

# Is Matsumoto's Generalization of the Feng-Rao Designed Minimum Distance for Binary Linear Codes Effective?

Junru Zheng<sup>†</sup>, Takayasu Kaida<sup>‡</sup>, Kyoki Imamura<sup>†</sup>

<sup>†</sup> Department of Computer Science and Electronics, Kyushu Institute of Technology  
680-4 Kawazu, Iizuka, Fukuoka 820-8501 JAPAN  
e-mail: {zheng, imamura}@capricorn.cse.kyutech.ac.jp

<sup>‡</sup> Department of Information and Electronic Engineering, Yatsushiro National College of Technology  
2627 Hirayama-shinmachi, Yatsushiro, Kumamoto 866-8501 JAPAN  
e-mail: kaida@as.yatsushiro-nct.ac.jp

## Abstract

The definition of the Feng-Rao designed minimum distance, first introduced into algebraic geometry codes, has been extended to the case of general linear codes by Miura. In Miura's definition the Feng-Rao designed minimum distance  $d_{FR}$  is determined by an ordered basis related to a given linear code over a finite field  $F_q$ . Matsumoto gave a generalized definition  $\hat{d}_{FR}$  of  $d_{FR}$  with three ordered bases  $W_n, U_n, V_n$ . The basis  $W_n$  is used for defining the linear code, and the bases  $U_n$  and  $V_n$  are used for computing a syndrome matrix. We have Miura's definition if we assume  $U_n = V_n = W_n$  in Matsumoto's definition. In this paper we discuss the choice of three bases by Matsumoto's definition for binary linear codes. From some properties and some numerical examples of Matsumoto's  $\hat{d}_{FR}$  we conjecture that Matsumoto's generalization is not so effective for binary linear codes compared with Miura's definition.

**Keywords** : *binary linear code, Feng-Rao designed minimum distance, ordered basis, Miura's definition, Matsumoto's definition.*

## 1 Introduction

The Feng-Rao designed minimum distance and the Feng-Rao decoding were originally introduced into algebraic geometry codes [1]. They have been extended to the case of general linear codes over a finite field by Miura [3]. Miura's definition of the Feng-Rao designed minimum distance  $d_{FR}$  for an  $(n, k)$  linear code  $C$  over a finite field  $F_q$  of order  $q$  depends on the choice of an ordered basis  $W_n = \{\mathbf{w}_1, \mathbf{w}_2, \dots, \mathbf{w}_n\}$  of the vector space  $F_q^n$  with dimension  $n$  over  $F_q$ . It is interesting to find such an optimum ordered basis  $W_n$  as  $d_{FR}$  is maximum, since the Feng-Rao decoding algorithm can correct up to  $\lfloor (d_{FR} - 1)/2 \rfloor$  errors. Recently the authors showed some properties of the Feng-Rao designed minimum distance  $d_{FR}$  by Miura for binary codes and cyclic codes [4, 5]. Recently the definition of  $d_{FR}$  of linear codes has been slightly generalized by Matsumoto [2], which uses three ordered bases  $U_n = \{\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_n\}$ ,  $V_n = \{\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n\}$  and  $W_n = \{\mathbf{w}_1, \mathbf{w}_2, \dots, \mathbf{w}_n\}$  of

$F_q^n$  instead of one in case of Miura's definition, i.e.,  $W_n$  is used for defining the linear code, and  $U_n, V_n$  are used for computing a syndrome matrix in Matsumoto's definition and Miura's definition is included by assumption  $U_n = V_n = W_n$ .

In this paper we discuss the choice of three bases by Matsumoto's definition for binary linear codes. Consequently we conjecture that Matsumoto's generalization for binary linear codes is not so effective compared with Miura's definition by some properties and some numerical examples of Matsumoto's  $d_{FR}$ .

## 2 Definitions and properties of the Feng-Rao Designed Minimum Distance

In this section we will briefly review results of [3] and [2] necessary for the following discussions in this paper.

