Homogeneous Weights of Matrix Product Codes over Finite Principal Ideal 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

In this paper, the homogeneous weights of matrix product codes over finite principal ideal rings are studied and a lower bound for the minimum homogeneous weights of such matrix product codes is obtained.

Key words: Finite principal ideal ring, homogeneous weight, matrix product code.

1 Introduction

Matrix product codes over finite fields were introduced in [1]. Many well-known constructions can be formulated as matrix product codes, for example, the $(a|a+b)$-construction, the $(a+x|b+x|a+b+x)$-construction, and, some quasi-cyclic codes can be rewritten as matrix product codes, see [13]. The reference [1] also introduced non-singular by columns matrices and exhibited a lower bound for the minimum Hamming distances of matrix product codes over finite fields constructed by such matrices. More references on matrix product codes appeared later, e.g., in [9, 10, 11, 15, 16].

Codes over finite rings have also been studied from many perspectives since the seminal work [8]. It was also shown later in [18] that a finite Frobenius ring is suitable as an alphabet for linear coding. Further, [6] showed that, for any finite ring, there is a Frobenius module which is suitable as an alphabet for linear coding. Inspired by the idea of module coding, [19] proved that the biggest class of finite rings which are suitable as alphabets for linear coding consists of the finite Frobenius rings.

Finite principal ideal rings form an important subclass of finite Frobenius rings. In particular, all the residue rings $\mathbf{Z}_N$ of integers modulo an integer $N>1$ are principal ideal rings. It is well known that a finite commutative ring is a principal ideal ring if and only if it is a product of finite chain rings. The reference [17] extended the lower bound obtained in [1] for the minimum Hamming distances of matrix product codes with non-singular by columns matrices over finite fields to the minimum homogeneous weights of matrix product codes over finite chain rings.

In this paper, we consider matrix product codes over finite commutative principal ideal rings, and extend the result on the lower bound for the minimum homogeneous weights of matrix product codes over finite chain rings to matrix product codes over finite commutative principal ideal rings.

In the next section, necessary notations and fundamentals are introduced as preliminaries. In Section 3, we state our main theorem, its corollaries and some remarks. Since the proof of the main theorem is long and technical, it is deferred to Section 4.

2 Preliminaries

In this paper, R is always a finite commutative ring.

For the finite commutative ring R and a positive integer ℓ, any non-empty subset C of R^ℓ is called a code over R of length ℓ, or more precisely, an (ℓ, M) code over R, where $M = |C|$ denotes the cardinality of C; the code C over R is said to be linear if C is an R-submodule of R^ℓ. Recall that the usual Hamming weight w_H on R, i.e., $w_H(0) = 0$ and $w_H(r) = 1$ for all non-zero $r \in R$, induces in a standard way the *Hamming weight* on R^ℓ, denoted by w_H again, and the *Hamming distance* d_H on R^ℓ as follows: $w_H(\mathbf{x}) = \sum\limits_{i=1}^{\ell} w_H(x_i)$ for $\mathbf{x} = (x_1, \cdots, x_\ell) \in R^\ell$, and $d_H(\mathbf{x}, \mathbf{x}') = w_H(\mathbf{x} - \mathbf{x}')$ for $\mathbf{x}, \mathbf{x}' \in R^\ell$. We also let $d_H(C) = \min\limits_{\mathbf{c} \neq \mathbf{c}' \in C} d_H(\mathbf{c}, \mathbf{c}')$. This is known as the *minimum Hamming distance* of the code C.

On the other hand, a *homogeneous weight* on the finite commutative ring R is defined to be a non-negative real function w_h from R to the real number field which satisfies the following two conditions:

- $w_h(r) = w_h(r')$ for $r, r' \in R$, provided $Rr = Rr'$,
- there is a positive real number λ such that $\sum\limits_{x \in Rr} w_h(x) = \lambda |Rr|$ for any non-zero $r \in R$, where $|Rr|$ denotes the cardinality of the set Rr.

It has been shown in [7] that such a function is uniquely determined (up to a scalar λ) on R as follows

$$w_h(r) = \lambda \left(1 - \frac{\mu(0, Rr)}{\varphi(Rr)}\right), \tag{2.1}$$

where μ is the Möbius function on the lattice of all the principal ideals of R, and $\varphi(Rr)$ denotes the number of elements $x \in Rr$ such that $Rx = Rr$. Thus, the homogeneous weight is uniquely determined up to a positive multiple λ. In the rest of the paper, we always take $\lambda = 1$ in (2.1) for convenience, and denote the uniquely determined homogeneous weight by w_h. As with the Hamming weight, the function w_h on the ring R induces a function w_h on R^ℓ and a two-variable function d_h on R^ℓ; and $d_h(C) = \min\limits_{\mathbf{c}\neq\mathbf{c}'\in C} d_h(\mathbf{c},\mathbf{c}')$ is said to be the *minimum homogeneous distance* of the code C.

Let $A = (a_{ij})_{m\times\ell}$ be an $m \times \ell$ matrix over the finite commutative ring R, and let $C_1, \cdots, C_m$ be codes over R of length n. Then

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

is called a *matrix product code*, where the codewords $\mathbf{c}_j$ of C_j are written as column vectors, hence $(\mathbf{c}_1, \cdots, \mathbf{c}_m)$ are $n \times m$ matrices.

We say that a square matrix over R is *non-singular* if its determinant is a unit of R. By usual linear algebra, a non-singular matrix over R is an invertible matrix over R. Following [1], we say that the $m \times \ell$ matrix A is *non-singular by columns* if, for any $k \le m$, any $k \times k$ determinant within the first k rows of A is a unit of R. It is clear that, if A is non-singular by columns, then any matrix obtained from A by permuting its columns is still non-singular by columns. We say that a matrix A is *column-permutably upper triangular* if A can be transformed by some suitable permutation of the columns to an upper triangular matrix $A' = (a'_{ij})_{m\times\ell}$ (i.e., $a'_{ij} = 0$ for all $1 \le j < i \le m$).

From now on, we always assume that R is a finite commutative *principal ideal ring*, i.e., R is a finite commutative ring in which any ideal can be generated by one element, or equivalently, there are finite chain rings $R_1, \cdots, R_s$ and an isomorphism:

$$R \xrightarrow{\cong} R_1 \times \cdots \times R_s\,, \qquad r \longmapsto (r_1, \cdots, r_s). \tag{2.2}$$

With this isomorphism, we can identify R with $R_1 \times \cdots \times R_s$ and write $r = (r_1, \cdots, r_s)$. For $t = 1, \cdots, s$, by J_t we denote the unique maximal ideal of the chain ring R_t (note that $J_t = 0$ if R_t is a field). Hence R_t/J_t is a finite field, and we further assume that

$$F_t = R_t/J_t \cong \mathrm{GF}(q_t) \ \text{ for } t = 1, \cdots, s, \quad \text{and} \ \ q_1 \le q_2 \le \cdots \le q_s, \tag{2.3}$$

where $\mathrm{GF}(q_t)$ denotes the Galois field of order q_t. For each t, there is an integer $e_t \ge 1$, called the *nilpotency index of the chain ring R_t*, such that

$$J_t^{e_t-1} \ne 0 \quad \text{but} \quad J_t^{e_t} = 0, \qquad t = 1, \cdots, s. \tag{2.4}$$

Note that $J_t^0 = R_t$ for any t.

