On Lowest-Density MDS Codes*

Mario Blaum
IBM Research Division
Almaden Research Center
650 Harry Road
San Jose, CA 95120, USA

Ron M. Roth
Computer Science Department
Technion
Haifa 32000, Israel

Abstract

Let $\mathbb{F}_q$ denote the finite field $GF(q)$ and let b be a positive integer. MDS codes over the symbol alphabet $\mathbb{F}_q^b$ are considered that are linear over $\mathbb{F}_q$ and have sparse ("low density") parity-check and generator matrices over $\mathbb{F}_q$ that are systematic over $\mathbb{F}_q^b$. Lower bounds are presented on the number of nonzero elements in any systematic parity-check or generator matrix of an $\mathbb{F}_q$-linear MDS code over $\mathbb{F}_q^b$, along with upper bounds on the length of any MDS code that attains those lower bounds. A construction is presented that achieves those bounds for certain redundancy values. The building block of the construction is a set of sparse nonsingular matrices over $\mathbb{F}_q$ whose pairwise differences are also nonsingular. Bounds and constructions are presented also for the case where the systematic condition on the parity-check and generator matrices is relaxed to be over $\mathbb{F}_q$, rather than over $\mathbb{F}_q^b$.

Keywords: Disk arrays; Group codes; Low-density codes; MDS codes; Sparse matrices.

*This work was supported in part by grants No. 92-00210 and No. 95-00522 from the United-States–Israel Binational Science Foundation (BSF), Jerusalem, Israel. This work was presented in part at the *IEEE Information Theory Workshop*, Haifa, Israel (June 1996), and in part at the *IEEE Information Theory Workshop*, San Diego, California (February 1998).

1 Introduction

Let $\mathbb{F}_q$ denote the finite field $GF(q)$. A code $\mathcal{C}$ over $\mathbb{F}_q^b$ is said to be $\mathbb{F}_q$-*linear* if $\mathcal{C}$ is a vector space over $\mathbb{F}_q$. Such a code is a group code with $\mathbb{F}_q^b$ as the underlying group (see [5], [12], and the references therein). Clearly, every linear code over $GF(q^b)$ is an $\mathbb{F}_q$-linear code over $\mathbb{F}_q^b$. The converse, however, is not true.

Let $\mathcal{C}$ be a code of length n over $\mathbb{F}_q^b$ and minimum Hamming distance d, where the distance is measured with respect to symbols of $\mathbb{F}_q^b$. By the Singleton bound for (not necessarily linear) codes over $\mathbb{F}_q^b$ we have

$$d \ \leq \ n + 1 - \log_{q^b} |\mathcal{C}|$$

(see [5], [11, p. 319]). Codes that attain this bound are called maximum-distance separable (MDS) codes. In particular, the size of an MDS code over $\mathbb{F}_q^b$ must be a power of $|\mathbb{F}_q^b| = q^b$. It follows that the dimension, over $\mathbb{F}_q$, of any $\mathbb{F}_q$-linear MDS code over $\mathbb{F}_q^b$ must be a multiple of b. Hence, we will characterize any $\mathbb{F}_q$-linear MDS code $\mathcal{C}$ over $\mathbb{F}_q^b$ by a pair of integers $[n, k]$, where n is the length of $\mathcal{C}$ (measured in symbols of $\mathbb{F}_q^b$) and $k = \log_{q^b} |\mathcal{C}|$. Note that kb is the dimension of $\mathcal{C}$ as a linear space over $\mathbb{F}_q$. The redundancy of $\mathcal{C}$ is given by $r = n - k$ and the minimum distance equals $r + 1$. Reed-Solomon codes over $GF(q^b)$ are examples of $\mathbb{F}_q$-linear MDS codes over $\mathbb{F}_q^b$.

Each codeword of a code $\mathcal{C}$ of length n over $\mathbb{F}_q^b$ can be regarded as a word of length nb over $\mathbb{F}_q$, simply by interpreting each symbol of $\mathbb{F}_q^b$ as a block of length b over $\mathbb{F}_q$. The resulting set of words defines a code of length nb and size $|\mathcal{C}|$ over $\mathbb{F}_q$, which we denote by $(\mathcal{C})_{\mathbb{F}_q}$. Clearly, $\mathcal{C}$ is $\mathbb{F}_q$-linear over $\mathbb{F}_q^b$ if and only if $(\mathcal{C})_{\mathbb{F}_q}$ is linear over $\mathbb{F}_q$.

By a parity-check matrix (respectively, generator matrix) of an $\mathbb{F}_q$-linear code over $\mathbb{F}_q^b$ we mean a parity-check matrix (respectively, generator matrix) over $\mathbb{F}_q$ of $(\mathcal{C})_{\mathbb{F}_q}$.

For a positive integer ℓ, let I_ℓ denotes the $\ell \times \ell$ identity matrix over $\mathbb{F}_q$.

Definition 1.1 *Let T be an $mb \times nb$ matrix over $\mathbb{F}_q$ with $m \leq n$ (e.g., T can be a parity-check or generator matrix of an $\mathbb{F}_q$-linear code $\mathcal{C}$ over $\mathbb{F}_q^b$). The matrix T is said to be systematic if I_{mb} is a submatrix of T such that the columns of I_{mb} are aligned with m symbols of $\mathbb{F}_q^b$; namely, when we write $T = (\, T_1 \ T_2 \ \ldots \ T_n \,)$, where each T_i is an $mb \times b$ submatrix of T, then the columns of I_{mb} occupy m of the submatrices T_i.*

Example 1.1 The following is a systematic parity-check matrix of a $[5, 3]$ $\mathbb{F}_2$-linear code $\mathcal{C}$ over $\mathbb{F}_2^2$:

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

The corresponding generator matrix is

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

Notice that the associated binary code $(\mathcal{C})_{\mathbb{F}_2}$ is a $[10, 6]$ code. □

In this work, we consider $\mathbb{F}_q$-linear $[n, k]$ MDS codes over $\mathbb{F}_q^b$ that have systematic parity-check matrices over $\mathbb{F}_q$ with the smallest possible number of nonzero entries; equivalently, these codes have systematic generator matrices over $\mathbb{F}_q$ with the smallest possible number of nonzero entries. Indeed, this equivalence follows by recalling that $(\, A \;\; I_{rb} \,)$ is a parity-check matrix of an $\mathbb{F}_q$-linear $[n, k{=}n{-}r]$ code $\mathcal{C}$ over $\mathbb{F}_q^b$ if and only if $(\, I_{kb} \;\; -A^T \,)$ is a generator matrix of $\mathcal{C}$.

We describe next an application of such codes in disk arrays [6]. We number the disks in an array from 0 to $n{-}1$ and divide each disk into symbols (e.g., sectors), each sector consisting of b units. We assume hereafter that a unit is one bit and so symbols will be regarded as elements of $\mathbb{F}_2^b$. In practice, a unit can be h bits long (e.g., it can be a byte or a word), in which case we regard each unit as an element of $\mathbb{F}_{2^h}$; alternatively, we can regard the disk array as h independently interleaved arrays. Each symbol in the array is indexed by (i, j), where j is the index of the disk and i is the index of the symbol within each disk. The ℓth bit in the (i, j)th symbol will be assigned the index (i, j, ℓ). Given an $\mathbb{F}_2$-linear $[n, k]$ code $\mathcal{C}$ over $\mathbb{F}_2^b$, data is recorded into the disks such that for each i, the symbols at locations (i, j), $j = 0, 1, \ldots, n{-}1$, form a codeword of $\mathcal{C}$. The first k disks are assigned to carry the information symbols, and the remaining $n{-}k$ disks carry the redundancy symbols. We use a $kb \times nb$ systematic generator matrix $G = (g_{s,t})$ of $\mathcal{C}$ with I_{kb} occupying its first kb columns.

When writing a bit at a given location (i_0, j_0, ℓ_0), $j_0 < k$, we need to update the bits at all locations (i_0, j, ℓ) for which $g_{bj_0+\ell_0, bj+\ell} = 1$. This motivates us to minimize the number of 1's in G. The systematic presentation allows the fastest possible retrieval of information at the bit level, symbol level, or disk level. Also, a small number of 1's in the parity-check matrix implies a small number of additions (XORs) while computing the syndrome if decoding is required upon disk failure. In general, when the underlying field is nonbinary, we will require that the number of nonzero entries in the parity-check matrix be the smallest possible (this assumes that the complexity of multiplication by a known constant is comparable to that of addition). Hence, our goal is to combine distance properties with complexity: we seek for codes that are optimal in terms of minimum distance (i.e., MDS codes), and, among those, we look for codes that are optimal with respect to their coding complexity in the sense of minimizing the number of nonzero entries in the parity-check and generator matrices.

We present here a construction of $\mathbb{F}_q$-linear MDS codes over $\mathbb{F}_q^b$ that is optimal with respect to those two criteria. The building block of our construction is a maximal set of sparse nonsingular matrices over $\mathbb{F}_q$ whose difference set consists of nonsingular matrices. Sets of matrices with the mentioned property might be of interest in their own right, independently of our motivation herein. We present constructions of two such sets of matrices in Section 2. As it turns out, the case $q = 2$ poses an impediment that disappears in larger fields, thus making the binary case unique. The second set construction in Section 2, having slightly weaker properties compared to the first set construction, is intended primarily to overcome the difficulty posed in the binary case. Hence, our special treatment of the binary field will not be only because of the application in mind, but rather because this field seems to stand out as more difficult than larger fields.

