



About the generalized Hamming weights of matrix-product codes

Rodrigo San-José¹

Received: 17 July 2024 / Revised: 26 December 2024 / Accepted: 8 February 2025 /
Published online: 14 March 2025
© The Author(s) 2025

Abstract

We derive a general lower bound for the generalized Hamming weights of nested matrix-product codes, with a particular emphasis on the cases with two and three constituent codes. We also provide an upper bound which is reminiscent of the bounds used for the minimum distance of matrix-product codes. When the constituent codes are two Reed–Solomon codes, we obtain an explicit formula for the generalized Hamming weights of the resulting matrix-product code. We also deal with the non-nested case for the case of two constituent codes.

Keywords Linear codes · Matrix-product codes · Generalized Hamming weights · Reed–Solomon codes

Mathematics Subject Classification Primary 94B05; Secondary 94B65 · 11T71

1 Introduction

The generalized Hamming weights (GHWs) of a linear code were introduced by Wei in Wei (1991), and they are a generalization of the minimum distance. Indeed, the GHWs of a code are obtained as the minimum of the cardinalities of the supports of all its subcodes of a fixed dimension r , e.g., for $r = 1$ one obtains the minimum distance. They give finer information about the code, and, in terms of applications, they characterize its performance on the wire-tap channel of type II and as a t -resilient function (Wei 1991), they have applications to list decoding (Guruswami 2003; Gopalan et al. 2011), their relative version has applications to secret sharing (Kurihara et al. 2012), and the rank-metric version has applications to network coding (Martínez-Peñas 2016; Oggier and Sboui 2012; Kurihara et al. 2015). This has motivated the study of GHWs in general (Helleseth et al. 1992), as well as the computation

This work was supported in part by the following grants: Grant TED2021-130358B-I00 funded by MICIU/AEI/10.13039/501100011033 and by the “European Union NextGenerationEU/PRTR”, Grant PID2022-138906NB-C21 funded by MICIU/AEI/ 10.13039/501100011033 and by ERDF/EU, and FPU20/01311 funded by the Spanish Ministry of Universities.

✉ Rodrigo San-José
rodrigo.san-jose@uva.es

¹ IMUVA-Mathematics Research Institute, Universidad de Valladolid, 47011 Valladolid, Spain

of these parameters for well known families of codes, such as cyclic codes (Janwa and Lal 1997; Yang et al. 2015; Feng et al. 1992) (also see Helleseth et al. 1977), Reed–Muller codes (Heijnen and Pellikaan 1998), Cartesian codes (Beelen and Datta 2018), hyperbolic codes (Camps-Moreno et al. 2024a), and algebraic geometry codes (Barbero and Munuera 2000; Munuera 1994; Camps-Moreno et al. 2024b), among others. Nevertheless, the computation of the GHWs of a code is, in general, a difficult problem, and they are still unknown for many families of codes.

Matrix-product codes (MPCs) were introduced by Blackmore and Norton in Blackmore and Norton (2001). They have received a lot of attention since then (van Asch 2008; Fan et al. 2014a, b; Liu and Liu 2020), and they have found applications in many different contexts (Luo et al. 2023a, b; Galindo et al. 2015, 2023). This technique utilizes an $s \times h$ matrix A and s linear codes C_1, \dots, C_s of length n , and provides a new code of length nh (see Definition 2.1). From the properties of the constituent codes, one can derive properties of the corresponding MPC. Most notably, one can obtain a lower bound for the minimum distance of the MPC from the minimum distance of the constituent codes (Blackmore and Norton 2001; Özbudak and Stichtenoth 2002), but one can also derive self-orthogonality properties for some matrices (Galindo et al. 2015; Mankean and Jitman 2016; Jitman and Mankean 2017) or decoding algorithms (Hernando et al. 2009; Hernando and Ruano 2013; Hernando et al. 2012).

The aim of this work is to study the GHWs of an MPC in terms of those of its constituent codes. By doing this, one can consider families of codes with known GHWs, and derive different codes with bounded GHWs using the MPC construction. This allows us to substantially expand the families of codes for which we have bounds for their GHWs. This work can also be seen as a generalization of the bounds given for the minimum distance in Blackmore and Norton (2001) and Özbudak and Stichtenoth (2002). In Sect. 3, we focus on the case of 2×2 matrices, without requiring the constituent codes to be nested. In Theorem 3.1, we give a lower bound for the GHWs of the corresponding MPC in terms of the GHWs of the constituent codes, and their sum and intersection. For the minimum distance of the code, this provides a refinement of the usual bounds for the $(u, u + v)$ and $(u + v, u - v)$ constructions (see Pellikaan et al. 2018, Thm. 2.1.32 & Prop. 2.1.39), which is showcased in Example 3.5. In Sect. 4, by requiring the constituent codes to be nested, we generalize the techniques from Sect. 3 to obtain a lower bound for the GHWs of an MPC for an arbitrary non-singular by columns (NSC) matrix, and, in Sects. 4.1 and 4.2, we describe it explicitly for the cases of two (Corollary 4.7) and three (Theorem 4.8) constituent codes. To complement these lower bounds, in Sect. 5 we provide an upper bound for the GHWs of MPCs, whose expression is reminiscent of the bounds obtained for the minimum distance in Blackmore and Norton (2001) and Özbudak and Stichtenoth (2002). In Sect. 6, we apply our results for specific families of codes. In particular, we show that our bounds are sharp when we consider two Reed–Solomon codes and a 2×2 NSC matrix (Theorem 6.1), therefore obtaining the weight hierarchy of these types of codes. We also test the bounds given in Corollary 4.7 and Theorem 4.8 for the case of two and three constituent Reed–Muller codes, and they give the true values of the GHWs in all the cases we have checked.

2 Preliminaries

Let \mathbb{F}_q be the finite field of q elements, where q is a power of a prime p . We start by defining MPCs as in Blackmore and Norton (2001).

Definition 2.1 Let $C_1, \dots, C_s \subseteq \mathbb{F}_q^n$ be linear codes of length n , which we call *constituent codes*, and let $A = (a_{ij}) \in \mathbb{F}_q^{s \times h}$ be an $s \times h$ matrix, with $s \leq h$. Given $v_\ell \in C_\ell$, for $\ell = 1, \dots, s$, we define

$$[v_1, \dots, v_s] \cdot A = \left(\sum_{\ell=1}^s a_{\ell 1} v_\ell, \dots, \sum_{\ell=1}^s a_{\ell h} v_\ell \right) \in \mathbb{F}_q^{nh}. \quad (1)$$

Then the *matrix-product code* C associated to A and C_1, \dots, C_s is

$$C = [C_1, \dots, C_s] \cdot A := \{[v_1, \dots, v_s] \cdot A : v_\ell \in C_\ell, \ell = 1, \dots, s\} \subseteq \mathbb{F}_q^{nh}.$$

For each vector $c \in C$, we have a natural subdivision of the coordinates in h blocks of length n , i.e.,

$$c = (c_1, c_2, \dots, c_h), \quad c_i \in \mathbb{F}_q^n, \quad i = 1, \dots, h.$$

Example 2.2 One can recover the usual $(u, u + v)$ construction (sometimes called Plotkin sum) of the codes C_1 and C_2 as an MPC code as follows:

$$[C_1, C_2] \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \{(v_1, v_1 + v_2) : v_1 \in C_1, v_2 \in C_2\}.$$

Definition 2.3 We denote by e_i , $1 \leq i \leq h$, the standard vectors of \mathbb{Z}_2^h , i.e., the vectors whose only nonzero entry is equal to 1 and it is in the i -th position. Let $y \in \mathbb{Z}_2^h$. Then we define

$$C(y) := \{c \in C : c_i = 0 \text{ for each } i \in \text{supp}(y)\}.$$

In other words, $C(y)$ is similar to a shortening at the blocks given by $\text{supp}(y)$, but without puncturing those coordinates.

Note that we are using subindices for vectors to express different things: to stress that a vector v_ℓ belongs to C_ℓ , to denote the i -th block c_i of a codeword $c \in C$, and to denote the standard vectors e_i of \mathbb{Z}_2^h . We will use different letters (v , c and e) and subindices (i and ℓ), which, together with the context, will help to clear any possible confusion.

With respect to the parameters of MPCs, it is clear that the length is nh , and the dimension is $k = k_1 + \dots + k_s$, where $k_\ell = \dim C_\ell$, $1 \leq \ell \leq s$, if A has full rank. In what follows, we always assume that A has full rank. For the minimum distance, we have to introduce some notation. Let us denote by $R_\ell = (a_{\ell 1}, \dots, a_{\ell h})$ the element of \mathbb{F}_q^h given by the ℓ -th row of A , for $1 \leq \ell \leq s$. We denote by δ_ℓ the minimum distance of the code C_{R_ℓ} generated by $\{R_1, \dots, R_\ell\}$ in \mathbb{F}_q^h . In Özbudak and Stichtenoth (2002) it is proven that

$$d_1(C) \geq \min\{d_1(C_1)\delta_1, \dots, d_1(C_s)\delta_s\}, \quad (2)$$

where $d_1(D)$ denotes the minimum distance the code D . Moreover, in Hernando et al. (2009), the authors prove that the previous bound is sharp if $C_s \subset \dots \subset C_1$.

When working with MPCs, it is usual to consider the following condition, introduced in Blackmore and Norton (2001).

