This document is downloaded from DR-NTU (https://dr.ntu.edu.sg)
Nanyang Technological University, Singapore.

Matrix product codes over finite commutative Frobenius rings

Fan, Yun; Ling, San; Liu, Hongwei

2014

Fan, Y., Ling, S., & Liu, H. (2014). Matrix product codes over finite commutative Frobenius rings. Designs, Codes and Cryptography, 71(2), 201-227.

https://hdl.handle.net/10356/101989

https://doi.org/10.1007/s10623-012-9726-y

© 2012 Springer Science+Business Media.This is the author created version of a work that has been peer reviewed and accepted for publication by Designs, Codes and Cryptography, Springer Science+Business Media. It incorporates referee’s comments but changes resulting from the publishing process, such as copyediting, structural formatting, may not be reflected in this document. The published version is available at: [http://dx.doi.org/10.1007/s10623-012-9726-y].

Downloaded on 23 Aug 2022 12:56:02 SGT

Matrix Product Codes over Finite Commutative Frobenius Rings

Yun Fan[1], San Ling[2], Hongwei Liu[1]

[1]School of Mathematics and Statistics, Central China Normal University, Wuhan 430079, China
[2]Division of Mathematical Sciences, School of Physical & Mathematical Sciences, Nanyang Technological University, Singapore 637616, Singapore

Abstract

Properties of matrix product codes over finite commutative Frobenius rings are investigated. The minimum distance of matrix product codes constructed with several types of matrices is bounded in different ways. The duals of matrix product codes are also explicitly described in terms of matrix product codes.

Keywords: matrix product code, Frobenius ring, minimum distance, dual code, quasi-cyclic code.

Mathematics Subject Classification (2010): 94B05, 94B65, 15B33

1 Introduction

In coding theory, an interesting and important question is to construct codes from smaller ones and to explore their properties via those of the smaller ones. There have been many such constructions, for example, the $(u|u+v)$-construction and the $(a+x|b+x|a+b+x)$-construction. It was shown in [8] that quasi-cyclic codes over finite fields with co-index coprime to the characteristic of the finite fields can be constructed from linear codes of lower dimension in a similar way, and the $(a+x|b+x|a+b+x)$-construction is one such special case. A more general construction, called the *matrix product code*, which is formed by m codes of length n over a finite field and an $m \times l$ matrix over the finite field, was proposed and studied in [1]. Many, though not all, quasi-cyclic codes can be rewritten as matrix product codes, for suitably chosen matrices. It was further shown in [14] that the codes constructed by algebraic geometry in [11] are in fact matrix product codes. In [1], a class of matrices, called *non-singular by columns* matrices, was introduced, and some lower bounds were obtained for the minimum distance of the matrix product codes constructed with such matrices. However, most matrices for quasi-cyclic codes, including the matrix for the $(a+x|b+x|a+b+x)$-construction, are not non-singular by columns. For general matrix product codes over finite fields, a lower bound for the minimum distance was obtained in [14]. Decoding methods for some matrix product codes were also discussed in [4], [5] and [7]. Other related works may be found in [6], [10] and [13].

On the other hand, coding over finite rings has attracted much attention since the seminal work in [3]. It was pointed out in the important works [17] and [18] that only finite Frobenius rings are suitable for coding alphabets, in the sense that several fundamental properties of codes over finite fields still hold for codes over such rings. For example, the double dual property, which says that the double dual coincides with the original linear code, holds for linear codes over finite Frobenius rings. A special class of finite Frobenius rings consists of the finite chain rings, and codes over finite chain rings have been investigated from many perspectives. Recently, in [16], matrix product codes over finite chain rings were studied and the lower bound on the minimum distance of matrix product codes by non-singular by columns matrices

Email addresses: yunfan02@yahoo.com.cn (Yun Fan); lingsan@ntu.edu.sg (San Ling); h_w_liu@yahoo.com.cn (Hongwei Liu).

in [1] was extended to the minimum homogeneous distance. Some quasi-cyclic codes over finite chain rings have also been decomposed into matrix product codes in [9], though the terminology "matrix product code" was not used.

In this paper, we extend previous works on matrix product codes in two directions. First, we formulate matrix product codes over finite commutative Frobenius rings, and explore their general properties, mainly, the minimum distance and the structure of the duals. Second, we consider new classes of matrices, which contain the class of non-singular by columns matrices as a special case, for which we can bound the minimum distance of matrix product codes thus constructed more precisely and more tightly, and for which self-dual matrix product codes can be constructed efficiently. The understanding of dual codes, as well as self-orthogonality and self-duality of codes, is a natural and important question in coding theory.

The organization of the paper is as follows.

Section 2 contains facts on matrices over finite commutative rings which are needed for later sections, but which may not be readily available in the literature.

In Section 3, we formulate matrix product codes over finite commutative Frobenius rings, and give two lower bounds for the minimum distance of such codes. We also prove that the dual code of a matrix product code is also a matrix product code whose structure is described precisely. Not only does this extend earlier results in [1] and [16], it also does not require the matrix to be a square matrix.

In Section 4, we introduce a class of matrices, called *strongly full-row-rank (SFRR) matrices* (see Definition 4.3), which is bigger than the class of non-singular by columns matrices and also contains certain matrices associated to quasi-cyclic codes. We exhibit more precise lower bounds for the minimum distance of matrix product codes constructed with these matrices, as well as for their dual codes. Besides extending corresponding results in [1], conditions for which these lower bounds are attained are also given.

Inspired by the matrix for the $(a+x|b+x|a+b+x)$-construction, in Section 5 we consider special matrices, named *two-way* (m')*-SFRR matrices* (see Definition 5.1), and obtain lower and upper bounds for the minimum distance of matrix product codes constructed with these matrices. These bounds cover some known bounds for the minimum distance of codes obtained from the $(a+x|b+x|a+b+x)$-construction as special cases. For such matrices, we also show a condition (see Definition 5.3) which is useful for the construction of self-orthogonal matrix product codes.

2 Matrices over Finite Commutative Rings

In this paper, R is always a finite commutative ring. Writing the identity element 1 of the ring R as the sum of the primitive idempotents of R, we obtain an isomorphism

$$R \xrightarrow[\varphi]{\cong} R_1 \oplus \cdots \oplus R_s, \quad r \longmapsto (r^{(1)}, \cdots, r^{(s)}), \tag{2.1}$$

where $R_1, \cdots, R_s$ are local commutative rings. With the isomorphism (2.1), in the following we usually identify R with $R_1 \oplus \cdots \oplus R_s$ and just write $r = (r^{(1)}, \cdots, r^{(s)})$.

The finite commutative ring R is called a *Frobenius ring* if R is self-injective (i.e., the regular module is injective), or equivalently, $(C^{\perp})^{\perp} = C$ for any submodule C of any free R-module R^n, where $C^{\perp}$ denotes the orthogonal submodule of C with respect to the usual Euclidean inner product on R^n. Moreover, in this case, $|C^{\perp}||C| = |R|^n$ for any submodule C of R^n, where $|C|$ denotes the cardinality of C. This is one of the reasons why only finite Frobenius rings are suitable for coding alphabets. With the isomorphism (2.1), R is Frobenius if and only if every local component R_i is Frobenius, and the finite local commutative ring R_i is Frobenius if and only if R_i has a unique minimal ideal. Note that, in the non-commutative case, a self-injective ring is called a *quasi-Frobenius ring*, while one more condition is required for it to become a Frobenius ring. However, in the commutative case, a finite quasi-Frobenius ring is exactly a finite Frobenius ring. The reader may refer to [17] for more details on Frobenius rings.

By $\mathrm{M}_{m\times l}(R)$, we mean the set of all $m \times l$ matrices over R. For $A \in \mathrm{M}_{m\times l}(R)$, we denote the transpose of the matrix A by A^T. Given matrices A of size $m \times l$ and B of size $m \times l'$, we use $(A|B)$ to denote the matrix of size $m \times (l + l')$ formed by concatenating A and B. If C is another matrix of size $m' \times l$, the $(m + m') \times l$ matrix $\begin{pmatrix} A \\ \hline C \end{pmatrix}$ is similarly defined (by concatenating vertically). We also let 0 denote

the zero matrix, where the size will either be obvious from the context or specified whenever necessary. Similarly, we denote the $m \times m$ identity matrix by I_m, or simply I if the size is clear from the context.

Any matrix $A = (a_{ij})_{m\times l} \in \mathrm{M}_{m\times l}(R)$ can be written as

$$A = \left(A^{(1)}, \cdots, A^{(s)}\right), \qquad A^{(k)} = \left(a_{ij}^{(k)}\right)_{m\times l} \in \mathrm{M}_{m\times l}(R_k), \quad 1 \le k \le s, \tag{2.2}$$

where the matrix addition and product are the coordinate-wise addition and product, respectively.

Consider the free R-module R^n of rank n. Any element $\mathbf{a} = (a_1, \cdots, a_n)^T$ (written as a column vector) of R^n is also called a vector, and we let $\mathbf{0}$ denote the zero vector. With the identification in (2.1), we can write

$$R^n = R_1^n \oplus \cdots \oplus R_s^n, \quad \mathbf{a} = \left(\mathbf{a}^{(1)}, \cdots, \mathbf{a}^{(s)}\right),$$

where $\mathbf{a}^{(k)} = (a_1^{(k)}, \cdots, a_n^{(k)})^T$, for $1 \le k \le s$, is a column vector in R_k^n.

Definition 2.1. *For any integer $t \ge 1$, let $\mathbf{a}_i = (a_{i1}, \cdots, a_{in}) \in R^n$, where $i = 1, \cdots, t$. The vectors $\mathbf{a}_1, \cdots, \mathbf{a}_t$ are said to be* linearly dependent *if there exists $(b_1, \cdots, b_t)$ in the set difference $R^t \setminus \{\mathbf{0}\}$ such that $b_1\mathbf{a}_1 + \cdots + b_t\mathbf{a}_t = \mathbf{0}$; otherwise, $\mathbf{a}_1, \cdots, \mathbf{a}_t$ are said to be* linearly independent.

If an R-submodule of R^n is generated by vectors $\mathbf{a}_1, \cdots, \mathbf{a}_t$ which are linearly independent, then it is a free R-module of rank t and we say that $\mathbf{a}_1, \cdots, \mathbf{a}_t$ form a *basis* of the free submodule.

The proof of the following result is straight-forward, so we omit it here.

Lemma 2.2. *The vectors $\mathbf{a}_1, \cdots, \mathbf{a}_t \in R^n$ are linearly dependent if and only if there is an index k, with $1 \le k \le s$, such that $\mathbf{a}_1^{(k)}, \cdots, \mathbf{a}_t^{(k)} \in R_k^n$ are linearly dependent.*

Remark 2.3. The following is an equivalent formulation of Lemma 2.2:
"The vectors $\mathbf{a}_1, \cdots, \mathbf{a}_t \in R^n$ are linearly independent if and only if, for all k with $1 \le k \le s$, the vectors $\mathbf{a}_1^{(k)}, \cdots, \mathbf{a}_t^{(k)} \in R_k^n$ are linearly independent."

Definition 2.4. *Let $A = (a_{ij})_{m\times l}$ be a matrix over R.*

(i) If the rows of A are linearly independent, then we say that A is a full-row-rank (FRR) *matrix.*

(ii) If there is an $l \times m$ matrix B over R such that $AB = I$, then we say that A is right-invertible *and B is a* right inverse *of A.*

(iii) If $m = l$ and the determinant $\det A$ is a unit of R, then we say that A is non-singular.

(iv) If, for every t with $1 \le t \le m$, any $t\times t$ submatrix of the first (resp., last) t rows of A is non-singular, then we say that A is non-singular by columns *(resp.,* reversely non-singular by columns*).*

Remark 2.5. (i) It is obvious that, if A is a matrix over R of size $m \times l$, and P, Q are invertible matrices over R of size $l \times l$ and $m \times m$, respectively, then A, AP and QA are all FRR provided one of them is FRR.

(ii) By Remark 2.3, a matrix A over R is FRR if and only if the matrices $A^{(k)}$ over R_k in (2.2), for $k = 1, \cdots, s$, are all FRR.

As in usual linear algebra, the following two types of operations are called elementary row (or column) operations on matrices over R:

- adding a multiple of a row (column) to another row (column),
- multiplying a row (column) by a unit of R.