For two vectors  $\mathbf{x} = (x_1, x_2, \dots, x_n)$  and  $\mathbf{y} = (y_1, y_2, \dots, y_n) \in F_q^n$ , their product  $\mathbf{x}\mathbf{y}$  is defined as  $\mathbf{x}\mathbf{y} = (x_1y_1, x_2y_2, \dots, x_ny_n) \in F_q^n$ . We will call  $W_n = \{\mathbf{w}_1, \mathbf{w}_2, \dots, \mathbf{w}_n\} \subseteq F_q^n$  an ordered basis of  $F_q^n$  if  $W_n$  is a basis of  $F_q^n$  and the ordering of  $n$  vectors  $\mathbf{w}_1, \mathbf{w}_2, \dots, \mathbf{w}_n$  has meaning. The subset  $W_i$  of  $W_n$  is defined by  $W_i = \{\mathbf{w}_1, \mathbf{w}_2, \dots, \mathbf{w}_i\}$  for  $1 \leq i \leq n$ .

**Definition 1** For a vector  $\mathbf{b} \in F_q^n$ , the map of an ordered basis  $W_n$  denoted by  $\sigma: F_q^n \rightarrow \{0, 1, 2, \dots, n\}$  is defined as

$$\sigma(\mathbf{b}) = \min\{i | \mathbf{b} \in \text{Span}\{W_i\}, 0 \leq i \leq n\},$$

where  $\text{Span}\{W_i\}$  is a subspace of  $F_q^n$  spanned by  $W_i$  and  $\text{Span}\{W_0\} = \{\mathbf{0}\}$ .

**Definition 2** Let  $\mathbf{u}_i \in U_n$ ,  $\mathbf{v}_j \in V_n$ . The product  $\mathbf{u}_i\mathbf{v}_j$  of  $\mathbf{u}_i$  and  $\mathbf{v}_j$  for an ordered basis  $W_n$  is said to be well-behaved if  $\sigma(\mathbf{u}_u\mathbf{v}_v) < \sigma(\mathbf{u}_i\mathbf{v}_j)$  for any  $1 \leq u \leq i$ ,  $1 \leq v \leq j$ ,  $(u, v) \neq (i, j)$ .

Let  $W$  be a subset of an ordered basis  $W_n$  of  $F_q^n$ . The linear code  $C(W_n, W)$  over  $F_q$  is defined as

$$C(W_n, W) = \text{Span}\{W\}^\perp \subset F_q^n,$$

where  $\text{Span}\{W\}^\perp$  means the set of all vectors in  $F_q^n$  orthogonal to  $\text{Span}\{W\}$ .

## 2.1 Miura's Definition of the Feng-Rao Designed Minimum Distance $d_{FR}$

**Definition 3** For  $1 \leq s \leq n$ , we define  $N(s)$  as

$$N(s) = \#\left\{ (i, j) \mid \begin{array}{l} \sigma(\mathbf{w}_i\mathbf{w}_j) = s, 1 \leq i, j \leq n, \\ \mathbf{w}_i\mathbf{w}_j \text{ is well-behaved} \end{array} \right\},$$

where  $\#A$  means the cardinality of set  $A$ . For an ordered basis  $W_n$  of  $F_q^n$  we define  $N(W_n)$  as  $N(W_n) = (N(1), N(2), \dots, N(n))$ .

**Lemma 1** [3] We have  $0 \leq N(s) \leq s$ , for  $1 \leq s \leq n$ .

**Definition 4** The Feng-Rao designed minimum distance of the linear code  $C(W_n, W)$  is denoted as  $d_{FR}(C, W_n)$  and defined as

$$d_{FR}(C, W_n) = \min\{N(s) | \mathbf{w}_s \in W_n \setminus W, 1 \leq s \leq n\},$$

where  $W_n \setminus W$  is the subset of  $W_n$  without the elements of  $W$ .