Definition 2.4 Let A be an $s \times h$ matrix, and let A_t be the matrix formed by the first t rows of A . For $1 \leq j_1 < \dots < j_t \leq h$, we denote by $A(j_1, \dots, j_t)$ the $t \times t$ matrix consisting of the columns j_1, \dots, j_t of A_t . A matrix A is *non-singular by columns* if $A(j_1, \dots, j_t)$ is non-singular for each $1 \leq t \leq s$ and $1 \leq j_1 < \dots < j_t \leq h$. In particular, an NSC matrix has full rank.

Example 2.5 Let $\mathbb{F}_q = \{\beta_1, \dots, \beta_q\}$. For $1 \leq s \leq q$, the Vandermonde matrix

$$V_m = \begin{pmatrix} 1 & \cdots & 1 \\ \beta_1 & \cdots & \beta_q \\ \vdots & \ddots & \vdots \\ \beta_1^{s-1} & \cdots & \beta_q^{s-1} \end{pmatrix}$$

is an NSC matrix. Also $V_M(j_1, \dots, j_h)$ is NSC for any $s \leq h \leq q$ and $1 \leq j_1 < \dots < j_h \leq q$.

In Blackmore and Norton (2001) it is shown that, if A is NSC, then the codes C_{R_ℓ} are MDS (i.e., $\delta_\ell = h - \ell + 1$), for $1 \leq \ell \leq s$. This implies that the bound (2) becomes

$$d_1(C) \geq \min\{hd_1(C_1), (h-1)d_1(C_2), \dots, (h-s+1)d_1(C_s)\} \quad (3)$$

for the case of an NSC matrix.

One of the goals of this work is to generalize the bounds (2) and (3) to the case of the GHWs of C , which we introduce now. Let $D \subset C$ be a subcode. The support of D , denoted by $\text{supp}(D)$, is defined as

$$\text{supp}(D) := \{i : \exists u = (u_1, \dots, u_{nh}) \in D, u_i \neq 0\}.$$

Note that, in this case, u_i is just the i -th coordinate of u , not the i -th block of length n of u . Let $1 \leq r \leq \dim C$. The r -th generalized Hamming weight of C , denoted by $d_r(C)$, is defined as

$$d_r(C) := \min\{|\text{supp}(D)| : D \text{ is a subcode of } C \text{ with } \dim D = r\},$$

where $|A|$ denotes the cardinality of a set A . Throughout the paper, we will denote $d_0(C) = 0$.

Remark 2.6 Given a basis $B = \{b_1, \dots, b_k\}$ for a subcode D , we have that

$$\text{supp}(D) = \bigcup_{i=1}^k \text{supp}(b_i).$$

The GHWs satisfy the following general properties for any linear code C , as shown in Wei (1991).

Theorem 2.7 (Monotonicity) *For an $[n, k]$ linear code C with $k > 0$ we have*

$$1 \leq d_1(C) < d_2(C) < \dots < d_k(C) \leq n.$$

Corollary 2.8 (Generalized Singleton Bound) *For an $[n, k]$ linear code C we have*

$$d_r(C) \leq n - k + r, \quad 1 \leq r \leq k.$$

We say that a code C is t -MDS if $d_t(C) = n - k + t$, for some $1 \leq t \leq \dim C$. If a code is t -MDS for $t < \dim C$, it is also $(t+1)$ -MDS by Theorem 2.7 and Corollary 2.8. Thus, one usually studies what is the first t such that C is t -MDS.

Remark 2.9 For an MDS code C , by Theorem 2.7 and Corollary 2.8 we have

$$d_r(C) = n - k + r,$$

for all $1 \leq r \leq k$.

Going back to MPCs, the block structure that we have allows us to divide the support of the code as follows.

Definition 2.10 Let $C \subset \mathbb{F}_q^{nh}$. Then we define

$$\text{supp}_i(C) := \text{supp}(C) \cap \{(i-1) \cdot n + 1, \dots, i \cdot n\}, \quad 1 \leq i \leq h.$$

It is clear that

$$\text{supp}(C) = \bigsqcup_{i=1}^h \text{supp}_i(C).$$

This implies

$$|\text{supp}(C)| = \sum_{i=1}^h |\text{supp}_i(C)|. \quad (4)$$

3 A bound for the GHWs of the MPCs with 2×2 matrices

In this section, we give a lower bound for the GHWs of MPCs obtained with a 2×2 matrix A , which we also assume to be NSC. If we denote

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix},$$

since A is NSC, we have $a_{1j} \neq 0$, $1 \leq j \leq 2$. Moreover, we also cannot have $a_{21} = a_{22} = 0$. Since exchanging the order of the columns of A produces a permutation equivalent MPC code, we will assume that $a_{22} \neq 0$. Let $C_1, C_2 \subset \mathbb{F}_q^n$, and $1 \leq r \leq \dim C_1 + \dim C_2$. We denote $[r] := \{0, 1, \dots, r\}$ and $[r]^2 := [r] \times [r]$. We consider the set

$$Y_2 := \left\{ (\alpha_1, \alpha_2) \in [r]^2 : \begin{array}{l} r - \dim(C_1 + C_2) \leq \alpha_1 \leq \dim C_2 \\ r - \dim(C_1 + C_2) \leq \alpha_2 \leq \dim(C_1 \cap C_2) \\ \alpha_1 + \alpha_2 \leq r \end{array} \right\}.$$

We give now the main result of the section, bounding from below the GHWs of an MPC in terms of the GHWs of sums and intersections of the constituent codes.

Theorem 3.1 Let $C_1, C_2 \subset \mathbb{F}_q^n$, and let $C = [C_1, C_2] \cdot A$, with A as above. Let $1 \leq r \leq \dim C = \dim C_1 + \dim C_2$. Then

$$d_r(C) \geq \min_{(\alpha_1, \alpha_2) \in Y_2} B_{\alpha_1, \alpha_2},$$

where

$$B_{\alpha_1, \alpha_2} = \max\{d_{r-\alpha_1}(C_1 + C_2), d_{\alpha_2}(C_1 \cap C_2)\} + \max\{d_{r-\alpha_2}(C_1 + C_2), d_{\alpha_1}(C_2)\}.$$

Proof Let $D \subset C$ be a subcode with $\dim D = r$. We will associate a pair (α_1, α_2) to D , and we will see that

$$|\text{supp}(D)| \geq B_{\alpha_1, \alpha_2}.$$

We consider the following subcodes of D (recall Definition 2.3):

$$D_1 = D(e_1), \quad D_2 = D(e_2), \quad \text{and} \quad D_3 = D/(D(e_1) + D(e_2)),$$

where D_3 is regarded as a subcode of D by fixing some set of representatives of the quotient vector space. It is clear that

$$D = D_1 \oplus D_2 \oplus D_3.$$

If we denote $\alpha_1 = \dim D_1$ and $\alpha_2 = \dim D_2$, we have that $\dim D_3 = r - \alpha_1 - \alpha_2 \geq 0$. Moreover, by (4), we have

$$|\text{supp}(D)| = \sum_{i=1}^2 |\text{supp}_i(D)|.$$

Now we will bound $|\text{supp}_i(D)|$ from below, for $1 \leq i \leq 2$. We start with $i = 1$. Let \mathcal{B}_1 , \mathcal{B}_2 and \mathcal{B}_3 be any fixed bases for D_1 , D_2 , and D_3 , respectively. We consider the basis $\mathcal{B} = \mathcal{B}_1 \cup \mathcal{B}_2 \cup \mathcal{B}_3$ for D . We can use Remark 2.6, and notice that

$$\text{supp}_1(D_1) = \bigcup_{b \in \mathcal{B}_1} \text{supp}_1(b) = \emptyset.$$

Therefore, $\text{supp}_1(D) = \text{supp}_1(D_2 \oplus D_3)$. Now we have two ways to bound $|\text{supp}_1(D_2 \oplus D_3)|$:

(a) Let \mathcal{B}' be the set

$$\mathcal{B}' := \{c_1 : c = (c_1, c_2) \in \mathcal{B}_2 \cup \mathcal{B}_3\},$$

that is, the set formed by the first block of the vectors in $\mathcal{B}_2 \cup \mathcal{B}_3$, which has size $r - \alpha_1$. From the definition of MPCs (see (1)), $\mathcal{B}' \subset C_1 + C_2$. Moreover, \mathcal{B}' is a linearly independent set because, otherwise, we would have a linear combination of vectors of $\mathcal{B}_2 \cup \mathcal{B}_3$ in D_1 , a contradiction. Thus,

$$|\text{supp}_1(D)| = |\text{supp}_1(D_2 \oplus D_3)| \geq d_{r-\alpha_1}(C_1 + C_2).$$