Lemma 2.6. *Assume that R is a finite local ring and $A = (a_{ij})_{m\times l}$ is a matrix over R. Then A is FRR if and only if $m \le l$ and there is an invertible $l \times l$ matrix P over R such that $AP = (\,I \mid 0\,)_{m\times l}$. In particular, A is FRR if and only if A is right invertible.*

Proof. Note that R has a unique maximal ideal J such that the set difference $R \setminus J$ is just the set of all units of R. Since R is finite, there is an integer $e > 0$ such that $J^e = 0$ but $J^{e-1} \neq 0$ (e is called the *nilpotency index* of J, and we adopt the convention that $e = 1$ if R is a field). Thus we can pick a $\delta \in J^{e-1}$ with $\delta \neq 0$. For any row $(a_{i1}, \cdots, a_{il})$ of A, we claim that

- *There is an entry a_{ij} which is a unit of R.*

For, otherwise, all $a_{i1}, \cdots, a_{il}$ belong to J and hence all $\delta a_{i1}, \cdots, \delta a_{il}$ belong to $J^e = \{0\}$, that is, $\delta \cdot (a_{i1}, \cdots, a_{il}) = \mathbf{0}$, and the row $(a_{i1}, \cdots, a_{il})$ of A is linearly dependent, which contradicts the assumption that A is FRR.

Therefore, in the first row of A, we can find a unit. After some suitable permutation of the columns, we can assume that a_{11} is a unit. With appropriate elementary operations on the columns, we can transform A into an FRR matrix as follows:

$$\begin{pmatrix} 1 & 0 & \cdots & 0 \\ a'_{21} & a'_{22} & \cdots & a'_{2l} \\ \cdots & \cdots & \cdots & \cdots \\ a'_{m1} & a'_{m2} & \cdots & a'_{ml} \end{pmatrix}.$$

Next we assert that

- *Some a'_{2j}, for $2 \leq j \leq l$, is a unit of R.*

Assuming the contrary, then $\delta a'_{21} \cdot (1, 0, \cdots, 0) - \delta(a'_{21}, a'_{22}, \cdots, a'_{2l}) = \mathbf{0}$, which contradicts the assumption that the above matrix is FRR.

One can continue with elementary operations on the columns in the same manner, until the desired form $(\, I \mid 0 \,)$ is obtained. □

Now we return to the general case where R may be not local, and we identify R with the direct sum $R_1 \oplus \cdots \oplus R_s$ of local Frobenius rings R_k, $k = 1, \cdots, s$, by the isomorphism (2.1). Then we obtain the following:

Corollary 2.7. *$A \in \mathrm{M}_{m \times l}(R)$ is FRR if and only if A is right-invertible.*

Proof. By Remark 2.5(ii), the matrix A over R is FRR if and only if every $A^{(k)}$ over R_k, for $k = 1, \cdots, s$, is FRR (see (2.2)). Further, by Lemma 2.6, for $k = 1, \cdots, s$, every $A^{(k)} \in \mathrm{M}_{m \times l}(R_k)$, is FRR if and only if there is $B^{(k)} \in \mathrm{M}_{l \times m}(R_k)$ such that $A^{(k)} B^{(k)} = I$. Setting $B = \left(B^{(1)}, \cdots, B^{(s)}\right) \in \mathrm{M}_{l \times m}(R)$, we obtain $AB = I$. □

The following corollary follows from a typical linear algebra argument.

Corollary 2.8. *Let A be in $\mathrm{M}_{m \times m}(R)$. The following statements are equivalent:*

(i) A is invertible.

(ii) A is non-singular.

(iii) A is FRR.

Proposition 2.9. *Let $A \in \mathrm{M}_{m \times l}(R)$ be FRR and let $X = (x_1, \cdots, x_l)^T$, where x_i's are variables. Then the set of solutions of the linear equation system $AX = \mathbf{0}$ is a free submodule in R^l of rank $l - m$ and we have an FRR $(l - m) \times l$ matrix G over R whose rows form a basis of this free submodule.*

Proof. First, assume that R is local. By Lemma 2.6, we have an invertible matrix P of size $l \times l$ such that $AP = (\, I \mid 0 \,)_{m \times l}$. The set of solutions of the linear equation system $(AP)Y = \mathbf{0}$ in variables $Y = (y_1, \cdots, y_l)^T$ is clearly a free submodule of R^l of rank $l - m$ with the rows of the matrix $(\, 0 \mid I \,)_{(l-m) \times l}$ as a basis. Rewriting $AX = \mathbf{0}$ as $(AP)(P^{-1}X) = \mathbf{0}$, we see that the set of solutions of $AX = \mathbf{0}$ is a free submodule of R^l of rank $l - m$ with the rows of the matrix $G = (\, 0 \mid I \,)_{(l-m) \times l} P^T$ as a basis.

Returning to the general case where R is a commutative Frobenius ring, we have the identification in (2.1). For each index $1 \leq k \leq s$, we have a linear equation system $A^{(k)} X^{(k)} = \mathbf{0}$ with the matrix $A^{(k)}$ over the local ring R_k being FRR (see Lemma 2.2), so we have an FRR matrix $G^{(k)}$ over R_k of size

$(l-m)\times l$ such that the rows of $G^{(k)}$ form a basis of the free submodule of R_k^l of the solutions of the system $A^{(k)}X^{(k)}=\mathbf{0}$. With the identification (2.2), we can construct a matrix $G=\left(G^{(1)},\cdots,G^{(s)}\right)$ over R of size $(l-m)\times l$ which is FRR too, and any vector $\mathbf{a}\in R^l$ is a solution of the system $AX=\mathbf{0}$ if and only if $\mathbf{a}$ is a combination of the rows of G. In other words, the set of solutions of the system $AX=\mathbf{0}$ is a free submodule of R^l of rank $l-m$ with the rows of G as a basis. □

Remark 2.10. With A, G as in Proposition 2.9, denote by L_G and L_A the free submodules of R^l generated by the rows of G and A, respectively. With the usual Euclidean inner product $\langle -,-\rangle$ on R^l, Proposition 2.9 says that $(L_A)^\perp = L_G$. As a consequence, we see that

- *If R is a finite commutative Frobenius ring, then a submodule V of R^l is free if and only if its orthogonal submodule $V^\perp$ is free.*

The "only if" part is just Proposition 2.9. For the "if" part, taking a generator matrix A of $V^\perp$ (i.e., A is FRR and $V^\perp = L_A$), since R is a Frobenius ring, we have that $V=(V^\perp)^\perp=(L_A)^\perp=L_G$ is free.

Proposition 2.11. *Any FRR $m\times l$ matrix A over R can be, by appending rows, extended to an invertible $l\times l$ matrix $\tilde{A}=\left(\frac{A}{A'}\right)$ (equivalently, any set of linearly independent vectors of R^l can be extended to a basis of R^l). Furthermore, for any such extension $\tilde{A}=\left(\frac{A}{A'}\right)$, partitioning $\tilde{A}^{-1}=(B\,|\,B')$ into an $l\times m$ submatrix B and an $l\times(l-m)$ submatrix B', we have that B is a right inverse of A and B'^T is a generator matrix of the submodule of solutions of the linear equation system $AX=\mathbf{0}$.*

Proof. By Lemma 2.6, we have a right inverse B of A, and we denote by $B_1,\cdots,B_m$ the columns of B. By Proposition 2.9, we have an $(l-m)\times l$ matrix G whose rows form a basis of the free submodule of solutions of the linear equation system $AX=\mathbf{0}$, and we denote by $G_1^T,\cdots,G_{l-m}^T$ the columns of G^T. Then we form an $l\times l$ matrix $\tilde{B}=(B\,|\,G^T)$. Suppose $d_1,\cdots,d_m,e_1,\cdots,e_{l-m}\in R$ such that

$$d_1B_1+\cdots+d_mB_m+e_1G_1^T+\cdots+e_{l-m}G_{l-m}^T=\mathbf{0}. \tag{2.3}$$

Then, since G_i^T's are solutions of $AX=\mathbf{0}$, we have

$$\mathbf{0}=d_1AB_1+\cdots+d_mAB_m+e_1AG_1^T+\cdots+e_{l-m}AG_{l-m}^T=d_1AB_1+\cdots+d_mAB_m.$$

However, since $AB=I$, we get that $d_1=\cdots=d_m=0$. Returning to (2.3), we have that $e_1G_1^T+\cdots+e_{l-m}G_{l-m}^T=\mathbf{0}$, hence $e_1=\cdots=e_{l-m}=0$ since G is FRR. Thus, $\tilde{B}$ is a square matrix with linearly independent columns and it is hence invertible. Expressing $\tilde{B}^{-1}$ as $\tilde{B}^{-1}=\left(\frac{A''}{A'}\right)$, where A'' and A' are formed by the first m and the last $l-m$ rows, respectively, of $\tilde{B}^{-1}$, we can rewrite $\tilde{B}^{-1}\tilde{B}=I$ as

$$\left(\frac{A''}{A'}\right)\cdot(B\,|\,G^T)=\begin{pmatrix}A''B & A''G^T\\ A'B & A'G^T\end{pmatrix}=\begin{pmatrix}I & 0\\ 0 & I\end{pmatrix}.$$

In particular, $A'\cdot(B\,|\,G^T)=(0\,|\,I)$. On the other hand, it follows from our choices of B and G that $A\cdot(B\,|\,G^T)=(I\,|\,0)$. Therefore,

$$\left(\frac{A}{A'}\right)\cdot(B\,|\,G^T)=\begin{pmatrix}AB & AG^T\\ A'B & A'G^T\end{pmatrix}=\begin{pmatrix}I & 0\\ 0 & I\end{pmatrix}. \tag{2.4}$$

Thus $\left(\frac{A}{A'}\right)$ is right invertible, which, by Corollary 2.8, means that it is invertible and $(B\,|\,G^T)$ is an inverse of it.

Similar to the equality (2.4), for any $(l-m)\times l$ matrix A', $l\times m$ matrix B and $l\times(l-m)$ matrix B', the equality $\left(\frac{A}{A'}\right)\cdot(B\,|\,B')=\begin{pmatrix}I & 0\\ 0 & I\end{pmatrix}$ implies that $AB=I$ and $AB'=0$. □

3 Matrix Product Codes over Frobenius Rings

Starting from this section till the end of this paper, we assume that R is always a finite commutative Frobenius ring, with decomposition into a direct product of finite local commutative Frobenius rings $R_1, \ldots, R_s$ as in (2.1).

Any non-empty subset C of R^n is called a code over R of length n and any vector in C is called a codeword. Let M denote the cardinality of C, i.e., $M = |C|$. Then C is said to be an (n, M) code over R. If C is an R-submodule of R^n, then C is called a linear code. With respect to the usual Euclidean inner product, we have the dual code $C^\perp$ which is always linear. When $C \subseteq C^\perp$ (resp., $C = C^\perp$), we say that C is self-orthogonal (resp., self-dual). If C is linear, then $(C^\perp)^\perp = C$ and $|C| \cdot |C^\perp| = |R|^n$, as we have noted in Section 2.

Let $A = (a_{ij})_{m\times l} \in \mathrm{M}_{m\times l}(R)$. For any index $1 \le k \le m$, we denote by $U_A(k)$ the linear code over R of length l generated by the ith rows of A, for $i = 1, 2, \cdots, k$, and denote by $L_A(k)$ the linear code over R of length l generated by the ith rows of A, for $i = k, k+1, \cdots, m$. In particular, $U_A(m) = L_A(1)$ is the linear code over R of length l generated by all the rows of A. Thus, the set of solutions of the linear equation system $AX = \mathbf{0}$ is just the dual code $L_A(1)^\perp$ of the code $L_A(1)$. If A is FRR, then $L_A(1)$ is a free submodule of R^l of rank m, while its dual $L_A(1)^\perp$ is a free submodule of R^l of rank $l - m$, and the matrix G in Proposition 2.9 is a generator matrix of $L_A(1)^\perp$, i.e., $L_A(1)^\perp = L_G(1)$. For convenience, we also define $U_A(0)$ and $L_A(m+1)$ to be the zero code.

Any $n \times m$ matrix can be viewed as a word over R of length nm, so any non-empty subset D of $\mathrm{M}_{n\times m}(R)$ can be viewed as a code over R of length nm. From this point of view, for any two words $\mathbf{w}, \mathbf{v} \in \mathrm{M}_{n\times m}(R)$, the Euclidean inner product can be computed as follows

$$\langle \mathbf{w}, \mathbf{v} \rangle = \mathrm{tr}(\mathbf{w}\mathbf{v}^T), \tag{3.1}$$

where $\mathrm{tr}(\mathbf{w}\mathbf{v}^T)$ denotes the trace of the $n \times n$ matrix $\mathbf{w}\mathbf{v}^T$. For: writing $\mathbf{w} = (w_{ij})_{n\times m}$, $\mathbf{v} = (v_{ij})_{n\times m}$, then $\mathrm{tr}(\mathbf{w}\mathbf{v}^T) = \sum_{i=1}^{n}\sum_{j=1}^{m} w_{ij}v_{ij}$, which is just the Euclidean inner product of $\mathbf{w}$ and $\mathbf{v}$. Note that (3.1) holds for any matrix size, including the usual words written in the form of row or column vectors.

