$

and $dist(f(a), f(b)) \leq n - t$, which is contradiction.

Example 2.10. Let $(G, \star)$ be a finite Abelian group. Suppose that $: G \to G$ is a map. Define the map

$$f : G^2 \to G^2,$$

$$f(g_1, g_2) = (g_1 \star g_2, g_1 \star (g_2)).$$

If the mappings and

$$: G \to G,$$

$$(g) = g \star (g),$$

are both group isomorphisms, then f is a $(2, 2, G)$-MDS map.

Proof. By Theorem 2.9, it suffices to show that the square sub-functions of f are parametric invertible. There are five square sub-functions. Suppose that $c \in G$ is fixed. The parametric functions

$$h_1 : G \to G,$$

$$h_1(g;c) = g \star c;$$

and

$$h_2 : G \to G;$$
$$h_2(g;c) = c \star g;$$

and

$$h_3 : G \to G;$$
$$h_3(g;c) = g \star \ (c);$$

are invertible because G is a group. The parametric function

$$h_4 : G \to G;$$
$$h_4(g;c) = c \star \ (g);$$

is invertible because   is a group isomorphism. Now suppose that the function

$$h_5 = f \ : G^2 \to G^2;$$
$$f \ (g_1;g_2) = (g_1 \star g_2; g_1 \star \ (g_2));$$

is not invertible. Suppose that we have

$$(g_1 \star g_2; g_1 \star \ (g_2)) = (g_1' \star g_2'; g_1' \star \ (g_2'));$$

with

$$(g_1;g_2) \neq (g_1';g_2'):$$

Then we have

$$g_1 \star g_2 = g_1' \star g_2';$$
$$g_1 \star \ (g_2) = g_1' \star \ (g_2');$$

which leads to

$$g_1 \star (g_1')^{-1} = g_2' \star g_2^{-1};$$
$$g_1 \star (g_1')^{-1} = \ (g_2' \star g_2^{-1});$$

by isomorphicity of . So, we get

$$(g_2' \star g_2^{-1}) \star (g_1 \star (g_1')^{-1})^{-1} = e_G;$$

or

$$(g_2' \star g_2^{-1}) = e_G;$$

which means that $g_2 = g_2'$ by isomorphicity of . Thus, $g_1 = g_1'$ which is a contradiction.

Note 2.11. In some fields of mathematics, the morphism   in Example 2.10 is called "orthomorphic" [13].

References

[1] Daniel Augot, Matthieu Finiasz, "Exhaustive Search for Small Dimension Recursive MDS Diffusion Layers for Block Ciphers and Hash Functions", ISIT 2013: 1551-1555.

[2] M. Blaum, R. M. Roth: On Lowest Density MDS Codes. IEEE TRANSACTIONS ON INFORMATION THEORY, vol. 45(1), pp. 46-59 (January 1999)

[3] J. Daemen, V. Rijmen, AES proposal: Rijndael. Selected as the Advanced Encryption Standard. Available from http://nist.gov/aes

[4] P. Ekdahl, T. Johansson, SNOW a new stream cipher, Proceedings of first NESSIE Workshop, Heverlee, Belgium, 2000

[5] A. Klimov, Applications of T-functions in Cryptography, Thesis for the degree of Ph.D., Weizmann Institute of Science, 2005.

[6] San Ling, Chaoping Xing, Coding Theory: A First Course, Cambridge University Press, 2004.

[7] F. J. MacWilliams and N.J.A. Sloane, The Theory of Error-Correcting Codes, North-Holland, Amsterdam, 1998.

[8] A. Mahmoodi Rishakani, S. M. Dehnavi, M. R. Mirzaee Shamsabad, Hamidreza Maimani, Einollah Pasha, "New Concepts in Design of Lightweight MDS Diffusion Layers", ISCISC'14, University of Tehran, Tehran, Iran, 2014.

[9] Mahdi Sajadieh, Mohammad Dakhilalian, Hamid Mala, Pouyan Sepehrdad: Recursive Diffusion Layers for Block Ciphers and Hash Functions. FSE 2012: 385-401

[10] B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, N. Ferguson, Twofish: A 128-bit Block Cipher; 15 June, 1998

[11] Douglas R. Stinson, "Combinatorial Designs: Constructions and Analysis", Springer-Verlag, 2003.

[12] S. Vaudenay, "On the Need for Multipermutations: Cryptanalysis of MD4 and SAFER", In B. Preenel, editor, Fast Software Encryption. Proceedings, LNCS 1008, (1995), 286-297.

[13] J. Zhou, A Note on the Constructions of Orthomorphic Permutations, International Journal of Network Security, Vol.10, No.1, PP.57-61, Jan. 2010.