We list some easy facts for later use. Since any ideal I of R has the form $I = I_1 \times \cdots \times I_s$ with I_t being an ideal of R_t for $t = 1, \cdots, s$, it follows that $R/I = R_1/I_1 \times \cdots \times R_s/I_s$ is still a principal ideal ring.

Next, if elements $u_{t1}, u_{t2}, \cdots, u_{tq_t}$ of R_t satisfy that

$$F_t = R_t/J_t = \big\{u_{t1} + J_t,\, u_{t2} + J_t,\, \cdots,\, u_{tq_t} + J_t\big\},$$

then, for any integer k with $0 < k \le e_t$ and any element a of the set difference $J_t^{k-1} \setminus J_t^k$, we have that

$$J_t^{k-1}/J_t^k = \big\{u_{t1}a + J_t^k,\ u_{t2}a + J_t^k,\ \cdots,\ u_{tq_t}a + J_t^k\big\}. \tag{2.5}$$

Recall Formula (2.1) and rewrite it as (recall that we have set $\lambda = 1$):

$$w_h(r) = 1 - \tfrac{\mu(r)}{\varphi(r)},$$

where $\mu(r) = \mu(0, Rr)$ and $\varphi(r) = \varphi(Rr)$. Since R is a product of chain rings as in Eqn (2.2) and $(r_1, \cdots, r_s) \in R_1 \times \cdots \times R_s$, both μ and φ satisfy that

$$\mu\big((r_1, \cdots, r_s)\big) = \mu(r_1)\cdots\mu(r_s), \quad \varphi\big((r_1, \cdots, r_s)\big) = \varphi(r_1)\cdots\varphi(r_s);$$

thus, the homogeneous weight w_h on R is (see [5, Theorem 4.1])

$$w_h(r) = w_h(r_1, \cdots, r_s) = 1 - \textstyle\prod_{t=1}^{s} \frac{\mu(r_t)}{\varphi(r_t)}.$$

Further, for $r_t \in R_t$, there is (as long as $r_t \ne 0$) a unique integer f_{r_t} with $0 < f_{r_t} \le e_t$ such that $r_t \in J_t^{e_t - f_{r_t}} \setminus J_t^{e_t - f_{r_t} + 1}$, then we have (see [5] for details):

$$\mu(r_t) = \begin{cases} 1, & r_t = 0, \\ -1, & f_{r_t} = 1, \\ 0, & f_{r_t} > 1, \end{cases} \qquad \varphi(r_t) = \begin{cases} 1, & r_t = 0, \\ q_t - 1, & f_{r_t} = 1, \\ q_t^{f_{r_t}} - q_t^{f_{r_t}-1}, & f_{r_t} > 1. \end{cases}$$

For a non-zero element $r = (r_1, \cdots, r_s)$ of R, setting

$$T_r = \{1 \le t \le s \mid r_t \ne 0\}, \qquad \bar{T}_r = \{t \in T_r \mid r_t \in J_t^{e_t - 1}\}, \tag{2.6}$$

we obtain a formula to calculate the homogeneous weight on R as follows:

$$w_h(r_1, \cdots, r_s) = \begin{cases} 0, & r = 0, \\ 1, & \bar{T}_r \ne T_r, \\ 1 - (-1)^{|T_r|} \prod\limits_{t \in T_r} \frac{1}{q_t - 1}, & \bar{T}_r = T_r. \end{cases} \tag{2.7}$$

From Formula (2.7) one can see that (take any $q_2 \ge q_1$ if $s = 1$):

$$1 - \tfrac{1}{(q_1-1)(q_2-1)} \le w_h(r) \le 1 + \tfrac{1}{q_1 - 1}, \qquad \forall\ \ 0 \ne r \in R. \tag{2.8}$$

We next recall a few facts on matrices over a finite commutative principal ideal ring R. For any t, by (2.3), we have a surjective homomorphism

$$\rho_t :\ R \longrightarrow F_t, \qquad r \longmapsto \rho_t(r) \tag{2.9}$$

with kernel $I_t = R_1 \times \cdots \times R_{t-1} \times J_t \times R_{t+1} \times \cdots \times R_s$, i.e., $R/I_t \cong R_t/J_t = F_t$. By a fundamental argument on determinants in linear algebra, one can prove (alternatively, a proof may be found in classical references such as [14]):

Lemma 2.1. *Let $A = (a_{ij})_{m\times\ell}$ be an $m \times \ell$ matrix over R.*

(i) If A is non-singular by columns, then, for any non-trivial quotient ring $\bar{R} = R/I$ (i.e., I is an ideal of R with $I \neq R$), the matrix $\bar{A} = \big(\bar{a}_{ij}\big)_{m\times\ell}$ over $\bar{R}$ is non-singular by columns.

(ii) If the matrix $\rho_t(A) = \big(\rho_t(a_{ij})\big)_{m\times\ell}$ over F_t is non-singular by columns for all $t = 1, \cdots, s$, then A is non-singular by columns.

By the above lemma and with the help of Eqn (2.5), it is easy to prove the following result which is an extension of [1, Prop. 3.3] and [17, Prop. 1].

Lemma 2.2. *Assume that $m > 1$. There exists an $m \times \ell$ matrix over R which is non-singular by columns if and only if $m \le \ell \le \min\{q_1, \cdots, q_s\}$.*

The following result has appeared in [3, Lemma 4.1].

Lemma 2.3. *Assume that an $m\times\ell$ matrix A over R is non-singular by columns and $1 \le k \le m$. Then the minimum Hamming distance of the linear code in R^ℓ generated by the first k rows of A is $\ell - k + 1$.*

3 The main results

We keep the notations of (2.2), (2.3) and (2.4). In this section, we state our main theorem, its corollaries and some remarks. The main theorem will be proved in the next section.

Theorem 3.1. *Let the notations be as in (2.2) and (2.3), and assume that $q_2 > q_1 + 1$ provided $s > 1$. Let $A = (a_{ij})_{m\times\ell}$ be an $m \times \ell$ matrix over R which is non-singular by columns, and let C_j be an (n, M_j) code over R, for $j = 1, \cdots, m$. Then $C = [C_1, \cdots, C_m]A$ is an $\big(n\ell, \prod_{j=1}^{m} M_j\big)$-code over R with*

$$d_h(C) \ge \min\big\{\ell d_h(C_1),\ (\ell-1)d_h(C_2),\ \cdots,\ (\ell-m+1)d_h(C_m)\big\}. \tag{3.1}$$

Furthermore, equality holds in (3.1) if one of the following conditions is satisfied:

(C1) *A is column-permutably upper triangular;*

(C2) *$C_1, C_2, \cdots, C_m$ are linear codes and $C_1 \supseteq C_2 \supseteq \cdots \supseteq C_m$.*

With the help of the results in [3], we have a consequence of the theorem for the dual codes of matrix product codes.