(b) We consider the set

$$\mathcal{B}'' = \{c_1 : c = (c_1, c_2) \in \mathcal{B}_2\}.$$

As the vectors of \mathcal{B}_2 are linearly independent and they have $c_2 = 0$, the vectors in \mathcal{B}'' are linearly independent. Let $c_1 \in \mathcal{B}''$. Then

$$(c_1, 0) = [v_1, v_2] \cdot A = (a_{11}v_1 + a_{21}v_2, a_{12}v_1 + a_{22}v_2),$$

for some $v_1 \in C_1$, $v_2 \in C_2$. Hence,

$$0 = a_{12}v_1 + a_{22}v_2 \implies v_1 = (-a_{22}/a_{12})v_2,$$

since $a_{12} \neq 0$. We are assuming $a_{22} \neq 0$, which implies $v_1, v_2 \in C_1 \cap C_2$. Therefore, $c_1 = a_{11}v_1 + a_{21}v_2 \in C_1 \cap C_2$ and $\mathcal{B}'' \subset C_1 \cap C_2$. We have obtained

$$|\text{supp}_1(D)| = |\text{supp}_1(D_2 \oplus D_3)| \geq d_{\alpha_2}(C_1 \cap C_2).$$

Using both bounds, we get

$$|\text{supp}_1(D)| \geq \max\{d_{r-\alpha_1}(C_1 + C_2), d_{\alpha_2}(C_1 \cap C_2)\}.$$

An analogous argument applies to $\text{supp}_2(D)$, taking into account that a_{21} can be zero. This means that in (b) we can only argue that $v_1, v_2 \in C_2$. We obtain the bound

$$|\text{supp}_2(D)| \geq \max\{d_{r-\alpha_2}(C_1 + C_2), d_{\alpha_1}(C_2)\}.$$

Thus,

$$|\text{supp}(D)| = |\text{supp}_1(D)| + |\text{supp}_2(D)| \geq B_{\alpha_1, \alpha_2}.$$

For any subcode D , from the arguments in (a) and (b) we deduce that the parameters $\alpha_1 = \dim D(e_1)$ and $\alpha_2 = \dim D(e_2)$ satisfy $(\alpha_1, \alpha_2) \in Y$, which concludes the proof. \square

We have given the bound in the most general form. However, depending on whether a_{21} is zero or not, it is possible to improve the bound from the previous result, as we show next. If $a_{21} \neq 0$, consider the set

$$Y'_2 := \left\{ (\alpha_1, \alpha_2) \in [r]^2 : \begin{array}{l} r - \dim(C_1 + C_2) \leq \alpha_i \leq \dim C_1 \cap C_2, \ i = 1, 2 \\ \alpha_1 + \alpha_2 \leq r \end{array} \right\}.$$

Corollary 3.2 *With the notation as before, if $a_{21} \neq 0$, then*

$$d_r(C) \geq \min_{(\alpha_1, \alpha_2) \in Y'_2} B_{\alpha_1, \alpha_2},$$

where

$$B_{\alpha_1, \alpha_2} = \max\{d_{r-\alpha_1}(C_1 + C_2), d_{\alpha_2}(C_1 \cap C_2)\} + \max\{d_{r-\alpha_2}(C_1 + C_2), d_{\alpha_1}(C_1 \cap C_2)\}.$$

Proof Following the proof of Theorem 3.1, if $a_{21} \neq 0$, then in (b) we have $v_1, v_2 \in C_1 \cap C_2$ for both blocks $i = 1, 2$. \square

In the case of $a_{21} = 0$, we consider instead the set

$$Y''_2 := \left\{ (\alpha_1, \alpha_2) \in [r]^2 : \begin{array}{l} r - \dim(C_1) \leq \alpha_1 \leq \dim C_2 \\ r - \dim(C_1 + C_2) \leq \alpha_2 \leq \dim C_1 \cap C_2 \\ \alpha_1 + \alpha_2 \leq r \end{array} \right\}.$$

Corollary 3.3 *With the notation as before, if $a_{21} = 0$, then*

$$d_r(C) \geq \min_{(\alpha_1, \alpha_2) \in Y''_2} B_{\alpha_1, \alpha_2},$$

where

$$B_{\alpha_1, \alpha_2} = \max\{d_{r-\alpha_1}(C_1), d_{\alpha_2}(C_1 \cap C_2)\} + \max\{d_{r-\alpha_2}(C_1 + C_2), d_{\alpha_1}(C_2)\}.$$

Proof We follow the proof of Theorem 3.1. If $a_{21} = 0$, then for any $c \in C$, we have $c_1 \in C_1$, improving the bound obtained in (a) for the first block. \square

Remark 3.4 The ideas in this section are a generalization of the arguments from (San-José 2024), where the author computes a particular generator matrix for any subcode of a projective Reed-Muller code that is given by two parameters, α and γ . Those parameters play the role of $r - \alpha_2$ and α_1 , respectively, in this section.

Note that, if $C_2 \subset C_1$, then all the bounds given in this section coincide. However, as we show in the next example, if we do not have this nested condition, then we can obtain different bounds in Corollaries 3.2 and 3.3. Moreover, in the next example we also show that, if the codes are not nested, our bounds can refine the usual bounds for the minimum distance of the $(u, u + v)$ and $(u + v, u - v)$ constructions by considering $d_1(C_1 + C_2)$ and $d_1(C_1 \cap C_2)$.

Table 1 GHWs of C_1 , C_2 and $C_1 + C_2$

| GHWs\ r | 1 | 2 | 3 | 4 | 5 |
|------------------|---|---|---|---|---|
| $d_r(C_1)$ | 3 | 6 | 8 | – | – |
| $d_r(C_2)$ | 5 | 8 | – | – | – |
| $d_r(C_1 + C_2)$ | 3 | 5 | 6 | 7 | 8 |

Table 2 Lower bounds from Corollaries 3.2 and 3.3

| Bound\ r | 1 | 2 | 3 | 4 | 5 |
|-----------------------|---|----|----|----|----|
| Lower bound for D_1 | 5 | 8 | 11 | 14 | 16 |
| Lower bound for D_2 | 6 | 10 | 12 | 14 | 16 |

Table 3 GHWs of D_1 and D_2

| GHWs\ r | 1 | 2 | 3 | 4 | 5 |
|------------|---|----|----|----|----|
| $d_r(D_1)$ | 5 | 8 | 11 | 14 | 16 |
| $d_r(D_2)$ | 6 | 10 | 12 | 15 | 16 |

Example 3.5 Let $q = 3$, and consider

$$G_1 = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ -1 & 1 & 0 & 1 & -1 & 1 & 0 & 1 \\ -1 & 1 & -1 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}, \quad G_2 = \begin{pmatrix} -1 & 0 & 1 & 1 & -1 & 1 & -1 & 0 \\ 1 & 1 & 0 & 1 & -1 & -1 & -1 & -1 \end{pmatrix}.$$

Let C_1 and C_2 be the linear codes whose generator matrices are G_1 and G_2 . Then, one can check that $C_1 \cap C_2 = \{0\}$, and the GHWs of C_1 , C_2 and $C_1 + C_2$ are given in Table 1.

Now we define the matrices

$$A_1 := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad A_2 := \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},$$

which correspond to the $(u, u + v)$ and $(u + v, u - v)$ constructions, respectively. Let $D_1 = [C_1, C_2] \cdot A_1$, $D_2 = [C_1, C_2] \cdot A_2$. The usual bounds for the minimum distance of D_1 and D_2 would give $\min\{2d_1(C_1), d_1(C_2)\} = 5$ (see Pellikaan et al. 2018, Thm. 2.1.32 & Prop. 2.1.39). However, our bounds from Corollaries 3.2 and 3.3 give the values from Table 2.

Note that the bound for $d_1(D_2)$ has been improved to 6. Also, notice that the bounds obtained from Corollaries 3.2 and 3.3 are different in this case for A_1 and A_2 . This is noteworthy since, as we said before, the usual bounds for the minimum distance of the $(u, u + v)$ construction and the $(u + v, u - v)$ construction are the same (assuming $d_1(C_1) \leq d_1(C_2)$). The true values of the GHWs are given in Table 3, showing that our bounds are sharp in this case, except in the case $r = 4$ for D_2 .

In this case, since $C_1 \cap C_2 = \{0\}$, the lower bounds from Corollaries 3.2 and 3.3 are particularly easy to compute. Indeed, if $a_{21} \neq 0$ (the case of A_2), we have $Y'_2 = \{(0, 0)\}$. Thus, the bound from Corollary 3.2 is just

$$d_r(D_2) \geq B_{0,0} = 2d_r(C_1 + C_2).$$

For the case $a_{21} = 0$, we obtain $Y_2'' = \{(\alpha_1, 0) \in [r]^2 : r - 3 \leq \alpha_1 \leq 2\}$, and the bound from Corollary 3.3 is

$$d_r(D_1) \geq \min_{(\alpha_1, 0) \in Y_2''} B_{\alpha_1, 0} = \min_{(\alpha_1, 0) \in Y_2''} \{d_{r-\alpha_1}(C_1) + \max\{d_r(C_1 + C_2), d_{\alpha_1}(C_2)\}\}.$$

For example, for $r = 3$, we have $Y_2'' = \{(0, 0), (1, 0), (2, 0)\}$, and

$$d_3(D_1) \geq \min\{8 + \max\{3, 0\}, 6 + \max\{6, 5\}, 3 + \max\{6, 8\}\} = 11.$$

4 A bound for the GHWs of nested MPCs with NSC matrices

In this section, we will show how to obtain a lower bound for the GHWs of MPCs with s constituent codes. We will assume that the codes are nested, i.e., $C_s \subset \cdots \subset C_1 \subset \mathbb{F}_q^n$. We consider A an $s \times h$ NSC matrix over \mathbb{F}_q with $s \leq h$. By Blackmore and Norton (2001, Prop. 3.3), this implies that $h \leq q$. Let $C = [C_1, \dots, C_s] \cdot A$. From Luo et al. (2023b, Lem. 6) we have the following result.