Our code construction is described in Section 4. One instance of our construction is an $\mathbb{F}_2$-linear $[k+2, k]$ MDS code over $\mathbb{F}_2^b$, where $b+1$ is an odd prime and k is any integer in the range $1 \leq k \leq b+1$: the code has a systematic parity-check matrix in which the average number of 1's per row equals $k + 1 + \frac{k-1}{2b}$; equivalently, the code has a systematic generator matrix in which the average number of 1's per row equals $3 + \frac{1}{b}(1 - \frac{1}{k})$. Those parameters turn out to be optimal, in view of the bounds that we present in Sections 3 and 5. The construction lends itself to simple decoding procedures. We also consider $\mathbb{F}_q$-linear MDS codes over $\mathbb{F}_q^b$ with sparse parity-check and generator matrices, where $q > 2$. For certain values of b, we can obtain such constructions from extensions of Reed-Solomon codes over $GF(q^b)$ (or over polynomial rings of size q^b over $\mathbb{F}_q$). We conclude the discussion in Section 4 with constructions for certain redundancy values greater than 2.

The problem of constructing $\mathbb{F}_2$-linear MDS codes over $\mathbb{F}_2^b$ with sparse ("low-density") systematic generator matrices was already addressed in [2], where the so-called EVENODD code was presented. The EVENODD code is a linear $[b+3, b+1]$ MDS code over $GF(2^b)$, where $b+1$ is an odd prime; as such, it is $\mathbb{F}_2$-linear over $\mathbb{F}_2^b$. Furthermore, the EVENODD construction has a systematic generator matrix in which the average number of 1's in a row equals $4 - (2/(b+1))$. On the other hand, the construction we present here yields $\mathbb{F}_2$-linear $[b+3, b+1]$ MDS codes over $\mathbb{F}_2^b$ with systematic generator matrices in which the average number of 1's in a row is $3 + (1/(b+1))$ (most rows contain three 1's and the rest contain four 1's).

It is interesting to point out that the bounds we present in Section 5 no longer hold if we weaken the systematic condition. In fact, Zaitsev et *al.* obtained in [13] a construction of $\mathbb{F}_2$-linear $[k+2, k]$ MDS codes over $\mathbb{F}_2^b$ whose parity-check and generator matrices are sparser than ours: the number of 1's in a row is $k+1$ in the parity-check matrix and 3 in the generator matrix. Also, the value of k can be as large as $2b-1$, namely, almost twice the maximal value of k in the construction of Section 4. However, the parity-check and generator matrices of their codes satisfy a weaker systematic property than that in Definition 1.1. We elaborate more on this in Section 6; in particular, we suggest a generalization of the construction in [13] for redundancy values greater than 2.

2 Sparse matrices with all-nonsingular difference set

The construction of MDS codes over $\mathbb{F}_q^b$ that we present in Section 4 makes use of a largest possible set of $b \times b$ matrices over $\mathbb{F}_q$ that satisfies the following three properties:

(P1) Each matrix in the set is nonsingular.

(P2) The difference of every two distinct matrices in the set is nonsingular.

(P3) Each matrix contains b nonzero entries.

Clearly, each matrix that satisfies (P1) must contain at least b nonzero entries. Matrices that satisfy (P1) and (P3) are called monomial matrices [11, p. 238]. In Section 2.1 we present a set of $b(q-1)$ matrices over $\mathbb{F}_q$ that satisfies (P1)–(P3) whenever the prime divisors of b also divide $q-1$. In particular, we can take b to be a power of $q-1$ (resulting in infinitely many values of b for every $q > 2$); also, we can take $b = 2^m$ when q is odd or take $b = 3^m$ when q is an even power of 2. The following bound states that our constructed set is the largest possible.

Proposition 2.1 *The size of any set of matrices over $\mathbb{F}_q$ that satisfies (P1)–(P3) does not exceed $b(q-1)$.*

Proof. The first rows of the matrices in any such set must be distinct, and there are $b(q-1)$ possible distinct rows. □

The bound of Proposition 2.1 is not always tight. For example, when $q = b = 3$, the largest set that satisfies (P1)–(P3) is of size 2. An extreme case is $q = 2$, where any nonempty set that satisfies (P1)–(P3) can contain only one matrix, which must be a permutation matrix: each row in the difference of two permutation matrices has an even number of 1's and so the difference of those matrices is singular. Therefore, properties (P1)–(P3) are too restrictive when $q = 2$ and allow only a trivial set. This motivates us to investigate what happens if we slightly relax property (P3). Specifically, in Section 2.2 we weaken property (P3) to read

(P3') Each matrix contains at most $b+1$ nonzero entries.

We present a set of $(b+1)(q-1)$ matrices over $\mathbb{F}_q$ that satisfies (P1)–(P3') (namely, (P1), (P2), and (P3')) whenever $b+1$ is an odd prime and b is divisible by $2(q-1)$. By Dirichlet's theorem, there are infinitely many such values of b for every q [8, p. 251]. Again, the constructed set is the largest possible, in view of the following result.

Proposition 2.2 *When $b > q$ or $b = q = 2$, the size of any set of matrices over $\mathbb{F}_q$ that satisfies (P1)–(P3') does not exceed $(b+1)(q-1)$.*

Proof. Let N be the size of a set X satisfying (P1)–(P3'). Each matrix in X has at most one row that contains two nonzero entries. Hence, there is a row index i such that at most N/b of the matrices in X have two nonzero entries in row i. By property (P2), the rows indexed by i in the remaining matrices in X must be distinct. Hence, $N - (N/b) \leq b(q-1)$, or $N \leq \lfloor b^2(q-1)/(b-1) \rfloor$. For $b > q$ this becomes $N \leq (b+1)(q-1)$.

A simple check reveals that the bound holds also for $b = q = 2$. □

The relaxation of property (P3) to (P3') thus allows the number of matrices in the set to grow from $b(q-1)$ to $(b+1)(q-1)$. This may be a marginal improvement for $q > 2$, but it is a significant one for $q = 2$. Indeed, as argued before, (P1)–(P3) can be satisfied for $q = 2$ only by sets of size 1. On the other hand, when we replace (P3) by (P3'), we will be able to attain the upper bound of Proposition 2.2 also when $q = 2$.

We point out that a construction of a set of matrices appears in [13, p. 200] that satisfies (P2) and (P3'), but not (P1) (in fact, all the matrices therein, with the exception of one, are singular); however, we need also (P1) for our purposes in Section 4.

2.1 Set of matrices satisfying (P1)–(P3)

For a positive integer b and an element $\alpha \in \mathbb{F}_q$, we define the $b \times b$ matrix C_α over $\mathbb{F}_q$ by

$$C_\alpha = \begin{pmatrix} 0 & 0 & \dots & 0 & \alpha \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \ddots & 0 & 0 \\ \vdots & \vdots & \ddots & 0 & \vdots \\ 0 & 0 & \dots & 1 & 0 \end{pmatrix} .$$

The matrix C_α is the companion matrix of the polynomial $\xi^b - \alpha$ over $\mathbb{F}_q$ (we adopt the definition of a companion matrix as it appears in [10, p. 68]; there are other references, such as [11, p. 106], that look at the transposed matrix instead). If we associate each column vector $\underline{x} = (x_\ell)_{\ell=0}^{b-1} \in \mathbb{F}_q$ with the polynomial $x(\xi) = \sum_{\ell=0}^{b-1} x_\ell \xi^\ell$, then the mapping $\underline{x} \mapsto C_\alpha^i \underline{x}$ over $\mathbb{F}_q^b$ maps $\underline{x}$ to a vector $\underline{y} = (y_\ell)_{\ell=0}^{b-1}$, where

$$y(\xi) \equiv \xi^i \cdot x(\xi) \pmod{(\xi^b - \alpha)} .$$

Let $\mathbb{F}_q^*$ denote the set $\mathbb{F}_q \setminus \{0\}$. When $\alpha \in \mathbb{F}_q^*$, the matrix C_α is nonsingular and contains

exactly b nonzero entries. The same holds for all the powers C_α^i. It follows that the set

$$\mathcal{U}_\alpha \;=\; \left\{ a \cdot C_\alpha^i \;:\; a \in \mathbb{F}_q^*,\; 0 \le i < b \right\}$$

satisfies (P1) and (P3). Note that the size of $\mathcal{U}_\alpha$ is $b(q-1)$. In fact, since $C_\alpha^b = \alpha \cdot I_b = \alpha \cdot C_\alpha^0$, it follows that $\mathcal{U}_\alpha$ is a subgroup of the group of all $b \times b$ monomial matrices over $\mathbb{F}_q$ under matrix multiplication.

Theorem 2.4 below provides a necessary and sufficient condition for $\mathcal{U}_\alpha$ to satisfy (P2). We will make use of the following lemma, which is taken from [10, p. 145, Problem 3.82]. We include here a short proof for completeness.

