Designs, Codes and Cryptography
https://doi.org/10.1007/s10623-025-01718-5

Linear codes in the folded Hamming distance and the quasi MDS property

Umberto Martínez-Peñas[1] · **Rubén Rodríguez-Ballesteros**[1]

Received: 1 July 2024 / Revised: 2 June 2025 / Accepted: 15 August 2025

Abstract
In this work, we study linear codes with the folded Hamming distance, or equivalently, codes with the classical Hamming distance that are linear over a subfield. This includes additive codes. We study MDS codes in this setting and define quasi MDS (QMDS) codes and dually QMDS codes, which attain a more relaxed variant of the classical Singleton bound. We provide several general results concerning these codes, including restriction, shortening, weight distributions, existence, density, geometric description and bounds on their lengths relative to their field or alphabet sizes. We provide explicit examples and a binary construction with optimal lengths relative to their field or alphabet sizes, which beats any MDS code (in terms of length compared to the field or alphabet size).

Keywords Additive codes · Finite geometry · Folded Hamming distance · MDS codes · Polynomial ideal codes · Weight distributions

Mathematics Subject Classification 94B05 · 94B27 · 94B65

1 Introduction

In this manuscript, we study linear codes in the folded Hamming distance or, equivalently, codes in the classical Hamming distance which are linear over a subfield (this includes additive codes).

We define quasi MDS codes (or QMDS codes), which lie in between classical MDS codes and almost MDS codes [12] (their dimensions are larger than those of almost MDS codes for a given minimum distance). We show that their duals are not QMDS in general and then

Communicated by I. Landjev.

Umberto Martínez-Peñas and Rubén Rodríguez-Ballesteros have contributed equally to this work.

✉ Umberto Martínez-Peñas
umberto.martinez@uva.es

Rubén Rodríguez-Ballesteros
ruben.rodriguez22@estudiantes.uva.es

[1] IMUVa-Mathematics Research Institute, University of Valladolid, P. de Belén, 7, 47011 Valladolid, Spain

define dually QMDS codes (both themselves and their duals are QMDS), which lie between classical MDS codes and near MDS codes [10]. As we show in Sect. 6, there exist dually QMDS codes whose lengths relative to their field or alphabet size beat the MDS conjecture [2]. This makes them an interesting family of codes to study, since they have better parameters than almost and near MDS codes and at the same time can be longer than any classical MDS code for a fixed field or alphabet size.

Linear codes in the folded Hamming distance have been studied in the context of byte error correction [11], low density MDS codes [7, 27] and recently in relation to quantum codes [3]. Notice also that linear codes in the folded Hamming distance can be seen as array or matrix codes with the Hamming distance defined column-wise [7, 27]. In particular, they are a special case of linear codes in the sum-rank distance [23]. However, most properties and constructions discussed in this manuscript simply do not hold for the sum-rank distance in general [8].

Interestingly, most capacity-achieving and efficient list-decodable codes turn out to be QMDS or dually QMDS codes in the folded Hamming distance. Such codes fall under the umbrella family of polynomial ideal codes [6, 24], which include in particular folded Reed–Solomon codes and (univariate) multiplicity codes (see [6]). We show their dually QMDS property in Sect. 4.

The contributions of this manuscript are as follows. In Sect. 2, we provide some preliminary definitions and results on the folded Hamming distance, mainly concerning duality and code equivalence. In Sect. 3, we introduce QMDS and dually QMDS codes, characterize their minimum distances and dimensions and study their restricted and shortened codes. In Sect. 4, we explicitly show the existence of dually QMDS for all parameters for large field sizes (using polynomial ideal codes) and then show that the family of dually QMDS codes is dense. In Sect. 5, we study their weight distributions, which make use of the previous results on restriction and shortening, and which will be later used for bounds on code lengths. In Sect. 6, we study how long (dually) QMDS codes can be. We provide two upper bounds on the code length relative to their field or alphabet sizes, some examples of QMDS codes and a general binary construction of dually QMDS codes with optimal lengths, longer than any MDS code (relative to the alphabet size). Finally, in the Appendix, we provide a 1-1 correspondence between equivalence classes of linear codes in the folded Hamming distance and equivalence classes of pseudo arcs, which are useful for constructing MSRD codes and PMDS codes [20, 22].

2 The folded Hamming distance

In this section, we introduce the folded Hamming distance, define duality and characterize its linear isometries. In the following, $\mathbb{F}_q$ denotes the finite field with q elements. We will also denote $[n] = \{1, 2, \ldots, n\}$ and $[m, n] = \{m, m+1, \ldots, n\}$ for integers $m \leq n$.

Definition 1 For $\mathbf{c} = (\mathbf{c}_1, \ldots, \mathbf{c}_n) \in \mathbb{F}_q^{rn}$, where $\mathbf{c}_i \in \mathbb{F}_q^r$ for $i \in [n]$, its r-folded Hamming weight is defined as $\mathrm{w}_F(\mathbf{c}) = |\{i \in [n] : \mathbf{c}_i \neq 0\}|$. We define the r-folded Hamming distance between $\mathbf{c}, \mathbf{d} \in \mathbb{F}_q^{rn}$ as $\mathrm{d}_F(\mathbf{c}, \mathbf{d}) = \mathrm{w}_F(\mathbf{c}-\mathbf{d})$. In general, a code is a subset $\mathcal{C} \subseteq \mathbb{F}_q^{rn}$. We define the minimum r-folded Hamming distance of $\mathcal{C}$ as $\mathrm{d}(\mathcal{C}) = \min\{\mathrm{d}_F(\mathbf{c}, \mathbf{d}) : \mathbf{c}, \mathbf{d} \in \mathcal{C}, \mathbf{c} \neq \mathbf{d}\}$. If $\mathcal{C} \subseteq \mathbb{F}_q^{rn}$ is $\mathbb{F}_q$-linear, notice that $\mathrm{d}(\mathcal{C}) = \min\{\mathrm{w}_F(\mathbf{c}) : \mathbf{c} \in \mathcal{C} \backslash \{0\}\}$.

Definition 2 We say that $\mathcal{C}$ is a code of type $[n, r, k, d]$ if $\mathcal{C} \subseteq \mathbb{F}_q^{rn}$ is $\mathbb{F}_q$-linear, k is its dimension over $\mathbb{F}_q$ and $d = \mathrm{d}(\mathcal{C})$ is its minimum r-folded Hamming distance. We also say

that n is the (r-folded) length of the code $\mathcal{C}$. We will only say folded Hamming distance instead of r-folded Hamming distance when r is clear from the context.

Observe that the classical Hamming distance in $\mathbb{F}_q^n$ is nothing more than the 1-folded Hamming distance (the case $r = 1$, in which $\mathbb{F}_q^{rn} = \mathbb{F}_q^n$). In general, the r-folded Hamming distance in $\mathbb{F}_q^{rn}$ is nothing but the classical Hamming distance of length n over the alphabet $\mathbb{F}_q^r$. For this reason, we call n the r-folded length. Notice that the alphabet size will be q^r, but we will focus on $\mathbb{F}_q$-linear codes.

Furthermore, $\mathbb{F}_q$-linear codes in $\mathbb{F}_q^{rn}$ with the r-folded Hamming distance are the same as $\mathbb{F}_q$-linear codes in $\mathbb{F}_{q^r}^n$ with the classical Hamming distance, due to the following. Let $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_r) \in \mathbb{F}_{q^r}^r$ be an ordered basis of $\mathbb{F}_{q^r}$ over $\mathbb{F}_q$. Define the expansion map $\varepsilon_{\boldsymbol{\beta}} : \mathbb{F}_{q^r} \longrightarrow \mathbb{F}_q^r$ by $\varepsilon_{\boldsymbol{\beta}}(c_1\beta_1 + \cdots + c_r\beta_r) = (c_1, \ldots, c_r)$, for $c_1, \ldots, c_r \in \mathbb{F}_q$. If we extend it componentwise, it is obvious that $\varepsilon_{\boldsymbol{\beta}} : \mathbb{F}_{q^r}^n \longrightarrow \mathbb{F}_q^{rn}$ is an $\mathbb{F}_q$-linear isometry considering the classical Hamming distance in $\mathbb{F}_{q^r}^n$ and the r-folded Hamming distance in $\mathbb{F}_q^{rn}$. Note, however, that over infinite fields (such as $\mathbb{R}$) there may be no field extension of degree r for every positive integer r.

Notice that additive codes with the classical Hamming distance in $\mathbb{F}_q^n$, where $q = p^r$ and p is prime, are thus equivalent to $\mathbb{F}_p$-linear codes with the folded Hamming distance in $\mathbb{F}_p^{rn}$.

We will focus on duality based on the usual inner product in $\mathbb{F}_q^{rn}$, given as follows.

Definition 3 We define the inner product between $\mathbf{c}, \mathbf{d} \in \mathbb{F}_q^{rn}$ as $\mathbf{c} \cdot \mathbf{d} = c_1d_1 + \cdots + c_{rn}d_{rn}$, where $\mathbf{c} = (c_1, \ldots, c_{rn})$ and $\mathbf{d} = (d_1, \ldots, d_{rn})$. Given an $\mathbb{F}_q$-linear code $\mathcal{C} \subseteq \mathbb{F}_q^{rn}$, we define its dual as $\mathcal{C}^\perp = \{\mathbf{d} \in \mathbb{F}_q^{rn} : \mathbf{c} \cdot \mathbf{d} = 0, \text{ for all } \mathbf{c} \in \mathcal{C}\}$.

Notice that the usual inner product in $\mathbb{F}_q^{rn}$ is not $\mathbb{F}_{q^r}$-bilinear when considered in $\mathbb{F}_{q^r}^n$ via the maps $\varepsilon_{\boldsymbol{\beta}}$. However, when considering $\mathbb{F}_{q^r}$-linear codes, their duals with respect to the usual inner products in $\mathbb{F}_{q^r}^n$ and $\mathbb{F}_q^{rn}$ coincide if we use appropriate expansion maps.

Proposition 4 *Let $\mathcal{C} \subseteq \mathbb{F}_{q^r}^n$ be an $\mathbb{F}_{q^r}$-linear code and let $\mathcal{C}^\perp \subseteq \mathbb{F}_{q^r}^n$ denote its dual with respect to the usual inner product in $\mathbb{F}_{q^r}^n$. If $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_r)$ and $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_r)$ are dual ordered bases of $\mathbb{F}_{q^r}$ over $\mathbb{F}_q$ (i.e., $\mathrm{Tr}(\beta_i\alpha_j) = \delta_{i,j}$, where* Tr *is the trace of $\mathbb{F}_{q^r}$ over $\mathbb{F}_q$), then*

$$\varepsilon_{\boldsymbol{\beta}}\left(\mathcal{C}^\perp\right) = \varepsilon_{\boldsymbol{\alpha}}(\mathcal{C})^\perp.$$

(Dual bases of $\mathbb{F}_{q^r}$ over $\mathbb{F}_q$ always exist, see [19, p. 54].)