Lemma 4.1 *Let $C_s \subset \cdots \subset C_1 \subset \mathbb{F}_q^n$ and A an $s \times h$ NSC matrix over \mathbb{F}_q . Let $C = [C_1, \dots, C_s] \cdot A$ and $c \in C$. We consider the h blocks of length n of c , that is, $c = (c_1, \dots, c_h)$. Let $0 \leq \ell \leq s - 1$. If there are exactly ℓ zero vectors among the blocks c_1, \dots, c_h , then $c_j \in C_{\ell+1}$, for every $1 \leq j \leq h$. If the number of zero vectors among c_1, \dots, c_h is greater than $s - 1$, then $c = 0$.*

Let $1 \leq i \leq h$, $1 \leq r \leq \dim C = \sum_{\ell=1}^s \dim(C_\ell)$, and $D \subset C$ a subcode of C with $\dim D = r$. For $0 \leq j \leq s - 1$, we define the vector space

$$D_j^i := \left(D(e_i) + \sum_{y \in \mathbb{Z}_2^h, \text{wt}(y)=j} D(y) \right) / D(e_i). \quad (5)$$

One way to think about D_j^i is that these are the codewords $c \in D$ with $c_i \neq 0$ (because we take the quotient by $D(e_i)$), and which can be generated by codewords of D with at least j zero blocks. Note that, since $D(y) \subset D(e_i)$ if $y_i = 1$, we have

$$D(e_i) + \sum_{y \in \mathbb{Z}_2^h, \text{wt}(y)=j} D(y) = D(e_i) + \sum_{y \in \mathbb{Z}_2^h, \text{wt}(y)=j, y_i=0} D(y).$$

Example 4.2 For $s = h = 2$ and $1 \leq i \leq 2$ we have

$$D_0^i = (D(e_i) + D) / D(e_i) = D / D(e_i), \quad D_1^i = (D(e_1) + D(e_2)) / D(e_i) \cong D(e_{i+1}),$$

where we understand the subindex $i + 1$ cyclically mod 2, i.e., $2 + 1 \equiv 1$. Note that the vector spaces D_1^i already appeared in the proof of Theorem 3.1.

We can consider a basis for this last vector space where every vector is either in some $D(y)$, with $\text{wt}(y) = j$, $y_i = 0$, or in $D(e_i)$. The classes of these vectors in (5) form a generating set, from which we can extract a basis \mathcal{B}_j^i (regarded in \mathbb{F}_q^{hn} by fixing some representatives) where every vector is in some $D(y)$, with $\text{wt}(y) = j$, and is not contained in $D(e_i)$. That is, each vector of \mathcal{B}_j^i has at least j zero blocks, and its i -th block is nonzero. We now define

$$\mathcal{B}_{j,i}^i := \{c_i : c \in \mathcal{B}_j^i\},$$

which is the set given by the i -th blocks of the vectors in \mathcal{B}_j^i .

Example 4.3 Following the setting of Example 4.2, we have

$$|\mathcal{B}_0^i| = \dim D_0^i = r - \dim D(e_i), \quad |\mathcal{B}_1^i| = \dim D_1^i = \dim D(e_{i+1}).$$

Now we can use the sets we have just defined to obtain a bound for $|\text{supp}_i(D)|$.

Lemma 4.4 *We have that*

$$|\text{supp}_i(D)| \geq d_{|\mathcal{B}_j^i|}(C_{j+1}).$$

Proof We claim that $\mathcal{B}_{j,i}^i$ is a linearly independent set. Indeed, if we assume it is linearly dependent, this would give a linear combination of vectors of \mathcal{B}_j^i in $D(e_i)$, a contradiction, since the classes of the vectors of \mathcal{B}_j^i are linearly independent in D_j^i (see (5)). By Lemma 4.1, we have $\mathcal{B}_{j,i}^i \subset C_{j+1}$, and

$$|\text{supp}_i(D)| \geq \left| \bigcup_{b \in \mathcal{B}_{j,i}^i} \text{supp}_i(b) \right| \geq d_{|\mathcal{B}_{j,i}^i|}(C_{j+1}) = d_{|\mathcal{B}_j^i|}(C_{j+1}).$$

□

From this lemma we can obtain a general result bounding the GHWs of an MPC. Note that \mathcal{B}_j^i depends on the subcode D , and we could write $\mathcal{B}_j^i(D)$ to make this explicit, but we avoid doing this for ease of notation.

Proposition 4.5 *Let $C_s \subset \dots \subset C_1 \subset \mathbb{F}_q^n$ be linear codes, A an $s \times h$ NSC matrix over \mathbb{F}_q with $s \leq h$, and $C = [C_1, \dots, C_s] \cdot A$. For $1 \leq r \leq \dim C = \sum_{\ell=1}^s \dim C_\ell$, we have*

$$d_r(C) \geq \min_{D \subset C, \dim D=r} \left(\sum_{i=1}^h \max\{d_{|\mathcal{B}_j^i|}(C_{j+1}), 0 \leq j \leq s-1\} \right).$$

Proof Let $D \subset C$ be a subcode with $\dim D = r$. Using Lemma 4.4 for every block i , $1 \leq i \leq h$, and taking into account (4), we obtain the bound

$$|\text{supp}(D)| \geq \sum_{i=1}^h \max\{d_{|\mathcal{B}_j^i|}(C_{j+1}), 0 \leq j \leq s-1\}.$$

The result follows from the definition of GHWs. □

Remark 4.6 For the case $r = 1$, this bound generalizes the bound from (3). Indeed, let $D \subset C$ with $\dim D = 1$, and consider i, j such that $|\mathcal{B}_j^i| = 1$ (since $r = 1$, $|\mathcal{B}_j^i|$ is either 0 or 1, and if all of them are 0, this would correspond to the subcode $D = \{0\}$). This means that D is generated by a vector c with at least j zero blocks, and with a nonzero i -th block. Let

$$j' := |\{k : c_k = 0\}|,$$

that is, the number of zero blocks of c . Then $|\mathcal{B}_{j'}^i| = 1$ since we can assume $\mathcal{B}_{j'}^i = \{c\}$. It follows from the definitions that, in this case, we have

$$|\mathcal{B}_k^i| = 1 \iff k \leq j', \quad c_i \neq 0,$$

and, thus, $|\mathcal{B}_k^i| = 0$ otherwise. Then, for any i such that $c_i \neq 0$, we have

$$\max\{d_{|\mathcal{B}_j^i|}(C_{j+1}), 0 \leq j \leq s-1\} = \max\{d_1(C_1), \dots, d_1(C_{j'+1})\} = d_1(C_{j'+1}).$$

Since c has exactly $h - j'$ nonzero blocks, we obtain

$$\sum_{i=1}^h \max\{d_{|\mathcal{B}_j^i|}(C_{j+1}), 0 \leq j \leq s-1\} = (h - j')d_1(C_{j'+1}),$$

which shows that the bound from Proposition 4.5 simplifies to (3) in this case.

The advantage of using Proposition 4.5 to compute the GHWs of C instead of the definition is that, even though the bound from Proposition 4.5 requires to compute a minimum over all the subcodes $D \subset C$ with $\dim D = r$, the values we are minimizing only depend on $|\mathcal{B}_j^i|$, e.g., see Remark 4.6. Now assume we have a set Y_s and a family of bounds $\{B_v\}_{v \in Y_s}$ such that for any subcode $D \subset C$ with $\dim D = r$, we have

$$\sum_{i=1}^h \max\{d_{|\mathcal{B}_j^i|}(C_{j+1}), 0 \leq j \leq s-1\} = B_v,$$

for some $v \in Y_s$. From Proposition 4.5 we obtain

$$d_r(C) \geq \min_{D \subset C, \dim D=r} \left(\sum_{i=1}^h \max\{d_{|\mathcal{B}_j^i|}(C_{j+1}), 0 \leq j \leq s-1\} \right) \geq \min_{v \in Y_s} B_v. \quad (6)$$

In the next subsections we show how to obtain a set Y_s and a family of bounds $\{B_v\}_{v \in Y_s}$ for the cases of $s = 2$ and $s = 3$, which are the most used cases for applications.