For an element $\omega \in \mathbb{F}_q^*$, we denote by $\mathcal{O}(\omega)$ the multiplicative order of ω in $\mathbb{F}_q$.

Lemma 2.3 *Let α and β be elements of $\mathbb{F}_q$ and let b and t be positive integers with $s = \gcd(b,t)$. Then $\xi^b - \alpha$ and $\xi^t - \beta$ are not relatively prime if and only if*

$$\beta^{b/s} \;=\; \alpha^{t/s} \;.$$

Proof. We start with the "if" part and assume that $\beta^{b/s} = \alpha^{t/s}$. Let γ_1, γ_2, ω_1, and ω_2 be elements in an extension field Φ of $\mathbb{F}_q$ such that $\gamma_1^b = \alpha$, $\gamma_2^t = \beta$, $\mathcal{O}(\omega_1) = b$, and $\mathcal{O}(\omega_2) = t/s$. Since $\gcd(b, t/s) = 1$ we have $\mathcal{O}(\omega_2/\omega_1) = (bt)/s$. Also,

$$\left(\frac{\gamma_1}{\gamma_2}\right)^{(bt)/s} \;=\; \frac{\left(\gamma_1^b\right)^{t/s}}{\left(\gamma_2^t\right)^{b/s}} \;=\; \frac{\alpha^{t/s}}{\beta^{b/s}} \;=\; 1 \;.$$

Therefore, there is an integer ℓ such that $\gamma_1/\gamma_2 = (\omega_2/\omega_1)^\ell$, or, equivalently, $\gamma_1\omega_1^\ell = \gamma_2\omega_2^\ell = \gamma$ for some $\gamma \in \Phi$. Now,

$$\gamma^b \;=\; \left(\gamma_1\omega_1^\ell\right)^b \;=\; \gamma_1^b\left(\omega_1^b\right)^\ell \;=\; \alpha \quad \text{and} \quad \gamma^t \;=\; \left(\gamma_2\omega_2^\ell\right)^t \;=\; \gamma_2^t\left(\omega_2^{t/s}\right)^{s\ell} \;=\; \beta \;.$$

That is, γ is a root in Φ of both $\xi^b - \alpha$ and $\xi^t - \beta$, thus implying that these two polynomials are not relatively prime.

Conversely, if $\xi^b - \alpha$ and $\xi^t - \beta$ are not relatively prime, then they have a common root γ in an extension field of $\mathbb{F}_q$; namely, $\gamma^b = \alpha$ and $\gamma^t = \beta$. Hence,

$$\gamma^{(bt)/s} \;=\; \left(\gamma^b\right)^{t/s} \;=\; \alpha^{t/s} \quad \text{and} \quad \gamma^{(bt)/s} \;=\; \left(\gamma^t\right)^{b/s} \;=\; \beta^{b/s} \;,$$

i.e., $\beta^{b/s} = \alpha^{t/s}$. This establishes the "only if" part. □

Theorem 2.4 *Let α be an element in $\mathbb{F}_q^*$ with $\mathcal{O}(\alpha) = e$. The difference of every two distinct matrices in $\mathcal{U}_\alpha$ is nonsingular if and only if every prime divisor of b divides e but not $(q-1)/e$.*

Proof. Up to a nonzero scalar multiple, every difference of two elements in $\mathcal{U}_\alpha$ takes the form $C_\alpha^j - \beta C_\alpha^i$, where $\beta \in \mathbb{F}_q^*$ and $0 \le i \le j < b$. Clearly, the matrix $C_\alpha^j - \beta C_\alpha^i$ is invertible whenever $i = j$ and $\beta \neq 1$ (the case $i = j$ and $\beta = 1$ corresponds to a difference of two identical matrices). Hence, we assume from now on in the proof that $i < j$. The matrix $C_\alpha^j - \beta C_\alpha^i$ represents a mapping $x(\xi) \mapsto y(\xi)$ over the ring, $\mathbb{F}_q[\xi]/(\xi^b - \alpha)$, of polynomials of degree $< b$ over $\mathbb{F}_q$ modulo $\xi^b - \alpha$, where

$$y(\xi) \;\equiv\; (\xi^j - \beta\xi^i) \cdot x(\xi) \pmod{(\xi^b - \alpha)} \,.$$

Hence, $C_\alpha^j - \beta C_\alpha^i$ is nonsingular if and only if the polynomial $\xi^j - \beta\xi^i$ is invertible modulo $\xi^b - \alpha$; this, in turn, is equivalent to saying that $\xi^j - \beta\xi^i$ and $\xi^b - \alpha$ are relatively prime. Write $\xi^j - \beta\xi^i = \xi^i(\xi^{j-i} - \beta)$ and recall that ξ^i is invertible modulo $\xi^b - \alpha$. It suffices to show that each of the following $(b-1)(q-1)$ polynomials,

$$\xi^t - \beta, \quad \beta \in \mathbb{F}_q^* \,, \quad 1 \le t < b \,,$$

is relatively prime to $\xi^b - \alpha$ if and only if b satisfies the conditions of the theorem.

We start with the "if" part. Assume that b satisfies the conditions of the theorem, and suppose to the contrary that there exists $\beta \in \mathbb{F}_q^*$ and $1 \le t < b$ such that $\xi^t - \beta$ is not relatively prime to $\xi^b - \alpha$. Let $s = \gcd(b, t)$, where $s < b$, and let u be a prime that divides b/s. By our assumption on b, the prime u also divides e, so e/u is an integer. Recalling that $(q-1)/e$ is also an integer, we have

$$\beta^{(b/s)(e/u)((q-1)/e)} \;=\; \beta^{(b/s)(q-1)/u} \;=\; 1 \,.$$

On the other hand, by Lemma 2.3 we have $\beta^{(b/s)(e/u)((q-1)/e)} = \alpha^v$, where v is the integer $(t/s)(e/u)((q-1)/e)$. Hence, $\alpha^v = 1$, which implies that e must divide v. However, u does not divide t/s since $\gcd(b/s, t/s) = 1$, and it does not divide $(q-1)/e$ because no prime divisor of b divides $(q-1)/e$. Hence, v and e/u have the same multiplicity of u in their prime factorizations. But this means that e cannot divide v, which is a contradiction.

We turn now to the "only if" part. Assume first that b has a prime divisor u that does not divide e, and let u^{-1} denote the inverse of u modulo e. Select $\beta = \alpha^{u^{-1}}$ and $t = b/u$. We have $\alpha = \beta^u$, and so $\xi^t - \beta$ divides $\xi^b - \alpha = \xi^{tu} - \beta^u$.

Suppose now that b has a prime divisor u that divides $(q-1)/e$. Since $\mathcal{O}(\alpha) = e$, there is a primitive element γ in $\mathbb{F}_q$ such that $\alpha = \gamma^{(q-1)/e}$. Select $\beta = \gamma^{(q-1)/(eu)}$ and $t = b/u$. Again we have $\alpha = \beta^u$, and $\xi^t - \beta$ divides $\xi^b - \alpha = \xi^{tu} - \beta^u$. □

In fact, when $q \not\equiv 3 \pmod 4$, the conditions on b in Theorem 2.4 are necessary and sufficient for $\xi^b - \alpha$ to be *irreducible* over $\mathbb{F}_q$; see [10, p. 124]. When $q \equiv 3 \pmod 4$, the conditions for irreducibility require, in addition, that b be not divisible by 4. When $\xi^b - \alpha$ is irreducible, every nontrivial polynomial of degree less than b over $\mathbb{F}_q$ is relatively prime to $\xi^b - \alpha$. Hence, every nontrivial linear combination over $\mathbb{F}_q$ of the matrices $I, C_\alpha, C_\alpha^2, \ldots, C_\alpha^{b-1}$

is nonsingular; in particular, irreducibility implies that the difference of every two distinct elements in $\mathcal{U}_\alpha$ is nonsingular.

To obtain the widest range of values of b that satisfy the conditions of Theorem 2.4, we will choose α to be primitive in $\mathbb{F}_q$. In this case, the conditions in the theorem boil down to requiring that the prime divisors of b also divide $q-1$; e.g., we can take $b = 2^m$ when q is odd or take $b = 3^m$ when $q = 2^{2h}$. When α is primitive, the set $\mathcal{U}_\alpha$ can also be written as $\{C_\alpha^i\}_{i=0}^{b(q-1)-1}$. Indeed, if $a = \alpha^s$ then, for $0 \le j < b$,

$$a \cdot \xi^j \;\equiv\; \alpha^s \cdot \xi^j \;\equiv\; \xi^{bs+j} \pmod{(\xi^b - \alpha)} .$$

Hence, the mappings $\underline{x} \mapsto a \cdot C_\alpha^j \underline{x}$ and $\underline{x} \mapsto C_\alpha^{bs+j}\underline{x}$ are identical for every $0 \le j < b$ and $0 \le s < q-1$.

2.2 Set of matrices satisfying (P1)–(P3')

Fix p to be an odd prime. Let ρ be a rational that can be written as a ratio a/b, where a and b are integers such that b is not divisible by p. We denote by $\langle\rho\rangle$ the unique integer m, $0 \le m < p$, such that $a \equiv bm \pmod{p}$.