Let A be an FRR $m \times l$ matrix over R, then the map

$$\mathrm{M}_{n\times m}(R) \longrightarrow \mathrm{M}_{n\times l}(R), \quad \mathbf{v} \longmapsto \mathbf{v}A$$

is an injective linear map, for: A has a right inverse B, so that, if $\mathbf{d}A = \mathbf{d}'A$, then $\mathbf{d} = \mathbf{d}I = \mathbf{d}AB = \mathbf{d}'AB = \mathbf{d}'$. Therefore, if the subset D of $\mathrm{M}_{n\times m}(R)$ is an (nm, M) code over R, then $DA = \{\mathbf{d}A \mid \mathbf{d} \in D\}$ is an (nl, M) code over R, and DA is linear if and only if D is linear.

Let C_j be an (n, M_j) code over R, for $j = 1, \cdots, m$. For $\mathbf{c}_1 \in C_1$, $\cdots$, $\mathbf{c}_m \in C_m$, we have an $n \times m$ matrix $(\mathbf{c}_1, \cdots, \mathbf{c}_m)$, where each $\mathbf{c}_j$ is written as a column vector. Hence, we have a subset of $\mathrm{M}_{n\times m}(R)$ as follows:

$$D = [C_1, \cdots, C_m] = \{(\mathbf{c}_1, \cdots, \mathbf{c}_m) \mid \mathbf{c}_1 \in C_1, \cdots, \mathbf{c}_m \in C_m\}.$$

Obviously, $[C_1, \cdots, C_m]$ is an $\left(nm, \prod_{j=1}^{m} M_j\right)$ code over R, and the code $[C_1, \cdots, C_m]$ is linear if and only if all $C_1, \cdots, C_m$ are linear.

Let A be an FRR $m \times l$ matrix over R. We have an $\left(nl, \prod_{j=1}^{m} M_j\right)$ code over R, called a *matrix product code* over R (see [1]), as follows:

$$[C_1, \cdots, C_m]A = \{(\mathbf{c}_1, \cdots, \mathbf{c}_m)A \mid \mathbf{c}_1 \in C_1, \cdots, \mathbf{c}_m \in C_m\}, \tag{3.2}$$

which is linear if all $C_1, \cdots, C_m$ are linear.

It is easy to check that $[C_1, \cdots, C_m]A = [C_1, \cdots, C_m]$ if $C_1, \cdots, C_m$ are all linear, A is square, and one of the following holds:

- A is a diagonal matrix,
- $C_1 \supseteq C_2 \supseteq \cdots \supseteq C_m$ and A is a lower triangular matrix,
- $C_1 = C_2 = \cdots = C_m$.

Any weight w on R can be extended to a weight on R^n in the obvious way, hence the distance d_w on R^n with respect to the weight w is defined by $d_w(\mathbf{c},\mathbf{c}') = w(\mathbf{c}-\mathbf{c}')$ for $\mathbf{c},\mathbf{c}' \in R^n$. The minimum distance of any code C with respect to the weight w, denoted by $d_w(C)$, is defined to be the minimum distance with respect to the weight w between any two distinct codewords in C; and we adopt the convention that $d_w(0) = n+1$ for the zero code $0 = \{\mathbf{0}\} \subseteq R^n$. In particular, we denote the Hamming weight by w_H and the Hamming distance by d_H, hence $d_H(C)$ denotes the minimum Hamming distance of C.

The following is a generalization of the main result of [14] to matrix product codes over finite Frobenius rings.

Theorem 3.1. *Let C_j be an (n, M_j) code over R, for $j = 1, \cdots, m$, and let $A = (a_{ij})_{m\times l}$ be an FRR matrix over R. Let w be a weight on R. Then $C = [C_1, \cdots, C_m]A$ is an $\left(nl, \prod_{j=1}^m M_j\right)$ code over R with minimum distance $d_w(C)$ satisfying*

$$d_w(C) \geq \min\left\{d_H(C_k)d_w\big(U_A(k)\big) \mid k = 1, \cdots, m\right\}, \tag{3.3U}$$

$$d_w(C) \geq \min\left\{d_H(C_k)d_w\big(L_A(k)\big) \mid k = 1, \cdots, m\right\}. \tag{3.3L}$$

Proof. Since A is FRR, by (3.2) we have that C is an $\left(nl, \prod_{j=1}^m M_j\right)$ code over R.

For any two distinct codewords $\mathbf{c} = (\mathbf{c}_1, \cdots, \mathbf{c}_m)A$, $\mathbf{c}' = (\mathbf{c}'_1, \cdots, \mathbf{c}'_m)A$ of C, let $\mathbf{c}_j - \mathbf{c}'_j = \mathbf{b}_j$, for $j = 1, \cdots, m$. Then $\mathbf{c} - \mathbf{c}' = (\mathbf{b}_1, \cdots, \mathbf{b}_m)A$ and $d_w(\mathbf{c},\mathbf{c}') = w(\mathbf{c}-\mathbf{c}') = w\big((\mathbf{b}_1, \cdots, \mathbf{b}_m)A\big)$. Note that there is an index k such that $\mathbf{b}_j = \mathbf{0}$ for all $j < k$ but $\mathbf{b}_k \neq \mathbf{0}$. Let A_i denote the ith row of A. Then the word $\mathbf{c} - \mathbf{c}'$ which is an $n \times l$ matrix over R is as follows:

$$\mathbf{c} - \mathbf{c}' = (\mathbf{0}, \cdots, \mathbf{0}, \mathbf{b}_k, \cdots, \mathbf{b}_m)A = (\mathbf{b}_k, \cdots, \mathbf{b}_m)\begin{pmatrix} A_k \\ \vdots \\ A_m \end{pmatrix},$$

where $\mathbf{b}_k = (b_{1k}, \cdots, b_{ik}, \cdots, b_{nk})^T$ with $b_{ik} \in R$. For each non-zero b_{ik}, we get the ith row of the matrix $\mathbf{c} - \mathbf{c}'$ as follows:

$$b_{ik}A_k + b_{i,k+1}A_{k+1} + \cdots + b_{im}A_m,$$

which is a non-zero codeword of the code $L_A(k)$. Therefore, the contribution to $d_w(\mathbf{c},\mathbf{c}')$ of the ith row of $\mathbf{c} - \mathbf{c}'$ is $w(b_{ik}A_k + b_{i,k+1}A_{k+1} + \cdots + b_{im}A_m) \geq d_w(L_A(k))$. Since $w_H(\mathbf{b}_k) = d_H(\mathbf{c}_k, \mathbf{c}'_k)$, the number of non-zero b_{ik} is at least $d_H(C_k)$. In conclusion, $d_w(\mathbf{c},\mathbf{c}') \geq d_H(C_k)d_w(L_A(k))$. Thus the inequality (3.3L) holds.

Similarly, for $\mathbf{c},\mathbf{c}'$ above, there is an index k' such that $\mathbf{b}_j = \mathbf{0}$ for all $j > k'$ but $\mathbf{b}_{k'} \neq \mathbf{0}$, so we can write $\mathbf{c} - \mathbf{c}'$ as follows:

$$\mathbf{c} - \mathbf{c}' = (\mathbf{b}_1, \cdots, \mathbf{b}_{k'}, \mathbf{0}, \cdots, \mathbf{0})A = (\mathbf{b}_1, \cdots, \mathbf{b}_{k'})\begin{pmatrix} A_1 \\ \vdots \\ A_{k'} \end{pmatrix},$$

and obtain that $d_w(\mathbf{c},\mathbf{c}') \geq d_H(C_{k'})d_w(U_A(k'))$. We are done for the inequality (3.3U). □

Remark 3.2. (i) Though, in the above proof, it is stated: "there is an index k such that ...", in fact any index k can appear when $\mathbf{c},\mathbf{c}'$ run over the choices of two distinct codewords of C, since we can choose $\mathbf{c}_j = \mathbf{c}'_j$, for $j \neq k$, and $\mathbf{c}_k \neq \mathbf{c}'_k$.

(ii) In general, the right hand sides of (3.3U) and (3.3L) are not strict lower bounds of the minimum distance (see Section 5).

(iii) The two lower bounds in (3.3U) and (3.3L) cannot be directly compared in general: sometimes (3.3U) is better than (3.3L), while some other times the opposite is true.

The following result describes the dual of a matrix product code constructed with an FRR matrix. It may be regarded as a generalization of [1, Theorem 6.6] and [16, Proposition 3], but here we do not require the matrix to be square.

Theorem 3.3. *Let $C_1, \cdots, C_m$ be codes over R of length n, and let $A \in \mathrm{M}_{m\times l}(R)$ be FRR. Assume that $B \in \mathrm{M}_{l\times m}(R)$ is a right inverse of A and $G \in \mathrm{M}_{(l-m)\times l}(R)$ is a generator matrix of the dual code $L_A(1)^\perp$ of $L_A(1)$. Set $\tilde{B} = \left(B \,|\, G^T\right)$. Then the dual code of $C = [C_1, \cdots, C_m]A$ is*

$$C^\perp = [\, C_1^\perp, \cdots, C_m^\perp, \underbrace{R^n, \cdots, R^n}_{l-m}]\tilde{B}^T = [C_1^\perp, \cdots, C_m^\perp]B^T + \mathrm{M}_{n\times(l-m)}(R)G. \tag{3.4}$$

Proof. We denote by $\hat{C}_j$ the linear code generated by the vectors in C_j, and by $\hat{C}$ the linear code generated by the vectors in C. It is then easy to check that $C_j^\perp = \hat{C}_j^\perp$, $\hat{C} = [\hat{C}_1, \cdots, \hat{C}_m]A$, and $C^\perp = \hat{C}^\perp$. Thus, without loss of generality, in the following we assume that $C_1, \cdots, C_m$ are all linear codes.

In the equality (2.4) within the proof of Proposition 2.11, we have seen that $\tilde{B} = \left(B \,|\, G^T\right)$ is an invertible $l \times l$ matrix such that A is the $m \times l$ submatrix of $\tilde{A} = \tilde{B}^{-1}$ formed by the first m rows of $\tilde{A}$, i.e., $\tilde{A} = \tilde{B}^{-1}$ is partitioned as $\tilde{A} = \left(\frac{A}{A'}\right)$. It is obvious that

$$C = [C_1, \cdots, C_m]A = [C_1, \cdots, C_m, \underbrace{0, \cdots, 0}_{l-m}]\tilde{A}. \tag{3.5}$$

Now we show that

$$[C_1^\perp, \cdots, C_m^\perp, \underbrace{R^n, \cdots, R^n}_{l-m}]\tilde{B}^T \ \subseteq \ C^\perp. \tag{3.6}$$

Let $\mathbf{c} = (\mathbf{c}_1, \cdots, \mathbf{c}_m, \mathbf{0}, \cdots, \mathbf{0})\tilde{A} \in C$ with $\mathbf{c}_j \in C_j$, and let $\mathbf{d} = (\mathbf{d}_1, \cdots, \mathbf{d}_m, \mathbf{w}_{m+1}, \cdots, \mathbf{w}_l)\tilde{B}^T$ with $\mathbf{d}_j \in C_j^\perp$ $(1 \le j \le m)$ and $\mathbf{w}_j \in R^n$ $(m+1 \le j \le l)$. By (3.1), we have

$$\begin{aligned}
\langle \mathbf{c}, \mathbf{d} \rangle &= \mathrm{tr}\left((\mathbf{c}_1, \cdots, \mathbf{c}_m, \mathbf{0}, \cdots, \mathbf{0})\tilde{A} \cdot \left((\mathbf{d}_1, \cdots, \mathbf{d}_m, \mathbf{w}_{m+1}, \cdots, \mathbf{w}_l)\tilde{B}^T\right)^T\right) \\
&= \mathrm{tr}\left((\mathbf{c}_1, \cdots, \mathbf{c}_m, \mathbf{0}, \cdots, \mathbf{0})\tilde{A}\tilde{B} \begin{pmatrix} \mathbf{d}_1^T \\ \vdots \\ \mathbf{d}_m^T \\ \mathbf{w}_{m+1}^T \\ \vdots \\ \mathbf{w}_l^T \end{pmatrix}\right).
\end{aligned}$$

Since $\tilde{A}\tilde{B} = I$ is the identity matrix, we obtain

$$\langle \mathbf{c}, \mathbf{d} \rangle = \mathrm{tr}\left((\mathbf{c}_1, \cdots, \mathbf{c}_m) \begin{pmatrix} \mathbf{d}_1^T \\ \vdots \\ \mathbf{d}_m^T \end{pmatrix}\right).$$

By the linearity of trace, we have

$$\langle \mathbf{c}, \mathbf{d} \rangle = \mathrm{tr}\left(\mathbf{c}_1\mathbf{d}_1^T + \cdots + \mathbf{c}_m\mathbf{d}_m^T\right) = \mathrm{tr}\left(\mathbf{c}_1\mathbf{d}_1^T\right) + \cdots + \mathrm{tr}\left(\mathbf{c}_m\mathbf{d}_m^T\right).$$

By (3.1) again, we obtain

$$\langle \mathbf{c}, \mathbf{d} \rangle = \langle \mathbf{c}_1, \mathbf{d}_1 \rangle + \cdots + \langle \mathbf{c}_m, \mathbf{d}_m \rangle = 0.$$

Thus (3.6) is proved.