We will use the notation  $d_{FR}(C, W_n)$  to show the ordered basis  $W_n$  explicitly.

**Lemma 2** [3] Let  $d$  be the true minimum distance of  $C(W_n, W)$ . Then we have  $d \geq d_{FR}(C, W_n)$ .

For a fixed linear code  $C$  we can choose many bases  $W_n$  such that  $C = C(W_n, W)$ .

**Definition 5** For a linear code  $C$  we define the set of all ordered bases such that  $C$  can be defined by this ordered basis, i.e.,

$$\mathcal{W}(C) = \{W_n | \exists W \subseteq W_n \text{ s.t. } C = C(W_n, W)\}.$$

Note that  $W$  is uniquely determined from  $C$  and  $W_n$ . Our purpose is to give an optimum ordered basis  $W_n$  for a given linear code  $C$ .

**Definition 6** The Feng-Rao designed minimum distance  $d_{FR}(C)$  of  $C$  by Miura is defined as

$$d_{FR}(C) = \max\{d_{FR}(C, W_n) | W_n \in \mathcal{W}(C)\}.$$

The ordered basis  $W_n$  satisfying

$$d_{FR}(C) = d_{FR}(C, W_n)$$

is called an optimum ordered basis for  $C$ .

## 2.2 Properties of Miura's $d_{FR}$

Next we will consider only binary linear codes over  $F_2$ . The following lemma [3, Lemma 3.3] and its corollary [3, Corollary 3.4] are essential in our discussions. We will quote them in case of binary linear codes, although Miura proved them in case of linear codes over any  $F_q$ . We will give their proof for the convenience of readers who will find difficulty in obtaining Miura's thesis [3].

**Lemma 3** Let  $W_n = \{\mathbf{w}_1, \mathbf{w}_2, \dots, \mathbf{w}_n\}$  be an ordered basis of  $F_q^n$  and  $\mathbf{w} \in F_2^n$ . If  $\sigma(\mathbf{w}_t\mathbf{w}) < t \leq n$ , then there exists at least one  $i$  such that  $\sigma(\mathbf{w}_i\mathbf{w}) \leq \sigma(\mathbf{w}_t\mathbf{w})$  and  $1 \leq i < t$ .

**Proof** We will show a contradiction if we assume

$$\sigma(\mathbf{w}_i\mathbf{w}) < \sigma(\mathbf{w}_t\mathbf{w}) \quad \text{for } i = 1, 2, \dots, t-1. \quad (1)$$

Let  $\sigma(\mathbf{w}_t\mathbf{w}) = s < t$ . We have

$$\mathbf{w}_t\mathbf{w} = \alpha_1\mathbf{w}_1 + \alpha_2\mathbf{w}_2 + \dots + \alpha_s\mathbf{w}_s, \quad \alpha_s \neq 0. \quad (2)$$

From the assumption (1) we also have

$$\mathbf{w}_i\mathbf{w} = \beta_{i,1}\mathbf{w}_1 + \beta_{i,2}\mathbf{w}_2 + \dots + \beta_{i,s-1}\mathbf{w}_{s-1}. \quad (3)$$

We have  $\mathbf{w}\mathbf{w} = \mathbf{w}$  for any binary vector  $\mathbf{w}$  and we have

$$\begin{aligned} \mathbf{w}_t\mathbf{w} &= \mathbf{w}_t\mathbf{w}\mathbf{w} = (\mathbf{w}_t\mathbf{w})\mathbf{w} \\ &= (\alpha_1\mathbf{w}_1 + \dots + \alpha_s\mathbf{w}_s)\mathbf{w} \\ &= \alpha_1\mathbf{w}_1\mathbf{w} + \dots + \alpha_s\mathbf{w}_s\mathbf{w} \end{aligned} \quad (4)$$

from (2). However (2) and (4) are contradiction, since the term  $\alpha_s \mathbf{w}_s$  in (2) is missing in the right-hand side of (4) because of (3).  $\square$