Corollary 3.2. *Keep the notations as in (2.2), (2.3), and assume that $q_2 > q_1 + 1$ provided $s > 1$. If A is an $m \times m$ matrix over R which is non-singular by columns, and C_j is an (n, M_j)-linear code over R, for $j = 1, \cdots, m$,* *then the dual code $C^\perp$ of the matrix product code $C = [C_1, \cdots, C_m]A$ is an $\big(nm,\ \prod_{j=1}^{m} (|R|^n/M_j)\big)$-linear code over R with*

$$d_h(C^\perp) \ge \min\big\{md_h(C_m^\perp),\ (m-1)d_h(C_{m-1}^\perp),\ \cdots,\ 1\cdot d_h(C_1^\perp)\big\}.$$

Furthermore, equality holds if one of the following conditions is satisfied:

(C1) *A is column-permutably upper triangular;*

(C2) *$C_1, C_2, \cdots, C_m$ are linear codes and $C_1 \supseteq C_2 \supseteq \cdots \supseteq C_m$.*

Proof. For a square matrix A over R which is non-singular by columns, it is shown in [3, Theorem 3.3] that A is invertible and $J(A^{-1})^T$ is non-singular by columns too, where $(A^{-1})^T$ denotes the transpose of the inverse A^{-1} and

$$J = \begin{pmatrix} 0 & \cdots & 0 & 1 \\ 0 & \cdots & 1 & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 1 & \cdots & 0 & 0 \end{pmatrix},$$

and $C^\perp = [C_1^\perp, \cdots, C_m^\perp](A^{-1})^T$. Noting that $JJ = I$, where I denotes the identity matrix, and $[C_1^\perp, \cdots, C_m^\perp]J = [C_m^\perp, \cdots, C_1^\perp]$, we have that

$$C^\perp = [C_1^\perp, \cdots, C_m^\perp]JJ(A^{-1})^T = [C_m^\perp, \cdots, C_1^\perp]J(A^{-1})^T.$$

It is easy to check that, if A satisfies (C1) then so does $J(A^{-1})^T$; and similarly for (C2). Thus the conclusions are derived from Theorem 3.1. □

In fact, in [3], a very precise description for the structure of $C^\perp$, where $C = [C_1, \cdots, C_m]A$, was obtained in a more general setting, where R is any finite commutative Frobenius ring and A does not need to be square and non-singular by columns. It is therefore possible to obtain a lower bound for the minimum homogeneous distance of $C^\perp$ in that general setting, see [4].

Remark 3.3. In the case when $s = 1$, i.e., R is a finite chain ring, Theorem 3.1 contains the result [17, Proposition 2] and a generalization of the main result of [9]; moreover, Corollary 3.2 bounds from below the homogeneous distance of the dual codes of matrix product codes.

The residue ring $\mathbf{Z}_N$ of integers modulo an integer $N > 1$ is one of the best-known finite principal ideal rings. Writing $N = p_1^{e_1} \cdots p_s^{e_s}$, where $p_1 < \cdots < p_s$ are primes and $e_t > 0$ for $t = 1, \cdots, s$, we see that the Chinese Remainder Theorem:

$$\begin{array}{ccc} \mathbf{Z}_N & \cong & \mathbf{Z}_{p_1^{e_1}} \times \cdots \times \mathbf{Z}_{p_s^{e_s}}, \\ r \pmod N & \mapsto & \big(r \pmod{p_1^{e_1}},\ \cdots,\ r \pmod{p_s^{e_s}}\big), \end{array}$$

is just the version for $\mathbf{Z}_N$ of the decomposition (2.2). Therefore, the assumption "$q_2 > q_1 + 1$ provided $s > 1$" in Theorem 3.1 translates into the assumption "$p_2 \ne 3$ provided $p_1 = 2$" for $\mathbf{Z}_N$; and we obtain the following result from Theorem 3.1 at once.

Corollary 3.4. *Let $N > 1$ be an integer which is not divisible by 6. Let A be an $m \times \ell$ matrix over $\mathbf{Z}_N$ which is non-singular by columns, and let C_j be an (n, M_j)-code over $\mathbf{Z}_N$, for $j = 1, \cdots, m$. Then $C = [C_1, \cdots, C_m]A$ is an $\big(n\ell, \prod_{j=1}^{m} M_j\big)$-code over $\mathbf{Z}_N$ with*

$$d_h(C) \ge \min\big\{\ell d_h(C_1),\ (\ell-1)d_h(C_2),\ \cdots,\ (\ell-m+1)d_h(C_m)\big\}. \tag{3.2}$$

Furthermore, equality holds if one of the following conditions is satisfied:

(C1) *A is column-permutably upper triangular;*

(C2) *$C_1, C_2, \cdots, C_m$ are linear codes and $C_1 \supseteq C_2 \supseteq \cdots \supseteq C_m$.*

There is also an analogous version of Corollary 3.2 for $\mathbf{Z}_N$, with the same assumption "N is not divisible by 6".

Remark 3.5. Recall that, to be a geometric distance, a two-variable real function must meet three conditions: it is positive, it is symmetric, and it satisfies the triangle inequality. It is known that the homogeneous distance d_h may not be a geometric distance. References [2] and [12] contain extensive studies on weights on integral residue rings: in particular, a necessary and sufficient condition for the homogeneous distance d_h on $\mathbf{Z}_N^\ell$ to be a geometric distance is that N is not divisible by 6. By Corollary 3.4 and Example 3.6 below, this condition is also necessary and sufficient for Inequality (3.2) to hold.

The assumption "$q_2 > q_1 + 1$ provided $s > 1$" in Theorem 3.1 will play a crucial role in the proof of the theorem. Moreover, the following example illustrates that the assumption cannot be removed.

Example 3.6. Let the notations be as in (2.2), (2.3) and (2.4). Assume that $s > 1$ and $q_1 + 1 = q_2 \le q_3 \le \cdots \le q_s$ and let $q = q_1$. Let $u_{t1}, u_{t2}, \cdots, u_{tq_t} \in R_t$ be as in Eqn (2.5). In the present case, we can choose them as follows:

- for $t = 1$, $u_{11} + J_1,\ \cdots, u_{1q} + J_1$ are just all the elements of $F_1 = R_1/J_1$;
- for $t = 2$, since $q_2 = q + 1$, we can take $u_{21} + J_2,\ \cdots,\ u_{2q} + J_2$ to be all non-zero elements of $F_2 = R_2/J_2$;
- for $t \ge 3$, since $q_t > q$, we can take $u_{t1} + J_t,\ \cdots,\ u_{tq} + J_t$ to be distinct elements of $F_t = R_t/J_t$.