Since R is a Frobenius ring, $|C_j^\perp| = \frac{|R|^n}{|C_j|}$, for $j = 1, \cdots, m$, and $|C^\perp| = \frac{|R|^{nl}}{|C|}$. It follows from (3.2) that

$$\begin{aligned}
\left|[C_1^\perp, \cdots, C_m^\perp, \underbrace{R^n, \cdots, R^n}_{l-m}]\tilde{B}^T\right| &= |C_1^\perp| \cdots |C_m^\perp| \cdot \underbrace{|R^n| \cdots |R^n|}_{l-m} \\
&= \frac{|R|^n}{|C_1|} \cdots \frac{|R|^n}{|C_m|} \cdot |R|^{n(l-m)} = \frac{|R|^{nl}}{|C|} = |C^\perp|.
\end{aligned}$$

Therefore, the equality in (3.6) must hold. In other words, we obtain

$$C^\perp = [\, C_1^\perp, \cdots, C_m^\perp, \underbrace{R^n, \cdots, R^n}_{l-m}]\tilde{B}^T,$$

which is the first equality in (3.4).

Further, since $\tilde{B}^T$ has the partitioned form $\tilde{B}^T = \begin{pmatrix} B^T \\ \hline G \end{pmatrix}$,

$$\begin{aligned} [C_1^\perp, \cdots, C_m^\perp, \underbrace{R^n, \cdots, R^n}_{l-m}]\tilde{B}^T &= [C_1^\perp, \cdots, C_m^\perp]B^T + [\underbrace{R^n, \cdots, R^n}_{l-m}]G \\ &= [C_1^\perp, \cdots, C_m^\perp]B^T + \mathrm{M}_{n\times(l-m)}(R)G, \end{aligned}$$

i.e., the second equality in (3.4) holds. □

Remark 3.4. By Proposition 2.11, the conclusion of Theorem 3.3 can be rewritten as follows: for any $l \times l$ matrix $\tilde{A} = \begin{pmatrix} A \\ \hline A' \end{pmatrix}$ and $\tilde{A}^{-1} = \begin{pmatrix} B \,|\, B' \end{pmatrix}$, we have that

$$C^\perp = [\, C_1^\perp, \cdots, C_m^\perp, \underbrace{R^n, \cdots, R^n}_{l-m}](\tilde{A}^{-1})^T = [C_1^\perp, \cdots, C_m^\perp]B^T + \mathrm{M}_{n\times(l-m)}(R)B'^T.$$

An $m \times l$ matrix A over R, where $m \le l$, is said to be *quasi-orthogonal* if AA^T is a diagonal square matrix where all the diagonal entries are units of R. For example, the matrix $\begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}$ is quasi-orthogonal if the characteristic of R is 2, while the matrix $\begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ is quasi-orthogonal if the characteristic of R is 3.

Theorem 3.5. *Let $C_1, \cdots, C_m$ be self-orthogonal linear codes over R of length n, let A be a quasi-orthogonal $m \times l$ matrix over R and let G be a generator matrix of the dual code $L_A(1)^\perp$ of $L_A(1)$. Then the dual code of $C = [C_1, \cdots, C_m]A$ is $C^\perp = [C_1^\perp, \cdots, C_m^\perp]A + \mathrm{M}_{n\times(l-m)}(R)G$. In particular, C is a self-orthogonal code.*

Proof. Assume that $AA^T = D = \begin{pmatrix} u_1 & & \\ & \ddots & \\ & & u_m \end{pmatrix}$, with u_i being units of R. Then $A^T D^{-1}$ is a right inverse of A. By the equality (2.4) in the proof of Proposition 2.11, the matrix $\begin{pmatrix} A^T D^{-1} | G^T \end{pmatrix}$ is invertible, hence $\begin{pmatrix} A^T | G^T \end{pmatrix} = \begin{pmatrix} A^T D^{-1} | G^T \end{pmatrix} \begin{pmatrix} D & \\ & I \end{pmatrix}$ is invertible. Thus, $\begin{pmatrix} A \\ \hline G \end{pmatrix} = \begin{pmatrix} A^T | G^T \end{pmatrix}^T$ and the product

$$\begin{pmatrix} A \\ \hline G \end{pmatrix} \begin{pmatrix} A^T | G^T \end{pmatrix} = \begin{pmatrix} D & \\ & GG^T \end{pmatrix} \tag{3.7}$$

are invertible; hence GG^T is an invertible $(l-m) \times (l-m)$ matrix, and $\begin{pmatrix} A^T | G^T \end{pmatrix} \begin{pmatrix} D^{-1} & \\ & (GG^T)^{-1} \end{pmatrix}$ is the inverse of $\begin{pmatrix} A \\ \hline G \end{pmatrix}$. Note that

$$\left(\begin{pmatrix} A^T | G^T \end{pmatrix} \begin{pmatrix} D^{-1} & \\ & (GG^T)^{-1} \end{pmatrix} \right)^T = \begin{pmatrix} D^{-1} & \\ & (GG^T)^{-1} \end{pmatrix} \begin{pmatrix} A \\ \hline G \end{pmatrix},$$

and that $[R^n, \cdots, R^n](GG^T)^{-1} = [R^n, \cdots, R^n]$. By Theorem 3.3, the dual code $C^\perp$ is as follows:

$$C^\perp = [C_1^\perp, \cdots, C_m^\perp, R^n, \cdots, R^n] \cdot \begin{pmatrix} D^{-1} & \\ & (GG^T)^{-1} \end{pmatrix} \begin{pmatrix} A \\ \hline G \end{pmatrix}.$$

Since $D^{-1} = \begin{pmatrix} u_1^{-1} & & \\ & \ddots & \\ & & u_m^{-1} \end{pmatrix}$ and clearly $u_j^{-1}C_j^\perp = C_j^\perp$, for $j = 1, \cdots, m$, we have

$$\begin{array}{rl} & [C_1^\perp, \cdots, C_m^\perp, R^n, \cdots, R^n] \cdot \begin{pmatrix} D^{-1} & \\ & (GG^T)^{-1} \end{pmatrix} \\ = & [u_1^{-1}C_1^\perp, \cdots, u_m^{-1}C_m^\perp, R^n, \cdots, R^n] \\ = & [C_1^\perp, \cdots, C_m^\perp, R^n, \cdots, R^n], \end{array}$$

so

$$\begin{array}{rcl} C^\perp & = & [C_1^\perp, \cdots, C_m^\perp, R^n, \cdots, R^n] \cdot \begin{pmatrix} A \\ G \end{pmatrix} \\ & = & [C_1^\perp, \cdots, C_m^\perp]A + \mathrm{M}_{n\times(l-m)}(R)G \\ & \supseteq & [C_1^\perp, \cdots, C_m^\perp]A \supseteq [C_1, \cdots, C_m]A = C. \end{array}$$

The proof is now complete. □

The following corollary follows immediately from Theorem 3.5:

Corollary 3.6. *Let $C_1, \cdots, C_m$ be self-dual linear codes over R of length n and let A be a quasi-orthogonal $m \times m$ matrix over R. Then $C = [C_1, \cdots, C_m]A$ is a self-dual code.*

4 Strongly Full-Row-Rank Matrices

Let C be a non-zero code over R of length n and set $M = |C|$ to be the cardinality of C. If $d_H(C) = 1$, then $M \leq |R|^{n-d_H(C)+1}$. In particular, we have $M \leq |R|^{n-d_H(C)+1}$ when $n = 1$. If $n > 1$ and $d_H(C) > 1$, by puncturing at the last coordinate, we get an $(n-1, M, \geq d-1)$ code C', where $d = d_H(C)$, and by induction, we obtain that $M \leq |R|^{(n-1)-(d-1)+1} = |R|^{n-d+1}$. By this well-known argument (e.g., see [12]), we have the following *Singleton bound* for codes over the Frobenius ring R:

$$d_H(C) \leq n - \log_{|R|} |C| + 1. \tag{4.1}$$

If a code C over R of length n attains the Singleton bound, i.e., the equality holds in (4.1), then we say that C is a *maximum distance separable* code over R, or an *MDS* code over R for short. Note, in particular, that $C = R^n$ is an MDS code. We also adopt the convention that the zero code is an MDS code (this is consistent with the convention that $d_H(0) = n + 1$).

Note that, if C is a free code over R of length l, then (4.1) becomes

$$d_H(C) \leq l - \mathrm{rank}(C) + 1,$$

and C is MDS if and only if, for any non-zero codeword $\mathbf{c} \in C$, we have $w_H(\mathbf{c}) > l - \mathrm{rank}(C)$. Moreover, a free code of length l and rank m, which we shall also call an $[l, m]$ code (over R), has FRR generator matrices of size $m \times l$.

The following result is well known for codes over finite fields (see, for example, [15, Theorems 5.3.2 and 5.3.3]).

Lemma 4.1. *Let $A \in \mathrm{M}_{m\times l}(R)$ be FRR and let $C = U_A(m)$ (i.e., C is the free code over R of length l generated by the rows of A). Then the following statements are equivalent:*

(i) C is an $[l, m]$ MDS code.

(ii) Any $m \times m$ submatrix of A is non-singular.

(iii) The dual code $C^\perp$ of C is an $[l, l-m]$ MDS code.

The proof of Lemma 4.1 is similar to that of [15, Theorems 5.3.2 and 5.3.3]. The analogous ingredients needed for our setting (over a finite commutative Frobenius ring) are found in Proposition 2.9 and Corollary 2.8.

Remark 4.2. (i) Note that there is another statement

- *"Any $(l-m)\times(l-m)$ submatrix of a check matrix of C is non-singular"*

which is equivalent to any of the three statements in Lemma 4.1, but it is already indirectly covered by Lemma 4.1.

(ii) If $C = R^l$, then A is invertible and $C^\perp = 0$. In this case, we adopt the convention that the zero code is an MDS code with zero as a generator matrix. Recall that we have also adopted the convention that $L_Q(l+1) = 0$, for any $l \times l$ matrix Q.

In view of Lemma 4.1, we introduce the following terminologies.

Definition 4.3. *Let A be an FRR $m \times l$ matrix over R.*

(i) If $U_A(m) = L_A(1)$ is an $[l, m]$ MDS code, then we say that A is a strongly full-row-rank (SFRR) matrix.

*(ii) For $t \geq 2$, if there is a sequence of indices $0 = i_0 < i_1 < \cdots < i_t = m$ such that $U_A(i_h)$, for $h = 0, 1, \cdots, t$, are MDS codes, then we say that A is an $(i_1, \cdots, i_{t-1})$-*SFRR matrix. *(When $t = 1$, A is just an SFRR matrix.)*

(iii) For $t \geq 2$, if there is a sequence of indices $1 = i_0 < i_1 < \cdots < i_{t-1} < i_t = m+1$ such that $L_A(i_h)$, for $h = 0, 1, \cdots, t$, are MDS codes, then we say that A is a reversely $(i_1, \cdots, i_{t-1})$-SFRR matrix. *(When $t = 1$, A is just an SFRR matrix.)*

Proposition 4.4. *Let $A \in \mathrm{M}_{m\times l}(R)$ be FRR and let $0 = i_0 < i_1 < \cdots < i_t = m$. Assume that $\tilde{A} \in \mathrm{M}_{l\times l}(R)$ is an invertible matrix with A as the submatrix consisting of its first m rows. Then A is an $(i_1, \cdots, i_{t-1})$-SFRR matrix if and only if $(\tilde{A}^{-1})^T$ is a reversely $(i_1+1, \cdots, i_{t-1}+1, m+1)$-SFRR matrix (or, if $m = l$, a reversely $(i_1+1, \cdots, i_{t-1}+1)$-SFRR matrix).*

Proof. Since $(\tilde{A}^{-1})^T$ is invertible, $L_{(\tilde{A}^{-1})^T}(1) = R^l$. Hence, $U_A(0) = 0$, $L_{(\tilde{A}^{-1})^T}(1)$ and $L_{(\tilde{A}^{-1})^T}(l+1) = 0$ are all MDS codes.

Let $k = i_h$ with $1 \leq h \leq t$. It is enough to show that $U_A(k) = U_{\tilde{A}}(k)$ is an MDS code if and only if $L_{(\tilde{A}^{-1})^T}(k+1)$ is an MDS code.

According to Proposition 2.11, we write $\tilde{A} = \left(\frac{A'}{A''}\right)$, where A' is the submatrix consisting of the first k rows of A, and write $\tilde{A}^{-1} = (B' \,|\, B'')$ correspondingly; then $U_A(k) = U_{A'}(k)$ and $U_{A'}(k)^\perp = L_{B''^T}(1) = L_{(\tilde{A}^{-1})^T}(k+1)$. Therefore, the proposition follows from Lemma 4.1 at once. □

Recall that a matrix $A = (a_{ij})_{m\times l}$ over R is said to be *non-singular by columns* if, for every t with $1 \leq t \leq m$, any $t \times t$ submatrix of the first t rows of A is non-singular.