**Corollary 1** *If  $\sigma(\mathbf{w}_i \mathbf{w}_j) = s$  and  $\mathbf{w}_i \mathbf{w}_j$  is well-behaved, then we have  $1 \leq i, j \leq s$ .*

**Proof** If we assume  $i > s$ , then application of Lemma 3 with  $t = i$  and  $\mathbf{w} = \mathbf{w}_j$  shows that  $\mathbf{w}_i \mathbf{w}_j$  is not well-behaved from the definition of well-behavedness. The proof of  $j \leq s$  is the same.  $\square$

Therefore we will prove the following theorem shown in [5].

**Theorem 1** *Any binary linear code has  $d_{FR}(C, W_n)$  equal to either one or an even number.*

This theorem tells that binary linear codes can not have an odd  $d_{FR}(C, W_n) \geq 3$ . Our proof of Theorem 1 is very simple as shown below.

First we use the following property which is obvious from the definition.

**Lemma 4** *If  $\mathbf{w}_i \mathbf{w}_j (i \neq j)$  is well-behaved, then  $\mathbf{w}_j \mathbf{w}_i$  is also well-behaved.*

Next we use the following lemma which is almost obvious from Corollary 1.

**Lemma 5** *If  $\mathbf{w}_i \mathbf{w}_i$  is well-behaved of  $W_n$ , then we have  $N(i) = 1$ .*

**Proof** For a binary vector  $\mathbf{w}_i$  we have  $\mathbf{w}_i \mathbf{w}_i = \mathbf{w}_i$  and  $\sigma(\mathbf{w}_i \mathbf{w}_i) = i$ . There can not exist another  $\mathbf{w}_u \mathbf{w}_v$ ,  $(u, v) \neq (i, i)$  which satisfies the condition that  $\sigma(\mathbf{w}_u \mathbf{w}_v)$

$= i$  and  $\mathbf{w}_u \mathbf{w}_v$  is well-behaved, since such  $\mathbf{w}_u$  and  $\mathbf{w}_v$  must satisfy  $1 \leq u, v \leq i$  from Corollary 1 and  $\sigma(\mathbf{w}_u \mathbf{w}_v)$  must be less than  $i$  because of  $\mathbf{w}_i \mathbf{w}_i$  being well-behaved.

**Proof of Theorem 1** We have  $N(1) = 1$  because of  $\sigma(\mathbf{w}_1 \mathbf{w}_1) = 1$ .

If  $\mathbf{w}_i \mathbf{w}_i$  is not well-behaved for  $i \geq 2$ , then  $N(i)$  is even for  $i \geq 2$  from Lemma 5. Therefore we have Theorem 1.

If there exists such a  $\mathbf{w}_i \in W_n \setminus W$  as  $\mathbf{w}_i \mathbf{w}_i$  is well-behaved, then we have  $N(i) = 1$  from Lemma 5 and  $d_{FR}(C, W_n) = 1$  from the definition of  $d_{FR}(C, W_n)$ .  $\square$

### 2.3 Matsumoto's Definition of Feng-Rao Designed Minimum Distance $\hat{d}_{FR}$

Miura's definition of the Feng-Rao designed minimum distance has been generalized to  $\hat{d}_{FR}$  by Matsumoto [2].

**Definition 7** *For  $1 \leq s \leq n$ , we define  $\hat{N}(s)$  as*

$$\hat{N}(s) = \# \left\{ (i, j) \mid \begin{array}{l} \sigma(\mathbf{u}_i \mathbf{v}_j) = s, 1 \leq i, j \leq n, \\ \mathbf{u}_i \mathbf{v}_j \text{ is well-behaved} \end{array} \right\}.$$

*For an ordered basis  $W_n, U_n$  and  $V_n$  of  $F_q^n$  we define  $\hat{N}(W_n, U_n, V_n)$  as  $\hat{N}(W_n, U_n, V_n) = (\hat{N}(1), \hat{N}(2), \dots, \hat{N}(n))$ .*

Our numerical experiments in case of all  $(7, k)$  linear codes by generating all the possible set of three bases show  $\hat{N}(1) \leq 1$  and  $\hat{N}(2) \leq 2$ . So we have the following conjecture.