Let $\beta_j = (u_{1j}, u_{2j}, \cdots, u_{sj}) \in R = R_1 \times \cdots \times R_s$ for $j = 1, \cdots, q$, and let

$$A = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \beta_1 & \beta_2 & \cdots & \beta_q \end{pmatrix}.$$

It is easy to see (cf. Lemma 2.2) that A is non-singular by columns. Let

$$a = (a_1, 0, 0, \cdots, 0),\ b = (0, b_2, 0, \cdots, 0) \in R = R_1 \times \cdots \times R_s,$$

where $a_1 \in J_1^{e_1-1} \setminus \{0\}$ and $b_2 \in J_2^{e_2-1} \setminus \{0\}$. Set $C_1 = Ra$ and $C_2 = Rb$, then both are linear codes over R of length 1. Then we have the matrix product code $C = [C_1, C_2]A$. By Formula (2.7), we have that

$$d_h(C_1) = w_h(a) = 1 + \tfrac{1}{q-1}\,, \quad d_h(C_2) = w_h(b) = 1 + \tfrac{1}{q_2-1} = 1 + \tfrac{1}{q}.$$

Since $1 + \frac{1}{q-1} > 1 + \frac{1}{q}$, we get

$$\min\{q d_h(C_1),\, (q-1)d_h(C_2)\} = (q-1)\big(1+\tfrac{1}{q}\big) = q - \tfrac{1}{q}.$$

On the other hand, there is a codeword $\mathbf{c}$ of C as follows:

$$\mathbf{c} = (a,b)A = (a + b\beta_1,\ a + b\beta_2,\ \cdots,\ a + b\beta_q)$$

with

$$a + b\beta_j = (a_1,\ b_2 u_{2j},\ 0, \cdots, 0), \qquad j = 1, \cdots, q.$$

By Eqn (2.5), $b_2 u_{2j}$, for $j = 1, \cdots, q$, are all the non-zero elements of $J_2^{e_2-1}$, and by Formula (2.7), $w_h(a + b\beta_j) = 1 - \frac{1}{(q_1-1)(q_2-1)} = 1 - \frac{1}{q(q-1)}$, so

$$w_h(\mathbf{c}) = q\big(1 - \tfrac{1}{q(q-1)}\big) = q - \tfrac{1}{q-1} < q - \tfrac{1}{q} = \min\{q d_h(C_1),\, (q-1)d_h(C_2)\}.$$

Therefore,

$$d_h(C) < \min\{q d_h(C_1),\, (q-1)d_h(C_2)\},$$

which implies that Inequality (3.1) does not hold for the matrix product code $C = [C_1, C_2]A$.

4 Proof of Theorem 3.1

We continue to keep the notations of (2.2), (2.3) and (2.4) and assume that $q = q_1 \le q_2 \le \cdots \le q_s$.

Let $A = (a_{ij})_{m\times\ell}$ be a matrix over R which is non-singular by columns; then $\ell \le q = q_1$ if $m > 1$ (see Lemma 2.2). Let $C_1, \cdots, C_m$ be codes over R of length n. Consider the matrix product code

$$C = [C_1, \cdots, C_m]A = \{(\mathbf{c}_1, \cdots, \mathbf{c}_m)A \,|\, \mathbf{c}_1 \in C_1,\, \cdots,\, \mathbf{c}_m \in C_m\}\,. \tag{4.1}$$

Since the proof of Inequality (3.1) is long and delicate, we put the key steps in Subsections 4.1–4.3; these subsections show that the following inequality holds for all $1 \le k \le m$ by splitting into various cases:

$$w_h\big((\mathbf{c}_1, \cdots, \mathbf{c}_k, \mathbf{0}, \cdots, \mathbf{0})A\big) \ge (\ell - k + 1) w_h(\mathbf{c}_k).$$

Subsection 4.4 then completes the proof of Theorem 3.1.

4.1 $k \times \ell$ Non-singular by Columns Matrices

Let A be as above, let $2 \le k \le m$, and let $A_1, \cdots, A_k$ be the first k rows of A.

Let $r_1, \cdots, r_k \in R$ with $r_k \neq 0$ and let $\alpha = r_1A_1 + \cdots + r_kA_k \in R^\ell$. We have seen from Lemma 2.3 that

$$w_H(\alpha) = w_H(r_1A_1 + \cdots + r_kA_k) \ge \ell - k + 1.$$

Lemma 4.1. *Let the notations be as above.*

(i) If $w_H(r_1A_1 + \cdots + r_kA_k) = \ell - k + 1$, then $w_h(r_1A_1 + \cdots + r_kA_k) = (\ell - k + 1)w_h(r_k)$.

(ii) If $w_H(r_1A_1 + \cdots + r_kA_k) > \ell - k + 1$ and one of the following two conditions holds:

- *$k \ge 3$,*
- *$k = 2$ and $\ell < q_1$,*

then $w_h(r_1A_1 + \cdots + r_kA_k) \ge (\ell - k + 1)w_h(r_k)$.

Proof. Write $\alpha = r_1A_1 + \cdots + r_kA_k = (\alpha_1, \cdots, \alpha_\ell)$, where

$$\alpha_j = r_1a_{1j} + \cdots + r_ka_{kj}, \qquad j = 1, \cdots, \ell.$$

(i) Since $w_H(r_1A_1 + \cdots + r_kA_k) = \ell - k + 1$, there are exact $k-1$ zeros among $\alpha_1, \cdots, \alpha_\ell$. Without loss of generality, we assume that $\alpha_1 = \cdots = \alpha_{k-1} = 0$ and $\alpha_j \neq 0$, for $j = k, k+1, \cdots, \ell$. In particular,

$$\begin{cases} r_1a_{11} + \cdots + r_{k-1}a_{k-1,1} & = & -r_ka_{k1} \\ r_1a_{12} + \cdots + r_{k-1}a_{k-1,2} & = & -r_ka_{k2} \\ \vdots \quad \vdots \quad \vdots & & \vdots \\ r_1a_{1,k-1} + \cdots + r_{k-1}a_{k-1,k-1} & = & -r_ka_{k,k-1}. \end{cases}$$

By the non-singularity by columns of A, the coefficient matrix $(a_{ji})_{(k-1)\times(k-1)}$ of the above linear system is non-singular, i.e., invertible, hence $r_1, \cdots, r_{k-1}$ are all linear combinations of $r_ka_{k1}, \cdots, r_ka_{k,k-1}$. Therefore, $r_j \in Rr_k$ for $j = 1, \cdots, k-1, k$; hence all $\alpha_j \in Rr_k$, i.e.,

$$0 \neq R\alpha_j \subseteq Rr_k\,, \qquad j = k, k+1, \cdots, \ell.$$

Suppose that there is an index t with $k \le t \le \ell$ such that $R\alpha_t \subsetneqq Rr_k$. Considering the quotient ring $\bar{R} = R/R\alpha_t$, then $\bar{r}_k \neq 0$ and $\bar{A} = (\bar{a}_{ij})_{m\times\ell}$ is still non-singular by columns (see Lemma 2.1). However,

$$\bar{\alpha}_1 = \cdots = \bar{\alpha}_{k-1} = 0 \quad \text{and} \quad \bar{\alpha}_t = 0,$$

hence

$$w_H(\bar{r}_1\bar{A}_1 + \cdots + \bar{r}_k\bar{A}_k) \le \ell - k < \ell - k + 1,$$

which contradicts the fact that $w_H(\bar{r}_1\bar{A}_1 + \cdots + \bar{r}_k\bar{A}_k) \geq \ell - k + 1$ (see Lemma 2.3). Therefore, $R\alpha_j = Rr_k$ for all $j = k, k+1, \cdots, \ell$, and

$$w_h(r_1A_1 + \cdots + r_kA_k) = \sum_{j=k}^{\ell} w_h(\alpha_j) = \sum_{j=k}^{\ell} w_h(r_k) = (\ell - k + 1)w_h(r_k).$$