From Lemma 4.1 and Proposition 4.4, we have the following obvious consequence which is a generalization of [1, Proposition 7.2 and Theorem 6.6(i)].

Corollary 4.5. *Let $A \in \mathrm{M}_{m\times l}(R)$ be FRR. Assume that $\tilde{A} \in \mathrm{M}_{l\times l}(R)$ is an invertible matrix that has A as the submatrix of its first m rows. Then the following statements are equivalent:*

(i) A is non-singular by columns.

(ii) A is a $(1, 2, \cdots, m-1)$-SFRR matrix.

(iii) $(\tilde{A}^{-1})^T$ is a reversely $(2, \cdots, m, m+1)$-SFRR matrix. (When $m = l$, $(\tilde{A}^{-1})^T$ is a reversely $(2, \cdots, m)$-SFRR matrix.)

In particular, when $m = l$, the square matrix A is non-singular by columns if and only if $(A^{-1})^T$ is reversely non-singular by columns.

Example 4.6. Let $T = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$, which is the matrix for the $(a + x|b + x|a + b + x)$-construction. Then T is a (2)-SFRR matrix, but T is not non-singular by columns because $U_T(1)$ is not MDS. We note that T is also a reversely (3)-SFRR matrix.

Observe also that $(T^{-1})^T = \begin{pmatrix} 0 & -1 & 1 \\ -1 & 0 & 1 \\ 1 & 1 & -1 \end{pmatrix}$ is a reversely (3)-SFRR matrix (cf. Proposition 4.4).

The following lower bound is a generalization of the main result of [1], and the condition for the equality is a generalization of [5, Theorem 1] to SFRR matrices over finite Frobenius rings.

Theorem 4.7. *Let $A \in \mathrm{M}_{m\times l}(R)$ be an $(i_1, \cdots, i_{t-1})$-SFRR matrix, where $0 = i_0 < i_1 < \cdots < i_t = m$. Let $C_1, \cdots, C_m$ be codes over R of length n and let $C = [C_1, \cdots, C_m]A$. Then*

$$d_H(C) \geq \min\big\{(l - i_h + 1)d_H(C_{k_h}) \mid h = 1, \cdots, t,\ i_{h-1} < k_h \leq i_h\big\}. \tag{4.2U}$$

Furthermore, if the following three conditions are satisfied:

(E1) *$C_1, \cdots, C_m$ are linear,*

(E2) *$C_1 = \cdots = C_{i_1}$, $C_{i_1+1} = \cdots = C_{i_2}$, $\cdots$, $C_{i_{t-1}+1} = \cdots = C_{i_t} (= C_m)$,*

(E3) *$C_{i_1} \supseteq C_{i_2} \supseteq \cdots \supseteq C_{i_t}$,*

then equality holds in (4.2U)*, i.e.,*

$$d_H(C) = \min\big\{(l - i_h + 1)d_H(C_{i_h}) \mid h = 1, \cdots, t\big\}. \tag{4.3U}$$

Remark 4.8. There is a dual version of Theorem 4.7, which we now state. Let A be a reversely $(i_1, \cdots, i_{t-1})$-SFRR $m \times l$ matrix over R, where $1 = i_0 < i_1 < \cdots < i_{t-1} < i_t = m + 1$. Then the analogue of (4.2U) is:

$$d_H(C) \geq \min\big\{(l - m + i_h)d_H(C_{k_h}) \mid h = 0, 1, \cdots, t - 1,\ i_h \leq k_h < i_{h+1}\big\}. \tag{4.2L}$$

With further conditions (E1*)=(E1) and

(E2*) $(C_1 =)C_{i_0} = \cdots = C_{i_1-1}$, $C_{i_1} = \cdots = C_{i_2-1}$, $\cdots$, $C_{i_{t-1}} = \cdots = C_m$,

(E3*) $C_{i_0} \subseteq C_{i_1} \subseteq \cdots \subseteq C_{i_{t-1}}$,

the analogous version of the equality (4.3U) is:

$$d_H(C) = \min\big\{(l - m + i_h)d_H(C_{i_h}) \mid h = 0, 1, \cdots, t - 1\big\}. \tag{4.3L}$$

The proof for the dual version is the same as that for Theorem 4.7.

Proof of Theorem 4.7. By Theorem 3.1 (3.3U), we have that

$$d_H(C) \geq \min\big\{d_H(U_A(k))d_H(C_k) \mid 1 \leq k \leq m\big\}.$$

If $i_{h-1} < k \leq i_h$, then $U_A(k) \subseteq U_A(i_h)$, so $d_H(U_A(k)) \geq d_H(U_A(i_h)) = l - i_h + 1$. Hence

$$d_H(U_A(k))d_H(C_k) \geq (l - i_h + 1)d_H(C_k), \qquad i_{h-1} < k \leq i_h.$$

The inequality (4.2U) holds.

In order to prove (4.3U), first we show that the following lemma holds.

Lemma 4.9. *Let A be as in Theorem 4.7 and set $m_h = i_h - i_{h-1}$, for $h = 1, \cdots, t$. Then there is a block lower triangular matrix Q:*

$$Q = \begin{pmatrix} Q_1 & & & \\ * & Q_2 & & \\ \vdots & \ddots & \ddots & \\ * & \cdots & * & Q_t \end{pmatrix}, \tag{4.4}$$

with Q_h being an invertible $m_h \times m_h$ matrix for each $h = 1, \cdots, t$, such that QA is a block upper triangular matrix

$$QA = \begin{pmatrix} I_{m_1} & * & \cdots & * & \cdots & * \\ & I_{m_2} & \cdots & * & \cdots & * \\ & & \ddots & \vdots & \vdots & \vdots \\ & & & I_{m_t} & \cdots & * \end{pmatrix}, \tag{4.5}$$

where, for $h = 1, \cdots, t$, the i_hth row of QA takes the form

$$\big(\underbrace{0, \cdots, 0}_{i_h - 1}, \ 1, u_{i_h, i_h+1}, \ \cdots, \ u_{i_h, l}\big) \tag{4.6}$$

with $u_{i_h,j}$ being a unit of R for every $j = i_h + 1, \cdots, l$.

Proof. Write $A = (a_{ij})_{m \times l}$, and consider the top-left $i_1 \times i_1$ submatrix $A_1 = (a_{ij})_{i_1 \times i_1}$. By the assumption on A and Lemma 4.1, the submatrix A_1 is non-singular, hence there is an $m_1 \times m_1$ (recall that $m_1 = i_1$) invertible matrix Q_1 such that $Q_1 A_1 = I_{m_1}$. Setting

$$Q' = \begin{pmatrix} Q_1 & & & \\ & I_{m_2} & & \\ & & \ddots & \\ & & & I_{m_t} \end{pmatrix},$$

it follows that

$$Q'A = \begin{pmatrix} I_{m_1} & * & \cdots & * \\ * & * & \cdots & * \\ \vdots & \vdots & \vdots & \vdots \\ * & * & \cdots & * \end{pmatrix}.$$

By adding suitable multiples of the rows in the first row partition to the rows in the other row partitions, we obtain an invertible matrix

$$Q'' = \begin{pmatrix} Q_1 & & & \\ * & I_{m_2} & & \\ \vdots & & \ddots & \\ * & & & I_{m_t} \end{pmatrix}$$

such that

$$Q''A = \begin{pmatrix} I_{m_1} & * & \cdots & * \\ & * & \cdots & * \\ & \vdots & \vdots & \vdots \\ & * & \cdots & * \end{pmatrix}.$$

Note that, by the properties of determinants and Lemma 4.1, $U_{Q''A}(i_h)$, for $h = 1, \cdots, t$, are still MDS codes. The top-left $i_2 \times i_2$ submatrix of $Q''A$ looks like

$$\left(\begin{array}{c|c} I_{m_1} & * \\ \hline & A_2 \end{array}\right),$$

which should be non-singular, hence A_2 is an invertible $m_2 \times m_2$ matrix, where $m_2 = i_2 - i_1$. Thus we can repeat the above process until Q satisfying conditions (4.4) and (4.5) is found.

Note that the i_hth row of QA in (4.5) has the form of (4.6), except that it remains to show that $u_{i_h,j}$, for all $j \geq i_h + 1$, are units of R. Consider the $i_h \times i_h$ submatrix of QA formed by the first i_h rows and the 1st, 2nd, $\cdots$, $(i_h - 1)$th and the jth columns:

$$\begin{pmatrix} 1 & \cdots & * & * \\ & \ddots & \vdots & \vdots \\ & & 1 & * \\ & & & u_{i_h,j} \end{pmatrix}.$$

Since $U_{QA}(i_h)$ is still an MDS code, this submatrix is non-singular, hence its determinant $u_{i_h,j}$ is a unit of R. □

With the notations in Lemma 4.9, we return to the proof of Theorem 4.7. Note that $Q^{-1} = (r_{ij})_{m\times m}$ is also a block lower triangular matrix

$$Q^{-1} = (r_{ij})_{m\times m} = \begin{pmatrix} Q_1^{-1} & & & \\ * & Q_2^{-1} & & \\ \vdots & \ddots & \ddots & \\ * & \cdots & * & Q_t^{-1} \end{pmatrix},$$

that is,

$$r_{ij} = 0, \qquad i \leq i_h < j, \quad h = 1, \cdots, t-1.$$

Then

$$\begin{aligned} C &= [C_1, \cdots, C_m]A = [C_1, \cdots, C_m]Q^{-1}QA \\ &= [C_1, \cdots, C_m]Q^{-1} \cdot \begin{pmatrix} I_{m_1} & * & \cdots & * & \cdots & * \\ & I_{m_2} & \cdots & * & \cdots & * \\ & & \ddots & \vdots & \vdots & \vdots \\ & & & I_{m_t} & \cdots & * \end{pmatrix}. \end{aligned}$$

For any $(\mathbf{c}_1, \cdots, \mathbf{c}_m) \in [C_1, \cdots, C_m]$, write $(\mathbf{c}_1, \cdots, \mathbf{c}_m)Q^{-1} = (\mathbf{c}'_1, \cdots, \mathbf{c}'_m)$ with

$$\mathbf{c}'_k = r_{1k}\mathbf{c}_1 + \cdots + r_{mk}\mathbf{c}_m.$$

For $h = 1, \cdots, t$ and $i_{h-1} < k \leq i_h$, since $r_{ik} = 0$ for $i \leq i_{h-1}$, we have

$$\mathbf{c}'_k = r_{i_{h-1}+1,k}\mathbf{c}_{i_{h-1}+1} + r_{i_{h-1}+2,k}\mathbf{c}_{i_{h-1}+2} + \cdots + r_{mk}\mathbf{c}_m;$$

so, by the conditions (E1),(E2) and (E3), we have that $\mathbf{c}'_k \in C_k$. Hence, $\mathbf{c}'_k \in C_k$ for all $k = 1, \cdots, m$, implying $[C_1, \cdots, C_m]Q^{-1} \subseteq [C_1, \cdots, C_m]$. Moreover, Q^{-1} is an invertible matrix, so $[C_1, \cdots, C_m]Q^{-1} = [C_1, \cdots, C_m]$. Therefore,

$$C = [C_1, \cdots, C_m](QA) = [C_1, \cdots, C_m] \begin{pmatrix} I_{m_1} & * & \cdots & * & \cdots & * \\ & I_{m_2} & \cdots & * & \cdots & * \\ & & \ddots & \vdots & \vdots & \vdots \\ & & & I_{m_t} & \cdots & * \end{pmatrix}.$$

By the inequality (4.2U) and the condition (E2),

$$d_H(C) \geq \min\big\{(l - i_h + 1)d_H(C_{i_h}) \mid h = 1, \cdots, t\big\}. \tag{4.7}$$

To prove (4.3U), it is enough to show that, for each h with $1 \leq h \leq t$, there is some $\mathbf{c} \in C$ such that $w_H(\mathbf{c}) = (l - i_h + 1)d_H(C_{i_h})$. For this purpose, we take $\mathbf{c}_{i_h} = (c_1, \cdots, c_n) \in C_{i_h}$ such that $w_H(\mathbf{c}_{i_h}) = d_H(C_{i_h})$. By (4.6), we get a codeword $\mathbf{c} \in C$ as follows:

$$\mathbf{c} = (\mathbf{0}, \cdots, \mathbf{0}, \mathbf{c}_{i_h}, \mathbf{0}, \cdots, \mathbf{0})(QA) = \big(\underbrace{\mathbf{0}, \cdots, \mathbf{0}}_{i_h - 1}, \ \mathbf{c}_{i_h}, \ u_{i_h,i_h+1}\mathbf{c}_{i_h}, \ \cdots, \ u_{i_h,l}\mathbf{c}_{i_h}\big).$$

Since $u_{i_h,j}$ are units for all $j \geq i_h + 1$, it follows that $w_H(u_{i_h,j}\mathbf{c}_{i_h}) = w_H(\mathbf{c}_{i_h}) = d_H(C_{i_h})$. Hence, we obtain that

$$w_H(\mathbf{c}) = w_H(\mathbf{c}_{i_h}) + w_H(u_{i_h,i_h+1}\mathbf{c}_{i_h}) + \cdots + w_H(u_{i_h,l}\mathbf{c}_{i_h}) = (l - i_h + 1)d_H(C_{i_h}),$$

which completes the proof of Theorem 4.7. □

We next consider the analogue of Theorem 4.7 for the dual code.