Definition 2.1 *Let p be an odd prime and let α be an element of $\mathbb{F}_q$. For $0 \le i < p$, define the $(p-1) \times (p-1)$ matrix $Q_\alpha^{(i)} = (\vartheta_{\ell,m})_{\ell,m=1}^{p-1}$ over $\mathbb{F}_q$ by*

$$\vartheta_{\ell,m} \;=\; \begin{cases} 1 & \text{if } \ell \ne p-i \text{ and } \langle m-\ell\rangle = i \\ -1 & \text{if } \ell = p-i \text{ and } m = i \\ -\alpha & \text{if } \ell = p-i \text{ and } m = \langle i/2\rangle \\ 0 & \text{otherwise} \end{cases} .$$

The matrix $Q_\alpha^{(0)}$ is the identity matrix I_{p-1}, and $Q_\alpha^{(1)}$ is the transposed companion matrix of the polynomial $\xi^{p-1} + \alpha\xi^{(p-1)/2} + 1$ over $\mathbb{F}_q$.

Example 2.1 For $p = 5$ we have $\langle 1/2\rangle = 3$ and the matrices $Q_\alpha^{(i)}$ are given by

$$Q_\alpha^{(1)} \;=\; \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & -\alpha & 0 \end{pmatrix} \qquad Q_\alpha^{(2)} \;=\; \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -\alpha & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

$$Q_\alpha^{(3)} \;=\; \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & -\alpha \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \qquad Q_\alpha^{(4)} \;=\; \begin{pmatrix} 0 & -\alpha & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

with $Q_\alpha^{(0)} = I_4$. $\square$

The matrix $Q_\alpha^{(0)}$ contains $p-1$ nonzero entries and each of the remaining matrices in the set contains at most p nonzero entries (when $\alpha \neq 0$, the only row in $Q_\alpha^{(i)}$ that contains two nonzero entries is the one indexed by $p-i$). Hence, the set

$$\mathcal{V}_\alpha \;=\; \left\{ a \cdot Q_\alpha^{(i)} \;:\; a \in \mathbb{F}_q^*,\; 0 \le i < p \right\}$$

satisfies (P3'). Note that the size of $\mathcal{V}_\alpha$ is $p(q-1) = (b+1)(q-1)$.

The next lemma summarizes several properties of the matrices $Q_\alpha^{(i)}$. In particular, we show that $\mathcal{V}_\alpha$ satisfies (P1).

For $0 < i < p$, let $P_i = \left((P_i)_{\ell,m} \right)_{\ell,m=1}^{p-1}$ be the $(p-1) \times (p-1)$ permutation matrix over $\mathbb{F}_q$ that corresponds to the permutation $\ell \mapsto \langle \ell i \rangle$ over $\{1, 2, \ldots, p-1\}$; namely, $(P_i)_{\ell,m} = 1$ if and only if $m = \langle \ell i \rangle$. Clearly, $P_{ij} = P_i P_j = P_j P_i$ and $P_i^{-1} = P_i^T = P_{\langle 1/i \rangle}$. Note that $P_{p-1} = P_{\langle -1 \rangle}$ represents the reversal permutation that maps ℓ to $p-\ell$.

Lemma 2.5 *For $0 < i < p$,*

$$\begin{array}{lllll}
\textit{(i)} & Q_\alpha^{(i)} & = & P_i^{-1} Q_\alpha^{(1)} P_i \;. \\
\textit{(ii)} & (Q_\alpha^{(i)})^{-1} & = & P_{p-1} Q_\alpha^{(i)} P_{p-1} \;. \\
\textit{(iii)} & (Q_\alpha^{(i)})^{-1} & = & Q_\alpha^{(p-i)} \;.
\end{array}$$

Proof. (i) By the definition of $Q_\alpha^{(1)}$, the (ℓ, m)th entry of $P_i^{-1} Q_\alpha^{(1)} P_i$ equals 1 if and only if $\langle (m/i) - (\ell/i) \rangle = 1$, unless $\langle \ell/i \rangle = \langle -1 \rangle$, in which case the (ℓ, m)th entry equals -1 if $\langle m/i \rangle = 1$ and equals $-\alpha$ if $\langle m/i \rangle = \langle 1/2 \rangle$. But these nonzero entries are the same as those in $Q_\alpha^{(i)}$.

(ii) We first prove the claim for $i = 1$. Let $S = (s_{\ell,m})_{\ell,m=1}^{p-1}$ be the matrix over $\mathbb{F}_q$ defined by

$$s_{\ell,m} \;=\; \begin{cases} 1 & \text{if } m-\ell = 1 \\ -1 & \text{if } \ell = p-1 \text{ and } m = 1 \\ 0 & \text{otherwise} \end{cases} .$$

We have $S^{-1} = S^T = P_{p-1} S P_{p-1}$. Write $Q_\alpha^{(1)} = S + E_\alpha$, where E_α is a matrix whose entries are zero except for the $(p-1, (p+1)/2)$th entry which is equal to $-\alpha$. It is easy to check that

$$E_\alpha \;=\; E_\alpha P_{p-1} S \;=\; -S P_{p-1} E_\alpha$$

and that $E_\alpha P_{p-1} E_\alpha = 0$. Hence,

$$\begin{array}{rcl}
(P_{p-1} Q_\alpha^{(1)} P_{p-1}) Q_\alpha^{(1)} & = & P_{p-1}(S + E_\alpha) P_{p-1} (S + E_\alpha) \\
& = & P_{p-1} S P_{p-1} S \;+\; P_{p-1} S P_{p-1} E_\alpha \;+\; P_{p-1} E_\alpha P_{p-1} S \;+\; P_{p-1} E_\alpha P_{p-1} E_\alpha \\
& = & I \;-\; P_{p-1} E_\alpha \;+\; P_{p-1} E_\alpha \;+\; 0 \\
& = & I \;.
\end{array}$$

By (i), we have for general i,

$$\begin{aligned}(P_{p-1}Q_\alpha^{(i)}P_{p-1})Q_\alpha^{(i)} &= (P_{p-1}P_i^{-1}Q_\alpha^{(1)}P_iP_{p-1})(P_i^{-1}Q_\alpha^{(1)}P_i)\\ &= P_i^{-1}((P_{p-1}Q_\alpha^{(1)}P_{p-1})Q_\alpha^{(1)})P_i\\ &= I\ .\end{aligned}$$

(iii) By (i) and (ii) we have

$$Q_\alpha^{(p-i)} \;=\; P_{p-i}^{-1}Q_\alpha^{(1)}P_{p-i} \;=\; P_{p-1}(P_i^{-1}Q_\alpha^{(1)}P_i)P_{p-1} \;=\; P_{p-1}Q_\alpha^{(i)}P_{p-1} \;=\; (Q_\alpha^{(i)})^{-1}\ ,$$

as claimed. □

The following theorem provides sufficient conditions on p and α so that $\mathcal{V}_\alpha$ satisfies (P2).

Theorem 2.6 *Let p be a prime such that $p-1$ is divisible by $2(q-1)$ and let α be an element in $\mathbb{F}_q^*$ such that the polynomial $\xi^2+\alpha\xi+1$ is irreducible over $\mathbb{F}_q$. Then the difference of any two distinct matrices in $\mathcal{V}_\alpha$ is nonsingular.*

Proof. We show that for every $0 \le i,j < p$, $i \ne j$, and every $\beta \in \mathbb{F}_q^*$, the matrix $Q_\alpha^{(j)} - \beta Q_\alpha^{(i)}$ is nonsingular. We do this by proving that for every vector $\underline{z} = (z_\ell)_{\ell=1}^{p-1}$ over $\mathbb{F}_q$, we can solve

$$(Q_\alpha^{(j)} \;-\; \beta Q_\alpha^{(i)})\underline{x} \;=\; \underline{z} \tag{1}$$

uniquely for the vector $\underline{x} = (x_\ell)_{\ell=1}^{p-1}$.

Define $\Delta = \langle j-i\rangle$, $L = \langle i/\Delta\rangle$, and $M = \langle -j/\Delta\rangle = p-1-L$. We first prove by induction on ℓ that

$$x_{\langle \ell\Delta\rangle} \;=\; \begin{cases} \beta^{\ell-1}x_\Delta \;+\; \displaystyle\sum_{t=L-\ell+1}^{L-1} \beta^{t-(L-\ell+1)} z_{\langle -t\Delta\rangle} & \text{if } 0 < \ell \le L \qquad \text{(a)} \\ \beta^{\ell+1}x_{p-\Delta} \;-\; \displaystyle\sum_{t=M+\ell+1}^{M-1} \beta^{-t+M+\ell} z_{\langle t\Delta\rangle} & \text{if } -M \le \ell < 0 \qquad \text{(b)} \end{cases} \tag{2}$$

(note that part (a) of (2) becomes vacuous when $i = 0$, since in this case $L = 0$; similarly, part (b) is vacuous when $j = M = 0$). In fact, it suffices to prove (2)(a), since (b) follows by switching the roles of i and j (indeed, the switch $i \leftrightarrow j$ implies the changes $\Delta \leftrightarrow p-\Delta$ and $M \leftrightarrow L$; also, (1) becomes $(Q_\alpha^{(j)} - \beta^{-1}Q_\alpha^{(i)})\underline{x} = -\beta^{-1}\underline{z}$, which means that β and $\underline{z}$ become β^{-1} and $-\beta^{-1}\underline{z}$, respectively).