(ii) In this case, there are at least $\ell - k + 2$ non-zeros among $\alpha_1, \cdots, \alpha_\ell$. By Inequality (2.8), we get

$$w_h(\alpha) \geq (\ell - k + 2)\left(1 - \tfrac{1}{(q_1-1)(q_2-1)}\right) \tag{4.2}$$

and

$$(\ell - k + 1)\left(1 + \tfrac{1}{q_1-1}\right) \geq (\ell - k + 1)w_h(r_k). \tag{4.3}$$

It is an elementary calculation to check that

$$(x+1)\left(1 - \tfrac{1}{(q_1-1)(q_2-1)}\right) \geq x\left(1 + \tfrac{1}{q_1-1}\right) \iff x \leq q_1 - 1 - \tfrac{q_1}{q_2}. \tag{4.4}$$

Recall that $\ell \leq q_1 \leq q_2$. If $k \geq 3$, or if $k = 2$ and $\ell < q_1$, then $\ell - k + 1 \leq q_1 - 1 - \frac{q_1}{q_2}$. In both cases, we can apply Formula (4.4) to (4.2) and (4.3), with $x = \ell - k + 1$, and obtain $w_h(\alpha) \geq (\ell - k + 1)w_h(r_k)$. □

Proposition 4.2. *Let A and $\mathbf{c}_1 \in C_1, \cdots, \mathbf{c}_k \in C_k$ be as in (4.1) and assume that $\mathbf{c}_k \neq \mathbf{0}$. If one of the following two conditions holds:*

- $k \geq 3$,
- $k = 2$ *and* $\ell < q_1$,

then

$$w_h\big((\mathbf{c}_1, \cdots, \mathbf{c}_k, \mathbf{0}, \cdots, \mathbf{0})A\big) \geq (\ell - k + 1)w_h(\mathbf{c}_k).$$

Proof. Let $c_{i_1k}, \cdots, c_{i_wk}$ be all the non-zero entries of $\mathbf{c}_k = (c_{1k}, \cdots, c_{nk})^T$. Then $w_h(\mathbf{c}_k) = w_h(c_{i_1k}) + \cdots + w_h(c_{i_wk})$. Noting that the ith row of the matrix $(\mathbf{c}_1, \cdots, \mathbf{c}_k, \mathbf{0}, \cdots, \mathbf{0})A$ is $c_{i1}A_1 + \cdots + c_{ik}A_k$, where $A_1, \cdots, A_k$ are as above, we have

$$\begin{aligned} w_h\big((\mathbf{c}_1, \cdots, \mathbf{c}_k, \mathbf{0}, \cdots, \mathbf{0})A\big) &= \textstyle\sum_{i=1}^{n} w_h\big(c_{i1}A_1 + \cdots + c_{ik}A_k\big) \\ &\geq \textstyle\sum_{t=1}^{w} w_h\big(c_{i_t1}A_1 + \cdots + c_{i_tk}A_k\big) \\ &\geq \textstyle\sum_{t=1}^{w} (\ell - k + 1)w_h(c_{i_tk}) \\ &= (\ell - k + 1)w_h(\mathbf{c}_k), \end{aligned}$$

where the second "$\geq$" follows from Lemma 4.1. □

4.2 $2 \times q_1$ Non-singular by Columns Matrices

In the following, we let $q = q_1$ and assume that $A = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \beta_1 & \beta_2 & \cdots & \beta_q \end{pmatrix}$ is a $2 \times q$ matrix over R which is non-singular by columns. Write

$$\beta_j = (u_{1j}, u_{2j}, \cdots, u_{sj}) \in R_1 \times R_2 \times \cdots \times R_s.$$

Let $a, b \in R$ with $b \neq 0$, and write $a = (a_1, \cdots, a_s)$ and $b = (b_1, \cdots, b_s)$ with $a_t, b_t \in R_t$ for $t = 1, \cdots, s$. Consider the word

$$\alpha = (a, b)A = (\alpha_1, \cdots, \alpha_q) \in R^q, \tag{4.5}$$

where

$$\alpha_j = a + b\beta_j = \big(a_1 + b_1 u_{1j},\ \cdots,\ a_s + b_s u_{sj}\big), \qquad j = 1, \cdots, q.$$

Then $w_H(\alpha) \geq q - 1$. From Lemma 4.1(i), we have seen that

$$w_h(\alpha) = (q-1)w_h(b) \qquad \text{if } \ w_H(\alpha) = q - 1. \tag{4.6}$$

In the following, we further assume that $\alpha_j \neq 0$ for all $j = 1, \cdots, q$.

Lemma 4.3. *If $w_h(b) = 1$, then $w_h(\alpha) \geq (q-1)w_h(b)$.*

Proof. Since $w_h(b) = 1$, there is at least one k such that $b_k \notin J_k^{e_k - 1}$. Take $I_k = R_1 \times \cdots \times R_{k-1} \times J_k^{e_k-1} \times R_{k+1} \times \cdots \times R_s$, and consider the quotient ring $\bar{R}_k := R/I_k \cong R_k/J_k^{e_k-1}$. Then the matrix $\bar{A}$ over $\bar{R}_k$ is still non-singular by columns (see Lemma 2.1), $\bar{b} = \bar{b}_k \neq 0$, and the elements

$$\alpha_j = \big(a_1 + b_1 u_{1j},\ \cdots,\ a_k + b_k u_{kj},\ \cdots,\ a_s + b_s u_{sj}\big), \quad j = 1, \cdots, q,$$

are mapped to

$$\bar{\alpha}_j = \bar{a}_k + \bar{b}_k \bar{u}_{kj}, \qquad j = 1, \cdots, q.$$

Then, for the word $\bar{\alpha} = (\bar{a}, \bar{b})\bar{A} = \big(\bar{\alpha}_1, \cdots, \bar{\alpha}_q\big)$ over $\bar{R}_k$, its Hamming weight satisfies $w_H(\bar{\alpha}) \geq q - 1$. Since $q \geq 2$, there is at least one non-zero entry, say $\bar{\alpha}_t \neq 0$, i.e., $a_k + b_k u_{kt} \notin J_k^{e_k-1}$. Hence, $w_h(\alpha_t) = 1$. Noting that $w_h(\alpha_j) \geq 1 - \frac{1}{(q-1)(q_2-1)}$ for $j \neq t$ (see Formula (2.8)), we have

$$w_h(\alpha) = \sum_{j=1}^{q} w_h(\alpha_j) \geq 1 + (q-1)\left(1 - \tfrac{1}{(q-1)(q_2-1)}\right) \geq q - 1 = (q-1)w_h(b). \quad \square$$

Note that $w_h(b) \neq 1$ if and only if $b_t \in J_t^{e_t-1}$ for $t = 1, \cdots, s$.