**Conjecture 1** *We have  $0 \leq \hat{N}(s) \leq s$ , for  $1 \leq s \leq n$ .*

**Definition 8** *The Feng-Rao designed minimum distance by Matsumoto of the linear code  $C(W_n, W)$  is denoted as  $\hat{d}_{FR}(C, W_n, U_n, V_n)$  and defined as*

$$\hat{d}_{FR}(C, W_n, U_n, V_n) = \min \left\{ \hat{N}(s) \mid \begin{array}{l} \mathbf{w}_s \in W_n \setminus W, \\ 1 \leq s \leq n \end{array} \right\},$$

**Lemma 6** [2] *Let  $d$  be the true minimum distance of  $C(W_n, W)$ . Then we have  $d \geq \hat{d}_{FR}(C, W_n, U_n, V_n)$ .*

**Definition 9** *For a linear code  $C$  we define the set of all triples with three ordered bases such that  $C$  can be defined by an ordered basis  $W_n$ , i.e.,*

$$\mathcal{T}(C) = \left\{ (W_n, U_n, V_n) \mid \begin{array}{l} \exists W \subseteq W_n \text{ s.t.} \\ C = C(W_n, W) \text{ and} \\ U_n, V_n \text{ are ordered} \\ \text{bases of } F_q^n \end{array} \right\}.$$

Note that  $W$  is uniquely determined from  $C$  and  $W_n$ . Moreover  $U_n$  and  $V_n$  are not concerned with the linear code  $C$ . Our purpose is to give an optimum triple of three ordered bases  $(W_n, U_n, V_n)$  for a given linear code  $C$ .

**Definition 10** *The Feng-Rao designed minimum distance  $\hat{d}_{FR}(C)$  of  $C$  by Matsumoto is defined as*

$$\hat{d}_{FR}(C) = \max \{ \hat{d}_{FR}(C, W_n, U_n, V_n) \mid (W_n, U_n, V_n) \in \mathcal{T}(C) \}.$$

*The triple of three ordered bases  $(W_n, U_n, V_n)$  satisfying  $\hat{d}_{FR}(C) = \hat{d}_{FR}(C, W_n, U_n, V_n)$  is called an optimum triple for  $C$ .*

### 2.4 An Example of Matsumoto's $\hat{d}_{FR}$

Next we will consider only binary linear codes over  $F_2$ . First, we show an example of a triple of three bases in order to discuss Matsumoto's generalization of  $\hat{d}_{FR}$ .

**Example** For (7,4) linear code, let three ordered basis be as follows:

$$\begin{aligned} \mathbf{w}_1 = \mathbf{u}_1 &= (1 \ 0 \ 1 \ 1 \ 1 \ 0 \ 0), \\ \mathbf{w}_2 = \mathbf{u}_2 &= (0 \ 1 \ 0 \ 1 \ 1 \ 1 \ 0), \\ \mathbf{w}_3 = \mathbf{u}_3 &= (0 \ 0 \ 1 \ 0 \ 1 \ 1 \ 1), \\ \mathbf{w}_4 = \mathbf{u}_4 &= (0 \ 0 \ 0 \ 1 \ 1 \ 0 \ 0), \\ \mathbf{w}_5 = \mathbf{u}_5 &= (0 \ 0 \ 0 \ 0 \ 0 \ 1 \ 1), \\ \mathbf{w}_6 = \mathbf{u}_6 &= (0 \ 0 \ 0 \ 1 \ 0 \ 1 \ 0), \\ \mathbf{w}_7 = \mathbf{u}_7 &= (0 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0). \end{aligned}$$