The induction base $\ell = 1$ is trivial. By the induction hypothesis, assume that the equality

$$x_{\langle(\ell-1)\Delta\rangle} \;=\; \beta^{\ell-2}x_\Delta \;+\; \sum_{t=L-\ell+2}^{L-1} \beta^{t-(L-\ell+2)} z_{\langle -t\Delta\rangle} \tag{3}$$

holds for some ℓ in the range $1 < \ell \leq L$. Recalling that $\langle L\Delta\rangle = i$ and $\langle (L{+}1)\Delta\rangle = j$, it follows that for $1 < \ell \leq L$ we have $\langle(\ell{-}1{-}L)\Delta\rangle \notin \{p{-}i, p{-}j\}$. So, by equating the $\langle(\ell{-}1{-}L)\Delta\rangle$th components of both sides in $(Q_\alpha^{(j)} - \beta Q_\alpha^{(i)})\underline{x} = \underline{z}$, we obtain

$$x_{\langle j+(\ell-1-L)\Delta\rangle} \;-\; \beta x_{\langle i+(\ell-1-L)\Delta\rangle} \;=\; z_{\langle(\ell-1-L)\Delta\rangle} \;,$$

or

$$x_{\langle \ell\Delta\rangle} \;=\; \beta x_{\langle(\ell-1)\Delta\rangle} \;+\; z_{\langle -(L-\ell+1)\Delta\rangle} \;.$$

This, combined with (3), yields (2)(a).

Next we show that we can solve for x_Δ (when $i \neq 0$) and $x_{p-\Delta}$ (when $j \neq 0$). Equating the $(p{-}i)$th components of both sides in $(Q_\alpha^{(j)} - \beta Q_\alpha^{(i)})\underline{x} = \underline{z}$ yields

$$x_\Delta \;+\; \beta(x_i \;+\; \alpha x_{\langle i/2\rangle}) \;=\; z_{p-i} \;. \tag{4}$$

Substituting $\ell = L$ in (2)(a), we obtain

$$x_i \;=\; \beta^{L-1} x_\Delta \;+\; \sum_{t=1}^{L-1} \beta^{t-1} z_{\langle -t\Delta\rangle} \;. \tag{5}$$

Now, suppose that L is even (in which case M is also even). Substituting $\ell = L/2$ in (2)(a), we obtain

$$x_{\langle i/2\rangle} \;=\; \beta^{L/2-1} x_\Delta \;+\; \sum_{t=L/2+1}^{L-1} \beta^{t-(L/2+1)} z_{\langle -t\Delta\rangle} \;. \tag{6}$$

The relations (4), (5), and (6) form a set of three linear equations in the unknowns x_Δ, x_i, and $x_{\langle i/2\rangle}$, and the matrix of this set of equations is given by

$$B \;=\; \begin{pmatrix} 1 & \beta & \alpha\beta \\ -\beta^{L-1} & 1 & 0 \\ -\beta^{L/2-1} & 0 & 1 \end{pmatrix} .$$

Now, it is easy to see that $\det(B) = 1 + \alpha\beta^{L/2} + \beta^L$. Since we assume that the polynomial $\xi^2 + \alpha\xi + 1$ has no roots in $\mathbb{F}_q$, we have $\det(B) \neq 0$ and we can solve (4)–(6) for x_Δ. By switching the roles of i and j it can be shown that we can solve also for $x_{p-\Delta}$.

Assume now that L and M are odd (so both i and j are nonzero). In this case, we can substitute $\ell = (L{-}p)/2 = -(M{+}1)/2$ in (2)(b) to obtain

$$x_{\langle i/2\rangle} \;=\; \beta^{-(M-1)/2} x_{p-\Delta} \;-\; \sum_{t=(M+1)/2}^{M-1} \beta^{-t+(M-1)/2} z_{\langle t\Delta\rangle} \tag{7}$$

instead of (6). In addition, we will need the counterparts of (4), (5), and (7) obtained when the roles of i and j are switched. Namely,

$$x_{p-\Delta} \;+\; (1/\beta)(x_j \;+\; \alpha x_{\langle j/2\rangle}) \;=\; -z_{p-j}/\beta \;, \tag{8}$$

$$x_j \;=\; \beta^{-(M-1)} x_{p-\Delta} \;-\; \sum_{t=1}^{M-1} \beta^{-t} z_{\langle t\Delta\rangle} \;, \tag{9}$$

and

$$x_{\langle j/2\rangle} \;=\; \beta^{(L-1)/2} x_\Delta \;+\; \sum_{t=(L+1)/2}^{L-1} \beta^{t-(L+1)/2} z_{\langle -t\Delta\rangle} \;. \tag{10}$$

The relations (4), (5), (7), and (8)–(10) form a set of six linear equations in the unknowns x_Δ, x_i, $x_{\langle i/2\rangle}$, $x_{p-\Delta}$, x_j, and $x_{\langle j/2\rangle}$, and the matrix of this set of equations is given by

$$\hat{B} \;=\; \left(\begin{array}{ccc|ccc} 1 & \beta & \alpha\beta & 0 & 0 & 0 \\ -\beta^{L-1} & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & -\beta^{-(M-1)/2} & 0 & 0 \\ \hline 0 & 0 & 0 & 1 & 1/\beta & \alpha/\beta \\ 0 & 0 & 0 & -\beta^{-(M-1)} & 1 & 0 \\ -\beta^{(L-1)/2} & 0 & 0 & 0 & 0 & 1 \end{array}\right) \;.$$

It is fairly easy to verify that

$$\det(\hat{B}) \;=\; (1+\beta^L)(1+\beta^{-M}) - \alpha^2\beta^{(L-M)/2} \;=\; (1+\beta^L)(1+\beta^{L-(p-1)}) - \alpha^2\beta^{L-(p-1)/2} \;. \tag{11}$$

Since we assume that $q-1$ divides $(p-1)/2$, it follows that $\beta^{(p-1)/2} = 1$; so,

$$\det(\hat{B}) \;=\; (1+\beta^L)^2 \;-\; \alpha^2\beta^L \;=\; ((1+y)^2 \;-\; \alpha^2 y)\,\Big|_{y=\beta^L} \;.$$

On the other hand,

$$(1+y)^2 \;-\; \alpha^2 y \;=\; \alpha^2(\xi^2 + \alpha\xi + 1)\,\Big|_{\xi=-(1+y)/\alpha} \;.$$

So, $\det(\hat{B}) \neq 0$ whenever α is nonzero and $\xi^2 + \alpha\xi + 1$ has no roots in $\mathbb{F}_q$. □

The conditions on p and α in Theorem 2.6 are sufficient but not necessary. In fact, we can trade the divisibility condition on $p-1$ with stronger conditions on α. For example, suppose that we require only that $p-1$ be divisible by $q-1$; for odd q, such a condition on p is strictly weaker than the one stated in Theorem 2.6. Then, from (11) we will now require that the two values, $(1+\beta^L)^2 \pm \alpha^2\beta^L$, be nonzero. This happens if the polynomials $(1+y)^2 \pm \alpha^2 y$ are irreducible over $\mathbb{F}_q$, and we can achieve that for odd q if and only if $\alpha^2 \pm 4$ are non squares in $\mathbb{F}_q$.

The appendix contains explicit formulas for solving $(Q_1^{(j)} - \beta Q_1^{(i)})\underline{x} = \underline{z}$ for $\underline{x}$ in the special case $q = 2$.

3 "Lowest-density" bounds on MDS codes

We present here lower bounds on the number of nonzero entries in the parity-check and generator matrices of $\mathbb{F}_q$-linear MDS codes over $\mathbb{F}_q^b$, as well as upper bounds on the dimension and redundancy of codes that attain those bounds. The construction in Section 4 that is based on the matrix set of Section 2.1 attains those bounds for $q > 2$ and for certain redundancy or dimension values. Stronger bounds can be stated for the case $q = 2$, but we defer those bounds to Section 5.

Propositions 3.1 and 3.2 below are straightforward extensions of well-known properties of parity-check matrices of conventional linear MDS codes (see [11, Ch. 11]).

Proposition 3.1 *Let $H = (\, H_1 \; H_2 \; \ldots \; H_n \,)$ be an $rb \times nb$ parity-check matrix of an $\mathbb{F}_q$-linear $[n, k{=}n{-}r]$ code $\mathcal{C}$ over $\mathbb{F}_q^b$, where each H_i is an $rb \times b$ submatrix of H. Then $\mathcal{C}$ is MDS if and only if the rb columns of any r distinct submatrices H_i form a linearly independent set over $\mathbb{F}_q$.*

Proposition 3.2 *Let $H = (\, A \; I_{rb} \,)$ be an $rb \times nb$ systematic parity-check matrix of an $\mathbb{F}_q$-linear $[n, k{=}n{-}r]$ code $\mathcal{C}$ over $\mathbb{F}_q^b$ and write $A = (A_{i,j})_{i,j=1}^{r\,;\,k}$, where each $A_{i,j}$ is a $b \times b$ block submatrix of A. Then $\mathcal{C}$ is MDS if and only if every square submatrix of A consisting of full block submatrices $A_{i,j}$ is nonsingular.*

An $\mathbb{F}_q$-*dual code* of an $\mathbb{F}_q$-linear code $\mathcal{C}$ over $\mathbb{F}_q^b$ is the unique $\mathbb{F}_q$-linear code $\mathcal{C}^\perp$ over $\mathbb{F}_q^b$ such that $(\mathcal{C}^\perp)_{\mathbb{F}_q}$ is the (conventional) dual code of $(\mathcal{C})_{\mathbb{F}_q}$ over $\mathbb{F}_q$ [11, Ch. 1]; namely,

$$(\mathcal{C}^\perp)_{\mathbb{F}_q} \;=\; ((\mathcal{C})_{\mathbb{F}_q})^\perp$$

(recall the notation $(\mathcal{C})_{\mathbb{F}_q}$ from Section 1).