Lemma 4.4. *If $b = (b_1, \cdots, b_s)$ with $b_t \in J_t^{e_t-1}$, for $t = 1, \cdots, s$, and $w_h(a) = 1$, then $w_h(\alpha) \geq (q-1)w_h(b)$.*

Proof. Similar to the proof above, we can assume that $a_k \notin J_k^{e_k-1}$ for some k. Since $b_k \in J_k^{e_k-1}$, it follows that $a_k + b_k u_{kj} \notin J_k^{e_k-1}$ for all $j = 1, \cdots, q$. Thus $w_h(\alpha_j) = 1$ for all $j = 1, \cdots, q$, and

$$w_h(\alpha) = \sum_{j=1}^{q} w_h(\alpha_j) = q = (q-1)\left(1 + \tfrac{1}{q-1}\right) \geq (q-1)w_h(b). \qquad \square$$

From now on, we further assume that

$$a = (a_1, \cdots, a_s),\ \ b = (b_1, \cdots, b_s) \ \text{ with } a_t, b_t \in J_t^{e_t-1} \ \text{ for } t = 1, \cdots, s, \tag{4.7}$$

and let

$$T_a = \{1 \leq t \leq s \mid a_t \neq 0\}, \quad T_b = \{1 \leq t \leq s \mid b_t \neq 0\}, \quad T = T_a \cup T_b. \tag{4.8}$$

Lemma 4.5. *Let $t_0 = \min_{t \in T} t$. If $q < q_{t_0}$, then $w_h(\alpha) \geq (q-1)w_h(b)$.*

Proof. Since $b = (0, \cdots, 0, b_{t_0}, \cdots, b_s)$, by Formula (2.7), we have that $w_h(b) \leq 1 + \frac{1}{q_{t_0}-1}$. On the other hand, $a_j + b_j u_{tj} = 0$ for any $t < t_0$, so

$$\alpha_j = (0, \cdots, 0, a_j + b_j u_{t_0 j}, \cdots, a_j + b_j u_{sj}),$$

hence $w_h(\alpha_j) \geq 1 - \frac{1}{(q_{t_0}-1)(q_{t_0+1}-1)}$ (when $t_0 = s$, set q_{t_0+1} to be any integer greater than q_{t_0}). Since $q - 1 \leq q_{t_0} - 2 \leq q_{t_0} - 1 - \frac{q_{t_0}}{q_{t_0+1}}$, we can use (4.4) to obtain

$$\begin{aligned} w_h(\alpha) &= \sum_{j=1}^{q} w_h(\alpha_j) \geq q\left(1 - \tfrac{1}{(q_{t_0}-1)(q_{t_0+1}-1)}\right) \\ &\geq (q-1)\left(1 + \tfrac{1}{q_{t_0}-1}\right) \geq (q-1)w_h(b). \qquad \square \end{aligned}$$

In the following, we further assume that

$$1 \in T\,, \quad \text{and} \quad q_2 > q_1 + 1 \text{ if } s > 1. \tag{4.9}$$

Lemma 4.6. *If $T_b = \{t'\}$ contains only one index t' with $1 \leq t' \leq s$, then $w_h(\alpha) \geq (q-1)w_h(b)$.*

Proof. First, assume that $t' = 1$. Then $b = (b_1, 0, \cdots, 0) \in R_1 \times \cdots \times R_s$ with $0 \neq b_1 \in J_1^{e_1-1}$, so $w_h(b) = 1 + \frac{1}{q-1}$ (recall that $q = q_1$), and

$$\alpha_j = \big(a_1 + b_1 u_{1j},\ a_2,\ \cdots,\ a_s\big).$$

Taking $I = J_1 \times R_2 \times \cdots \times R_s$ and $\bar{R} = R/I \cong R_1/J_1 = F_1$, then

$$\bar{A} = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \bar{u}_{11} & \bar{u}_{12} & \cdots & \bar{u}_{1q} \end{pmatrix}$$

is a matrix over the field F_1 which is still non-singular by columns, so as elements of the field F_1, the entries $\bar{u}_{11}, \bar{u}_{12}, \cdots, \bar{u}_{1q}$ must be distinct. Since $|F_1| = q$, we conclude that $\bar{u}_{11}, \bar{u}_{12}, \cdots, \bar{u}_{1q}$ must consist of all the elements of F_1. By Eqn (2.5), $b_1 u_{11},\ b_1 u_{12},\ \cdots,\ b_1 u_{1q}$ are just all the elements of $J_1^{e_1-1}$, hence

$$a_1 + b_1 u_{11},\ a_1 + b_1 u_{12},\ \cdots,\ a_1 + b_1 u_{1q}$$

are again just all the elements of $J_1^{e_1-1}$. In other words, exactly one of them is 0, and the other $(q-1)$ terms are non-zero. By Formula (2.7),

$$w_h(\alpha_j) = \begin{cases} 1 - (-1)^{|T|} \cdot \prod\limits_{t \in T} \frac{1}{q_t - 1}\,, & \text{if } a_1 + b_1 u_{1j} \neq 0, \\ 1 + (-1)^{|T|} \cdot \prod\limits_{1 \neq t \in T} \frac{1}{q_t - 1}\,, & \text{if } a_1 + b_1 u_{1j} = 0. \end{cases}$$

Therefore,

$$\begin{aligned} w_h(\alpha) &= \sum_{j=1}^{q} w_h(\alpha_j) \\ &= \left(1 + (-1)^{|T|} \cdot \prod_{1 \neq t \in T} \frac{1}{q_t - 1}\right) + (q-1)\left(1 - (-1)^{|T|} \cdot \prod_{t \in T} \frac{1}{q_t - 1}\right) \\ &= 1 + (-1)^{|T|} \cdot \prod_{1 \neq t \in T} \frac{1}{q_t - 1} + (q-1) - (-1)^{|T|} \cdot \prod_{1 \neq t \in T} \frac{1}{q_t - 1} \\ &= q = (q-1)\left(1 + \frac{1}{q-1}\right) = (q-1) w_h(b). \end{aligned}$$

Note that the above argument still works well for $T = \{1\}$ (in particular, it works well for $s = 1$) provided we adopt the convention that $\prod\limits_{1 \neq t \in T} \frac{1}{q_t - 1} = 1$.

Next, we assume that $t' > 1$. Then $s \geq 2$ and

$$w_h(b) \leq 1 + \tfrac{1}{q_2 - 1},$$

$$w_h(\alpha_j) \geq 1 - \tfrac{1}{(q-1)(q_2-1)}, \qquad j = 1, \cdots, q.$$

Since $q_2 \geq q + 2$, i.e., $q_2 - 1 \geq q + 1$, and $q \geq 2$, it follows that:

$$\begin{aligned} w_h(\alpha) - (q-1) w_h(b) &\geq q\left(1 - \tfrac{1}{(q-1)(q_2-1)}\right) - (q-1)\left(1 + \tfrac{1}{q_2-1}\right) \\ &= 1 - \tfrac{q}{(q-1)(q_2-1)} - \tfrac{q-1}{q_2-1} \\ &= 1 - \tfrac{q}{(q-1)(q_2-1)} - \tfrac{(q-1)^2}{(q-1)(q_2-1)} \\ &\geq 1 - \tfrac{q + (q-1)^2}{(q-1)(q+1)} = \tfrac{q-2}{q^2-1} \geq 0. \end{aligned}$$