4.1 The case $h = 2$

For the case $s = h = 2$ we can recover what we obtained in Sect. 3 for the nested case. We recall that if $C_2 \subset C_1$, we have $Y_2 = Y'_2 = Y''_2$ (using the notation from Sect. 3), and

$$Y_2 = \left\{ (\alpha_1, \alpha_2) \in [r]^2 : \begin{array}{l} r - \dim C_1 \leq \alpha_i \leq \dim C_2, \quad 1 \leq i \leq 2 \\ \alpha_1 + \alpha_2 \leq r \end{array} \right\}.$$

Corollary 4.7 Let $C_2 \subset C_1 \subset \mathbb{F}_q^n$, $C = [C_1, C_2] \cdot A$, for some 2×2 NSC matrix A . Consider $1 \leq r \leq \dim C_1 + \dim C_2$, and

$$B_{\alpha_1, \alpha_2} = \max\{d_{r-\alpha_1}(C_1), d_{\alpha_2}(C_2)\} + \max\{d_{r-\alpha_2}(C_1), d_{\alpha_1}(C_2)\},$$

for $(\alpha_1, \alpha_2) \in Y_2$. Then

$$d_r(C) \geq \min_{(\alpha_1, \alpha_2) \in Y_2} B_{\alpha_1, \alpha_2}.$$

Proof Let $D \subset C$ with $\dim D = r$. Let $\alpha_i = \dim D(e_i)$, $1 \leq i \leq 2$, and note that $|\mathcal{B}_0^i| = r - \alpha_{i+1}$ (we consider $i+1 \bmod 2$ for the subindex, with representatives $\{1, 2\}$), and $|\mathcal{B}_1^i| = \alpha_i$. The first set of conditions about α_i , $1 \leq i \leq 2$, follow from the fact that $\mathcal{B}_{j,i}^i \subset C_{j+1}$ and $|\mathcal{B}_j^i| = |\mathcal{B}_{j,i}^i|$, for $j = 0, 1$. The condition $\alpha_1 + \alpha_2 \leq r$ arises from the fact that $D(e_1) + D(e_2) \subset D$, and $D(e_1) \cap D(e_2) = \{0\}$. Therefore, by Proposition 4.5 and (6), we obtain the result. \square

4.2 The case $h = 3$

We now apply our techniques to the case $s = h = 3$. Throughout this section, when a subindex is greater than 3, we consider its reduction modulo 3, with representatives $\{1, 2, 3\}$. For instance, for $i = 2$, we have $e_{i+1} + e_{i+2} = e_3 + e_1$. We denote $[r]^{3,3,1} := [r]^3 \times [r]^3 \times [r]$, and let

$$Y_3 := \left\{ (\alpha, \gamma, \beta) \in [r]^{3,3,1} : \begin{array}{l} \gamma_i \leq \dim C_3, \quad 1 \leq i \leq 3 \\ \max\{r - \dim C_1, \gamma_{i+1} + \gamma_{i+2}\} \leq \alpha_i, \quad 1 \leq i \leq 3 \\ \alpha_{i+1} + \alpha_{i+2} - \gamma_i \leq \beta, \quad 1 \leq i \leq 3 \\ \beta \leq \min \left\{ \sum_{i=1}^3 (\alpha_i - \gamma_i), \dim C_2 + \min\{\alpha_i, 1 \leq i \leq 3\} \right\} \end{array} \right\}.$$

Theorem 4.8 Let $C_3 \subset C_2 \subset C_1 \subset \mathbb{F}_q^n$ and $C = [C_1, C_2, C_3] \cdot A$, for some 3×3 NSC matrix A . Consider $1 \leq r \leq \sum_{\ell=1}^3 \dim C_\ell$. For $(\alpha, \gamma, \beta) \in Y_3$, let

$$B_{\alpha, \gamma, \beta} = \sum_{i=1}^3 \max\{d_{r-\alpha_i}(C_1), d_{\beta-\alpha_i}(C_2), d_{\gamma_i}(C_3)\}.$$

Then we have

$$d_r(C) \geq \min_{(\alpha, \gamma, \beta) \in Y_3} B_{\alpha, \gamma, \beta}.$$

Proof Let $D \subset C$ with $\dim D = r$. We consider $\alpha_i = \dim D(e_i)$, $\gamma_i = \dim D(e_{i+1} + e_{i+2})$ and $\beta = \dim(\sum_{j=1}^3 D(e_j))$, for $1 \leq i \leq 3$. We claim

$$|B_j^i| = \begin{cases} \dim D/D(e_i) = r - \alpha_i & \text{if } j = 0, \\ \dim(\sum_{k=1}^3 D(e_k))/D(e_i) = \beta - \alpha_i & \text{if } j = 1, \\ \dim(D(e_i) + \sum_{k < \ell} D(e_k + e_\ell))/D(e_i) = \gamma_i & \text{if } j = 2. \end{cases} \quad (7)$$

The cases $j = 0$ and $j = 1$ are straightforward. For $j = 2$, we have

$$D(e_i) + \sum_{k < \ell} D(e_k + e_\ell) = D(e_i) + D(e_{i+1} + e_{i+2})$$

since $D(e_i + e_j) \subset D(e_i)$, for any $j \neq i$. Taking into account that $D(e_i) \cap D(e_{i+1} + e_{i+2}) = D((1, 1, 1)) = \{0\}$, we have

$$\dim(D(e_i) + \sum_{k < \ell} D(e_k + e_\ell))/D(e_i) = \dim(D(e_i) + D(e_{i+1} + e_{i+2})) - \dim D(e_i) = \gamma_i.$$

Let $\alpha = (\alpha_1, \alpha_2, \alpha_3)$, and $\gamma = (\gamma_1, \gamma_2, \gamma_3)$. Now we check that $(\alpha, \gamma, \beta) \in Y_3$ (we want to use (6)). It is clear that $0 \leq \gamma_i$, and, since $\gamma_i = |B_2^i| = |B_{2,i}^i|$ and $B_{2,i}^i \subset C_3$, we have $\gamma_i \leq \dim C_3$, for $1 \leq i \leq 3$. Similarly, we have $r - \alpha_i = |B_0^i|$, which implies $r - \alpha_i \leq \dim C_1$, i.e., $r - \dim C_1 \leq \alpha_i$, for $1 \leq i \leq 3$. Now we note that

$$D(e_i + e_{i+2}) + D(e_i + e_{i+1}) \subset D(e_i).$$

Taking into account that $D(e_i + e_{i+2}) \cap D(e_i + e_{i+1}) = D((1, 1, 1)) = \{0\}$, we deduce that $\gamma_{i+1} + \gamma_{i+2} \leq \alpha_i$, $1 \leq i \leq 3$. Regarding the first condition for β in Y , we note that

$$\beta = \dim \left(\sum_{i=1}^3 D(e_i) \right) \geq \dim(D(e_{k+1}) + D(e_{k+2})) = \alpha_{k+1} + \alpha_{k+2} - \gamma_k,$$

for $1 \leq k \leq 3$. It is clear that $\beta \leq r$, and, since $\beta - \alpha_i = |\mathcal{B}_1^i| = |\mathcal{B}_{1,i}^i|$ and $\mathcal{B}_{1,i}^i \subset C_2$, we have $\beta - \alpha_i \leq \dim C_2$, $1 \leq i \leq 3$. The last condition we need to prove is $\beta \leq \sum_{i=1}^3 (\alpha_i - \gamma_i)$. Note that, using the formula for the dimension of the sum of vector spaces twice, we have

$$\dim \left(\sum_{i=1}^3 D(e_i) \right) = \sum_{i=1}^3 \alpha_i - \gamma_k - \dim(D(e_k) \cap (D(e_{k+1}) + D(e_{k+2}))),$$

for any $1 \leq k \leq 3$. Since $D(e_k + e_{k+1}) + D(e_k + e_{k+2}) \subset D(e_k) \cap (D(e_{k+1}) + D(e_{k+2}))$, we conclude

$$\beta = \dim \left(\sum_{i=1}^3 D(e_i) \right) \leq \sum_{i=1}^3 \alpha_i - \gamma_k - (\gamma_{k+2} + \gamma_{k+1}) = \sum_{i=1}^3 (\alpha_i - \gamma_i).$$

Thus, we have proved that $(\alpha, \gamma, \beta) \in Y_3$ and, if we note the expressions in (7), we have also proved that

$$\sum_{i=1}^3 \max\{d_{|\mathcal{B}_j^i|}(C_{j+1}), 0 \leq j \leq 3-1\} = B_{\alpha, \gamma, \beta},$$

for some $(\alpha, \gamma, \beta) \in Y_3$. We obtain the result by (6). \square

Remark 4.9 As we have seen in the proof of the previous result, we have incorporated some of the relations between the dimensions of $D(e_i)$, $D(e_{i+1} + e_{i+2})$ and $\sum_{k=1}^3 D(e_k)$, for $1 \leq i \leq 3$, using α_i , γ_i and β , respectively. In fact, many of the relations between these dimensions that one could expect can be derived from the ones included in the definition of Y . For example, we have

$$\dim(D(e_i)) + \dim(D(e_{i+1} + e_{i+2})) = \dim(D(e_i) + D(e_{i+1} + e_{i+2})) \leq \dim \left(\sum_{i=1}^3 D(e_i) \right).$$

This means that we should have $\alpha_i + \gamma_i \leq \beta$, for $1 \leq i \leq 3$. This is a consequence of the conditions we gave for Y because

$$\beta \geq \alpha_{i+1} + \alpha_{i+2} - \gamma_i \geq \alpha_{i+1} + \gamma_{i+1}, \quad 1 \leq i \leq 3,$$

since we also impose the condition $\alpha_{i+2} \geq \gamma_i + \gamma_{i+1}$.

Theorem 4.8 can also be used to give a bound for the GHWs in the case $s = 2$, $h = 3$, as the next result shows. In this case, we denote $[r]^{3,1} = [r]^3 \times [r]$.