Lemma 3.3 *Let $\mathcal{C}$ be an $\mathbb{F}_q$-linear $[n, k{=}n{-}r]$ MDS code over $\mathbb{F}_q^b$. Then $\mathcal{C}^\perp$ is an $\mathbb{F}_q$-linear $[n, r]$ MDS code over $\mathbb{F}_q^b$.*

Proof. Let $G = (\, G_1 \; G_2 \; \ldots \; G_n \,)$ be a $kb \times nb$ generator matrix of $\mathcal{C}$ where each G_i is a $kb \times b$ submatrix of G. Suppose to the contrary that the submatrix $\tilde{G} = (\, G_{i_1} \; G_{i_2} \; \ldots \; G_{i_k} \,)$ is singular. Then there is a nonzero vector $\underline{x} \in \mathbb{F}_q^{kb}$ such that $\underline{x}\tilde{G} = \underline{0}$. It follows that the codeword $\underline{x}G$ of $(\mathcal{C})_{\mathbb{F}_q}$ has Hamming weight less than $r{+}1$, where the weight is measured in symbols of $\mathbb{F}_q^b$. This however implies the contradiction that $\mathcal{C}$ is not MDS. Hence, the kb columns of any k distinct submatrices G_i form a linearly independent set over $\mathbb{F}_q$. The lemma now follows from Proposition 3.1. □

Proposition 3.4 *Let $\mathcal{C}$ be an $\mathbb{F}_q$-linear $[n, k{=}n{-}r]$ MDS code over $\mathbb{F}_q^b$ with an $rb \times nb$ parity-check matrix H and a $kb \times nb$ generator matrix G—both matrices over $\mathbb{F}_q$.*

(a) There are at least $k{+}1$ nonzero entries in each row of H.

(b) There are at least $r{+}1$ nonzero entries in each row of G.

Proof. Every row in G is a nonzero codeword of $(\mathcal{C})_{\mathbb{F}_q}$, and since $\mathcal{C}$ is MDS, the Hamming weight, over $\mathbb{F}_q$, of each such row must be at least $r{+}1$. Similarly, by Lemma 3.3, the code $\mathcal{C}^\perp$ is MDS; therefore, the Hamming weight of each row in H must be at least $k{+}1$. □

Proposition 3.5 *Let $\mathcal{C}$ be an $\mathbb{F}_q$-linear MDS code over $\mathbb{F}_q^b$. The bound in Proposition 3.4(a) is attained by some systematic parity-check matrix H if and only the bound in Proposition 3.4(b) is attained by some systematic generator matrix G.*

Proof. We start with the "only if" part. Let H be an $rb \times nb$ systematic parity-check matrix of $\mathcal{C}$ and suppose that H attains the bound of Proposition 3.4(a). Up to permutation of columns, the matrix H has the form $(\, A \;\; I_{rb} \,)$, where A is an $rb \times kb$ matrix in which each row has exactly k nonzero entries. Hence, the total number of nonzero entries in A is krb; so, up to permutation of columns, the matrix $(\, I_{kb} \;\; -A^T \,)$ is a systematic generator matrix of $\mathcal{C}$ that attains the bound of Proposition 3.4(b).

The "if" part follows by duality from Lemma 3.3. □

Theorem 3.6 *Let $\mathcal{C}$ be an $\mathbb{F}_q$-linear $[n, k{=}n{-}r]$ MDS code over $\mathbb{F}_q^b$ and suppose that $\mathcal{C}$ has a systematic parity-check matrix that attains the bound of Proposition 3.4(a).*

(i) If $k \le 1$ or $r \le 1$, then $n = k{+}r$ can take any positive integer value.

(ii) Otherwise,

$$k \;\le\; b(q{-}1) \quad \textit{and} \quad r \;\le\; b(q{-}1)\,.$$

Proof. (i) The cases $k = 0$ or $r = 0$ are trivial. When $r = 1$, we have the $[n, n{-}1]$ parity code over $\mathbb{F}_q^b$ for arbitrary n with the systematic $b \times nb$ parity-check matrix $H = (\, I_b \; I_b \; \ldots \; I_b \,)$. This matrix is also a generator matrix of the $[n, 1]$ repetition code over $\mathbb{F}_q^b$, which proves the claim for $k = 1$.

(ii) Let $H = (\, A \;\; I_{rb} \,)$ be a systematic parity-check matrix of $\mathcal{C}$ with exactly $k{+}1$ nonzero entries in each row. Write $A = (A_{i,j})_{i,j=1}^{r\,,\,k}$, where each $A_{i,j}$ is a $b \times b$ block submatrix of A. By Proposition 3.2 every matrix $A_{i,j}$ is nonsingular. Since we assume that every row in H contains exactly $k{+}1$ nonzero entries, each matrix $A_{i,j}$ must contain exactly b nonzero

entries. It follows that for every $1 \leq i \leq r$, the set $\{A_{i,j}\}_{j=1}^{k}$ satisfies (P1) and (P3). Without loss of generality we can assume that $A_{1,j} = I_b$ for $1 \leq j \leq k$, in which case Proposition 3.2 implies that any set $\{A_{i,j}\}_{j=1}^{k}$, $i > 1$, must satisfy (P2). Hence, by Proposition 2.1 we must have $k \leq b(q-1)$, thus proving the first bound in part (ii). The second bound is obtained by duality from Proposition 3.5. □

4 New construction of MDS codes

In this section, we present a construction of $\mathbb{F}_q$-linear $[n, k{=}n{-}r]$ MDS codes over $\mathbb{F}_q^b$ for $r \leq 4$. The construction has the sparsest systematic parity-check and generator matrices possible. Furthermore, given those properties, our construction attains the largest possible dimension when $r = 2$ (and also when $r = 3$ and q is even). The case $r = 2$ will be discussed in Section 4.1, whereas the values $r = 3, 4$ will be treated in Section 4.2.

4.1 Redundancy 2

Let $\mathcal{B} = \{B_1, B_2, \ldots, B_k\}$ be a set of $b \times b$ matrices over $\mathbb{F}_q$ and consider the code $\mathcal{C}_\mathcal{B}$ defined by the parity-check matrix

$$H_\mathcal{B} \;=\; \begin{pmatrix} I & I & I & \ldots & I & I & 0 \\ B_1 & B_2 & B_3 & \ldots & B_k & 0 & I \end{pmatrix} ,$$

where $I = I_b$. A generator matrix of $\mathcal{C}_\mathcal{B}$ is given by

$$G_\mathcal{B} \;=\; \begin{pmatrix} I & 0 & 0 & \ldots & 0 & -I & -B_1^T \\ 0 & I & 0 & \ldots & 0 & -I & -B_2^T \\ 0 & 0 & I & \ldots & 0 & -I & -B_3^T \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & I & -I & -B_k^T \end{pmatrix} .$$

Proposition 4.1 *The code $\mathcal{C}_\mathcal{B}$ is an $\mathbb{F}_q$-linear $[k{+}2, k]$ MDS code over $\mathbb{F}_q^b$ if and only if $\mathcal{B}$ satisfies (P1)–(P2).*

Proof. This follows directly from Proposition 3.2. □

Suppose now that $\mathcal{B}$ satisfies (P1)–(P3). The number of nonzero entries in each row of $H_\mathcal{B}$ is $k{+}1$, and the number of nonzero entries in each row of $G_\mathcal{B}$ is 3, thus attaining the bounds of Proposition 3.4. In particular, this will be the case if $\mathcal{B}$ is a subset of a set $\mathcal{U}_\alpha$, introduced in Section 2.1, with b and α taken so that $\mathcal{U}_\alpha$ satisfies (P1)–(P3) (see Theorem 2.4).

Furthermore, when $\mathcal{B} = \mathcal{U}_\alpha$, the dimension k of $\mathcal{C}_{\mathcal{U}_\alpha}$ is $b(q-1)$, thereby attaining the upper bound on k of Theorem 3.6(ii).