In other words, $w_h(\alpha) \geq (q-1) w_h(b)$. $\square$

Lemma 4.7. *If $|T_b| \ge 2$, then $w_h(\alpha) \ge (q-1)w_h(b)$.*

Proof. By Formula (2.7), $w_h(b) = 1 - (-1)^{|T_b|} \prod\limits_{t \in T_b} \frac{1}{q_t - 1}$, thus

$$w_h(b) \le 1 + \frac{1}{(q-1)(q_2-1)(q_3-1)}$$

(put any $q_3 \ge q_2$ if $s = 2$). On the other hand, by (2.8), we have

$$w_h(\alpha_j) \ge 1 - \frac{1}{(q-1)(q_2-1)}.$$

Noting that $q_2 - 1 \ge q + 1$ and $q_3 - 1 > q - 1 \ge 1$, we have that

$$\begin{array}{ll} & w_h(\alpha) - (q-1)w_h(b) \\ \ge & q\left(1 - \frac{1}{(q-1)(q_2-1)}\right) - (q-1)\left(1 + \frac{1}{(q-1)(q_2-1)(q_3-1)}\right) \\ = & 1 - \frac{q}{(q-1)(q_2-1)} - \frac{1}{(q_2-1)(q_3-1)} \\ > & 1 - \frac{q}{(q-1)(q+1)} - \frac{1}{(q+1)(q-1)} \\ = & 1 - \frac{1}{q-1} \;\ge\; 0. \end{array}$$

We have obtained the desired inequality $w_h(\alpha) \ge (q-1)w_h(b)$. □

Summarizing Eqn (4.6) and Lemmas 4.3–4.7, we have that, if $q_2 > q_1 + 1$ provided $s > 1$, then the homogeneous weight of the word (4.5) satisfies

$$w_h\big((a,b)A\big) \ge (q-1)w_h(b). \tag{4.10}$$

Thus, similar to Proposition 4.2, we obtain the following conclusion.

Proposition 4.8. *Let $A = (a_{ij})_{m \times q_1}$ be non-singular by columns, and let $\mathbf{c}_1 \in C_1$, $\mathbf{c}_2 \in C_2$ and $\mathbf{c}_2 \ne \mathbf{0}$. Assume the following condition holds*

- $q_2 > q_1 + 1$ *provided* $s > 1$.

Then

$$w_h\big((\mathbf{c}_1, \mathbf{c}_2, \mathbf{0}, \cdots, \mathbf{0})A\big) \ge (q_1 - 1)w_h(\mathbf{c}_2).$$

Proof. It is clear that, for any $q_1 \times q_1$ diagonal matrix D whose diagonal entries are all units of R, we have that

$$w_h\big((\mathbf{c}_1, \mathbf{c}_2, \mathbf{0}, \cdots, \mathbf{0})AD\big) = w_h\big((\mathbf{c}_1, \mathbf{c}_2, \mathbf{0}, \cdots, \mathbf{0})A\big). \tag{4.11}$$

Since A is non-singular by columns, any element of the first row of A is a unit of R, so there is a suitable diagonal matrix D such that all entries of the first row of AD are 1. Thus, we can assume that the first row of A is the all-1 vector. Then, as in the proof of Proposition 4.2, we can obtain the conclusion of the proposition by using (4.10) . □

4.3 $1 \times \ell$ Non-singular by Columns Matrices

A $1\times\ell$ non-singular by columns matrix is none other than a matrix consisting of only one row, all of whose entries are units. This is essentially the key ingredient in the proof of the following result.

Proposition 4.9. *Let $A = (a_{ij})_{m\times\ell}$ be non-singular by columns, and $\mathbf{0} \neq \mathbf{c}_1 = (c_{11}, \cdots, c_{n1})^T \in C_1$. Then*

$$w_h\big((\mathbf{c}_1,\, \mathbf{0}, \cdots, \mathbf{0})A\big) \geq \ell w_h(\mathbf{c}_1).$$

Proof. By the non-singularity by columns of A, all the entries $a_{11}, \cdots, a_{1\ell}$ of the first row of A are units in R. Thus,

$$w_h\big((\mathbf{c}_1,\, \mathbf{0}, \cdots, \mathbf{0})A\big) = \sum_{j=1}^{\ell} w_h(a_{1j}\mathbf{c}_1) = \sum_{j=1}^{\ell} w_h(\mathbf{c}_1) = \ell w_h(\mathbf{c}_1). \qquad \square$$

4.4 Completion of the Proof of Theorem 3.1

Now we can complete the proof of Theorem 3.1.

First, we prove Inequality (3.1).

Let $\mathbf{c} = (\mathbf{c}_1, \cdots, \mathbf{c}_m)A$ and $\mathbf{c}' = (\mathbf{c}'_1, \cdots, \mathbf{c}'_m)A$ be any two distinct codewords of the code C. Then, not all of $\mathbf{b}_j = \mathbf{c}_j - \mathbf{c}'_j$, for $j = 1, \cdots, m$, are zero. Hence, $\mathbf{c} - \mathbf{c}' = (\mathbf{b}_1, \cdots, \mathbf{b}_m)A \neq \mathbf{0}$ and

$$d_h(\mathbf{c}, \mathbf{c}') = w_h(\mathbf{c} - \mathbf{c}') = w_h\big((\mathbf{b}_1, \cdots, \mathbf{b}_m)A\big).$$

It is enough to show that $d_h(\mathbf{c}, \mathbf{c}')$ is bounded below by one of the entries in the braces of the right hand side of (3.1) of Theorem 3.1. Since not all of $\mathbf{b}_1, \cdots, \mathbf{b}_m$ are $\mathbf{0}$, there is an index k with $1 \leq k \leq m$ such that $\mathbf{b}_k \neq \mathbf{0}$ but $\mathbf{b}_{k+1} = \cdots = \mathbf{b}_m = \mathbf{0}$.

If $k = 1$, by Proposition 4.9, we have

$$d_h(\mathbf{c}, \mathbf{c}') = w_h\big((\mathbf{b}_1, \mathbf{0}, \cdots, \mathbf{0})A\big) \geq \ell w_h(\mathbf{b}_1) = \ell w_h(\mathbf{c}_1 - \mathbf{c}'_1) \geq \ell d_h(C_1).$$

Suppose that $k = 2$, then $m \geq 2$ and, by Lemma 2.2, $\ell \leq q_1$.