Proof By counting dimensions over $\mathbb{F}_q$, we only need to show that $\varepsilon_{\boldsymbol{\beta}}\left(\mathcal{C}^\perp\right) \subseteq \varepsilon_{\boldsymbol{\alpha}}(\mathcal{C})^\perp$. Now this holds since, given $\mathbf{c} = (c_1, \ldots, c_n) \in \mathcal{C}$ and $\mathbf{d} = (d_1, \ldots, d_n) \in \mathcal{C}^\perp$, with $\varepsilon_{\boldsymbol{\beta}}(c_i) = (c_{i,1}, \ldots, c_{i,r})$ and $\varepsilon_{\boldsymbol{\alpha}}(d_i) = (d_{i,1}, \ldots, d_{i,r})$, for $i \in [n]$, we have that

$$0 = \mathrm{Tr}(0) = \mathrm{Tr}\left(\sum_{i=1}^{n} c_i d_i\right) = \sum_{i=1}^{n}\sum_{j=1}^{r}\sum_{k=1}^{r} c_{i,j}d_{i,k}\mathrm{Tr}(\beta_j\alpha_k) = \sum_{i=1}^{n}\sum_{j=1}^{r} c_{i,j}d_{i,j}.$$

□

Finally, we notice that the folded Hamming distance in $\mathbb{F}_q^{rn}$ coincides with the sum-rank distance in such a space by considering a vector in $\mathbb{F}_q^{rn}$ as a tuple of n matrices over $\mathbb{F}_q$ of size $1 \times r$. See [23] for more information on the sum-rank distance. In particular, the $\mathbb{F}_q$-linear isometries for the folded Hamming distance are known, see [21, Th. 2].

Proposition 5 [[21]] *Let $\phi : \mathbb{F}_q^{rn} \longrightarrow \mathbb{F}_q^{rn}$ be an $\mathbb{F}_q$-linear vector space isomorphism. Then $\mathrm{w}_F(\phi(\mathbf{c})) = \mathrm{w}_F(\mathbf{c})$, for all $\mathbf{c} \in \mathbb{F}_q^{rn}$, if and only if there exist invertible matrices $A_1, \ldots, A_n \in \mathrm{GL}_r(\mathbb{F}_q)$ and a permutation $\sigma : [n] \longrightarrow [n]$ such that, for all $\mathbf{c}_1, \ldots, \mathbf{c}_n \in \mathbb{F}_q^r$,*

$$\phi(\mathbf{c}_1, \ldots, \mathbf{c}_n) = \left(\mathbf{c}_{\sigma(1)} A_1, \ldots, \mathbf{c}_{\sigma(n)} A_n\right).$$

Definition 6 We say that two linear codes $\mathcal{C}, \mathcal{C}' \subseteq \mathbb{F}_q^{rn}$ are equivalent if there is an $\mathbb{F}_q$-linear isometry for the folded Hamming distance $\phi : \mathbb{F}_q^{rn} \longrightarrow \mathbb{F}_q^{rn}$ such that $\mathcal{C}' = \phi(\mathcal{C})$.

The following result is straightforward from Proposition 5.

Corollary 7 *Two linear codes are equivalent if, and only if, so are their duals.*

However, note that the results that we will obtain in this manuscript are either unkown or simply do not hold for the sum-rank distance in general. For instance, MacWilliams equations (Theorem 5) do not exist in general for the sum-rank distance [8].

Throughout the remainder of the manuscript, linear will mean $\mathbb{F}_q$-linear. Notice that the alphabet size will be considered as q^r, i.e., it is not the same as the size of the field of linearity.

3 Quasi MDS codes

In this section, we provide a relaxed version of the Singleton bound and define and study QMDS and dually QMDS codes.

Item 1 in the following proposition is equivalent to the classical Singleton bound for linear or non-linear codes in the classical Hamming distance [17, Th. 2.4.1]. Item 2 is straightforward from Item 1, and Item 3 is the dual statement.

Proposition 8 *Let $\mathcal{C}$ be a linear code of type $[n, r, k, d]$ and let $\mathcal{C}^\perp$ be its dual, of type $[n, r, rn - k, d^\perp]$. Then*

1. $k \leq r(n - d + 1)$,
2. $d \leq n - \lceil \frac{k}{r} \rceil + 1 = n - \lfloor \frac{k-1}{r} \rfloor$, *and*
3. $d^\perp \leq \lfloor \frac{k}{r} \rfloor + 1 = \lceil \frac{k+1}{r} \rceil$.

As usual, a linear code is MDS if it attains the bound in Item 1. If $r \mid k$ (necessary for the code to be MDS), then Items 1 and 2 coincide. However, when $r \nmid k$, the second bound may be attained but the first one cannot. This motivates the following definition.

Definition 9 We say that a linear code of type $[n, r, k, d]$ is quasi-MDS or QMDS if $d = n - \lceil \frac{k}{r} \rceil + 1 = n - \lfloor \frac{k-1}{r} \rfloor$. A linear MDS code is a QMDS code such that $r \mid k$.

Remark 10 Considering $\mathbb{F}_q$-linear codes in $\mathbb{F}_{q^r}^n$ with the classical Hamming distance, which is equivalent to $\mathbb{F}_q$-linear codes in $\mathbb{F}_q^{rn}$ with the r-folded Hamming distance (see Sect. 2), we have that the dimension of an $\mathbb{F}_q$-linear code $\mathcal{C} \subseteq \mathbb{F}_{q^r}^n$ is of the form $k = r\lfloor \frac{k}{r} \rfloor + \rho$ with $0 \leq \rho < r$. If $d = \mathrm{d}(\mathcal{C})$ (its classical minimum Hamming distance in $\mathbb{F}_{q^r}^n$ or its minimum r-folded Hamming distance in $\mathbb{F}_q^{rn}$), then:

1. $\mathcal{C}$ is MDS (in the classical sense) when $k = r(n - d + 1)$.
2. $\mathcal{C}$ is QMDS but not MDS when $k = r(n - d) + \rho$ and $0 < \rho < r$.
3. $\mathcal{C}$ is almost MDS [12] when $k = r(n - d)$.

Therefore, for a prefixed ambient space ($\mathbb{F}_{q^r}^n$ in the classical Hamming distance or $\mathbb{F}_q^{rn}$ in the r-folded Hamming distance) and a given minimum distance, we see that QMDS codes lie in between classical MDS codes and almost MDS codes in terms of dimensions for a given minimum distance.

The dual of a linear MDS code is MDS, also for the folded Hamming distance. The following result has been independently proven in [7, Lemma 3.3], [27, Th. 1] and [3, Th. 9].

Proposition 11 ([3, 7, 27]) *A linear code $\mathcal{C} \subseteq \mathbb{F}_q^{rn}$ is MDS if, and only if, so is its dual.*

However, this is not the case for QMDS codes in general.

Example 12 Over any field, the linear code of type [3, 3, 4, 2] with the following generator matrix is QMDS but its dual is of type [3, 3, 5, 1], thus not QMDS:

$$G = \left(\begin{array}{ccc|ccc|ccc} 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \end{array}\right).$$

This motivates the following definition (we will give examples in Sects. 4 and 6).

Definition 13 A linear code is dually QMDS if both itself and its dual are QMDS.

Remark 14 A q-analog of QMDS and dually QMDS codes have been considered before [9], called quasi maximum rank distance (QMRD) and dually QMRD codes. However, in the rank metric there exist linear MRD codes for any choice of parameters [13]. In contrast, QMDS and dually QMDS codes may attain lengths and alphabet sizes not achievable by MDS codes as we show in Sect. 6. Other properties make the folded-Hamming-metric counterpart different in essence, such as the density results (Sect. 4) or their applications in practice [3, 6, 7].

A first observation is that the dually QMDS property is preserved by equivalence, which follows from Corollary 7.

Proposition 15 *A code that is equivalent to a dually QMDS code is also dually QMDS.*

We may also characterize dually QMDS codes in terms of the sum of the distances of the code and its dual.

Proposition 16 *Let $\mathcal{C}$ be a linear code of type $[n, r, k, d]$ and let $\mathcal{C}^\perp$ be its dual, of type $[n, r, rn-k, d^\perp]$. If $r \mid k$, then either $d + d^\perp = n + 2$ or $d + d^\perp \leq n$, whereas if $r \nmid k$, then $d + d^\perp \leq n + 1$. Furthermore, the following hold:*

1. *$\mathcal{C}$ is MDS if, and only if, $\mathcal{C}^\perp$ is MDS if, and only if, $d + d^\perp = n + 2$.*
2. *$\mathcal{C}$ is dually QMDS and $r \nmid k$ if, and only if, $d + d^\perp = n + 1$.*

Proof If we add the Singleton bounds for $\mathcal{C}$ and $\mathcal{C}^\perp$ (Items 2 and 3 in Proposition 8), we obtain

$$d + d^\perp \leq \left(n - \left\lceil \frac{k}{r} \right\rceil + 1\right) + \left(\left\lfloor \frac{k}{r} \right\rfloor + 1\right) \leq n + 2.$$

Notice however that, if $r \nmid k$, then $\lceil \frac{k}{r} \rceil = \lfloor \frac{k}{r} \rfloor + 1$, which implies in this case that $d + d^\perp \leq n+1$. Note also that, if $r \mid k$ and $d + d^\perp = n+1$, then $\mathcal{C}$ is MDS but $\mathcal{C}^\perp$ is not (or viceversa), which is not possible by Proposition 11. Thus if $r \mid k$ and $d + d^\perp < n+2$, then $d + d^\perp \leq n$.

In particular, $d + d^\perp = n+2$ may only happen if $r \mid k$, in which case it must also hold that $k = r(n-d+1)$ and $rn - k = r(n - d^\perp + 1)$, and $\mathcal{C}$ (thus $\mathcal{C}^\perp$) is MDS. Conversely, if $\mathcal{C}$ (thus $\mathcal{C}^\perp$) is MDS, then we have $d + d^\perp = n+2$, and Item 1 is proven.

Similarly, if $r \nmid k$ and $d + d^\perp = n+1$, then equalities in both Items 2 and 3 in Proposition 8 must hold, i.e., $\mathcal{C}$ is dually QMDS. The reversed implication is straightforward and Item 2 is proven. □

Remark 17 Notice that for $\mathbb{F}_q$-linear near MDS codes [10] in $\mathbb{F}_q^{rn}$ for the r-folded Hamming distance (or, equivalently, in $\mathbb{F}_{q^r}^n$ for the classical Hamming distance), it holds that $d + d^\perp = n$. Since $d + d^\perp = n+2$ for MDS codes and $d + d^\perp = n+1$ for dually QMDS codes which are not MDS, we see that the latter lies in between classical MDS codes and near MDS codes in terms of $d + d^\perp$, as stated in the Introduction. See also Remark 10.

As in the classical case of MDS codes, we may characterize QMDS codes in terms of their generator and parity-check matrices. We start with the following result, which generalizes [17, Cor. 1.4.14 & Th. 1.4.15] from $r = 1$ to $r \geq 1$ in general. For a $k \times (rn)$ matrix $G = (G_1 | \ldots | G_n)$, where G_i is of size $k \times r$, we say that G_i is the ith column block of G formed by r columns.

Proposition 18 *Let $\mathcal{C}$ be a linear code of type $[n, r, k, d]$ with generator matrix G and parity-check matrix H.*

1. *d is the maximum number such that the submatrix formed by the $r(n-d+1)$ columns of any set of $n-d+1$ column blocks of G has rank k.*
2. *$d-1$ is the maximum number such that the submatrix formed by the $r(d-1)$ columns of any set of $d-1$ column blocks of H has rank $r(d-1)$.*

Proof For Item 1, d is the minimum number such that it is possible to obtain zeros in $n-d$ column blocks by making (nontrivial) linear combinations with the rows of G. As a consequence, any submatrix formed by the columns of G in $n-d+1$ column blocks must have rank k since $k \leq r(n-d+1)$, and there exists $n-d$ column blocks in G whose $r(n-d)$ columns form a matrix of rank lower than k.

For Item 2, since $HG^\intercal = 0$, any set of $n-d+1$ column blocks of G has maximum rank if, and only if, it is not possible to obtain zeros in $n - (n-d+1) = d-1$ column blocks in nontrivial linear combinations of the rows of H. In other words, any submatrix formed by the columns of H in $d-1$ column blocks must have rank $r(d-1)$ since $r(d-1) \leq rn - k$. □

As a consequence, we obtain the following characterizations of QMDS codes, which recovers the characterizations of classical MDS codes [17, Th. 2.4.3] when $r = 1$.

