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]. 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
\[
    \text{dist}(a, b) = |\{i | a_i \neq b_i, 1 \leq i \leq n\}|.
\]

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. We define the (differential) branch number of a map $f : A^k \rightarrow A^n$, as

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

Definition 2.3. Let $A$ be a nonempty finite set and $k$ and $n$ be two natural numbers. We call a map $f : A^k \rightarrow A^n$, $(k,n,A)$-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 $f : A^r \rightarrow B$ 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 $A$ and $B$ be two nonempty finite sets, $r$ be a natural number and $f : A^r \rightarrow B$ be a map. Suppose that $I = \{i_1, i_2, \ldots, i_t\}$ 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 2.7. Let $A$ be a nonempty finite set and $k$ and $n$ be two natural numbers. A map $f : A^k \rightarrow A^n$ can be represented as a vector $(f_1, f_2, \ldots, f_n)$ of functions. Here, $f_i : A^k \rightarrow A$, $1 \leq i \leq n$, is called the $i$-th component (projection) function of $f$.

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

$$f^J_I : A^k \rightarrow A^t,$$

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

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

$$a = (a_1, a_2, \ldots, a_k),$$
$$b = (b_1, b_2, \ldots, b_k),$$

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 $f^J_I$ is not parametric invertible, due to the existances 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 $f^J_I$ is not parametric invertible. Then, there exist $a, b \in A$ with $f^J_I(a) = f^J_I(b)$ and $a_i = b_i, i \notin I$. This means that

$$dist(a,b) \leq t,$$
$$dist(f(a),f(b)) \leq n - t,$$

which is contradiction. \qed

**Definition 2.10.** Let $(G,\star)$ be a finite group and $\phi$ be an isomorphism on $G$ such that the mapping $\psi$ on $G$ with $\psi(g) = g^{-1} \star \phi(g)$ is also an isomorphism. Then the isomorphism $\phi$ is called 'orthomorphic'.

**Note 2.11.** In some cases, the orthomorphicity of $\phi$ in Definition 2.10, is equivalent to orthomorphicity of $\rho(g) = g \star \phi(g)$. For instance, this is the case for the additive groups of finite fields of characteristic 2.

**Lemma 2.12.** Let $(G,\star)$ be a finite group satisfying the property mentioned in Note 2.11 and $\phi$ be an orthomorphism on $G$. Then the following map is $(2,2,G)$-MDS:

$$f : G^2 \to G^2,$$
$$f(g_1, g_2) = (g_1 \star g_2, g_1 \star \phi(g_2)).$$
**Proof.** We show that if the mappings $\phi$ and 
\[ \psi : G \rightarrow G, \]
\[ \psi(g) = g * \phi(g), \]
are both group isomorphisms, then $f$ is a $(2, 2, G)$-MDS map: 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. Consider the following parametric functions
\begin{align*}
h_1, h_2, h_3, h_4 : & \ G \rightarrow G, \\
h_1(g, c) = & \ h_2(c, g) = g * c, \\
h_3(g, c) = & \ g * \phi(c), \\
h_4(c, g) = & \ c * \phi(g). \\
\end{align*}
The parametric functions $h_1$, $h_2$ and $h_3$ are invertible because $G$ is a group. The parametric function $h_4$ is invertible because $\phi$ is an isomorphism. Now suppose that the function $h_5 = f$ is not invertible. Suppose that for $(g_1, g_2) \neq (g_1', g_2')$ we have
\[ (g_1 * g_2, g_1 * \phi(g_2)) = (g_1' * g_2', g_1' * \phi(g_2')). \]
Then we have
\begin{align*}
g_1 * g_2 &= g_1' * g_2', \\
g_1 * \phi(g_2) &= g_1' * \phi(g_2'); \\
\end{align*}
which leads to
\begin{align*}
g_1 * (g_1')^{-1} &= g_2' * g_2^{-1}, \\
g_1 * (g_1')^{-1} &= \phi(g_2' * g_2^{-1}), \\
\end{align*}
by isomorphicity of $\phi$. So, we get
\[ \phi(g_2' * g_2^{-1}) * (g_1 * (g_1')^{-1})^{-1} = e_G. \]
Since by Note 2.11 the mapping $\rho$ with $\rho(g) = g^{-1} * \phi(g)$ is an isomorphism, then we have $g_2 = g_2'$. So $g_1 = g_1'$, which is a contradiction. \hfill \Box

**Example 2.13.** Let $G = \{e, a, b, c\}$ be the Klein 4-group and
\[ \phi : G \rightarrow G, \]
\[ \phi(e) = e, \ \phi(a) = b, \ \phi(b) = c, \ \phi(c) = a. \]
It is easy to see that $\phi$ is an orthomorphism on $G$. So, by Lemma 2.12, the following mapping is a $(2, 2, G)$-MDS map:
\[ f : G^2 \rightarrow G^2, \]
\[ f(g_1, g_2) = (g_1 * g_2, g_1 * \phi(g_2)). \]
REFERENCES