Corollary 4.10 Let $C_2 \subset C_1 \subset \mathbb{F}_q^n$, $C = [C_1, C_2] \cdot A$, for some 2×3 NSC matrix A . Let

$$Y'_3 = \left\{ (\alpha, \beta) \in [r]^{3,1} : \begin{array}{l} r - \dim C_1 \leq \alpha_i, \quad 1 \leq i \leq 3 \\ \alpha_{i+1} + \alpha_{i+2} \leq \beta, \quad 1 \leq i \leq 3 \\ \beta \leq \min \left\{ \sum_{i=1}^3 \alpha_i, \dim C_2 + \min\{\alpha_i, 1 \leq i \leq 3\} \right\} \end{array} \right\}.$$

For $(\alpha, \beta) \in Y'_3$ we consider

$$B_{\alpha, \beta} = \sum_{i=1}^3 \max\{d_{r-\alpha_i}(C_1), d_{\beta-\alpha_i}(C_2)\}.$$

Then we have

$$d_r(C) \geq \min_{(\alpha, \beta) \in Y'_3} B_{\alpha, \beta}.$$

Proof This can be obtained directly from Theorem 4.8 by setting $C_3 = \{0\}$. \square

Example 4.11 Let $q = 4$ and $n = 4$. In this example (and throughout the rest of the paper) we denote by $\text{RS}(k)$ the Reed–Solomon code of length n and dimension k . Note that, by Remark 2.9, we know the GHWs of Reed–Solomon codes. Let $k_1 = 3$ and $k_2 = 1$. We will compute the bound from Corollary 4.10 for the code $C = [\text{RS}(k_1), \text{RS}(k_2)] \cdot A$ and $r = 2$, where

$$A = \begin{pmatrix} 1 & a & 1 \\ 1 & 1 & 0 \end{pmatrix},$$

and where a is a primitive element of \mathbb{F}_4 . We start by computing Y'_3 . First, we have $0 \leq \alpha_i \leq r = 2$, for $1 \leq i \leq 3$. For β , we have the conditions $\alpha_{i+1} + \alpha_{i+2} \leq \beta$, for $1 \leq i \leq 3$, and $\beta \leq \min\{\sum_{i=1}^3 \alpha_i, 1 + \min\{\alpha_i, 1 \leq i \leq 3\}\}$, besides the condition $\beta \leq r = 2$. It is straightforward to check that $\{(0, 0, 0)\} \times \{0\} \in Y'_3$. If we consider $\alpha = (1, 0, 0)$, then, looking at the conditions for β , this implies $\beta = 1$, and we have $\{(1, 0, 0)\} \times \{1\} \in Y'_3$. Similarly, we have $\{(0, 1, 0)\} \times \{1\}, \{(0, 0, 1)\} \times \{1\} \in Y'_3$. Finally, if we take $\alpha = (1, 1, 1)$, this implies $\beta = 2$ and $\{(1, 1, 1)\} \times \{2\} \in Y'_3$. In fact, one can check that these are all the elements of Y'_3 . For example, if we have $\alpha = (1, 1, 0)$, then we must also have $\alpha_1 + \alpha_2 = 2 \leq \beta$, but $\beta \leq 1 + \min\{\alpha_i, 1 \leq i \leq 3\} = 1$, a contradiction. A similar reasoning applies to $\alpha = (1, 0, 1)$ or $\alpha = (0, 1, 1)$, and also for the cases where $\alpha_i = 2$ for some $1 \leq i \leq 3$.

Therefore, we have

$$Y'_3 = \{(0, 0, 0)\} \times \{0\}, \{(1, 0, 0), (0, 1, 0), (0, 0, 1)\} \times \{1\}, \{(1, 1, 1)\} \times \{2\}.$$

Now we compute $B_{\alpha, \beta}$, for each $(\alpha, \beta) \in Y'_3$:

$$B_{(0,0,0),0} = 3d_2(\text{RS}(k_1)) = 3(n - k_1 + 2) = 9,$$

$$B_{(1,0,0),1} = B_{(0,1,0),1} = B_{(0,0,1),1} = d_1(\text{RS}(k_1)) + 2 \max\{d_2(\text{RS}(k_1)), d_1(\text{RS}(k_2))\} = 10,$$

$$B_{(1,1,1),1} = 3d_1(\text{RS}(k_2)) = 3(n - k_2 + 1) = 12.$$

Hence, we obtain

$$d_2(C) \geq \min_{(\alpha, \beta) \in Y'_3} B_{\alpha, \beta} = 9.$$

It can be checked with a computer that this is the true value of $d_2(C)$.

5 An upper bound for the GHWs

In this section we give an upper bound for the GHWs of MPCs, complementing the previous section, as this will allow us to ensure that our bound is sharp when both bounds coincide. For this result, we do not require A to be NSC. We recall that $R_\ell = (a_{\ell 1}, \dots, a_{\ell h})$ is the ℓ -th row of A , for $1 \leq \ell \leq s$; δ_ℓ is the minimum distance of the code C_{R_ℓ} generated by $\{R_1, \dots, R_\ell\}$; and A_ℓ is the matrix formed by the first ℓ rows of A . The proof of the following result is a generalization of the proof in Hernando et al. (2009, Thm. 1) for the minimum distance.

Proposition 5.1 Let $C_s \subset \cdots \subset C_1 \subset \mathbb{F}_q^n$, and $C = [C_1, \dots, C_s] \cdot A$, where $A \in \mathbb{F}_q^{s \times h}$ has full rank. Let $1 \leq r \leq \dim C_1$ and let $1 \leq \ell \leq s$ be such that $r \leq \dim C_\ell$. Then

$$d_r(C) \leq d_r(C_\ell) \delta_\ell.$$

Proof Let $1 \leq \ell \leq s$ be such that $r \leq \dim C_\ell$. We will obtain a subcode $D \subset C$ with $\dim D = r$ and $|\text{supp}(D)| = d_r(C_\ell) \delta_\ell$. First, we consider a subcode $D_\ell \subset C_\ell$ with $\dim D_\ell = r$ and $|\text{supp}(D_\ell)| = d_r(C_\ell)$. Let $f = \sum_{j=1}^\ell \lambda_j R_j$, with $\lambda_j \in \mathbb{F}_q$, be a codeword of C_{R_ℓ} with $\text{wt}(f) = \delta_\ell$. Then we claim that

$$D := \{[\lambda_1 v_1, \dots, \lambda_\ell v_\ell, v_{\ell+1}, \dots, v_s] \cdot A : v_1 = v_2 = \cdots = v_\ell \in D_\ell, v_{\ell+1} = v_{\ell+2} = \cdots = v_s = 0\}$$

is a subcode of C with $\dim D = r$ and $|\text{supp}(D)| = d_r(C_\ell) \cdot \delta_\ell$. It is clear that $D \subset C$ because $D_\ell \subset C_\ell \subset \cdots \subset C_1$, and $\dim D = r$ since A has full rank. Let $v \in D_\ell$, then

$$[\lambda_1 v, \dots, \lambda_\ell v] \cdot A_\ell = \left(\sum_{j=1}^\ell a_{j1} \lambda_j v, \dots, \sum_{j=1}^\ell a_{jh} \lambda_j v \right) = (vf_1, \dots, vf_h),$$

where $f = (f_1, \dots, f_h) \in \mathbb{F}_q^h$, that is, f_i is the i -th coordinate of f , for $1 \leq i \leq h$. Hence,

$$D = \{(vf_1, \dots, vf_h) \in C : v \in D_\ell\}.$$

From this expression and the fact that $|\text{supp}(D_\ell)| = d_r(C_\ell)$, we obtain

$$|\text{supp}_j(D)| = \begin{cases} d_r(C_\ell) & \text{if } f_j \neq 0, \\ 0 & \text{if } f_j = 0. \end{cases}$$

Since $\text{wt}(f) = \delta_\ell$, we have $|\text{supp}(D)| = d_r(C_\ell) \cdot \delta_\ell$. \square

Remark 5.2 In the previous result, if A is NSC, then by Blackmore and Norton (2001, Prop. 7.2) we have $\delta_\ell = (h - \ell + 1)$, for $1 \leq \ell \leq s$. Moreover, if A is triangular (that is, a column permutation of an upper triangular matrix), then the previous result holds even if the codes are not nested [this was already known to be true for the minimum distance (Blackmore and Norton 2001, Thm. 3.7)]. Indeed, we just need to consider

$$D' := \{[v_1, \dots, v_s] \cdot A : v_\ell \in D_\ell, v_j = 0 \text{ if } j \neq \ell\},$$

where we take D_ℓ as in the proof of Proposition 5.1. Since A is triangular, we have

$$D' = \{(a_{\ell 1} v, \dots, a_{\ell h} v) : v \in D_\ell\},$$

where $a_{\ell j}$ is nonzero for exactly $h - \ell + 1$ values of j , which implies $|\text{supp}(D)| = d_r(C_\ell) \cdot \delta_\ell$.

Note that the previous result does not provide any upper bound if $r > \dim C_1$, and, when $r = \dim C_1$, it only gives $d_r(C) \leq h \cdot n = N$, which cannot be sharp if $\dim C_2 \geq 1$ due to the monotony of the GHWs. This contrasts with the case of the minimum distance ($r = 1$), where one gets that the minimum of the bounds provided in Proposition 5.1 is always sharp (Hernando et al. 2009, Thm. 1). Nevertheless, for lower values of r , this bound performs well, as we see in the following example (and as we will see in Theorem 6.1).

Example 5.3 Using the setting from Example 4.11, from Proposition 5.1, we obtain

$$d_2(C) \leq 3d_2(\text{RS}(k_1)) = 9.$$

Thus, from this we can also deduce that the bound given in Example 4.11 is sharp.