Corollary 19 *Let $\mathcal{C}$ be a linear code of type $[n, r, k, d]$ with generator matrix G and parity-check matrix H. The following are equivalent:*

1. *$\mathcal{C}$ is QMDS.*
2. *Any $k \times r\lceil \frac{k}{r} \rceil$ submatrix of G formed by $\lceil \frac{k}{r} \rceil$ column blocks has rank k.*
3. *Any $(rn-k) \times r(n - \lceil \frac{k}{r} \rceil)$ submatrix of H formed by $n - \lceil \frac{k}{r} \rceil$ column blocks has rank $r(n - \lceil \frac{k}{r} \rceil)$.*

In particular, $\mathcal{C}$ is dually QMDS if, and only if, any $k \times r\lceil \frac{k}{r} \rceil$ submatrix of G formed by $\lceil \frac{k}{r} \rceil$ column blocks has rank k and any $k \times r\lfloor \frac{k}{r} \rfloor$ submatrix of G formed by $\lfloor \frac{k}{r} \rfloor$ column blocks has rank $r\lfloor \frac{k}{r} \rfloor$.

Remark 20 Note that Proposition 11 follows immediately from the previous corollary.

We now turn to restricted and shortened codes. Apart from being of interest on their own, we will use them when computing the weight distribution of dually QMDS codes in Sect. 5.

Definition 21 Given $I \subseteq [n]$, we define the projection $\pi_I : \mathbb{F}_q^{rn} \longrightarrow \mathbb{F}_q^{r|I|}$ such that $\pi_I(\mathbf{c}_1, \ldots, \mathbf{c}_n) = (\mathbf{c}_i)_{i \in I}$, for $\mathbf{c}_1, \ldots, \mathbf{c}_n \in \mathbb{F}_q^r$.

Definition 22 Given a code $\mathcal{C} \subseteq \mathbb{F}_q^{rn}$ and $I \subseteq [n]$, we define the restricted code $\mathcal{C}^I = \pi_I(\mathcal{C})$, the null subcode $\mathcal{C}(I) = \mathcal{C} \cap \ker(\pi_I)$ and the shortened code $\mathcal{C}_I = \pi_I(\mathcal{C}([n] \backslash I))$.

Restricting and shortening QMDS codes yield again QMDS codes.

Proposition 23 *Let $\mathcal{C}$ be a linear code of type $[n, r, k, d]$.*

1. *$\mathcal{C}$ is QMDS if, and only if, $\mathcal{C}^I$ is of dimension k for all $I \subseteq [n]$ with $r|I| \geq k$.*
2. *If $\mathcal{C}$ is QMDS, then $\mathcal{C}^I$ is of dimension k^I with $r(|I| - 1) < k^I \leq r|I|$ for all $I \subseteq [n]$ with $r|I| < k$.*
3. *$\mathcal{C}$ is QMDS if, and only if, $\mathcal{C}_I = 0$ for all $I \subseteq [n]$ with $r(n - |I|) \geq k$.*
4. *If $\mathcal{C}$ is QMDS, then $\mathcal{C}_I$ is of dimension k_I with $k - r(n - |I|) \leq k_I < k - r(n - |I|) + r$ for all $I \subseteq [n]$ with $r(n - |I|) < k$.*

Furthermore, if $\mathcal{C}$ is QMDS, then so are $\mathcal{C}^I$ and $\mathcal{C}_I$, for all $I \subseteq [n]$.

Proof Item 1 (including the fact that $\mathcal{C}^I$ is QMDS) follows directly from Corollary 19.

For Item 3, we have $d > n - \lceil \frac{k}{r} \rceil$ if, and only if, $\mathcal{C}_I = 0$ for all $I \subseteq [n]$ with $|I| \leq n - \lceil \frac{k}{r} \rceil$, which is equivalent to $r(n - |I|) \geq k$.

Next we prove Item 2. Let $I \subseteq [n]$ with $r|I| < k$. Consider a generator matrix G of $\mathcal{C}$, and let G_I be the submatrix of G formed by the column blocks indexed by I. Since G_I is of size $k \times (r|I|)$ and $r|I| < k$, there can be at most $r - 1$ columns in G_I that linearly depend on the rest of the columns of G_I (otherwise there is a $k \times r\lceil \frac{k}{r} \rceil$ submatrix of G of rank smaller than k, contradicting Corollary 19). Hence $k^I = \dim(\mathcal{C}^I) \geq r|I| - (r - 1) > r(|I| - 1)$ and any nonzero linear code in $\mathbb{F}_q^{r|I|}$ of such a dimension is QMDS.

Finally we prove Item 4. Let $I \subseteq [n]$ with $r(n - |I|) < k$. We have $k - k_I = \dim(\pi_{[n]\backslash I}(\mathcal{C})) \leq r(n - |I|)$. Thus

$$\mathrm{d}(\mathcal{C}_I) \geq d = n - \left\lceil \frac{k}{r} \right\rceil + 1 \geq n - \left\lceil \frac{r(n - |I|) + k_I}{r} \right\rceil + 1 = |I| - \left\lceil \frac{k_I}{r} \right\rceil + 1.$$

By the Singleton bound, $\mathcal{C}_I$ is QMDS and the inequalities above are equalities. In particular, $k_I + r(n - |I|) \leq r\lceil \frac{k}{r} \rceil < k + r$, hence $k_I < k - r(n - |I|) + r$. □

Similarly, any restriction and shortening of a dually QMDS code is again a dually QMDS code. Moreover, their dimensions characterize the dually QMDS property.

Theorem 1 *For a linear code $\mathcal{C}$ of type $[n, r, k, d]$, the following are equivalent:*

1. *$\mathcal{C}$ is dually QMDS.*
2. *$\dim(\mathcal{C}^I) = k$ if $r|I| \geq k$ and $\dim(\mathcal{C}^I) = r|I|$ if $r|I| < k$, for all $I \subseteq [n]$.*

3. $\dim(\mathcal{C}_I) = k - r(n - |I|)$ *if* $r(n - |I|) \leq k$ *and* $\dim(\mathcal{C}_I) = 0$ *if* $r(n - |I|) > k$, *for all* $I \subseteq [n]$.

Furthermore, if $\mathcal{C}$ *is dually QMDS, then so are* $\mathcal{C}^I$ *and* $\mathcal{C}_I$, *for all* $I \subseteq [n]$.

Proof We first show that Item 2 implies Item 1. We will repeatedly use $(\mathcal{C}^I)^\perp = (\mathcal{C}^\perp)_I$ (see [17, Th. 1.5.7]). First, from $\dim(\mathcal{C}^I) = k$ if $r|I| \geq k$, we deduce that $\mathcal{C}$ is QMDS by Proposition 23. Next, if $|I| \leq \lfloor \frac{k}{r} \rfloor$, then

$$\dim((\mathcal{C}^\perp)_I) = \dim((\mathcal{C}^I)^\perp) = r|I| - \dim(\mathcal{C}^I) = r|I| - r|I| = 0,$$

which means that $\mathrm{d}(\mathcal{C}^\perp) \geq \lfloor \frac{k}{r} \rfloor + 1$, and we conclude that $\mathcal{C}$ is dually QMDS.

Using $(\mathcal{C}^I)^\perp = (\mathcal{C}^\perp)_I$, one can similarly show that Item 3 implies Item 1. Therefore, we only need to prove that Item 1 implies Items 2 and 3, and that $\mathcal{C}^I$ and $\mathcal{C}_I$ are dually QMDS.

Assume that $\mathcal{C}$ is dually QMDS. First, $\mathcal{C}^I$ and $\mathcal{C}_I$ are QMDS by Proposition 23. Using that $(\mathcal{C}^I)^\perp = (\mathcal{C}^\perp)_I$, $(\mathcal{C}_I)^\perp = (\mathcal{C}^\perp)^I$ and that $\mathcal{C}^\perp$ is also QMDS, we deduce that both $\mathcal{C}^I$ and $\mathcal{C}_I$ are dually QMDS, again by Proposition 23.

We now compute dimensions. If $r|I| \geq k$, then $\dim(\mathcal{C}^I) = k$ by Proposition 23. Now assume that $r|I| < k$. Since $\mathcal{C}^\perp$ is QMDS and $r(n - |I|) > \dim(\mathcal{C}^\perp)$, then $\dim((\mathcal{C}^\perp)_I) = 0$ by Proposition 23. Using again $(\mathcal{C}^I)^\perp = (\mathcal{C}^\perp)_I$, we have

$$\dim(\mathcal{C}^I) = r|I| - \dim((\mathcal{C}^I)^\perp) = r|I| - \dim((\mathcal{C}^\perp)_I) = r|I|.$$

We now turn to $\mathcal{C}_I$. First, using once again $(\mathcal{C}^I)^\perp = (\mathcal{C}^\perp)_I$, we have that

$$\dim(\mathcal{C}_I) = \dim(((\mathcal{C}^\perp)^I)^\perp) = r|I| - \dim((\mathcal{C}^\perp)^I).$$

Using the formula for $\dim((\mathcal{C}^\perp)^I)$ already computed (since $\mathcal{C}^\perp$ is dually QMDS), we obtain the formula for $\dim(\mathcal{C}_I)$ given in the proposition. □

We now illustrate how the dimension formulas in Theorem 1 do not hold for all QMDS codes.

Example 24 Consider the QMDS code $\mathcal{C}$ of type $[3, 3, 4, 2]$ from Example 12. If $I = \{3\}$, then $\dim(\mathcal{C}^I) = 2 \neq 3$ and if $I = \{1, 2\}$, then $\dim(\mathcal{C}_I) = 2 \neq 1$.

4 Existence and density of dually QMDS codes

In this section we show that dually QMDS codes exist for all parameters given a sufficiently large finite field. We first give an existential result, which also shows that the family of such codes is dense (they appear with probability approaching 1 for large fields). Then we show that the explicit codes known as polynomial ideal codes [6, 24] are dually QMDS covering general parameters for sufficiently large finite fields. Later in Sect. 6, we explore dually QMDS over small finite fields relative to their code length.

For the existence and density, we will make use of the DeMillo-Lipton-Schwartz-Zippel bound [18, Lemma 16.2]. We denote by $\mathbb{F}_q[x_1, x_2, \ldots, x_m]$ the polynomial ring in m variables $x_1, x_2, \ldots, x_m$ over $\mathbb{F}_q$. For $F \in \mathbb{F}_q[x_1, x_2, \ldots, x_m]$, we consider $\deg(F)$ as its total degree and we denote $Z(F) = \{\mathbf{a} \in \mathbb{F}_q^m : F(\mathbf{a}) = 0\}$.

Lemma 25 (**DeMillo-Lipton-Schwartz-Zippel** [18]) *Let* $F \in \mathbb{F}_q[x_1, x_2, \ldots, x_m]$. *Then*

$$|Z(F)| \leq \deg(F) \cdot q^{m-1}.$$

Proposition 26 *Let n, k, r be positive integers and let $\mathbb{F}_q$ be a finite field such that $k \leq rn$ and*

$$C(n,r,k) := k\binom{n}{\lceil \frac{k}{r} \rceil}\binom{r\lceil \frac{k}{r} \rceil}{k} + r\left\lfloor \frac{k}{r} \right\rfloor \binom{n}{\lfloor \frac{k}{r} \rfloor}\binom{k}{r\lfloor \frac{k}{r} \rfloor} < q.$$

1. *There exists at least one dually QMDS code $\mathcal{C}$ of type $[n, r, k, d]$, $d = n - \lceil \frac{k}{r} \rceil + 1$.*
2. *The probability that a code $\mathcal{C}$ of type $[n, r, k, d]$ (where d is not fixed) chosen uniformly at random is dually QMDS is at least $1 - \frac{C(n,r,k)}{q}$.*

Proof We only need to prove Item 2. Choosing a code of type $[n, r, k, d]$ (where d is not fixed) uniformly at random is equivalent to choosing a full-rank $k \times (rn)$ matrix G over $\mathbb{F}_q$ (modulo multiplying on the left by invertible $k \times k$ matrices over $\mathbb{F}_q$). We consider the entries of G as variables $x_1, x_2, \ldots, x_m$ with $m = krn$, and an instantiation of G consists in choosing a point in $\mathbb{F}_q^m$ uniformly at random and evaluating the variables $x_1, x_2, \ldots, x_m$ in such a point.