Observe that an element $a \cdot C_\alpha^t$ of $\mathcal{U}_\alpha$ represents multiplication by $a\xi^t$ in the ring, $\mathbb{F}_q[\xi]/(\xi^b - \alpha)$, of polynomials over $\mathbb{F}_q$ modulo $\xi^b - \alpha$. Hence, $\mathcal{C}_{\mathcal{U}_\alpha}$ can be regarded as a code over $\mathbb{F}_q[\xi]/(\xi^b - \alpha)$ with a parity-check matrix

$$\begin{pmatrix} 1 & 1 & \dots & 1 & \dots & 1 & 1 & \dots & 1 & 1 & 0 \\ a_1 & a_1\xi & \dots & a_1\xi^{b-1} & \dots & a_{q-1} & a_{q-1}\xi & \dots & a_{q-1}\xi^{b-1} & 0 & 1 \end{pmatrix}, \tag{12}$$

where $\{a_1, \dots, a_{q-1}\} = \mathbb{F}_q^*$. Clearly, when $\xi^b - \alpha$ is irreducible then $\mathbb{F}_q[\xi]/(\xi^b - \alpha)$ is a field and $\mathcal{C}_{\mathcal{U}_\alpha}$ is a code obtained from an extended Reed-Solomon code (see [11, p. 323]) by shortening [11, p. 29]. Recall, however, that when $q \equiv 3 \pmod 4$, the set $\mathcal{U}_\alpha$ may satisfy (P1)–(P3) even when $\xi^b - \alpha$ is reducible; in such a case we obtain MDS codes over non-field rings (see also [4], [3]). Following the discussion at the end of Section 2.1, when α is primitive we can write (12) as

$$\begin{pmatrix} 1 & 1 & 1 & \dots & 1 & 1 & 0 \\ 1 & \xi & \xi^2 & \dots & \xi^{b(q-1)-1} & 0 & 1 \end{pmatrix}.$$

We turn now to the case $q = 2$ and assume that $\mathcal{B}$ satisfies property (P1)–(P3'). Further, we assume that exactly one matrix in $\mathcal{B}$, say B_1, is a permutation matrix (recall that two or more permutation matrices necessarily violate (P2)). The number of 1's in B_i is equal to b if $i = 1$ and is equal to $b+1$ if $i > 1$. Hence, the average number of 1's per row in $H_\mathcal{B}$ and $G_\mathcal{B}$ is $k + 1 + \frac{k-1}{2b}$ and $3 + \frac{1}{b}(1 - \frac{1}{k})$, respectively. (In addition, the number of 1's in each row in $H_\mathcal{B}$ is either $k+1$ or $k+2$; similarly, the number of 1's in each row in $G_\mathcal{B}$ is either 3 or 4.) As we show in Proposition 5.2 below, these are the smallest averages possible in every systematic parity-check and generator matrices of any $\mathbb{F}_2$-linear $[k+2, k]$ MDS code over $\mathbb{F}_2^b$.

Recall the construction $\mathcal{V}_\alpha$ from Section 2.2. Let b be an integer so that $b+1$ is a prime and, for such b, take $\mathcal{B}$ to be any subset of $\mathcal{V}_1$ over $\mathbb{F}_2$ that contains the identity matrix. By Theorem 2.6 such a set $\mathcal{B}$ satisfies (P1)–(P3') and, so, the respective code $\mathcal{C}_\mathcal{B}$ is MDS. Furthermore, when $\mathcal{B} = \mathcal{V}_1$, the dimension k of $\mathcal{C}_{\mathcal{V}_1}$ is $b+1$, thereby attaining an upper bound that we prove below in Theorem 5.3. In comparison, the EVENODD construction of [2] has a parity-check matrix $H_\mathcal{B}$ with a set $\mathcal{B}$ in which each of the matrices B_i, $i > 1$, has a row that is all 1's.

Example 1.1 provides the parity-check and generator matrices of code $\mathcal{C}_{\mathcal{V}_1}$ over $\mathbb{F}_2^2$. The code $\mathcal{C}_{\mathcal{V}_1}$ over $\mathbb{F}_2^4$ can be obtained from the matrices in Example 2.1.

It follows from Proposition 3.5 that if $\mathcal{C}_\mathcal{B}$ is an MDS code that attains the lower bounds of Proposition 3.4, then so does the $[k+2, 2]$ dual code $\mathcal{C}_\mathcal{B}^\perp$. Clearly, if $\mathcal{C}_\mathcal{B}$ attains the upper bound on k of Theorem 3.6(ii), then $\mathcal{C}_\mathcal{B}^\perp$ attains the upper bound on r in that theorem.

We show next how to decode any MDS code $\mathcal{C}_\mathcal{B}$ when one symbol is in error or, alternatively, when two symbols have been erased.

Let $(\underline{c}_\ell)_{\ell=1}^{k+2}$ be the transmitted codeword and $(\underline{z}_\ell)_{\ell=1}^{k+2}$ be the received word, where $\underline{c}_\ell, \underline{z}_\ell \in \mathbb{F}_q^b$. The syndrome values of $(\underline{z}_\ell)_{\ell=1}^{k+2}$ over $\mathbb{F}_q^b$, with respect to the parity-check matrix $H_{\mathcal{B}}$, are given by

$$\begin{array}{ccccccccccc} \underline{s}_0 & = & \underline{z}_1 & + & \underline{z}_2 & + & \cdots & + & \underline{z}_k & + & \underline{z}_{k+1} \\ \underline{s}_1 & = & B_1\underline{z}_1 & + & B_2\underline{z}_2 & + & \cdots & + & B_k\underline{z}_k & + & \underline{z}_{k+2} \end{array} \quad . \tag{13}$$

Assume that only one error has occurred in, say, location i, $1 \le i \le k+2$; namely, $\underline{z}_\ell = \underline{c}_\ell$ for $\ell \ne i$ and $\underline{z}_i = \underline{c}_i + \underline{e}_i$, $\underline{e}_i \ne 0$. If $i = k+1$ then $\underline{s}_0 = \underline{e}_{k+1}$ and $\underline{s}_1 = \underline{0}$, while if $i = k+2$ then $\underline{s}_0 = \underline{0}$ and $\underline{s}_1 = \underline{e}_{k+2}$. Consider now the case where i is in the range $1 \le i \le k$. Here, $\underline{s}_0 = \underline{e}_i$ and $\underline{s}_1 = B_i\underline{e}_i$; so, $\underline{s}_1 = B_i\underline{s}_0$. Since $\mathcal{C}_{\mathcal{B}}$ is capable of correcting one error, there is exactly one index i for which $\underline{s}_1 = B_i\underline{s}_0$; this index, i, gives the error location. Circuits implementing the product $B_i\underline{s}_0$ can be made very efficient when $\mathcal{B} \subseteq \mathcal{U}_\alpha$ or $\mathcal{B} \subseteq \mathcal{V}_\alpha$, since then the matrices B_i represent linear operations which are very similar to cyclic shifts. We summarize next the decoding procedure of one error.

Algorithm 4.1 (Correcting one error by $\mathcal{C}_{\mathcal{B}}$) *Let $(\underline{z}_\ell)_{\ell=1}^{k+2}$ be a received word and let the syndrome values $\underline{s}_0$ and $\underline{s}_1$ be given by (13).*

1. *If $\underline{s}_0 = \underline{0}$ or $\underline{s}_1 = \underline{0}$ then output $(\underline{z}_\ell)_{\ell=1}^{k}$ and exit.*
2. *Else, let i be the unique index for which $\underline{s}_1 = B_i\underline{s}_0$.*
3. *Let $\underline{z}_i \leftarrow \underline{z}_i - \underline{s}_0$, output $(\underline{z}_\ell)_{\ell=1}^{k}$ and exit.*

Notice that the algorithm produces as output the k information symbols (one of which has possibly been corrected), discarding the two check symbols.

Next we consider erasure recovery. Assume that the received word is $(\underline{z}_\ell)_{\ell=1}^{k+2}$ and that entries i and j, $1 \le i < j \le k+2$, have been erased. We initially set $\underline{z}_i = \underline{z}_j = \underline{0}$. If $j = k+2$, then $\underline{e}_i = \underline{s}_0$. If $j = k+1$, then $\underline{s}_0 = \underline{e}_i + \underline{e}_{k+1}$ and $\underline{s}_1 = B_i\underline{e}_i$; so, $\underline{e}_i = B_i^{-1}\underline{s}_1$ and $\underline{e}_{k+1} = \underline{s}_0 - B_i^{-1}\underline{s}_1$. Finally if $1 \le i < j \le k$, then

$$\underline{s}_0 \;=\; \underline{e}_i + \underline{e}_j \quad \text{and} \quad \underline{s}_1 \;=\; B_i\underline{e}_i + B_j\underline{e}_j \;,$$

thus yielding

$$\underline{e}_j \;=\; (B_j - B_i)^{-1}(\underline{s}_1 - B_i\underline{s}_0) \quad \text{and} \quad \underline{e}_i \;=\; \underline{s}_0 - \underline{e}_j \;.$$

Lemma 7.1 in the appendix provides the formulas for multiplying by $(B_j - B_i)^{-1}$ when $q = 2$ and $\mathcal{B} = \mathcal{V}_1$. The procedure for recovering two erasures is summarized below.

Algorithm 4.2 (Recovering two erasures by $\mathcal{C}_{\mathcal{B}}$) Let $(\underline{z}_\ell)_{\ell=1}^{k+2}$ be a received word where locations i and j, $1 \le i < j \le k+2$, have been erased, and set initially $\underline{z}_i = \underline{z}_j = \underline{0}$. Let $\underline{s}_0$ and $\underline{s}_1$ be given by (13).