Let $A \in \mathrm{M}_{m\times l}(R)$ be an $(i_1, \cdots, i_{t-1})$-SFRR matrix, where $0 = i_0 < i_1 < \cdots < i_t = m$. Let $C_1, \cdots, C_m$ be codes over R of length n and let $C = [C_1, \cdots, C_m]A$. From Theorem 3.3, we recall that the dual code is

$$C^\perp = [C_1^\perp, \cdots, C_m^\perp, \underbrace{R^n, \cdots, R^n}_{l-m}](\tilde{A}^{-1})^T, \tag{4.8}$$

where $\tilde{A} \in \mathrm{M}_{l\times l}(R)$ is an invertible matrix with A as the submatrix consisting of its first m rows (see Remark 3.4). Now we estimate the minimum distance of $C^\perp$. If $m < l$, we have $C_{m+1}^\perp = \cdots = C_l^\perp = R^n$ and set $i_{t+1} = l$ for convenience.

Theorem 4.10. *Let the notations be as above. Then*

$$d_H(C^\perp) \geq \min\big\{(i_h + 1)d_H(C_{k_h}^\perp) \mid h = 0, 1, \cdots, t,\ i_h < k_h \leq i_{h+1}\big\}. \tag{4.9}$$

Furthermore, if the following three conditions are satisfied:

(E1) $C_1, \cdots, C_m$ *are linear,*

(E2) $C_1 = \cdots = C_{i_1}$, $C_{i_1+1} = \cdots = C_{i_2}$, $\cdots$, $C_{i_{t-1}+1} = \cdots = C_{i_t}$,

(E3) $C_{i_1} \supseteq C_{i_2} \supseteq \cdots \supseteq C_{i_t}$,

then equality holds in (4.9)*, i.e.,*

$$d_H(C^\perp) = \min\big\{(i_h + 1)d_H(C_{i_{h+1}}^\perp) \mid h = 0, 1, \cdots, t\big\}. \tag{4.10}$$

Remark 4.11. If $m < l$ (i.e., A is not square), then in the braces of the right hand side of (4.9), the terms for $h = t$ are:

$$(i_t + 1)d_H(C_{k_t}^\perp) = m + 1, \qquad i_t = m < k_t \leq l = i_{t+1}.$$

Accordingly, in (4.10), the term corresponding to $h = t$ is $m + 1$.

On the other hand, when $m = l$, then in (4.9), there is no term for $h = t$ since no k satisfies $l < k \leq l$. Accordingly, in (4.10), there is no term $m + 1$ for $h = t$.

Proof of Theorem 4.10. Let $\tilde{B} = \tilde{A}^{-1}$. For $\tilde{A}$, we have that

- $U_{\tilde{A}}(i_h) = U_A(i_h)$, for $h = 0, 1, \cdots, t$, are MDS codes.

By Proposition 4.4, this is equivalent to

- $L_{\tilde{B}^T}(i_h + 1)$, for $h = 0, 1, \cdots, t$, are MDS codes. (Note that $L_{\tilde{B}^T}(l + 1)$ is trivially MDS.)

Since $\mathrm{rank}\big(L_{\tilde{B}^T}(i_h + 1)\big) = l - i_h$, we have that

$$d_H\big(L_{\tilde{B}^T}(i_h + 1)\big) = l - (l - i_h) + 1 = i_h + 1, \qquad h = 0, 1, \cdots, t.$$

By the dual of Theorem 4.7 (see (4.2L)), we have that

$$d_H(C^\perp) \geq \min\big\{\,(i_h + 1)d_H(C_{k_h}^\perp) \mid h = 0, 1, \cdots, t,\ i_h < k_h \leq i_{h+1}\big\}.$$

However, note that, if $i_t = m < l$, then, for any k with $m < k \leq l$, we have that $C_k^\perp = R^n$, hence $d_H(C_k^\perp) = 1$; so the terms for $h = t$ in the braces are:

$$(i_t + 1)d_H(C_{k_t}^\perp) = m + 1, \qquad i_t = m < k_t \leq l = i_{t+1}.$$

The inequality (4.9) is proved.

Further, assume that the conditions (E1), (E2) and (E3) hold. Then, for the dual codes, the following conditions hold:

(E1*) $C_1^\perp, \cdots, C_m^\perp$ are linear (note: $C_{m+1}^\perp, \cdots, C_l^\perp$ are trivially linear),

(E2*) $C_1^\perp = \cdots = C_{i_1}^\perp$, $C_{i_1+1}^\perp = \cdots = C_{i_2}^\perp$, $\cdots$, $C_{i_{t-1}+1}^\perp = \cdots = C_{i_t}^\perp$, (note: $C_{m+1}^\perp = \cdots = C_l^\perp$ trivially),

(E3*) $C_{i_0+1}^\perp \subseteq C_{i_1+1}^\perp \subseteq \cdots \subseteq C_{i_{t-1}+1}^\perp \subseteq C_{i_t+1}^\perp = R^n$.

By the dual of Theorem 4.7 (see (4.3L)), we obtain the equality (4.10). (Note that, similar to the case of (4.9), when $m < l$, the term corresponding to $h = t$ is $m + 1$, while, for the case $m = l$, there is no term $m + 1$ for $h = t$.) □

As a special case, we have the following corollary on non-singular by columns matrices over R, which generalizes [1, Theorems 3.7 and 6.6] and [16, Propositions 2 and 4]. However, in our case, for the bound on $d_H(C^\perp)$, we do not require A to be square.

Corollary 4.12. *Let $A \in \mathrm{M}_{m\times l}(R)$ be non-singular by columns, let $C_1, \cdots, C_m$ be codes over R of length n, and let $C = [C_1, \cdots, C_m]A$. Then*

$$d_H(C) \geq \min\{\, l \cdot d_H(C_1),\ (l-1)d_H(C_2),\ \cdots,\ (l-m+1)d_H(C_m)\,\}$$

and

$$d_H(C^\perp) \geq \begin{cases} \min\{\, 1 \cdot d_H(C_1^\perp),\ 2 \cdot d_H(C_2^\perp),\ \cdots,\ m \cdot d_H(C_m^\perp),\ m+1\,\} & \text{if } m < l, \\ \min\{\, 1 \cdot d_H(C_1^\perp),\ 2 \cdot d_H(C_2^\perp),\ \cdots,\ m \cdot d_H(C_m^\perp)\,\} & \text{if } m = l. \end{cases}$$

Further, if $C_1, \cdots, C_m$ are linear and $C_1 \supseteq \cdots \supseteq C_m$, then equalities are attained in all these inequalities.

In the next section, we further discuss the properties of codes constructed with a special type of (m')-SFRR matrices, and provide two examples of codes constructed in this manner.

5 Two-Way (m')-SFRR Matrices

Recall that the well-known $(a+x|b+x|a+b+x)$-construction is associated with the matrix $T = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$ and the matrix product code $C = [C_1, C_1, C_2]T$. We have seen in Example 4.6 that T is a (2)-SFRR matrix (but not a non-singular by columns matrix), so (4.2U) of Theorem 4.7 can be applied to show that the minimum distance satisfies $d_H(C) \geq \min\{2d_H(C_1), d_H(C_2)\}$. On the other hand, T is also a reversely (3)-SFRR matrix, so (4.2L) of Theorem 4.7 is also applicable, yielding $d_H(C) \geq \min\{d_H(C_1), 3d_H(C_2)\}$. Therefore,

$$d_H(C) \geq \max\{\, \min\{2d_H(C_1), d_H(C_2)\},\ \min\{d_H(C_1), 3d_H(C_2)\}\,\}.$$

However, for this construction, there is another well-known estimation (e.g., see [2, Section V.B]):

$$\min\{d_H(C_1 \cap C_2),\ 2d_H(C_1), 3d_H(C_2)\} \geq d_H(C) \geq \min\{d_H(C_1 \cap C_2),\ 2d_H(C_1), 3d_H(C_1 + C_2)\}.$$

Though the two lower bounds above cannot be directly compared in general, in many cases the latter is better than the former. Furthermore, we also note that C is self-dual in many cases though T is not a quasi-orthogonal matrix.

Inspired by these observations, we introduce the following notion.

Definition 5.1. *Let $A \in \mathrm{M}_{m\times l}(R)$ be FRR. If there is an index m' with $1 \leq m' < m$ such that A is both an (m')-SFRR matrix and a reversely $(m'+1)$-SFRR matrix, then we say that A is a* two-way (m')-SFRR matrix.

Remark 5.2. For $m' + m'' = m$, any $m \times l$ matrix A can be written as $A = \left(\frac{A'}{A''}\right)$, where A' is an $m' \times l$ matrix consisting of the first m' rows of A while A'' is an $m'' \times l$ matrix consisting of the last m'' rows of A. With this partitioned form, A is a two-way (m')-SFRR matrix if and only if A', A'' and A are all SFRR matrices.

The following property is a key point for constructing self-orthogonal matrix product codes.

Definition 5.3. *Let an $m \times l$ matrix $A = \left(\frac{A'}{A''}\right)$ be partitioned into an $m' \times l$ matrix A' and an $m'' \times l$ matrix A'' as above. If every row of A' is orthogonal to every row of A'' with respect to the Euclidean inner product on R^l, then we say that A has a* partitioned orthogonal property*, or, more precisely, the* m'-partitioned orthogonal property*.*

A quasi-orthogonal two-way (m')-SFRR matrix obviously has the m'-partitioned orthogonal property.

Example 5.4. (i) As we have seen in Example 4.6, for any Frobenius ring R, $T = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$ is a two-way (2)-SFRR matrix. Furthermore, if R has characteristic 2, then T has the 2-partitioned orthogonal property, but T is not quasi-orthogonal. In fact, if R is the binary field, then T is the unique two-way (2)-SFRR matrix of order 3.

(ii) $A = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ is a two-way (1)-SFRR matrix provided the characteristic of R is different from 2. Moreover, A is also a quasi-orthogonal matrix.

If R is the binary field, then there are no two-way (1)-SFRR matrices of order 2 over R. However, if R is a field of characteristic 2 but not the binary field, taking any $1 \neq \omega \in R$, then $\begin{pmatrix} 1 & \omega \\ \omega & 1 \end{pmatrix}$ is a two-way (1)-SFRR matrix which is also a quasi-orthogonal matrix.

(iii) $\begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & -1 \\ 1 & 1 & 1 & 0 \\ 1 & -1 & 0 & 1 \end{pmatrix}$ is a two-way (2)-SFRR matrix if the characteristic $\operatorname{char} R \neq 2$.

However, if $3 \nmid \operatorname{char} R$ and $\operatorname{char} R > 2$, then $\begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & -1 \\ 1 & 1 & -1 & 0 \\ 1 & -1 & 0 & -1 \end{pmatrix}$ is a two-way (2)-SFRR matrix which is also a quasi-orthogonal matrix.

Note that, if R is the binary field, there are no two-way (m')-SFRR matrices over R of size 4×4, for any $1 \leq m' \leq 3$.

According to Remark 5.2, we can partition a two-way (m')-SFRR matrix A as $A = \left(\frac{A'}{A''}\right)$, where A' is an $m' \times l$ SFRR matrix and A'' is an $m'' \times l$ SFRR matrix. For linear codes $C_1, \cdots, C_m$ over R of length n, it is obvious that the following two matrix product codes are equivalent to each other:

$$\left[C_1, \cdots, C_{m'}, C_{m'+1}, \cdots, C_m\right] \left(\frac{A'}{A''}\right) \cong \left[C_{m'+1}, \cdots, C_m, C_1, \cdots, C_{m'}\right] \left(\frac{A''}{A'}\right).$$

Without loss of generality, we can further assume that $m' \geq m''$.