By Corollary 19, G generates a dually QMDS code if any $k \times r\lceil \frac{k}{r} \rceil$ submatrix of G formed by $\lceil \frac{k}{r} \rceil$ column blocks has rank k (QMDS condition), and any $k \times r\lfloor \frac{k}{r} \rfloor$ submatrix of G formed by $\lfloor \frac{k}{r} \rfloor$ column blocks has rank $r\lfloor \frac{k}{r} \rfloor$ (dual QMDS condition). This condition holds if all of the involved minors are nonzero, i.e., the product of all such minors is nonzero. Such a product is a polynomial $F \in \mathbb{F}_q[x_1, x_2, \ldots, x_m]$ of degree $\deg(F) = C(n, r, k) < q$. The probability that a point in $\mathbb{F}_q^m$, chosen uniformly at random, does not lie in $Z(F)$ is

$$\frac{q^m - |Z(F)|}{q^m} \geq \frac{q^m - \deg(F)q^{m-1}}{q^m} = 1 - \frac{C(n,r,k)}{q},$$

by Lemma 25, and we are done. □

Noting that $C(n, r, k)$ only depends on n, r, k and not on q, we conclude the following.

Corollary 27 *Dually QMDS codes are dense in the set of codes of type $[n, r, k, d]$ (where d is not fixed) since the probability that a uniformly random code of such a type is dually QMDS tends to 1 as q tends to infinity.*

Remark 28 In particular, the probability that a uniformly random code of type $[n, r, k, d]$ (where d is not fixed) is QMDS but not dually QMDS tends to 0 as q tends to infinity. That is, the family of such codes is sparse.

Remark 29 As shown in [15], maximum rank distance (MRD) codes which are linear over a subfield are not dense in general. Together with Corollary 27, this shows an essential difference between MRD and MDS codes that are linear over subfields. The question remains open in general for the sum-rank distance [23] (for MSRD codes that are linear over a subfield).

We now turn to an explicit construction that works for any choice of n, r, k, called polynomial ideal codes, introduced in [6], and their generalization [24]. However, their field size q is far from optimal in general (we will explore small field sizes in Sect. 6).

Definition 30 (**Polynomial ideal codes** [6, 24]) Let $F_1, F_2, \ldots, F_n \in \mathbb{F}_q[x]$ be pairwise coprime polynomials of degree r. By the Chinese remainder theorem, we have the $\mathbb{F}_q$-linear vector space isomorphism

$$\varphi : \frac{\mathbb{F}_q[x]}{\left(\prod_{i=1}^n F_i\right)} \longrightarrow \mathbb{F}_q^{rn} : F \mapsto (F \bmod F_i)_{i=1}^n,$$

where $F \bmod G$ denotes the remainder of the Euclidean division of F by G, which we identify with a vector in $\mathbb{F}_q^{\deg(G)}$ by writing its coefficients as a list. For $k \in [rn]$, we define the polynomial ideal code

$$\mathcal{C}_k^{PI}(F_1, F_2, \ldots, F_n) = \{\varphi(F) : F \in \mathbb{F}_q[x], \deg(F) < k\}.$$

Given also $A_1, \ldots, A_n \in \mathrm{GL}_r(\mathbb{F}_q)$, we define the generalized polynomial ideal code

$$\mathcal{C}_k^{PI}(F_1, \ldots, F_n; A_1, \ldots, A_n) = \{(\mathbf{c}_1 A_1, \ldots, \mathbf{c}_n A_n) : (\mathbf{c}_1, \ldots, \mathbf{c}_n) \in \mathcal{C}_k^{CR}(F_1, \ldots, F_n)\}.$$

Polynomial ideal codes recover as particular cases codes which are known to have good list-decoding properties, such as folded Reed–Solomon codes and multiplicity codes, see [6].

Clearly, generalized polynomial ideal codes are equivalent to polynomial ideal codes by Proposition 5. However, they will be necessary to express duals, as we show later.

First, we show that generalized polynomial ideal codes are always QMDS.

Theorem 2 *The generalized polynomial ideal code $\mathcal{C}_k^{PI}(F_1, \ldots, F_n; A_1, \ldots, A_n)$ from Definition 30 is QMDS of type $[n, r, k, d]$, $d = n - \lceil \frac{k}{r} \rceil + 1$.*

Proof It is enough to prove the result for polynomial ideal codes (i.e., A_i the identity matrix for all $i \in [n]$), by Proposition 5.

First, clearly the code is linear. We now show that it has dimension k. It is enough to show that if $F \in \mathbb{F}_q[x]$ of $\deg(F) < k$ satisfies $\varphi(F) = 0$, then $F = 0$, since the vector space of polynomials of degree less than k has dimension k. The condition $\varphi(F) = 0$ means that $\prod_{i=1}^n F_i$ divides F since $F_1, F_2, \ldots, F_n$ are pairwise coprime. However, $\deg(\prod_{i=1}^n F_i) = rn \geq k > \deg(F)$, thus it must hold that $F = 0$.

Now we show the QMDS property. Let $F \in \mathbb{F}_q[x]$ be such that $F \neq 0$ and $\deg(F) < k$. Assume that $d = \mathrm{d}_F(\mathcal{C}_k^{PI}(F_1, F_2, \ldots, F_n)) = \mathrm{w}_F(\varphi(F))$. Without loss of generality, we may assume that $F \bmod F_i = 0$, for $i \in [n - d]$. That is, $\prod_{i=1}^{n-d} F_i$ divides F since $F_1, F_2, \ldots, F_{n-d}$ are pairwise coprime. Therefore

$$r(n-d) = \deg\left(\prod_{i=1}^{n-d} F_i\right) \leq \deg(F) < k \leq r(n-d+1),$$

where the last inequality is the Singleton bound (Proposition 8). This means that $\lceil \frac{k}{r} \rceil = n - d + 1$, i.e., $\mathcal{C}_k^{PI}(F_1, F_2, \ldots, F_n)$ is QMDS and we are done. □

It remains to show that duals of generalized polynomial ideal codes are again QMDS. Such duals are hard to describe even in particular cases [24]. However, when F_i completely factorizes in $\mathbb{F}_q$, then the duals are of the same form [24, Th. 3.4].

Theorem 3 ([24]) *Let $a_{i,j} \in \mathbb{F}_q$, for $i \in [n]$ and $j \in [r]$, be such that $\{a_{i,1}, \ldots, a_{i,r}\} \cap \{a_{j,1}, \ldots, a_{j,r}\} = \varnothing$ if $i \neq j$ and such that $F_i = (x - a_{i,1}) \cdots (x - a_{i,r})$, for $i \in [n]$. Then for all $A_1, \ldots, A_n \in \mathrm{GL}_r(\mathbb{F}_q)$, there exist $B_1, \ldots, B_n \in \mathrm{GL}_r(\mathbb{F}_q)$ such that*

$$\mathcal{C}_k^{PI}(F_1, \ldots, F_n; A_1, \ldots, A_n)^\perp = \mathcal{C}_k^{PI}(F_1, \ldots, F_n; B_1, \ldots, B_n).$$

Combining Theorems 2 and 3, we deduce the following.

Corollary 31 *Let $a_{i,j} \in \mathbb{F}_q$, for $i \in [n]$ and $j \in [r]$, be such that $\{a_{i,1}, \ldots, a_{i,r}\} \cap \{a_{j,1}, \ldots, a_{j,r}\} = \varnothing$ if $i \neq j$ and such that $F_i = (x - a_{i,1}) \cdots (x - a_{i,r})$, for $i \in [n]$. Then for all $A_1, \ldots, A_n \in \mathrm{GL}_r(\mathbb{F}_q)$, the linear code $\mathcal{C}_k^{PI}(F_1, \ldots, F_n; A_1, \ldots, A_n)$ is dually QMDS.*

Notice that these codes may be constructed for $n = q$ (choosing $a_{i,1} = \ldots = a_{i,r}$, for all $i \in [n]$, which yields multiplicity codes). Observe that MDS codes (such that $r|k$) exist for $n = q^r + 1$. In Sect. 6, we will construct dually QMDS codes for $n = 2^{r+1} - 1$ over $\mathbb{F}_2$ for some dimensions that are not multiples of r.

Remark 32 We will see in Proposition 38 that a subcode of a QMDS code of the right dimension is again QMDS. In this way, one can obtain QMDS of any dimension for any length $n \leq q^r + 1$ by using extended Reed–Solomon codes. However, as we show in Remark 40, such subcodes are not always dually QMDS. To the best of our knowledge, the codes in Corollary 31 are the only dually QMDS codes that cover all possible lengths and dimensions (given sufficiently large fields).

5 Weight distributions

In this section, we study weight distributions of linear codes in the folded Hamming distance.

Definition 33 The (folded) weight distribution of a linear code $\mathcal{C} \subseteq \mathbb{F}_q^{rn}$ is defined as the numbers $A_j(\mathcal{C}) = |\{\mathbf{c} \in \mathcal{C} : \mathrm{w}_F(\mathbf{c}) = j\}|$, for $j \in [0, n]$.

We start by computing the weight distribution of dually QMDS codes. As in the classical MDS case, the weight distribution of dually QMDS codes only depends on their parameters, i.e., two dually QMDS codes of the same parameters have the same distribution. We later obtain a stronger result (Theorem 6) using MacWilliams equations. However, we give now a simple proof that only relies on Theorem 1.

Theorem 4 *Let $\mathcal{C}$ be a dually QMDS code of type $[n, r, k, d]$. Then $A_0 = 1$, $A_j = 0$ for all $j \in [d-1]$, and if $j \in [d, n]$, then*

$$A_j = \binom{n}{j} \sum_{i=0}^{j-d} (-1)^i \binom{j}{i} \left(q^{k-r(n-j+i)} - 1\right).$$

Proof The only non-trivial cases are those with $j \in [d, n]$. By Theorem 1, for $I \subseteq [n]$,

$$|\mathcal{C}_I| = \begin{cases} q^{k-r(n-|I|)} & \text{if } r(n-|I|) \leq k, \\ 1 & \text{if } r(n-|I|) > k. \end{cases} \tag{1}$$

Note that $N_t = \sum_{|I|=n-t} |\mathcal{C}_I|$ counts the number of words in $\mathcal{C}$ with folded weight $\leq n - t$, counted once for each $\mathcal{C}_I$ they appear in, where $|I| = n - t$. By (1), we have

$$N_t = \begin{cases} \binom{n}{t} q^{k-rt} & \text{if } rt \leq k, \\ \binom{n}{t} & \text{if } rt > k. \end{cases}$$

By the inclusion–exclusion principle, we deduce that

$$\begin{aligned} A_j &= \sum_{i=0}^{j} (-1)^i \binom{n-j+i}{i} N_{n-j+i} \\ &= \sum_{i=0}^{\lfloor \frac{k}{r} \rfloor + j - n} (-1)^i \binom{n-j+i}{i} \binom{n}{n-j+i} q^{k-r(n-j+i)} \\ &\quad + \sum_{i=\lfloor \frac{k}{r} \rfloor + j - n + 1}^{j} (-1)^i \binom{n-j+i}{i} \binom{n}{n-j+i}. \end{aligned}$$

Using $\binom{n-j+i}{i}\binom{n}{n-j+i} = \binom{n}{j}\binom{j}{i}$ and $\sum_{i=j-v+1}^{j} (-1)^i \binom{j}{i} = -\sum_{i=0}^{j-v} (-1)^i \binom{j}{i}$, we get

$$A_j = \binom{n}{j} \sum_{i=0}^{\lfloor \frac{k}{r} \rfloor + j - n} (-1)^i \binom{j}{i} \left(q^{k-r(n-j+i)} - 1\right),$$

for $j \in [d, n]$. Now, if $r \nmid k$, then we obtain the desired formula since $\lfloor \frac{k}{r} \rfloor + j - n = \lceil \frac{k}{r} \rceil - 1 + j - n = j - d$. Finally, if $r \mid k$, then $\lfloor \frac{k}{r} \rfloor + j - n = \frac{k}{r} - 1 + j - n = j - d + 1$, but the $(j-d+1)$th term in the sum is zero, and we obtain again the desired formula. □

In fact, when the code is not dually QMDS, we have certain degrees of freedom for the weight distribution of the code. We show this stronger result in Theorem 6 below. To prove it, we will need MacWilliams equations for the folded Hamming distance. MacWilliams equations for the folded Hamming distance can be derived from more general results [4, 14, 16]. However, in order to use them in our context and notation, it is shorter and easier to give a direct proof.