6 Examples for particular families of codes

We start by considering Reed–Solomon codes $RS(k)$ with dimension k and length $n \leq q$, for which we know the GHWs from Remark 2.9. In what follows, we denote

$$d_r(RS(k)) = \begin{cases} 0 & \text{if } r = 0 \\ n - k + r & \text{if } 1 \leq r \leq k, \\ \infty & \text{if } k < r. \end{cases} \quad (8)$$

Theorem 6.1 *Let $1 \leq k_2 \leq k_1 \leq n \leq q$, let A be 2×2 NSC matrix over \mathbb{F}_q , and let $RS(k_1, k_2) := [RS(k_1), RS(k_2)] \cdot A$. For $1 \leq r \leq \dim RS(k_1, k_2) = k_1 + k_2$, we have*

$$d_r(RS(k_1, k_2)) = \begin{cases} 2n + r - (k_1 + k_2) & \text{if } r > \max\{k_1 - k_2, k_2\}, \\ \min\{2d_r(RS(k_1)), d_r(RS(k_2))\} & \text{if } r \leq \max\{k_1 - k_2, k_2\}. \end{cases}$$

Proof Let $\alpha_i \neq 0$, $\alpha_i \neq r$, for $1 \leq i \leq 2$. First, we give a lower bound for $d_r(RS(k_1, k_2))$ using Corollary 4.7. By (8) we have

$$B_{\alpha_1, \alpha_2} = \sum_{i=1}^2 \max\{n - k_1 + r - \alpha_i, n - k_2 + \alpha_{i+1}\},$$

where $i + 1$ is understood to be $i + 1 \bmod 2$. This can be expressed as

$$B_{\alpha_1, \alpha_2} = \begin{cases} 2(n - k_1 + r) - (\alpha_1 + \alpha_2) & \text{if } r \geq k_1 - k_2 + \alpha_1 + \alpha_2, \\ 2(n - k_2) + \alpha_1 + \alpha_2 & \text{if } r < k_1 - k_2 + \alpha_1 + \alpha_2. \end{cases} \quad (9)$$

We now study the minimum of B_{α_1, α_2} for all $(\alpha_1, \alpha_2) \in Y_2$, with $\alpha_i \neq 0$, $\alpha_i \neq r$, using this expression. Recall that

$$Y_2 = \left\{ (\alpha_1, \alpha_2) \in [r]^2 : \begin{array}{l} r - \dim C_1 \leq \alpha_i \leq \dim C_2, \ 1 \leq i \leq 2 \\ \alpha_1 + \alpha_2 \leq r \end{array} \right\}.$$

Let $\xi := r - (k_1 - k_2)$, and $z = \alpha_1 + \alpha_2$. Consider $(\alpha_1, \alpha_2) \in Y_2$ with $\alpha_i \neq 0$, $\alpha_i \neq r$. Then we can rewrite (9) as

$$B(z) := B_{\alpha_1, \alpha_2} = \begin{cases} 2(n - k_2) + z & \text{if } z > \xi, \\ 2(n - k_1 + r) - z & \text{if } z \leq \xi. \end{cases}$$

As a function of z , we see that $B(z)$ is an increasing function for $z > \xi$ and a decreasing function for $z \leq \xi$. Thus, the minimum for $(\alpha_1, \alpha_2) \in Y_2$, $\alpha_i \neq 0$, $\alpha_i \neq r$, is always greater than or equal to

$$B(\xi) = 2n + r - (k_1 + k_2).$$

Now we study the minimum of B_{α_1, α_2} for $(\alpha_1, \alpha_2) \in Y_2$, $\alpha_1 = 0$, $0 < \alpha_2 < r$. As before, we can write

$$B_{0, \alpha_2} = \begin{cases} 2(n - k_1 + r) - \alpha_2 & \text{if } r \geq k_1 - k_2 + \alpha_2, \\ 2n + r - (k_1 + k_2) & \text{if } r < k_1 - k_2 + \alpha_2. \end{cases}$$

As a function of α_2 , this is constant for $\alpha_2 > r - (k_1 - k_2)$, and it is decreasing for $\alpha_2 \leq r - (k_1 - k_2)$. The minimum over α_2 , with $0 < \alpha_2 < r$, is greater than or equal to

$$B_{0, r - (k_1 - k_2)} = 2n + r - (k_1 + k_2) = B(\xi).$$

The only cases left to check are $(\alpha_1, \alpha_2) = (0, 0)$ and $(\alpha_1, \alpha_2) = (0, r)$, if they are in Y_2 (the rest of the cases are also covered by symmetry between α_1 and α_2). We have

$$B_{0,0} = 2(n - k_1 + r) = 2d_r(C_1), \quad B_{0,r} = n - k_2 + r = d_r(C_2).$$

Note that $(0, 0) \in Y_2$ if and only if $r - k_1 \leq 0$, and $(0, r) \in Y_2$ if and only if $r - k_1 \leq 0$ and $r \leq k_2$ (this last condition implies $r \leq k_1$). It is straightforward to check that $B(\xi) \leq B_{0,0}$ if and only if $r \geq k_1 - k_2$, $B_{0,r} \leq B(\xi)$ always (but $(0, r) \in Y_2$ only if $r \leq k_2$), and $B_{0,0} \leq B_{0,r}$ if and only if $r \leq k_1 - k_2 - (n - k_1)$. Therefore, by Corollary 4.7, we obtain

$$d_r(\text{RS}(k_1, k_2)) \geq \begin{cases} B(\xi) & \text{if } r > \max\{k_1 - k_2, k_2\}, \\ d_r(C_2) & \text{if } k_1 - k_2 \leq k_2 \text{ and } k_1 - k_2 < r \leq k_2, \\ 2d_r(C_1) & \text{if } k_1 - k_2 > k_2 \text{ and } k_2 < r \leq k_1 - k_2, \\ d_r(C_2) & \text{if } k_1 - k_2 - (n - k_1) < r \leq \min\{k_1 - k_2, k_2\}, \\ 2d_r(C_1) & \text{if } r \leq k_1 - k_2 - (n - k_1). \end{cases} \quad (10)$$

It is straightforward to check that this lower bound is equal to the formula in the statement of the result (with the notation from (8)). By Proposition 5.1 and Corollary 2.8, the previous bound is sharp for $1 \leq r \leq \dim \text{RS}(k_1, k_2)$. \square

Remark 6.2 Note that the previous result shows that $\text{RS}(k_1, k_2)$ is t -MDS, for $t = \max\{k_1 - k_2, k_2\}$. Also note that the proof of Theorem 6.1 also works for any pair of MDS codes C_1, C_2 with dimensions $\dim C_1 = k_1, \dim C_2 = k_2$, such that $C_2 \subset C_1$.

We turn our attention now to the family of Reed-Muller codes, which is closely related to MPCs, as we see next. We denote by $\text{RM}_q(v, m)$ the Reed-Muller code of degree v in m variables over \mathbb{F}_q . We take $\mathbb{F}_q = \{\alpha_1, \dots, \alpha_q\}$. Let

$$\binom{\alpha_j}{\alpha_i} := \frac{(\alpha_j - \alpha_1) \cdots (\alpha_j - \alpha_{i-1})}{(\alpha_i - \alpha_1) \cdots (\alpha_i - \alpha_{i-1})},$$

where we understand that if $i = 1$ or $i = j$ then $\binom{\alpha_j}{\alpha_i} = 1$, and $\binom{\alpha_j}{\alpha_i} = 0$ if and only if $1 \leq j \leq i - 1$. We consider the matrix

$$\text{GRM}_q := \begin{pmatrix} \binom{\alpha_1}{\alpha_1} & \binom{\alpha_2}{\alpha_1} & \cdots & \binom{\alpha_q}{\alpha_1} \\ \binom{\alpha_1}{\alpha_2} & \binom{\alpha_2}{\alpha_2} & \cdots & \binom{\alpha_q}{\alpha_2} \\ \vdots & \vdots & \ddots & \vdots \\ \binom{\alpha_1}{\alpha_q} & \binom{\alpha_2}{\alpha_q} & \cdots & \binom{\alpha_q}{\alpha_q} \end{pmatrix}.$$

In Blackmore and Norton (2001, Section 5), the authors prove that GRM_q is NSC, and they also prove the following result.

Theorem 6.3 *The Reed-Muller codes can be recursively defined by*

$$\text{RM}_q(v, 0) = \begin{cases} \{0\} & \text{if } v < 0, \\ \mathbb{F}_q & \text{if } v \geq 0, \end{cases}$$

and for $m \geq 1$

$$\text{RM}_q(v, m) = [\text{RM}_q(v, m - 1), \dots, \text{RM}_q(v - q + 1, m - 1)] \cdot \text{GRM}_q. \quad (11)$$

For $q = 2$ and $q = 3$, we get

$$\text{GRM}_2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \text{GRM}_3 = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}.$$

In particular, this recovers the well-known result that binary Reed-Muller codes can be constructed recursively using the $(u, u + v)$ construction.