Let $A \in \mathrm{M}_{m \times l}(R)$, let $m' + m'' = m$ with $m' \geq m'' \geq 1$, and let C' and C'' be linear codes over R of length n. We consider the matrix product code

$$C = [\underbrace{C', \cdots, C'}_{m'}, \underbrace{C'', \cdots, C''}_{m''}]A. \tag{5.1}$$

If A is a two-way (m')-SFRR matrix, then from (4.2U) and (4.2L) of Theorem 4.7, we have a lower bound for $d_H(C)$ as follows:

$$d_H(C) \geq \max \left\{ \begin{array}{l} \min\{(l - m' + 1)d_H(C'),\ (l - m + 1)d_H(C'')\}, \\ \min\{(l - m + 1)d_H(C'),\ (l - m'' + 1)d_H(C'')\} \end{array} \right\}. \tag{5.2}$$

Now we have some more bounds for $d_H(C)$ stated as follows.

Theorem 5.5. *Let the notations be as in* (5.1)*. If A is a two-way (m')-SFRR matrix, then*

$$d_H(C) \geq \min\big\{(l-m'+1)d_H(C'),\ (l-m''+1)d_H(C'+C''),\ (l-m+1)d_H(C'\cap C'')\big\} \tag{5.3}$$

and

$$d_H(C) \leq \min\big\{(l-m'+1)d_H(C'),\ (l-m''+1)d_H(C''),\ (l-m+1)d_H(C'\cap C'')\big\}. \tag{5.4}$$

Proof. Set $C_\cap = C'\cap C''$. Since $[C',\cdots,C',\ C'',\cdots,C''] \supseteq [C',\cdots,C',\ C_\cap,\cdots,C_\cap]$, we have $C = [C',\cdots,C',\ C'',\cdots,C'']A \supseteq [C',\cdots,C',\ C_\cap,\cdots,C_\cap]A$, so

$$d_H(C) \leq d_H\big([\underbrace{C',\cdots,C'}_{m'},\ \underbrace{C_\cap,\cdots,C_\cap}_{m''}]A\big).$$

Since $C'\supseteq C_\cap$, by (4.3U) of Theorem 4.7, we have

$$d_H\big([\underbrace{C',\cdots,C'}_{m'},\ \underbrace{C_\cap,\cdots,C_\cap}_{m''}]A\big) = \min\big\{(l-m'+1)d_H(C'),\ (l-m+1)d_H(C_\cap)\big\}, \tag{5.5}$$

thus

$$d_H\big(C\big) \leq \min\big\{(l-m'+1)d_H(C'),\ (l-m+1)d_H(C'\cap C'')\big\}. \tag{5.6}$$

Applying (4.3L) to $C = [C',\cdots,C',C'',\cdots,C'']A \supseteq [C_\cap,\cdots,C_\cap,C'',\cdots,C'']A$ and observing that $C_\cap \subseteq C''$, we obtain

$$d_H\big(C\big) \leq \min\big\{(l-m''+1)d_H(C''),\ (l-m+1)d_H(C'\cap C'')\big\}. \tag{5.7}$$

Combining (5.6) and (5.7), the conclusion (5.4) follows.

Now we proceed to prove (5.3). We partition A as $A = \left(\frac{A'}{A''}\right)$, where A' is the $m'\times l$ matrix consisting of the first m' rows of A while A'' is the $m''\times l$ matrix consisting of the last m'' rows of A. Assume that $\mathbf{c}'_1,\cdots,\mathbf{c}'_{m'}\in C'$, $\mathbf{c}''_1,\cdots,\mathbf{c}''_{m''}\in C''$ and $\big(\mathbf{c}'_1,\cdots,\mathbf{c}'_{m'},\ \mathbf{c}''_1,\cdots,\mathbf{c}''_{m''}\big)\neq\mathbf{0}$. We have a non-zero codeword of C as follows:

$$\mathbf{c} = \big(\mathbf{c}'_1,\cdots,\mathbf{c}'_{m'},\ \mathbf{c}''_1,\cdots,\mathbf{c}''_{m''}\big)A = \big(\mathbf{c}'_1,\cdots,\mathbf{c}'_{m'}\big)A' + \big(\mathbf{c}''_1,\cdots,\mathbf{c}''_{m''}\big)A''.$$

We consider the $m''\times m''$ submatrices of A'': there are two cases. For any matrix $M\in \mathrm{M}_{m\times l}(R)$ and $1\leq j_1<\cdots<j_s\leq l$, let $M(j_1,\cdots,j_s)$ denote the $m\times s$ submatrix of M consisting of the j_1th, $\cdots$, j_sth columns of M.

Case 1: There are m'' columns of A, say the j_1th, $\cdots$, $j_{m''}$th columns, such that

$$\big(\mathbf{c}'_1,\cdots,\mathbf{c}'_{m'}\big)A'(j_1,\cdots,j_{m''}) + \big(\mathbf{c}''_1,\cdots,\mathbf{c}''_{m''}\big)A''(j_1,\cdots,j_{m''}) = \mathbf{0}.$$

Note that $A''(j_1,\cdots,j_{m''})$ is an invertible $m''\times m''$ submatrix of A'' because A'' is an SFRR matrix. Then

$$\big(\mathbf{c}''_1,\cdots,\mathbf{c}''_{m''}\big)A''(j_1,\cdots,j_{m''}) = -\big(\mathbf{c}'_1,\cdots,\mathbf{c}'_{m'}\big)A'(j_1,\cdots,j_{m''}),$$

where the left hand side belongs to

$$[\underbrace{C'',\cdots,C''}_{m''}]A''(j_1,\cdots,j_{m''}) = [\underbrace{C'',\cdots,C''}_{m''}],$$

and the right hand side belongs to

$$[\underbrace{C',\cdots,C'}_{m'}]A'(j_1,\cdots,j_{m''}) \subseteq [\underbrace{C',\cdots,C'}_{m''}].$$

Thus

$$\big(\mathbf{c}''_1,\cdots,\mathbf{c}''_{m''}\big)A''(j_1,\cdots,j_{m''})\in[\underbrace{C'',\cdots,C''}_{m''}]\bigcap[\underbrace{C',\cdots,C'}_{m''}]=[\underbrace{C_\cap,\cdots,C_\cap}_{m''}].$$

It then follows that

$$\big(\mathbf{c}''_1,\cdots,\mathbf{c}''_{m''}\big)\in[\underbrace{C_\cap,\cdots,C_\cap}_{m''}]A''(j_1,\cdots,j_{m''})^{-1}=[\underbrace{C_\cap,\cdots,C_\cap}_{m''}].$$

Hence,

$$\mathbf{c}=\big(\mathbf{c}'_1,\cdots,\mathbf{c}'_{m'},\,\mathbf{c}''_1,\cdots,\mathbf{c}''_{m''}\big)A\in[\underbrace{C',\cdots,C'}_{m'},\,\underbrace{C_\cap,\cdots,C_\cap}_{m''}]A,$$

and by (5.5), we get

$$w_H(\mathbf{c})\geq\min\big\{(l-m'+1)d_H(C'),\ (l-m+1)d_H(C'\cap C'')\big\}. \tag{5.8}$$

Case 2: There are at most $m''-1$ columns of A, say the first s columns, where $s\leq m''-1$, such that

$$\big(\mathbf{c}'_1,\cdots,\mathbf{c}'_{m'}\big)A'(1,\cdots,s)+\big(\mathbf{c}''_1,\cdots,\mathbf{c}''_{m''}\big)A''(1,\cdots,s)=\mathbf{0}.$$

By the construction (5.1) of C, $\mathbf{c}$ is an $n\times l$ matrix. The above assumption means that any one of the last $l-m''+1$ columns of $\mathbf{c}$ is a non-zero vector of R^n. By the construction (5.1) of C, any column of $\mathbf{c}$ is a vector of $C'+C''$, so

$$w_H(\mathbf{c})\geq(l-m''+1)d_H(C'+C''). \tag{5.9}$$

Summarizing the discussions for the two cases, we see that, for any non-zero codeword $\mathbf{c}$ of C, one of (5.8) and (5.9) holds, so we obtain

$$d_H(C)\geq\min\big\{(l-m'+1)d_H(C'),\ (l-m+1)d_H(C'\cap C''),\ (l-m''+1)d_H(C'+C'')\big\},$$

which is just the required inequality (5.3). □

Remark 5.6. (i) For the proof of (5.3), if we start with considering the $m'\times m'$ submatrices of A', then we can obtain in a similar way that

$$d_H(C)\geq\min\big\{(l-m''+1)d_H(C''),\ (l-m+1)d_H(C'\cap C''),\ (l-m'+1)d_H(C'+C'')\big\}. \tag{5.10}$$

Observing that $l-m'+1\leq l-m''+1$ since we have assumed that $m'\geq m''$, and that $d_H(C'+C'')\leq d_H(C')$, we have that

$$(l-m'+1)d_H(C'+C'')\leq\min\{(l-m''+1)d_H(C'+C''),\ (l-m'+1)d_H(C')\},$$

so

$$\begin{aligned}&\min\big\{(l-m''+1)d_H(C''),\ (l-m+1)d_H(C'\cap C''),\ (l-m'+1)d_H(C'+C'')\big\}\\ \leq\ &\min\big\{(l-m'+1)d_H(C'),\ (l-m+1)d_H(C'\cap C''),\ (l-m''+1)d_H(C'+C'')\big\}.\end{aligned}$$

In other words, under the assumption that $m'\geq m''$, the bound (5.10) is not better than that of (5.3).

(ii) However, the bounds in (5.2) and (5.3) cannot be compared in general, because $d_H(C'')$ in (5.2) and $(l-m''+1)d_H(C'+C'')$ in (5.3) are not comparable in general. Thus, we can take the larger of (5.2) and (5.3) as a better lower bound for $d_H(C)$.

Theorem 5.7. *Let the notations be as in* (5.1). *Further assume that the matrix A has the m'-partitioned orthogonal property. If both C' and C'' are self-orthogonal, then C is self-orthogonal too. In particular, C is self-dual provided both C' and C'' are self-dual and A is invertible.*

Proof. Write $A = \left(\frac{A'}{A''}\right)$ with A' being the $m' \times l$ matrix consisting of the first m' rows of A and A'' the $m'' \times l$ matrix consisting of the last m'' rows of A. By the product of partitioned matrices,

$$AA^T = \left(\frac{A'}{A''}\right)\left(\, A'^T \mid A''^T \,\right) = \begin{pmatrix} A'A'^T & A'A''^T \\ A''A'^T & A''A''^T \end{pmatrix}.$$

By the m'-partitioned orthogonal property, we have that $A'A''^T = 0$ and $A''A'^T = 0$, so

$$AA^T = \begin{pmatrix} A'A'^T & \\ & A''A''^T \end{pmatrix}.$$

Then, for any two codewords

$$\mathbf{c} = \big(\mathbf{c}'_1, \cdots, \mathbf{c}'_{m'}, \mathbf{c}''_1, \cdots, \mathbf{c}''_{m''}\big)A \in C, \quad \mathbf{d} = \big(\mathbf{d}'_1, \cdots, \mathbf{d}'_{m'}, \mathbf{d}''_1, \cdots, \mathbf{d}''_{m''}\big)A \in C,$$

with $\mathbf{c}'_1, \cdots, \mathbf{c}'_{m'}, \mathbf{d}'_1, \cdots, \mathbf{d}'_{m'} \in C'$ and $\mathbf{c}''_1, \cdots, \mathbf{c}''_{m''}, \mathbf{d}''_1, \cdots, \mathbf{d}''_{m''} \in C''$, by (3.1), we have

$$\begin{aligned} \langle \mathbf{c}, \mathbf{d} \rangle &= \mathrm{tr}\big(\mathbf{c}\mathbf{d}^T\big) = \mathrm{tr}\left(\big(\mathbf{c}'_1, \cdots, \mathbf{c}'_{m'}, \mathbf{c}''_1, \cdots, \mathbf{c}''_{m''}\big)AA^T\big(\mathbf{d}'_1, \cdots, \mathbf{d}'_{m'}, \mathbf{d}''_1, \cdots, \mathbf{d}''_{m''}\big)^T\right) \\ = \quad & \mathrm{tr}\left(\big((\mathbf{c}'_1, \cdots, \mathbf{c}'_{m'})(A'A'^T), (\mathbf{c}''_1, \cdots, \mathbf{c}''_{m''})(A''A''^T)\big) \cdot \big(\mathbf{d}'_1, \cdots, \mathbf{d}'_{m'}, \mathbf{d}''_1, \cdots, \mathbf{d}''_{m''}\big)^T\right). \end{aligned}$$

However, $[C', \cdots, C'](A'A'^T) \subseteq [C', \cdots, C']$, so

$$(\mathbf{c}'_1, \cdots, \mathbf{c}'_{m'})(A'A'^T) = (\bar{\mathbf{c}}'_1, \cdots, \bar{\mathbf{c}}'_{m'}), \qquad \text{with } \ \bar{\mathbf{c}}'_1, \cdots, \bar{\mathbf{c}}'_{m'} \in C'.$$

Similarly,

$$(\mathbf{c}''_1, \cdots, \mathbf{c}''_{m''})(A''A''^T) = (\bar{\mathbf{c}}''_1, \cdots, \bar{\mathbf{c}}''_{m''}), \qquad \text{with } \ \bar{\mathbf{c}}''_1, \cdots, \bar{\mathbf{c}}''_{m''} \in C''.$$

Since both C' and C'' are self-orthogonal,

$$\begin{aligned} \langle \mathbf{c}, \mathbf{d} \rangle &= \mathrm{tr}\left(\big(\bar{\mathbf{c}}'_1, \cdots, \bar{\mathbf{c}}'_{m'}, \bar{\mathbf{c}}''_1, \cdots, \bar{\mathbf{c}}''_{m''}\big) \cdot \big(\mathbf{d}'_1, \cdots, \mathbf{d}'_{m'}, \mathbf{d}''_1, \cdots, \mathbf{d}''_{m''}\big)^T\right) \\ &= \mathrm{tr}\big(\bar{\mathbf{c}}'_1\mathbf{d}'^T_1\big) + \cdots + \mathrm{tr}\big(\bar{\mathbf{c}}'_{m'}\mathbf{d}'^T_{m'}\big) + \mathrm{tr}\big(\bar{\mathbf{c}}''_1\mathbf{d}''^T_1\big) + \cdots + \mathrm{tr}\big(\bar{\mathbf{c}}''_{m''}\mathbf{d}''^T_{m''}\big) \\ &= \langle \bar{\mathbf{c}}'_1, \mathbf{d}'_1 \rangle + \cdots + \langle \bar{\mathbf{c}}'_{m'}, \mathbf{d}'_{m'} \rangle + \langle \bar{\mathbf{c}}''_1, \mathbf{d}''_1 \rangle + \cdots + \langle \bar{\mathbf{c}}''_{m''}, \mathbf{d}''_{m''} \rangle \\ &= 0. \end{aligned}$$

Therefore, C is self-orthogonal.