Theorem 5 (MacWilliams Equations) *Let $\mathcal{C}$ be a code of type $[n, r, k, d]$, and let $A_j = A_j(\mathcal{C})$ and $A_j^\perp = A_j\left(\mathcal{C}^\perp\right)$, for $j \in [0, n]$. Then, for $v \in [0, n]$,*

$$\sum_{j=0}^{n-v} \binom{n-j}{v} A_j = q^{k-rv} \sum_{j=0}^{v} \binom{n-j}{n-v} A_j^\perp.$$

Proof Denote $k = \dim(\mathcal{C})$ and $k_I = \dim\left(\mathcal{C}^I\right)$, for $I \subseteq [n]$. We have

$$\sum_{j=0}^{n-v} \binom{n-j}{v} A_j = \sum_{|I|=v} q^{k-k_I}, \tag{2}$$

for $v \in [0, n]$, since both sides count the pairs $(\mathbf{c}, I)$ such that $\mathbf{c} \in \mathcal{C}$, $I \subseteq [n]$, $|I| = v$, and $\pi_I(\mathbf{c}) = \mathbf{0}$. First, for $\mathbf{c} \in \mathcal{C}$ such that $\mathrm{w}_F(\mathbf{c}) = j$, there are $\binom{n-j}{v}$ possible sets $I \subseteq [n]$ with $|I| = v$ and $\pi_I(\mathbf{c}) = \mathbf{0}$. Second, given $I \subseteq [n]$ with $|I| = v$, there are q^{k-k_I} words in $\mathcal{C}$ with zeros in the v blocks of I, since $\dim(\mathcal{C} \cap \ker(\pi_I)) = \dim(\mathcal{C}) - \dim(\pi_I(\mathcal{C})) = k - k_I$.

Next, the right-hand side of (2) equals

$$q^{k-rv} \sum_{|I|=v} \left|\left(\mathcal{C}^I\right)^\perp\right| = q^{k-rv} \sum_{|I|=v} \sum_{j=0}^{v} A_j\left(\left(\mathcal{C}^I\right)^\perp\right) = q^{k-rv} \sum_{j=0}^{v} \sum_{|I|=v} A_j\left(\left(\mathcal{C}^I\right)^\perp\right). \tag{3}$$

Now we prove that

$$\sum_{|I|=v} A_j\left(\left(\mathcal{C}^{\perp}\right)_I\right) = \binom{n-j}{v-j} A_j^{\perp}. \tag{4}$$

Both numbers count the possible pairs $(\mathbf{c}, I)$ such that $\mathbf{c} \in \mathcal{C}^{\perp}$, $\mathrm{w}_F(\mathbf{c}) = j$, $I \subseteq [n]$, $|I| = v$, and $\pi_{[n]\setminus I}(\mathbf{c}) = \mathbf{0}$. First, for $I \subseteq [n]$ with $|I| = v$, there are $A_j\left(\left(\mathcal{C}^{\perp}\right)_I\right)$ words in $\mathcal{C}^{\perp}$ with weight j and with zeros outside the v blocks of I. Second, for $\mathbf{c} \in \mathcal{C}^{\perp}$ such that $\mathrm{w}_F(\mathbf{c}) = j$, there are $\binom{n-j}{n-v} = \binom{n-j}{v-j}$ possible sets $I \subseteq [n]$ such that $|I| = v$ and $\pi_{[n]\setminus I}(\mathbf{c}) = \mathbf{0}$.

The theorem follows by using that (2) and (3) are equal, and applying (4) together with $\left(\mathcal{C}^I\right)^{\perp} = \left(\mathcal{C}^{\perp}\right)_I$ (see [17, Th. 1.5.7]). □

In order to give the strengthening of Theorem 4, we need the following preliminary lemma.

Lemma 34 *Consider the matrices* $M_n = \left((-1)^{n-i+j}\binom{j}{n-i}\right)_{i=0,j=0}^{n,n}$ *and* $N_n = \left(\binom{n-j}{i}\right)_{i=0,j=0}^{n,n}$, *of size* $(n+1)\times(n+1)$ *over* $\mathbb{Z}$, *where* $\binom{u}{v} = 0$ *if* $v > u$. *Then* $N_n = M_n^{-1}$.

Proof We prove that $M_n N_n = I_{n+1}$, the identity of size $n+1$. The product of the ith row of M_n and the jth column of N_n is

$$\sum_{\ell=0}^{n} (-1)^{n-i+\ell} \binom{\ell}{n-i} \binom{n-j}{\ell}. \tag{5}$$

If $i < j$, then clearly (5) equals 0. If $i = j$, then (5) becomes $(-1)^{2(n-i)}\binom{n-i}{n-i}\binom{n-i}{n-i} = 1$. Finally, if $i > j$, then (5) becomes

$$\sum_{\ell=n-i}^{n-j} (-1)^{n-i+\ell} \binom{\ell}{n-i} \binom{n-j}{\ell} = \sum_{\ell=0}^{i-j} (-1)^{\ell} \binom{n-i+\ell}{n-i} \binom{n-j}{i-j-\ell}. \tag{6}$$

Now, we have that $(1+x)^{-n+i-1} = \sum_{u=0}^{\infty}(-1)^u\binom{n-i+u}{n-i}x^u$ (see [1, p. 56]) and $(1+x)^{n-j} = \sum_{v=0}^{n-j}\binom{n-j}{v}x^v$. Using these series expansions in $\mathbb{Z}[\![x]\!]$, it is straightforward to see that the right-hand side of (6) coincides with the $(i-j)$th coefficient of $(1+x)^{-n+i-1}(1+x)^{n-j} = (1+x)^{i-j-1}$, which is zero. Therefore (6) equals zero if $i > j$ and we are done. □

We may now prove the above mentioned strengthening of Theorem 4.

Theorem 6 *Let* $\mathcal{C}$ *be a linear code of type* $[n, r, k, d]$, *and denote* $d^{\perp} = \mathrm{d}(\mathcal{C})$ *and* $A_j = A_j(\mathcal{C})$, *for* $j \in [0, n]$. *Then for* $j \in [n - d^{\perp} + 1, n]$, *it holds*

$$A_j = \sum_{i=0}^{j-n+d^{\perp}-1} (-1)^i \left(\binom{n}{j}\binom{j}{i}(q^{k-r(n-j+i)} - 1) - \sum_{v=d}^{n-d^{\perp}} \binom{n-j+i}{i}\binom{n-v}{n-j+i} A_v \right).$$

In particular, the whole weight distribution of $\mathcal{C}$ *is determined by* $A_d, A_{d+1}, \ldots, A_{n-d^{\perp}}$.

Proof Denote $A_j^{\perp} = A_j(\mathcal{C}^{\perp})$. Using $A_0 = A_0^{\perp} = 1$, $A_1 = \ldots = A_{d-1} = 0$ and $A_1^{\perp} = \ldots = A_{d^{\perp}-1}^{\perp} = 0$ in Theorem 5, we have, for $u \in [0, d^{\perp} - 1]$,

$$\sum_{j=n-d^{\perp}+1}^{n-u} \binom{n-j}{u} A_j = \binom{n}{u}(q^{k-ru} - 1) - \sum_{v=d}^{n-d^{\perp}} \binom{n-v}{u} A_v.$$

We can rewrite these equations in matrix form as

$$\begin{pmatrix} \binom{d^\perp-1}{0} & \binom{d^\perp-2}{0} & \cdots & \binom{1}{0} & \binom{0}{0} \\ \binom{d^\perp-1}{1} & \binom{d^\perp-2}{1} & \cdots & \binom{1}{1} & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \binom{d^\perp-1}{d^\perp-1} & 0 & \cdots & 0 & 0 \end{pmatrix} \begin{pmatrix} A_{n-d^\perp+1} \\ A_{n-d^\perp+2} \\ \vdots \\ A_n \end{pmatrix}$$

$$= \begin{pmatrix} \binom{n}{0}(q^k-1) & \binom{n-d}{0} & \binom{n-d+1}{0} & \cdots & \binom{d^\perp}{0} \\ \binom{n}{1}(q^{k-r}-1) & \binom{n-d}{1} & \binom{n-d+1}{1} & \cdots & \binom{d^\perp}{1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \binom{n}{d^\perp-1}(q^{k-r(d^\perp-1)}-1) & \binom{n-d}{d^\perp-1} & \binom{n-d+1}{d^\perp-1} & \cdots & \binom{d^\perp}{d^\perp-1} \end{pmatrix} \begin{pmatrix} 1 \\ -A_d \\ \vdots \\ -A_{n-d^\perp} \end{pmatrix}.$$

Since the matrix on the left-hand side is $N_{d^\perp-1}$, we may solve such linear equations by multiplying by $M_{d^\perp-1}$ on the left on both sides, by Lemma 34. This tedious calculation yields

$$\begin{aligned} A_j &= \sum_{i=n-j}^{d^\perp-1} (-1)^{n-j+i} \left(\binom{i}{n-j}\binom{n}{i}(q^{k-ir}-1) - \sum_{v=d}^{n-d^\perp} \binom{i}{n-j}\binom{n-v}{i} A_v \right) \\ &= \sum_{i=0}^{j-n+d^\perp-1} (-1)^i \left(\binom{n-j+i}{n-j}\binom{n}{n-j+i}(q^{k-(i+n-j)r}-1) \right. \\ &\quad \left. - \sum_{v=d}^{n-d^\perp} \binom{n-j+i}{n-j}\binom{n-v}{n-j+i} A_v \right), \end{aligned}$$

for $j \in [n-d^\perp+1, n]$, and the theorem follows by using $\binom{n-j+i}{n-j}\binom{n}{n-j+i} = \binom{n}{j}\binom{j}{i}$. □

Remark 35 In the case of dually QMDS codes, we have $d+d^\perp \in \{n+1, n+2\}$ by Proposition 16. In that case, we have $d > n-d^\perp$ and clearly Theorem 6 recovers Theorem 4 (notice that for linear MDS codes, Theorem 6 gives $A_{n-d^\perp+1} = A_{d-1} = 0$ as expected). In all other cases, it holds that $d+d^\perp \leq n$ and we have $n-d-d^\perp+1 \geq 1$ degrees of freedom for the weight distribution of the code according to Theorem 6.