Another important aspect of Reed-Muller codes in this context is that their GHWs are known (Heijnen and Pellikaan 1998). Therefore, they provide a family in which to test our bounds, in particular Corollary 4.7 and Theorem 4.8. For example, for $q = 2$, we can bound the GHWs of $\text{RM}_2(v, m)$ with Corollary 4.7 using the GHWs of $\text{RM}_2(v, m - 1)$ and $\text{RM}_2(v - 1, m - 1)$, and we can check if the bound is sharp because we know the true values of the GHWs of $\text{RM}_2(v, m)$. We can proceed similarly for the case of $q = 3$ using Theorem 4.8. Note that we can apply our results since GRM_q is NSC and $\text{RM}_q(v_1, m) \subset \text{RM}_q(v_2, m)$ if $v_1 \leq v_2$, i.e., the codes in (11) are nested.

For example, for $q = 2$, we have

$$\text{RM}_2(v, m) = \{(u, u + v) : u \in \text{RM}_2(v, m - 1), v \in \text{RM}_2(v - 1, m - 1)\}.$$

For $1 \leq r \leq \dim \text{RM}_2(v, m)$, the bound from Corollary 4.7 with $C_1 = \text{RM}_2(v, m - 1)$ and $C_2 = \text{RM}_2(v - 1, m - 1)$ would be

$$d_r(\text{RM}_2(v, m)) \geq \min_{(\alpha_1, \alpha_2) \in Y_2} B_{\alpha_1, \alpha_2}, \quad (12)$$

where

$$B_{\alpha_1, \alpha_2} = \max\{d_r - \alpha_1(\text{RM}_2(v, m - 1)), d_{\alpha_2}(\text{RM}_2(v - 1, m - 1)) \\ + \max\{d_r - \alpha_2(\text{RM}_2(v, m - 1)), d_{\alpha_1}(\text{RM}_2(v - 1, m - 1))\},$$

and

$$Y_2 = \left\{ (\alpha_1, \alpha_2) \in [r]^2 : \begin{array}{l} r - \dim \text{RM}_2(v, m - 1) \leq \alpha_1 \leq \dim \text{RM}_2(v - 1, m - 1), \\ r - \dim \text{RM}_2(v, m - 1) \leq \alpha_2 \leq \dim \text{RM}_2(v - 1, m - 1), \\ \alpha_1 + \alpha_2 \leq r \end{array} \right\}.$$

Since $d_r(\text{RM}_2(v, m))$ is known from Heijnen and Pellikaan (1998), we can compute the bound from (12) and check if whether it gives the true minimum distance or not. We have done this for any $2 \leq m \leq 10$ and any degree $0 \leq v \leq m(q - 1)$, and the bound (12) coincides with the corresponding GHW in all of those cases. This not only seems to indicate that the bound from Corollary 4.7 might be sharp for this family, but also showcases the fact that it can be computed efficiently even for large codes.

For the case $q = 3$, we have computed the bound from Theorem 4.8 for $2 \leq m \leq 3$ variables, which also gives the true value of the corresponding GHW of $\text{RM}_3(v, m)$, $1 \leq v \leq m(q - 1)$. Since this bound is more computationally intensive to compute than the one from Corollary 4.8, is not feasible to compute it for every possible degree for a larger number of variables. Notwithstanding the foregoing, we have tested a wide range of degrees for 4 and 5 variables, and we did not find any case in which the bound did not coincide with the GHW.

Funding Open Access funding provided thanks to the CRUE-CSIC agreement with Springer Nature.

Data availability Not applicable.

Declarations

Conflict of interest The author declares that he has no conflict of interest.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

References

- Barbero AI, Munuera C (2000) The weight hierarchy of Hermitian codes. *SIAM J Discret Math* 13(1):79–104
- Beelen P, Datta M (2018) Generalized Hamming weights of affine Cartesian codes. *Finite Fields Appl* 51:130–145
- Blackmore T, Norton GH (2001) Matrix-product codes over \mathbb{F}_q . *Appl Algebra Eng Commun Comput* 12(6):477–500
- Camps-Moreno E, García-Marco I, López HH, Márquez-Corbella I, Martínez-Moro E, Sarmiento E (2024a) On the generalized Hamming weights of hyperbolic codes. *J Algebra Appl* 23(07):2550062
- Camps-Moreno E, López HH, Matthews GL, San-José R (2024b) The weight hierarchy of decreasing norm-trace codes. *Designs, Codes and Cryptography*, to appear. [arXiv:2411.13375](https://arxiv.org/abs/2411.13375)
- Fan Y, Ling S, Liu H (2014a) Homogeneous weights of matrix product codes over finite principal ideal rings. *Finite Fields Appl* 29:247–267
- Fan Y, Ling S, Liu H (2014b) Matrix product codes over finite commutative Frobenius rings. *Des Codes Cryptogr* 71(2):201–227
- Feng GL, Tzeng KK, Wei VK (1992) On the generalized Hamming weights of several classes of cyclic codes. *IEEE Trans Inf Theory* 38(3):1125–1130
- Galindo C, Hernando F, Ruano D (2015) New quantum codes from evaluation and matrix-product codes. *Finite Fields Appl* 36:98–120
- Galindo C, Hernando F, Munuera C, Ruano D (2023) Locally recoverable codes from the matrix-product construction. [arXiv:2310.15703](https://arxiv.org/abs/2310.15703)
- Gopalan P, Guruswami V, Raghavendra P (2011) List decoding tensor products and interleaved codes. *SIAM J Comput* 40(5):1432–1462
- Guruswami V (2003) List decoding from erasures: bounds and code constructions. *IEEE Trans Inf Theory* 49(11):2826–2833
- Heijnen P, Pellikaan R (1998) Generalized Hamming weights of q -ary Reed–Muller codes. *IEEE Trans Inf Theory* 44(1):181–196
- Helleseth T, Kløve T, Mykkeltveit J (1977) The weight distribution of irreducible cyclic codes with block length $n_1((q^l - 1)/N)$. *Discret Math* 18(2):179–211
- Helleseth T, Kløve T, Ytrehus O (1992) Generalized Hamming weights of linear codes. *IEEE Trans Inf Theory* 38(3):1133–1140
- Hernando F, Ruano D. Decoding of matrix-product codes. *J. Algebra Appl.*, 12(4):1250185, 15, (2013)
- Hernando F, Lally K, Ruano D (2009) Construction and decoding of matrix-product codes from nested codes. *Appl Algebra Eng Commun Comput* 20(5–6):497–507
- Hernando F, Høholdt T, Ruano D (2012) List decoding of matrix-product codes from nested codes: an application to quasi-cyclic codes. *Adv Math Commun* 6(3):259–272
- Janwa H, Lal AK (1997) On the generalized Hamming weights of cyclic codes. *IEEE Trans Inf Theory* 43(1):299–308
- Jitman S, Mankean T (2017) Matrix-product constructions for Hermitian self-orthogonal codes. *Chamchuri J Math* 9:35–51
- Kurihara J, Uyematsu T, Matsumoto R (2012) Secret sharing schemes based on linear codes can be precisely characterized by the relative generalized hamming weight. *IEICE Trans Fundam Electron Commun Comput Sci* E95.A(11):2067–2075
- Kurihara J, Matsumoto R, Uyematsu T (2015) Relative generalized rank weight of linear codes and its applications to network coding. *IEEE Trans Inf Theory* 61(7):3912–3936

- Liu H, Liu J (2020) Homogeneous metric and matrix product codes over finite commutative principal ideal rings. *Finite Fields Appl* 64:101666, 29
- Luo G, Ezerman MF, Ling S (2023a) Three new constructions of optimal locally repairable codes from matrix-product codes. *IEEE Trans Inf Theory* 69(1):75–85
- Luo G, Ezerman MF, Ling S, Pan X (2023b) New families of MDS symbol-pair codes from matrix-product codes. *IEEE Trans Inf Theory* 69(3):1567–1587
- Mankean T, Jitman S (2016) Matrix-product constructions for self-orthogonal linear codes. In: 2016 12th International conference on mathematics, statistics, and their applications (ICMSA), pp 6–10
- Martínez-Peñas U (2016) On the similarities between generalized rank and Hamming weights and their applications to network coding. *IEEE Trans Inf Theory* 62(7):4081–4095
- Munuera C (1994) On the generalized Hamming weights of geometric Goppa codes. *IEEE Trans Inf Theory* 40(6):2092–2099
- Oggier F, Sboui A (2012) On the existence of generalized rank weights. In: 2012 International symposium on information theory and its applications. IEEE, Cambridge, MA, pp 406–410
- Özbudak F, Stichtenoth H (2002) Note on Niederreiter–Xing’s propagation rule for linear codes. *Appl Algebra Eng Commun Comput* 13(1):53–56
- Pellikaan R, Wu X-W, Bulygin S, Jurrius R (2018) Codes, cryptology and curves with computer algebra. Cambridge University Press, Cambridge
- San-José R (2024) A recursive construction for projective Reed–Muller codes. *IEEE Trans Inf Theory* 70(12):8511–8523
- van Asch B (2008) Matrix-product codes over finite chain rings. *Appl Algebra Eng Commun Comput* 19(1):39–49
- Wei VK (1991) Generalized Hamming weights for linear codes. *IEEE Trans Inf Theory* 37(5):1412–1418
- Yang M, Li J, Feng K, Lin D (2015) Generalized Hamming weights of irreducible cyclic codes. *IEEE Trans Inf Theory* 61(9):4905–4913

Publisher’s Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.