Assume that both C' and C'' are self-dual. Since $|C'||C'^{\perp}| = |R|^n$ and $|C''||C''^{\perp}| = |R|^n$, it follows that

$$|C'| = |C'^{\perp}| = |R|^{n/2} = |C''| = |C''^{\perp}|.$$

When A is invertible, we have $m = l$, so

$$|C| = |C'|^{m'}|C''|^{m''} = |R|^{(m'+m'')n/2} = |R|^{mn/2} = |R|^{ln/2}.$$

Furthermore, from $|C||C^{\perp}| = |R|^{ln}$, we have $|C^{\perp}| = |R|^{ln/2}$. Since $C \subseteq C^{\perp}$, it follows that $C = C^{\perp}$. $\square$

Example 5.8. Take R to be the binary field and $T = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$. Then T is a two-way (2)-SFRR matrix that has the 2-partitioned orthogonal property. Recall that the matrix product code construction $C = [C', C', C'']T$ in (5.1) is just the well-known $(a+x|b+x|a+b+x)$ construction. It is also a quasi-cyclic code of co-index 3 (see [8, Theorem 6.7]). The bounds in (5.3) and (5.4) of Theorem 5.5 give the following well-known estimation on the minimum distance of C (cf. [2, Section V.B]):

$$\min\{d_H(C' \cap C''),\, 2d_H(C'), 3d_H(C'')\} \geq d_H(C) \geq \min\{d_H(C' \cap C''),\, 2d_H(C'), 3d_H(C' + C'')\}.$$

Another lower bound is given by (5.2):

$$d_H(C) \geq \max\big\{\min\{2d_H(C'), d_H(C'')\},\ \min\{d_H(C'), 3d_H(C'')\}\big\}.$$

It was noted in Remark 5.6 that these two lower bounds cannot be compared directly in general. We now consider a few explicit examples. First, we set

Code	parameters	generator matrix	duality
C_1	$[4,1,4]$	$(1,1,1,1)$	self-orthogonal
C_2	$[4,2,2]$	$\begin{pmatrix}1&0&1&0\\0&1&1&1\end{pmatrix}$	not self-orthogonal
C_3	$[4,2,2]$	$\begin{pmatrix}1&0&1&0\\0&1&0&1\end{pmatrix}$	Type I self-dual
C_3'	$[4,2,2]$	$\begin{pmatrix}1&1&0&0\\0&0&1&1\end{pmatrix}$	Type I self-dual

(i) Take $C = [C_2, C_2, C_1]T$, with C_1, C_2 as above. Since $C_2 \cap C_1 = 0$ and $C_2 + C_1$ is a $[4,3,1]$ linear code with generator matrix $\begin{pmatrix}1&0&1&0\\0&1&1&1\\0&0&1&0\end{pmatrix}$, the bound (5.2) shows that $d_H(C) \geq 4$, while the bound (5.3) gives $d_H(C) \geq 3$. Therefore, in this case, the bound (5.2) is better than the bound (5.3). On the other hand, (5.4) shows that $d_H(C) \leq 4$, hence, $d_H(C) = 4$. Thus C is a $[12,5,4]$ binary linear code. It can be verified directly that C is not self-orthogonal. In fact, the following two codewords are not orthogonal to each other:

$$\begin{pmatrix}0&0&1\\0&1&1\\0&1&1\\0&1&1\end{pmatrix}T = \begin{pmatrix}1&1&1\\1&0&0\\1&0&0\\1&0&0\end{pmatrix} \quad \text{and} \quad \begin{pmatrix}1&0&1\\0&0&1\\1&0&1\\0&0&1\end{pmatrix}T = \begin{pmatrix}0&1&0\\1&1&1\\0&1&0\\1&1&1\end{pmatrix}.$$

(ii) Take $C = [C_3, C_3, C_3']T$ with C_3, C_3' as above. Since $C_3 \cap C_3' = C_1$ and $C_3 + C_3'$ is a $[4,3,2]$ linear code with generator matrix $\begin{pmatrix}1&0&1&0\\0&1&0&1\\0&0&1&1\end{pmatrix}$. The bound (5.2) shows that $d_H(C) \geq 2$, while the bound (5.3) gives $d_H(C) \geq 4$. Hence, in this case, the bound (5.2) is weaker than the bound (5.3). From (5.4), we obtain $d_H(C) \leq 4$, thus $d_H(C) = 4$. Further, both C' and C'' are self-dual in this case. Therefore, by Theorem 5.7, C is a self-dual $[12,6,4]$ binary linear code. However, C is not of Type II: this follows from [8, Proposition 7.1] with the fact that C_3' is not of Type II, but it can also be seen directly that the codeword

$$\begin{pmatrix}1&0&1\\0&1&1\\1&0&0\\0&1&0\end{pmatrix}T = \begin{pmatrix}0&1&0\\1&0&0\\1&0&1\\0&1&1\end{pmatrix}$$

does not have Hamming weight divisible by 4.

(iii) Take $C = [C_3, C_3, C_1]T$ with C_1, C_3 as above. Since $C_3 \supseteq C_1$, by (4.3U) we have that $d_H(C) = \min\{2d_H(C_3),\ d_H(C_1)\} = 4$. Hence, C is a $[12,5,4]$ binary linear code. Since C_3 is self-dual and C_1 is self-orthogonal, C is also self-orthogonal.

We summarize the above examples in the following:

Code C	parameters	duality	argument for $d_H(C)$
$[C_2, C_2, C_1]T$	$[12,5,4]$	not self-orthogonal	by (5.2)
$[C_3, C_3, C_3']T$	$[12,6,4]$	Type I self-dual	by (5.3)
$[C_3, C_3, C_1]T$	$[12,5,4]$	self-orthogonal	by (4.3U)

Example 5.9. Take R to be the binary field. Take $A = \begin{pmatrix} 1 & 1 & & & & \\ & 1 & 1 & & & \\ & & 1 & 1 & & \\ & & & 1 & 1 & \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix}$, which is a two-way (4)-SFRR matrix that has the 4-partitioned orthogonal property. In fact, A is the matrix for constructing quasi-cyclic codes of co-index 5, see [8, Theorem 6.14]. Similar to the construction of the $[24, 12, 8]$-Golay code from $[8, 4, 4]$-extended Hamming codes by the $(a + x|b + x|a + b + x)$-construction, we construct $C = [C', C', C', C', C'']A$, where C' and C'' are $[8, 4, 4]$ extended Hamming codes with generator matrices G' and G'', respectively, as follows:

$$G' = \begin{pmatrix} 1 & 1 & 0 & 1 & & & 1 \\ & 1 & 1 & 0 & 1 & & 1 \\ & & 1 & 1 & 0 & 1 & 1 \\ & & & 1 & 1 & 0 & 1 & 1 \end{pmatrix}, \qquad G'' = \begin{pmatrix} 1 & 0 & 1 & 1 & & & 1 \\ & 1 & 0 & 1 & 1 & & 1 \\ & & 1 & 0 & 1 & 1 & 1 \\ & & & 1 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

It is known that both C' and C'' are of Type II. Since $C' \cap C''$ is an $[8, 1, 8]$ code and $C' + C''$ is an $[8, 7, 2]$ code, by (5.3) and (5.4) we have that

$$8 = \min\{2 \cdot 4,\ 5 \cdot 2,\ 1 \cdot 8\} \leq d_H(C) \leq \min\{2 \cdot 4,\ 5 \cdot 4,\ 1 \cdot 8\} = 8,$$

that is, $d_H(C) = 8$. By Theorem 5.7, C is self-dual. Furthermore, since C'' is of Type II, so is C (see [8, Proposition 7.3]). We conclude that C is a $[40, 20, 8]$ Type II binary code.

Acknowledgements

This work was done while the first and third authors were visiting the Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore, in Autumn 2011. They are grateful for the hospitality and support. They also thank NSFC for the support through Grants No. 10871079 and No. 11171370. The work of S. Ling was partially supported by Singapore MOE-AcRF Tier 2 Research Grant T208B2204.

It is also the authors' pleasure to thank the anonymous referees for their helpful comments.

References

[1] T. Blackmore and G. H. Norton, *Matrix-product codes over* $\mathbb{F}_q$, Appl. Algebra Engrg. Comm. Comput., **12** (2001), 477–500.

[2] G. D. Forney, *Coset codes II: binary lattices*, IEEE Trans. Inform. Theory, **34** (1988), 1152–1187.

[3] A. R. Hammons, P.V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, *The* $\mathbf{Z}_4$*-linearity of Kerdock, Preparata, Goethals, and related codes*, IEEE Trans. Inform. Theory, **40** (1994), 301–319.

[4] F. Hernando, H. Høholdt and D. Ruano, *List decoding of matrix-product codes from nested codes: an application to quasi-cyclic codes*, 2012, http://arxiv.org/pdf/1201.6397.pdf.

[5] F. Hernando, K. Lally and D. Ruano, *Construction and decoding of matrix-product codes from nested codes*, Appl. Algebra Engrg. Comm. Comput., **20** (2009), 497–507.

[6] F. Hernando and D. Ruano, *New linear codes from matrix-product codes with polynomial units*, Adv. Math. Commun., **4** (2010), 363–367.

[7] F. Hernando and D. Ruano, *Decoding of matrix-product codes*, 2011, http://arxiv.org/pdf/1107.1529.pdf.

[8] S. Ling and P. Solé, *On the algebraic structure of quasi-cyclic codes I: finite fields*, IEEE Trans. Inform. Theory, **47** (2001), 2751–2760.

[9] S. Ling and P. Solé, *On the algebraic structure of quasi-cyclic codes II: chain rings*, Des., Codes and Crypto., **30** (2003), 113–130.

[10] E. Martínez-Moro, *A generalization of Niederreiter-Xing's propagation rule and its commutativity with duality*. IEEE Trans. Inform. Theory, **50** (2004), 701–702.

[11] H. Niederreiter and C. P. Xing, *A propagation rule for linear codes*, Appl. Algebra Engrg. Comm. Comput., **10** (2000), 425–432.

[12] G. H. Norton and A. Sălăgean, *On the Hamming distance of linear codes over a finite chain ring*, IEEE Trans. Inform. Theory, **46** (2000), 1060–1067.

[13] M. B. O. Medeni and E. M. Souidi, *Construction and bound on the performance of matrix-product codes*, Appl. Math. Sci. (Ruse), **5** (2011), 929–934.

[14] F. Özbudak and H. Stichtenoth, *Note on Niederreiter-Xing's propagation rule for linear codes*, Appl. Algebra Engrg. Comm. Comput., **13** (2002), 53–56.

[15] S. Roman, *Coding and Information Theory*, Graduate Texts in Mathematics **134**, Springer-Verlag, New York, 1992.

[16] B. van Asch, *Matrix-product codes over finite chain rings*, Appl. Algebra Engrg. Comm. Comput., **19** (2008), 39–49.

[17] J. Wood, *Duality for modules over finite rings and applications to coding theory*, Amer. J. Math., **121** (1999), 555–575.

[18] J. Wood, *Code equivalence characterizes finite Frobenius rings*, Proc. Amer. Math. Soc., **136** (2008), 699–706.