We conclude by noting that QMDS codes that are not dually QMDS never have the same weight distribution as dually QMDS codes. This fact follows by combining Theorems 4 and 5. It also follows by using Theorem 1 and noting that the first proof we gave of Theorem 4 only depends on the dimensions of the restricted codes.

Corollary 36 *A linear code $\mathcal{C}$ of type $[n,k,r,d]$ is dually QMDS if, and only if, its weight distribution $A_j(\mathcal{C})$, $j \in [n]$, is given as in Theorem 4.*

Example 37 Consider the code $\mathcal{C}$ of type $[3,3,4,2]$ from Example 12 over $\mathbb{F}_2$, which is QMDS but not dually QMDS. We observe that $A_2(\mathcal{C}) \geq 4$, since it has the following codewords of folded weight 2: $(1,0,0|1,0,0|0,0,0)$, $(0,1,0|0,1,0|0,0,0)$, $(0,0,1|0,0,0|0,1,0)$ and $(1,1,0|0,0,0|1,0,0)$. However, according to Theorem 4, a dually QMDS code of type $[3,3,4,2]$ over $\mathbb{F}_2$ satisfies $A_2 = 3$. Since there exists a dually QMDS code of type $[3,3,4,2]$ over $\mathbb{F}_2$ (a restriction of the code in Construction 1 for $r=3$), we conclude that there exist two QMDS codes with the same parameters and different weight distributions, in contrast with dually QMDS codes.

6 Long QMDS codes over small fields or alphabets

In this section, we study how long QMDS and dually QMDS codes can be over a given (preferably small) finite field or alphabet. We give two bounds and an optimal-length binary construction.

We start with a simple upper bound on the length n of QMDS codes given by the distance d and the field and alphabet sizes, q and q^r. This result is inspired by the discussion at the beginning of [25] and we prove it for arbitrary (linear or nonlinear) codes.

Theorem 7 *Let $\mathcal{C} \subseteq \mathbb{F}_q^{rn}$ be a (linear or nonlinear) code of size q^k and minimum distance $d = n - \lceil \frac{k}{r} \rceil + 1 \geq 3$ (in particular, if $\mathcal{C}$ is linear, then it is QMDS). Then*

$$n \leq d - 3 + q^{r\lceil \frac{k}{r} \rceil - k}(q^r + 1) \leq d - 3 + q^{r-1}(q^r + 1).$$

In particular, $\lceil \frac{k}{r} \rceil \leq q^{r\lceil \frac{k}{r} \rceil - k}(q^r + 1) - 2 \leq q^{r-1}(q^r + 1) - 2$.

Proof Let $I = [n] \setminus [d-3]$. Clearly $|\mathcal{C}^I| = q^k$ and $\mathrm{d}(\mathcal{C}^I) \geq 3$. Thus we may apply the classical Hamming bound to $\mathcal{C}^I$, i.e., the balls $\mathcal{B}(\mathbf{c}, 1)$ of folded Hamming radius 1 around every codeword $\mathbf{c} \in \mathcal{C}^I$ are pairwise disjoint. Thus

$$q^k \left(1 + (n - d + 3)(q^r - 1)\right) = |\mathcal{C}^I| \cdot |\mathcal{B}(\mathbf{0}, 1)| \leq |\mathbb{F}_q^{r|I|}| = q^{r(n-d+3)}.$$

This inequality can be rearranged as follows,

$$\begin{aligned} n &\leq d - 3 + \frac{q^{r(n-d+3)-k} - 1}{q^r - 1} \\ &= d - 3 + \frac{q^{r(\lceil \frac{k}{r} \rceil + 2)-k} - 1}{q^r - 1} \\ &= d - 3 + q^{r\lceil \frac{k}{r} \rceil - k} \cdot \frac{q^{2r} - 1}{q^r - 1} + \frac{q^{r\lceil \frac{k}{r} \rceil - k} - 1}{q^r - 1} \\ &< d - 3 + q^{r\lceil \frac{k}{r} \rceil - k}(q^r + 1) + 1, \end{aligned}$$

where in the last inequality we use that $0 \leq r\lceil \frac{k}{r} \rceil - k < r$, and we are done. □

Notice that if d is unrestricted, then the previous bound does not imply that n is restricted by q or r (although k is). However, in the case of dually QMDS codes, we can obtain bounds on d and n in terms of q and r based on their weight distributions (Theorem 4). This result generalizes [17, Cor. 7.4.3] from $r = 1$ to $r \geq 1$.

Theorem 8 *Let $\mathcal{C}$ be a dually QMDS code of type $[n, r, k, d]$ and denote $d^\perp = d(\mathcal{C}^\perp)$. Let $\varepsilon = r - (r\lceil \frac{k}{r} \rceil - k) \in [r]$ and $\delta = r - (k - r\lfloor \frac{k}{r} \rfloor) \in [r]$.*

1. *If $k > r$, then $d \leq q^r - 1 + \left\lfloor \frac{q^r - 1}{q^\varepsilon - 1} \right\rfloor$.*
2. *If $k < r(n-1)$, then $d^\perp = \lceil \frac{k+1}{r} \rceil \leq q^r - 1 + \left\lfloor \frac{q^r - 1}{q^\delta - 1} \right\rfloor$.*

In particular, if $r < k < r(n-1)$, then

$$n \leq \begin{cases} 2q^r - 2 & \text{if } r \mid k, \\ 2q^r - 3 + \left\lfloor \frac{q^r - 1}{q^\varepsilon - 1} \right\rfloor + \left\lfloor \frac{q^r - 1}{q^\delta - 1} \right\rfloor & \text{if } r \nmid k. \end{cases}$$

Proof The bound on n follows by adding the bounds in Items 1 and 2 and using Proposition 16 for $d + d^\perp$. Moreover, Item 2 is the dual statement of Item 1, hence we only prove the latter.

If $r \nmid k$, then $k > r$ implies $d^\perp \geq 2$ and $d = n + 1 - d^\perp \leq n - 1$ by Proposition 16. If $r \mid k$, then $k > r$ implies $k \geq 2r$, hence $d^\perp \geq 3$, thus $d = n+2-d^\perp \leq n-1$ too. Therefore in both cases ($r \mid k$ or not), we may consider A_{d+1}. By Theorem 4, we have that

$$A_{d+1} = \binom{n}{d+1}\left(q^{k+r(d+1-n)} - 1 - (d+1)\left(q^{k+r(d-n)} - 1\right)\right) \geq 0.$$

Now, we have $k + r(d-n) = k - r(\lceil \frac{k}{r} \rceil - 1) = \varepsilon$, and the previous inequality is equivalent to $q^{\varepsilon+r} - 1 \geq (d+1)\,(q^\varepsilon - 1)$. Therefore

$$d + 1 \leq \frac{q^{\varepsilon+r} - 1}{q^\varepsilon - 1} = \frac{q^{\varepsilon+r} - q^r + q^r - 1}{q^\varepsilon - 1} = q^r + \frac{q^r - 1}{q^\varepsilon - 1}.$$

□

We now turn to constructions. The first observation is that QMDS codes of lower dimension may be easily obtained from a given QMDS code (e.g., a given linear MDS code), as follows.

Proposition 38 *Let $\mathcal{C}$ be a QMDS code of type $[n, r, k, d]$ and let k' be an integer such that $r(\lceil \frac{k}{r} \rceil - 1) < k' < k$ (thus $\lceil \frac{k'}{r} \rceil = \lceil \frac{k}{r} \rceil$). Then any linear subcode of $\mathcal{C}$ of dimension k' is QMDS of type $[n, r, k', d]$.*

Corollary 39 *Let $\mathcal{C}$ be a linear MDS code of type $[n, r, r(n-1), 2]$, which exists over any field (take, e.g., the dual of the classical repetition code). For any integer k with $r(n-2) < k < r(n-1)$, any linear subcode of $\mathcal{C}$ of dimension k is a QMDS code of type $[n, r, k, 2]$.*

Thus there exist QMDS codes of dimension $r(n-2) < k < r(n-1)$ for any length n over any field. Thus the last bound in Theorem 8 does not hold for general QMDS codes when $r(n-2) < k < r(n-1)$. Moreover, since the distance is 2, this result also shows that the bound on n in Theorem 7 does not hold if $d \geq 3$ is not satisfied.

Remark 40 Notice that the QMDS codes from Corollary 39 may not be dually QMDS codes if n is longer than the bound in Theorem 8. In particular, one may not always obtain a dually QMDS code by choosing a subcode of a dually QMDS code as in Proposition 38.

Next we give a construction of optimal-length binary dually QMDS codes, longer than any MDS code, for a fixed alphabet size q^r. We first give an example.

Example 41 The linear code over $\mathbb{F}_2$ with the following generator matrix is dually QMDS of type $[7, 2, 3, 6]$:

$$G = \left(\begin{array}{cc|cc|cc|cc|cc|cc|cc} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \end{array}\right).$$

The distance of the code is 6 since any nontrivial $\mathbb{F}_2$-linear combination of the rows of G has exactly one zero block. Thus the code is QMDS. Moreover, since the rows of any block of G span the whole space $\mathbb{F}_2^2$, then the dual has distance 2 and thus the code is dually QMDS.

In order to provide the general construction, we need the following technical lemma.

Lemma 42 *Let r be a positive integer and let $\mathbf{e}_1, \ldots, \mathbf{e}_r \in \mathbb{F}_2^r$ be the vectors of the standard basis (i.e., $e_{i,j} = \delta_{i,j}$). Let $I = \{i_1, \ldots, i_t\} \subseteq [r+1]$ with $1 \leq i_1 < i_2 < \ldots < i_t \leq r+1$ and $t \geq 1$ (i.e., $I \neq \varnothing$). Finally, define $\mathbf{u}_{I,i} = \mathbf{e}_i$ for $i \in [i_t - 1]$, $\mathbf{u}_{I,i} = \mathbf{e}_{i-1}$ for $i \in [i_t + 1, r+1]$, $\mathbf{u}_{I,i_t} = \sum_{j=1}^{t-1} \mathbf{e}_{i_j}$ if $t \geq 2$ and $\mathbf{u}_{I,i_t} = \mathbf{0}$ if $t = 1$. Then, for any nonempty $J \subseteq [r+1]$, it holds that $\sum_{i \in J} \mathbf{u}_{I,i} = \mathbf{0}$ if, and only if, $J = I$.*

Proof First $\sum_{i \in J} \mathbf{u}_{I,i} = 2 \sum_{j=1}^{t-1} \mathbf{e}_{i_j} = \mathbf{0}$ if $J = I$. Now assume that $J \neq I$. If $i_t \notin J$, then all the components of $\sum_{i \in J} \mathbf{u}_{I,i}$ corresponding to $J \neq \varnothing$ equal 1, hence $\sum_{i \in J} \mathbf{u}_{I,i} \neq \mathbf{0}$. If $i_t \in J$, then there exists $j \in I \backslash J$ or $j \in J \backslash I$ with $j \neq i_t$. If $j < i_t$, then the jth component of $\sum_{i \in J} \mathbf{u}_{I,i}$ must be 1, and if $j > i_t$, then the $(j-1)$th component of $\sum_{i \in J} \mathbf{u}_{I,i}$ must be 1, thus $\sum_{i \in J} \mathbf{u}_{I,i} \neq \mathbf{0}$ and we are done. □

Construction 1 Let r be a positive integer and enumerate all the nonempty subsets of $[r+1]$ as $I_1, I_2, \ldots, I_n$, where $n = 2^{r+1} - 1$. Let $\mathcal{C} \subseteq \mathbb{F}_2^n$ be the linear code with generator matrix

$$G = \left(\begin{array}{c|c|c|c} \mathbf{u}_{I_1,1} & \mathbf{u}_{I_2,1} & \cdots & \mathbf{u}_{I_n,1} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{u}_{I_1,r+1} & \mathbf{u}_{I_2,r+1} & \cdots & \mathbf{u}_{I_n,r+1} \end{array} \right),$$

where $\mathbf{u}_{I_i,j}$ is as in the previous lemma, for $i \in [n]$ and $j \in [r+1]$.