If $\ell < q_1$, by Proposition 4.2, we have

$$\begin{aligned} d_h(\mathbf{c}, \mathbf{c}') &= w_h\big((\mathbf{b}_1, \mathbf{b}_2, \mathbf{0}, \cdots, \mathbf{0})A\big) \geq (\ell - 1)w_h(\mathbf{b}_2) \\ &= (\ell - 1)w_h(\mathbf{c}_2 - \mathbf{c}'_2) \geq (\ell - 1)d_h(C_2). \end{aligned}$$

Otherwise, $\ell = q_1$, and by Proposition 4.8, we still have

$$d_h(\mathbf{c}, \mathbf{c}') = w_h\big((\mathbf{b}_1, \mathbf{b}_2, \mathbf{0}, \cdots, \mathbf{0})A\big) \geq (\ell - 1)w_h(\mathbf{b}_2) \geq (\ell - 1)d_h(C_2).$$

The remaining case is that of $k > 2$. By Proposition 4.2, we obtain

$$\begin{aligned} d_h(\mathbf{c}, \mathbf{c}') &= w_h\big((\mathbf{b}_1, \cdots, \mathbf{b}_k, \mathbf{0}, \cdots, \mathbf{0})A\big) \geq (\ell - k + 1)w_h(\mathbf{b}_k) \\ &= (\ell - k + 1)w_h(\mathbf{c}_k - \mathbf{c}'_k) \geq (\ell - k + 1)d_h(C_k). \end{aligned}$$

Next, assume that A is column-permutably upper triangular. Since any permutation of columns does not change the weights and other parameters of the resulting codewords, we can assume that A is upper triangular:

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1m} & \cdots & a_{1\ell} \\ & a_{22} & \cdots & a_{2m} & \cdots & a_{2\ell} \\ & & \ddots & \vdots & \vdots & \vdots \\ & & & a_{mm} & \cdots & a_{m\ell} \end{pmatrix}.$$

Since A is non-singular by columns, every element of the first row is a unit of R. Similarly, every (2×2)-determinant within the first two rows is a unit, in particular, $\det \begin{pmatrix} a_{11} & a_{1j} \\ & a_{2j} \end{pmatrix}$ is a unit, i.e., every a_{2j}, for $j = 2, \cdots, \ell$, is a unit of R. Continuing this reasoning, we see that

- all a_{ij} for $1 \le i \le m$ and $i \le j \le \ell$ are units of R.

For any k with $1 \le k \le m$, take $\mathbf{c}_k, \mathbf{c}'_k \in C_k$ such that $d_h(\mathbf{c}_k, \mathbf{c}'_k) = d_h(C_k)$. We have two codewords of C as follows:

$$\mathbf{c} = (\mathbf{0}, \cdots, \mathbf{0}, \mathbf{c}_k, \mathbf{0}, \cdots, \mathbf{0})A, \qquad \mathbf{c}' = (\mathbf{0}, \cdots, \mathbf{0}, \mathbf{c}'_k, \mathbf{0}, \cdots, \mathbf{0})A,$$

whose homogeneous distance is

$$\begin{aligned} d_h(\mathbf{c}, \mathbf{c}') &= w_h(\mathbf{c} - \mathbf{c}') = w_h\big((\mathbf{0}, \cdots, \mathbf{0}, \mathbf{c}_k - \mathbf{c}'_k, \mathbf{0}, \cdots, \mathbf{0})A\big) \\ &= w_h\big(\mathbf{0}, \cdots, \mathbf{0}, a_{kk}(\mathbf{c}_k - \mathbf{c}'_k), \cdots, a_{k\ell}(\mathbf{c}_k - \mathbf{c}'_k)\big) \\ &= \sum_{j=k}^{\ell} w_h\big(a_{kj}(\mathbf{c}_k - \mathbf{c}'_k)\big) = \sum_{j=k}^{\ell} w_h(\mathbf{c}_k - \mathbf{c}'_k) \\ &= (\ell - k + 1) d_h(C_k). \end{aligned}$$

Thus $d_h(C) \le \min\{\ell d_h(C_1), \cdots, (\ell - m + 1) d_h(C_m)\}$. It follows that equality must hold in (3.1).

Finally, assume that $C_1, \cdots, C_m$ are linear and $C_1 \supseteq \cdots \supseteq C_m$. Write $A = (a_{ij})_{m \times \ell}$. Since a_{11} is a unit of R, we can add a suitable multiple of the first row to the ith row, for each $2 \le i \le m$, such that the entries of the first column of A below a_{11} are changed into 0, that is, there are $b_{21}, \cdots, b_{m1} \in R$ such that

$$\begin{pmatrix} 1 & & & \\ b_{21} & 1 & & \\ \vdots & & \ddots & \\ b_{m1} & & & 1 \end{pmatrix} \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1\ell} \\ a_{21} & a_{22} & \cdots & a_{2\ell} \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{m\ell} \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1\ell} \\ & a'_{22} & \cdots & a'_{2\ell} \\ & \vdots & \vdots & \vdots \\ & a'_{m2} & \cdots & a'_{m\ell} \end{pmatrix}.$$

Similarly, a'_{22} is also a unit of R, and we can add a suitable multiple of the second row to the ith row, for $3 \le i \le m$, such that the entries below a'_{22} of the second column are changed into 0. Continuing in the same manner, we obtain a lower triangular $m \times m$ matrix

$$P = \begin{pmatrix} 1 & & & \\ b_{21} & 1 & & \\ \vdots & \vdots & \ddots & \\ b_{m1} & b_{m2} & \cdots & 1 \end{pmatrix}$$

such that PA is an upper triangular matrix, which is still non-singular by columns.

Since

- $C = [C_1, \cdots, C_m]A = \big([C_1, \cdots, C_m]P^{-1}\big)(PA)$,
- P^{-1} still has the form $P^{-1} = \begin{pmatrix} 1 & & & \\ b'_{21} & 1 & & \\ \vdots & \vdots & \ddots & \\ b'_{m1} & b'_{m2} & \cdots & 1 \end{pmatrix}$,
- $[C_1, \cdots, C_m]P^{-1} = [C_1, \cdots, C_m]$ (since $C_1, \cdots, C_m$ are linear and $C_1 \supseteq C_2 \supseteq \cdots \supseteq C_m$),

it follows that

$$C = [C_1, \cdots, C_m](PA),$$

where PA is upper triangular. Hence, by the result above, equality holds in (3.1). □

Acknowledgements

Quite a part of 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. 11271005 and No. 11171370. Part of the work was also done when the second author was visiting the School of Mathematics and Statistics, Central China Normal University, Wuhan, in Spring 2012. The author acknowledges the support and hospitality received. The work of this author was partially supported by Singapore National Research Foundation Competitive Research Programme NRF-CRP2-2007-03.

References

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

[2] I. Constantinescu and W. Heise, *A metric for codes over residue class rings*, Problems of Information Transmission **33** (1997), no. 3, 208–213.

[3] Y. Fan, S. Ling and H. Liu, *Matrix product codes over finite commutative Frobenius rings*, Des. Codes Cryptogr. DOI 10.1007/s10623-012-9726-y, published online Jul 2012.

[4] Y. Fan, S. Ling and H. Liu, *On the homogeneous weight of the dual codes of matrix product codes over rings*, in preparation.

[5] Y. Fan and H. Liu, *Homogeneous weights of finite rings and Möbius functions* (Chinese), Math. Ann. (Chinese), **31A** (2010), 355–364.

[6] M. Greferath, A. A. Nechaev and R. Wisbauer, *Finite quasi-Frobenius modules and linear codes*, J. Algebra Appl. **3** (2004), no. 3, 247–272.

[7] M. Greferath and S.E. Schmidt, *Finite-ring combinatorics and MacWilliams equivalence theorem*, J. Combin. Theory A, **92** (2000), 17–28.

[8] 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.

[9] 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.

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

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

[12] T. Honold and A.A. Nechaev, *Fully weighted modules and representations of codes* (Russian), Problemy Peredachi Informatsii **35** (1999), no. 3, 18–39.

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

[14] B.R. McDonald, Finite Rings with Identity, New York: Marcel Dekker, 1974.

[15] 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.

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

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

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

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