$$\begin{aligned} \mathbf{v}_1 &= (0 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0), \\ \mathbf{v}_2 &= (0 \ 0 \ 0 \ 0 \ 0 \ 1 \ 1), \\ \mathbf{v}_3 &= (1 \ 0 \ 1 \ 1 \ 1 \ 0 \ 0), \\ \mathbf{v}_4 &= (0 \ 0 \ 0 \ 1 \ 1 \ 0 \ 0), \\ \mathbf{v}_5 &= (0 \ 1 \ 0 \ 1 \ 1 \ 1 \ 0), \\ \mathbf{v}_6 &= (0 \ 0 \ 1 \ 0 \ 1 \ 1 \ 1), \\ \mathbf{v}_7 &= (0 \ 0 \ 0 \ 1 \ 0 \ 1 \ 0). \end{aligned}$$

Since the matrix of  $\sigma(\mathbf{u}_i \mathbf{v}_j)$  is

$$\begin{bmatrix} 0 & 0 & 1 & 4 & 4 & 5 & 7 \\ 7 & 7 & 4 & 4 & 2 & 6 & 6 \\ 7 & 5 & 5 & 7 & 6 & 3 & 7 \\ 0 & 0 & 4 & 4 & 4 & 7 & 7 \\ 7 & 5 & 0 & 0 & 7 & 5 & 7 \\ 7 & 7 & 7 & 7 & 6 & 7 & 6 \\ 7 & 7 & 0 & 0 & 7 & 7 & 7 \end{bmatrix}.$$

Above matrix  $\sigma(\mathbf{u}_i \mathbf{v}_j)$  shows that  $\sigma(\mathbf{u}_1 \mathbf{v}_3) = 1$  and  $\mathbf{u}_1 \mathbf{v}_3$  is well-behaved, which contradicts with Corollary 1. Therefore in Matsumoto's definition we don't have Lemma 3 and Corollary 1, which are used in proving Theorem 1.

However our numerical experiments on  $(7, k)$  binary codes strongly suggest the following conjecture which is the same our previous Theorem 1.

**Conjecture 2** Any binary linear code has  $\hat{d}_{FR}(C, W_n, U_n, V_n)$  equal to either one or an even number.

### 3 Conclusion

In this paper we discussed Miura's definition and Masumoto's definition of the Feng-Rao designed minimum distance for binary linear codes. Matsumoto's definition is a generalization of Miura's definition. Some properties and examples induce some conjectures which tell Matsumoto's generalization is not effective compared with Miura's definition for binary linear codes.

Future works are giving proofs for these conjectures and investigate nonbinary linear codes.

### References

- [1] G.L. Feng, T.R.N. Rao, "Decoding algebraic geometric codes up to the designed minimum distance," *IEEE Trans. Inform. Theory*, vol. 39, pp. 36-47, Jan. 1993.
- [2] R. Matsumoto, "On the Feng-Rao Bound for the L-construction of Algebraic Geometric Codes," *IEICE Trans. Fundamentals*, vol. E83-A, No.5, pp. 923-926, May 2000.
- [3] S. Miura, *Study on Error Correcting Codes Based on Algebraic Geometry*, Ph.D. Dissertation, the University of Tokyo, 1997. (in Japanese)
- [4] J. Zheng, T. Kaida, K. Imamura, "A note on Feng-Rao designed minimum distance for cyclic codes," The Third International Conference on Information, Communications & Signal Processing (ICICS 2001), Singapore, Oct., 2001.
- [5] J. Zheng, T. Kaida, K. Imamura, "The Feng-Rao designed minimum distance of binary linear codes does not have an odd number except one," The First International Workshop on Sequence Designed and Applications for CDMA Systems (IWSDA 2001), pp. 146-149, Sep., 2001.