Theorem 9 *The linear code in Construction 1 is dually QMDS of type $[2^{r+1} - 1, r, r + 1, 2^{r+1} - 2]$.*

Proof Consider a nonzero codeword $\mathbf{c} = (\mathbf{c}_1, \ldots, \mathbf{c}_n) \in \mathcal{C}$, where $\mathbf{c}_i \in \mathbb{F}_2^r$, for $i \in [n]$. There exists a nonzero $\mathbf{x} = (x_1, \ldots, x_{r+1}) \in \mathbb{F}_2^{r+1}$ such that $\mathbf{c} = \mathbf{x}G$. Define $J = \{j \in [r+1] : x_j \neq 0\}$. Since $J \neq \varnothing$, there exists $i \in [n]$ such that $J = I_i$. By Lemma 42, we deduce that $\mathbf{c}_i = \sum_{j \in J} \mathbf{u}_{J,j} = \mathbf{0}$, whereas if $\ell \in [n] \backslash \{i\}$, then $\mathbf{c}_\ell = \sum_{j \in J} \mathbf{u}_{I_\ell,j} \neq \mathbf{0}$ since $J \neq I_\ell$. In other words, $\mathrm{w}_F(\mathbf{c}) = n - 1$, and therefore $\mathrm{d}(\mathcal{C}) = n - 1$. Since the generator matrix G is clearly of full rank $r+1$, we conclude that $\mathcal{C}$ is QMDS of type $[2^{r+1} - 1, r, r+1, 2^{r+1} - 2]$. Finally, for every $i \in [n]$, the rows in the ith block of G, $\mathbf{u}_{I_i,1}, \ldots, \mathbf{u}_{I_i,r+1}$, span the whole space $\mathbb{F}_2^r$, thus there cannot be a codeword in $\mathcal{C}^\perp$ of folded weight 1. We conclude that $\mathrm{d}(\mathcal{C}) \geq 2$, which means that $\mathcal{C}^\perp$ is also QMDS and $\mathcal{C}$ is dually QMDS. □

Remark 43 The distance $d = 2^{r+1} - 2$ of the code in Construction 1 attains the bound in Item 1 in Theorem 8. Observe that in that theorem, $\varepsilon = 1$, thus such a bound is

$$q^r - 1 + \frac{q^r - 1}{q^\varepsilon - 1} = 2^r - 1 + \frac{2^r - 1}{2 - 1} = 2^{r+1} - 2 = d.$$

Moreover, for an arbitrary linear or non-linear MDS code in $\mathbb{F}_q^{rn}$ of r-folded distance d (or equivalently in $\mathbb{F}_{q^r}^n$ with classical distance d) and size q^{rk}, it is known [25] that $n \leq 2q^r - 2$ if $r < k < r(n-1)$. Notice that $q^r = |\mathbb{F}_{q^r}| = |\mathbb{F}_q^{rn}|$ is the alphabet size considering the r-folded distance as the classical Hamming distance. In the case $q = 2$, we obtain $n \leq 2^{r+1} - 2$, but the code in Construction 1 attains the length $n = 2^{r+1} - 1$, thus is longer than any MDS code for the alphabet size 2^r.

We observe also that all the known (linear or non-linear) MDS codes in $\mathbb{F}_q^{rn}$ of r-folded distance d and of size q^{rk} satisfy $n \leq q^r + 1$. In the case $q = 2$, this means $n \leq 2^r + 1$. The code in Construction 1 satisfies $n = 2^{r+1} - 1 = 2^r + 1 + (2^r - 2)$, which is strictly larger than $2^r + 1$ for $r > 1$, for the same alphabet size 2^r. Note that the bound $n \leq q^r + 1$ (known as the MDS conjecture) holds for prime alphabet sizes [2].

From the proof of Theorem 9 we also conclude the following property.

Corollary 44 *The linear code in Construction 1 is a one-weight or constant-weight code, that is, all of its nonzero codewords have the same weight.*

Furthermore, these are the longest QMDS codes of dimension k with $r+1 \leq k \leq 2r$ over $\mathbb{F}_2$.

Proposition 45 *Let r and k be positive integers such that $r+1 \leq k \leq 2r$. If there exists a QMDS code of type $[n, r, k, n-1]$ over $\mathbb{F}_2$, then $n \leq 2^{r+1}-1$.*

Proof By choosing an $(r+1)$-dimensional subcode, we may assume that there exists a QMDS code of type $[n, r, r+1, n-1]$ over $\mathbb{F}_2$ by Proposition 38. Consider a generator matrix of the code $G = (G_1|\ldots|G_n)$, where G_i is a binary $(r+1)\times r$ matrix. If $\mathbf{v}_{i,1}, \ldots, \mathbf{v}_{i,r+1} \in \mathbb{F}_2^r$ denote the rows of G_i, then there must exist a nonempty $I_i \subseteq [r+1]$ such that $\sum_{j\in I_i} \mathbf{v}_{i,j} = \mathbf{0}$. Therefore, given a nonzero $\mathbf{x} = (x_1, \ldots, x_{r+1}) \in \mathbb{F}_2^{r+1}$, the codeword $\mathbf{c} = \mathbf{x}G$ is zero at least in the ith block if it holds that $I_i = \{j \in [r+1] : x_j = 0\}$ (I_i is the support of $\mathbf{x}$). Since the code has distance $n-1$, then the nonempty sets $I_1, \ldots, I_n$ must be all distinct, and thus $n \leq 2^{r+1}-1$. □

In fact, for $r+2 \leq k \leq 2r$, lengths $n = 2^{r+1}-1$ are not achievable over $\mathbb{F}_2$ by dually QMDS codes.

Proposition 46 *Assume that $r \geq 2$ and $r+2 \leq k \leq 2r$. If there exists a dually QMDS code of type $[n, r, k, n-1]$ over $\mathbb{F}_2$, then*

$$n \leq \frac{4}{3}(2^r-1)+1 < 2^{r+1}-2.$$

Proof By Theorem 8, we have that

$$n-1 = d \leq 2^r - 1 + \frac{2^r-1}{2^\varepsilon - 1},$$

where $\varepsilon = r - (r\lceil \frac{k}{r} \rceil - k) = r - (2r-k) = k-r \geq 2$. Therefore, we conclude that

$$n-1 \leq 2^r - 1 + \frac{2^r-1}{4-1} = \frac{4}{3}(2^r-1),$$

and we are done. □

We conclude the section with some examples of binary linear QMDS codes that are longer than any possible MDS code for a fixed alphabet size q^r.

Example 47 The linear code over $\mathbb{F}_2$ with the following generator matrix is QMDS of type $[9, 2, 13, 3]$:

$$G = \left(\begin{array}{ccccccccc|cc|cc|cc} 1&0&0&0&0&0&0&0&0&1&0&1&0&0&0\\ 0&1&0&0&0&0&0&0&0&0&1&0&0&0&1\\ 0&0&1&0&0&0&0&0&0&0&0&0&1&0&1\\ 0&0&0&1&0&0&0&0&0&1&0&1&1&0&0\\ 0&0&0&0&1&0&0&0&0&0&1&1&0&0&0\\ 0&0&0&0&0&1&0&0&0&0&0&0&1&0&1\\ 0&0&0&0&0&0&1&0&0&1&0&1&0&1&0\\ 0&0&0&0&0&0&0&1&0&1&1&0&0&0&1\\ 0&0&0&0&0&0&0&0&1&0&1&1&0&0&1\\ 0&0&0&0&0&0&0&0&0&0&0&0&1&1&1\\ 0&0&0&0&0&0&0&0&0&1&0&0&0&1&1\\ 0&0&0&0&0&0&0&0&0&0&1&1&1&0&1\\ 0&0&0&0&0&0&0&0&0&1&1&1&1&1&1 \end{array}\right).$$

Notice that a (linear or nonlinear) MDS code of distance $d = 3$ must satisfy $n \leq q^r + 1$ by Theorem 7. In the case $q = r = 2$ as in this example, it must satisfy $n \leq 5$. However, the QMDS code of distance $d = 3$ in this example satisfies $n = 9$. Note also that, for this code, $\lceil \frac{k+1}{r} \rceil = 7 > 6 \geq 2^r - 1 + \lfloor \frac{2^r-1}{2^s-1} \rfloor$, thus the bound on k in Theorem 8, Item 2, does not hold for general QMDS codes.

Example 48 The linear code over $\mathbb{F}_2$ with the following generator matrix is dually QMDS of type $[6, 2, 5, 4]$:

$$G = \left(\begin{array}{cc|cc|cc|cc|cc} 1&0&0&0&0&1&0&0&1&1\\ 0&1&0&0&0&0&1&1&0&1\\ 0&0&1&0&1&1&0&0&1&1\\ 0&0&0&1&0&0&1&1&1&0\\ 0&0&0&0&1&0&0&1&0&1 \end{array}\right).$$

According to the MDS conjecture, a (linear or nonlinear) MDS code in $\mathbb{F}_2^{rn}$ with $r = 2$ must satisfy $n \leq 2^r + 1 = 5$. However, the dually QMDS code in this example satisfies $n = 6$.

A Pseudo arcs: a geometric description

In this Appendix, we provide a finite-geometry counterpart of linear codes in the folded Hamming distance, which coincides with what is called arcs or pseudo arcs in the finite-geometry literature [3]. They generalize projective systems associated to linear codes in the classical Hamming distance [26] and partial spreads [5]. Furthermore, pseudo arcs are the building blocks of recent general families of MSRD and PMDS codes with small field sizes [20, 22].

Definition 49 A pseudo arc of type $[n, r, m, t]$ is a tuple $\mathcal{H} = (\mathcal{H}_i)_{i=1}^n$ such that

1. $\mathcal{H}_i \subseteq \mathbb{F}_q^m$ is an ($\mathbb{F}_q$-linear) subspace of $\dim(\mathcal{H}_i) = r$, for all $i \in [n]$.
2. t is the maximum positive integer such that $\mathcal{H}_i \cap (\sum_{j \in J} \mathcal{H}_j) = 0$, for all $i \in [n]$ and all $J \subseteq [n] \backslash \{i\}$ with $|J| = t - 1$ (i.e., any t of the subspaces are in direct sum).

Remark 50 A partial spread [5] is a pseudo arc of type $[n, r, m, t]$ with $t \geq 2$.

Remark 51 Definition 49 coincides with the definition at the beginning of [3, Sec. 4] after projectivization, except the parameter t is not considered to be maximum in [3].

We need to consider nondegenerate pseudo arcs in order to associate them to linear codes in the folded Hamming distance.

Definition 52 A pseudo arc $\mathcal{H} = (\mathcal{H}_i)_{i=1}^n$ of type $[n, r, m, t]$ is nondegenerate if $\sum_{i=1}^n \mathcal{H}_i = \mathbb{F}_q^m$.

We will now define a correspondence between pseudo arcs and linear codes in the folded Hamming distance.

Definition 53 Let $\mathcal{H} = (\mathcal{H}_i)_{i=1}^n$ be a pseudo arc of type $[n, r, m, t]$. We say that $\mathbf{h} = (\mathbf{h}_{i,j})_{i=1,j=1}^{n,r}$ is a basis of $\mathcal{H}$ if $\mathbf{h}_{i,1}, \ldots, \mathbf{h}_{i,r} \in \mathbb{F}_q^m$ are $m \times 1$ column vectors forming a basis of $\mathcal{H}_i$, for $i \in [n]$. Next, define the $m \times (rn)$ matrix

$$H_{\mathbf{h}} = (\mathbf{h}_{1,1}, \ldots, \mathbf{h}_{1,r} | \ldots | \mathbf{h}_{n,1}, \ldots, \mathbf{h}_{n,r}).$$

Finally, we define the linear code $\mathcal{C}_{\mathbf{h}} \subseteq \mathbb{F}_q^{rn}$ as that with parity-check matrix $H_{\mathbf{h}}$.

Conversely, given a linear code $\mathcal{C} \subseteq \mathbb{F}_q^{rn}$ of dimension $k = rn - m$ with a (full rank) parity-check matrix H, if $\mathbf{h}_{i,j} \in \mathbb{F}_q^{m \times 1}$ is the $((i-1)r + j)$th column of H, then we define $\mathcal{H}_H = (\mathcal{H}_i)_{i=1}^n$, where $\mathcal{H}_i$ is the subspace generated by $\mathbf{h}_{i,1}, \ldots, \mathbf{h}_{i,r}$, for $i \in [n]$.

We have the following exact correspondence between parameters.

Theorem 10 *1. If $\mathcal{H} = (\mathcal{H}_i)_{i=1}^n$ is a nondegenerate pseudo arc of type $[n, r, m, t]$ with basis $\mathbf{h}$, then $\mathcal{C}_{\mathbf{h}}$ is a linear code of type $[n, r, k, d]$ with $k = rn - m$ and $d = t + 1$.*

2. If $\mathcal{C}$ is a linear code of type $[n, r, k, d]$ and H is one of its parity-check matrices, then $\mathcal{H}_H$ is a nondegenerate pseudo arc of type $[n, r, m, t]$ with $m = rn - k$ and $t = d - 1$.

Proof Item 2 is proven similarly, thus we only prove Item 1. The fact that $\mathcal{H}$ is nondegenerate is equivalent to $H_{\mathbf{h}}$ having rank m. Thus $k = \dim(\mathcal{C}_{\mathbf{h}}) = rn - m$. Finally $d = t + 1$ follows by combining Proposition 18 (Item 2) and Definition 49 (Item 2). □

Remark 54 A similar connection is made in [20]. However, the notion of degenerateness of pseudo arcs is not considered there. In particular, the relations between the corresponding parameters could only be given in [20] as bounds (which are not always tight) instead of as exact equalities.

However the correspondence in Definition 53 is not bijective. In fact, for every pseudo arc, we may obtain multiple codes, and viceversa. In order to obtain a bijection, we need to consider equivalent codes (Definition 6) and equivalent pseudo arcs, which we now define.

Definition 55 Given pseudo arcs $\mathcal{H} = (\mathcal{H}_i)_{i=1}^n$ and $\mathcal{H}' = (\mathcal{H}'_i)_{i=1}^n$, both of type $[n, r, m, t]$, an equivalence between them is a pair (φ, σ), where $\sigma : [n] \longrightarrow [n]$ is a permutation and $\varphi : \mathbb{F}_q^m \longrightarrow \mathbb{F}_q^m$ is a vector space isomorphism such that $\mathcal{H}'_{\sigma(i)} = \varphi(\mathcal{H}_i)$, for all $i \in [n]$. If it exists, we say that $\mathcal{H}$ and $\mathcal{H}'$ are equivalent (and clearly one is degenerate if, and only if, so is the other).

We may now obtain a bijection between equivalence classes of linear codes (Definition 6) and pseudo arcs (Definition 55).

Theorem 11 *1. Let $\mathcal{H}$ and $\mathcal{H}'$ be equivalent nondegenerate pseudo arcs with bases $\mathbf{h}$ and $\mathbf{h}'$, respectively. Then $\mathcal{C}_{\mathbf{h}}$ and $\mathcal{C}_{\mathbf{h}'}$ are equivalent.*
2. Let $\mathcal{C}$ and $\mathcal{C}'$ be equivalent linear codes in $\mathbb{F}_q^{rn}$ with parity-check matrices H and H', respectively. Then $\mathcal{H}_H$ and $\mathcal{H}_{H'}$ are equivalent.

Proof Item 2 is proven similarly, thus we only prove Item 1. Let $\mathcal{H} = (\mathcal{H}_i)_{i=1}^n$ and $\mathcal{H}' = (\mathcal{H}'_i)_{i=1}^n$, both of type $[n, r, m, t]$, and let (φ, σ) be the equivalence between them. There exists an invertible matrix $B \in \mathrm{GL}_m(\mathbb{F}_q)$ such that $\varphi(\mathbf{x}) = B\mathbf{x}$, for every $m \times 1$ column vector $\mathbf{x} \in \mathbb{F}_q^m$. Now the equality $\mathcal{H}'_{\sigma(i)} = \varphi(\mathcal{H}_i)$ means that there exists an invertible matrix $A_i \in \mathrm{GL}_r(\mathbb{F}_q)$ such that

$$B(\mathbf{h}_{i,1}, \ldots, \mathbf{h}_{i,r}) = (\mathbf{h}'_{\sigma(i),1}, \ldots, \mathbf{h}'_{\sigma(i),r})A_i, \tag{7}$$

for every $i \in [n]$. Let P_σ be the only $(rn) \times (rn)$ matrix over $\mathbb{F}_q$ such that $(\mathbf{c}_1, \ldots, \mathbf{c}_n)P_\sigma = (\mathbf{c}_{\sigma(1)}, \ldots, \mathbf{c}_{\sigma(n)})$, for all $\mathbf{c}_1, \ldots, \mathbf{c}_n \in \mathbb{F}_q^r$. Then (7) is equivalent to

$$BH_{\mathbf{h}} = H_{\mathbf{h}'}P_\sigma \mathrm{Diag}(A_1, \ldots, A_n),$$

where $\mathrm{Diag}(A_1, \ldots, A_n)$ denotes the block diagonal matrix with $A_1, \ldots, A_n$ in the main diagonal. Thus we deduce that $\mathcal{C}_{\mathbf{h}}^\perp$ and $\mathcal{C}_{\mathbf{h}'}^\perp$ are equivalent by Proposition 5. Hence $\mathcal{C}_{\mathbf{h}}$ and $\mathcal{C}_{\mathbf{h}'}$ are equivalent by Corollary 7, and we are done. □

Combining Theorems 10 and 11, we conclude the following.

Corollary 56 *The correspondence in Definition 53 induces a bijection between equivalence classes of linear codes of type $[n, r, k, d]$ and equivalence classes of nondegenerate pseudo arcs of type $[n, r, m, t]$ with $m = rn - k$ and $t = d - 1$.*

As a consequence, all of the results in this paper concerning linear codes in the folded Hamming distance can be immediately translated to results for nondegenerate pseudo arcs. We leave the details to the reader.

Acknowledgements This work has been supported by MCIN/AEI/10.13039/501100011033 and the European Union NextGenerationEU/PRTR (Grant No. TED2021-130358B-I00), and by MICIU/AEI/10.13039/501100011033 and ERDF/EU (Grant No. PID2022-138906NB-C21).

Author Contributions The authors contributed equally to this work.

Funding Open access funding provided by FEDER European Funds and the Junta de Castilla y León under the Research and Innovation Strategy for Smart Specialization (RIS3) of Castilla y León 2021-2027.

Data Availability No datasets were generated or analysed during the current study.

Declarations

Conflict of interest The authors declare no conflict of interest.

References

1. Aigner M., Axler S.: A Course in Enumeration, vol. 238. Graduate Texts in Mathematics. Springer, Berlin (2007).
2. Ball S.: On sets of vectors of a finite vector space in which every subset of basis size is a basis. J. Eur. Math. Soc. **14**(3), 733–748 (2012).
3. Ball S., Gamboa G., Lavrauw M.: On additive MDS codes over small fields. Adv. Math. Commun. **17**(4), 1–17 (2023).
4. Barg A., Skriganov M.: Association schemes on general measure spaces and zero-dimensional Abelian groups. Adv. Math. **281**, 142–247 (2015).
5. Beutelspacher A.: Partial spreads in finite projective spaces and partial designs. Math. Z. **145**(3), 211–229 (1975).
6. Bhandari S., Harsha P., Kumar M., Sudan M.: Ideal-theoretic explanation of capacity-achieving decoding. IEEE Trans. Inf. Theory **70**(2), 1107–1123 (2024).
7. Blaum M., Roth R.M.: On lowest density MDS codes. IEEE Trans. Inf. Theory **45**(1), 46–59 (1999).
8. Byrne E., Gluesing-Luerssen H., Ravagnani A.: Fundamental properties of sum-rank-metric codes. IEEE Trans. Inf. Theory **67**(10), 6456–6475 (2021).
9. de la Cruz J., Gorla E., López H.H., Ravagnani A.: Weight distribution of rank-metric codes. Des. Codes Cryptogr. **86**, 1–16 (2018).
10. Dodunekov S.M., Landjev I.N.: On near-MDS codes. J. Geom. **54**, 30–43 (1995).
11. Etzion T.: Perfect byte-correcting codes. IEEE Trans. Inf. Theory **44**(7), 3140–3146 (1998).
12. Faldum A., Willems W.: Codes of small defect. Des. Codes Cryptogr. **10**, 341–350 (1997).
13. Gabidulin E.M.: Theory of codes with maximum rank distance. Probl. Inf. Transm. **21**(1), 1–12 (1985).
14. Gluesing-Luerssen H.: Fourier-reflexive partitions and MacWilliams identities for additive codes. Des. Codes Cryptogr. **75**, 543–563 (2015).
15. Gruica A., Ravagnani A.: Common complements of linear subspaces and the sparseness of MRD codes. SIAM J. Appl. Algebra Geom. **6**(2), 79–110 (2022).
16. Honold T., Landjev I.: MacWilliams identities for linear codes over finite Frobenius rings. In: Finite Fields and Applications: Proceedings of Fifth International Conference on Finite Fields Applications, pp. 276–292. Springer (2000).
17. Huffman W.C., Pless V.: Fundamentals of Error-Correcting Codes. Cambridge University Press, Cambridge (2003).
18. Jukna S.: Extremal Combinatorics: With Applications in Computer Science, vol. 571. Graduate Texts in Mathematics. Springer, Berlin (2011).
19. Lidl R., Niederreiter H.: Finite Fields, vol. 20. Encyclopedia of Mathematics and Its Applications. Addison-Wesley, Amsterdam (1983).
20. Liu S., Xing C.: Maximally recoverable local repairable codes from subspace direct sum systems. IEEE Trans. Inf. Theory **69**(4), 2300–2310 (2022).
21. Martínez-Peñas U.: Hamming and simplex codes for the sum-rank metric. Des. Codes Cryptogr. **88**, 1521–1539 (2020).
22. Martínez-Peñas U.: A general family of MSRD codes and PMDS codes with smaller field sizes from extended Moore matrices. SIAM J. Disc. Math. **36**(3), 1868–1886 (2022).
23. Martínez-Peñas U., Shehadeh M., Kschischang F.R.: Codes in the sum-rank metric, fundamentals and applications. Found. Trends Commun. Inf. Theory **19**(5), 814–1031 (2022).
24. Ron-Zewi N., Venkitesh S., Wootters M.: Efficient list-decoding of polynomial ideal codes with optimal list size (2024). Preprint: arXiv:2401.14517.
25. Singleton R.: Maximum distance q-nary codes. IEEE Trans. Inf. Theory **10**(2), 116–118 (1964).
26. Tsfasman M.A., Vlăduţ S.G.: Geometric approach to higher weights. IEEE Trans. Inf. Theory **41**(6), 1564–1588 (1995).
27. Xu L., Bohossian V., Bruck J., Wagner D.G.: Low-density MDS codes and factors of complete graphs. IEEE Trans. Inf. Theory **45**(6), 1817–1826 (1999).