1. If $j = k{+}1$ then let $\underline{z}_{k+1} \leftarrow -(\underline{s}_0 - B_i^{-1}\underline{s}_1)$.
2. Else if $1 \le j \le k$ then let $\underline{z}_j \leftarrow -(B_j - B_i)^{-1}(\underline{s}_1 - B_i\underline{s}_0)$.
3. Let $\underline{z}_i \leftarrow -(\underline{s}_0 + \underline{z}_j)$ and output $(\underline{z}_\ell)_{\ell=1}^k$.

4.2 Redundancy values 3 and 4

We may try to generalize the construction of Section 4.1 to larger redundancy values by considering the $\mathbb{F}_q$-linear $[n, k{=}n{-}r]$ code $\mathcal{C}_\mathcal{B}(r)$ over $\mathbb{F}_q^b$ with a parity-check matrix

$$H_\mathcal{B}(r) \;=\; \begin{pmatrix} I & I & \dots & I & I & 0 & 0 & \dots & 0 \\ B_1 & B_2 & \dots & B_k & 0 & I & 0 & \dots & 0 \\ B_1^2 & B_2^2 & \dots & B_k^2 & 0 & 0 & I & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ B_1^{r-1} & B_2^{r-1} & \dots & B_k^{r-1} & 0 & 0 & 0 & \dots & 1 \end{pmatrix} ,$$

where $\mathcal{B} = \{B_1, B_2, \dots, B_k\}$ is a subset of $\mathcal{U}_\alpha$. In particular, each power matrix B_i^ℓ contains (at most) b nonzero entries, and so each row of $H_\mathcal{B}(r)$ contains (at most) $k{+}1$ nonzero entries. Thus, if $\mathcal{C}_\mathcal{B}(r)$ is MDS then it attains the lower bounds of Proposition 3.4.

It will be convenient to analyze $\mathcal{C}_\mathcal{B}(r)$ through its representation as a code over the polynomial ring $\mathbb{F}_q[\xi]/(\xi^b - \alpha)$, in which case we will interchange between a matrix B_i and the element β_i associated with it in the set

$$\left\{ a\xi^t \;:\; a \in \mathbb{F}_q^*,\; 0 \le t < b \right\} .$$

Consider the case $r = 3$. By Proposition 3.2 the code $\mathcal{C}_\mathcal{B}(3)$ is MDS if and only if every square submatrix of

$$A_\mathcal{B}(3) \;=\; \begin{pmatrix} 1 & 1 & \dots & 1 \\ \beta_1 & \beta_2 & \dots & \beta_k \\ \beta_1^2 & \beta_2^2 & \dots & \beta_k^2 \end{pmatrix}$$

is invertible in $\mathbb{F}_q[\xi]/(\xi^b - \alpha)$. Every submatrix of $A_\mathcal{B}(3)$ that is of the Vandermonde type will be invertible when the differences $\beta_j - \beta_i$, $1 \le i < j \le k$, are all invertible (equivalently, when the matrices $B_j - B_i$ are nonsingular); this follows from the known formula for the determinant of a Vandermonde matrix [11, p. 116]. The only submatrices of $A_\mathcal{B}(3)$ that are not of the Vandermonde type are the 2×2 submatrices whose entries belong to the first and third rows of $A_\mathcal{B}(3)$, namely, the submatrices

$$\begin{pmatrix} 1 & 1 \\ \beta_i^2 & \beta_j^2 \end{pmatrix} .$$

The determinant of the latter matrix is $\beta_j^2 - \beta_i^2 = (\beta_j - \beta_i)(\beta_j + \beta_i)$, so $\beta_j + \beta_i$ should also be invertible in $\mathbb{F}_q[\xi]/(\xi^b - \alpha)$. This condition certainly holds if q is even and $\mathcal{B}$ is a subset of a set $\mathcal{U}_\alpha$ that satisfies (P1)–(P2) (see Theorem 2.4). So, when q is even we obtain $\mathbb{F}_q$-linear $[k{+}3, k]$ MDS codes over $\mathbb{F}_q^b$ that attain the lower bounds of Proposition 3.4, where k can be as large as the bound, $b(q{-}1)$, of Theorem 3.6(ii).

When q is odd, the elements $\beta_j + \beta_i$ will be invertible unless $\beta_i = -\beta_j$. Therefore, we can let $\mathcal{B}$ be any subset of $\mathcal{U}_\alpha$ that contains at most one matrix out of the element pair $\pm B$, thus obtaining a $[k{+}3, k]$ MDS code that attains the lower bound of Proposition 3.4. The value of k can get here to $b(q{-}1)/2$, which is still linearly growing with $b(q{-}1)$, yet short of the upper bound of Theorem 3.6(ii).

Consider now the case $r = 4$. The code $\mathcal{C}_\mathcal{B}(4)$ is MDS if and only if every square submatrix of

$$A_\mathcal{B}(4) \;=\; \begin{pmatrix} 1 & 1 & \dots & 1 \\ \beta_1 & \beta_2 & \dots & \beta_k \\ \beta_1^2 & \beta_2^2 & \dots & \beta_k^2 \\ \beta_1^3 & \beta_2^3 & \dots & \beta_k^3 \end{pmatrix}$$

is invertible in $\mathbb{F}_q[\xi]/(\xi^b - \alpha)$. The non-Vandermonde type submatrices of $A_\mathcal{B}(4)$ are

$$\begin{pmatrix} 1 & 1 \\ \beta_i^2 & \beta_j^2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ \beta_i^3 & \beta_j^3 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 & 1 \\ \beta_i & \beta_j & \beta_\ell \\ \beta_i^3 & \beta_j^3 & \beta_\ell^3 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 & 1 \\ \beta_i^2 & \beta_j^2 & \beta_\ell^2 \\ \beta_i^3 & \beta_j^3 & \beta_\ell^3 \end{pmatrix},$$

with the respective determinants $\beta_j^2 - \beta_i^2$, $\beta_j^3 - \beta_i^3$,

$$(\beta_i - \beta_j)(\beta_i - \beta_\ell)(\beta_j - \beta_\ell)(\beta_i + \beta_j + \beta_\ell)\,,$$

and

$$(\beta_i\beta_j\beta_\ell)^3(\beta_i^{-1} - \beta_j^{-1})(\beta_i^{-1} - \beta_\ell^{-1})(\beta_j^{-1} - \beta_\ell^{-1})(\beta_i^{-1} + \beta_j^{-1} + \beta_\ell^{-1})\,.$$

It follows that $\mathcal{C}_\mathcal{B}(4)$ is MDS if for any distinct β_j, β_j, and β_ℓ, the elements

$$\beta_j \pm \beta_i\,, \quad \beta_j^3 - \beta_i^3\,, \quad \beta_i + \beta_j + \beta_\ell\,, \quad \text{and} \quad \beta_i^{-1} + \beta_j^{-1} + \beta_\ell^{-1}\,, \tag{14}$$

are all invertible in $\mathbb{F}_q[\xi]/(\xi^b - \alpha)$.

We next show a construction of a set $\mathcal{B}$ for $q = 2^h$ where the elements in (14) are invertible. When h is odd, the size of $\mathcal{B}$ is within the range $b(q{+}1)(1 \pm 2q^{-1/2})/4$, and when h is even, the size of $\mathcal{B}$ is guaranteed to be at least $b(q{+}1)(1 - 2q^{-1/2})/8$. In either case we obtain $[k{+}4, k]$ MDS codes for values of k that are linearly growing with $b(q{-}1)$ but again short of the upper bound of Theorem 3.6(ii).

We assume that $\mathcal{U}_\alpha$ satisfies (P1)–(P2), and when q is even this implies that $\xi^b - \alpha$ is irreducible (see Theorem 2.4 and [10, p. 124]). So, $\mathbb{F}_q[\xi]/(\xi^b - \alpha)$ is a field and an element in the field is invertible if and only if it is nonzero.

Clearly, the expressions $\beta_j \pm \beta_i$ in (14) are nonzero for $j \neq i$ whenever q is even. As for the expression $\beta_j^3 - \beta_i^3$, recall that each β_i has the form $a_i \xi^{t_i}$ where $a_i \in \mathbb{F}_q^*$ and $0 \leq t_i < b$; so, $\beta_j^3 = \beta_i^3$ is equivalent to

$$a_i^3 \xi^{3t_i} \equiv a_j^3 \xi^{3t_j} \pmod{(\xi^b - \alpha)} . \tag{15}$$

Note that (15) can hold only if $3t_i \equiv 3t_j \pmod{b}$. Without loss of generality we can assume that $t_i \leq t_j$ and write $3(t_j - t_i) = \ell b$ for some $\ell \in \{0, 1, 2\}$. By (15) we have

$$(a_i/a_j)^3 \equiv \xi^{\ell b} \equiv \alpha^\ell \pmod{\xi^b - \alpha} ,$$

namely, $(a_i/a_j)^3 = \alpha^\ell$ for some $\ell \in \{0, 1, 2\}$. We now show that this implies $t_i = t_j$, i.e., $\ell = 0$. Suppose this is false, which means that $(a_i/a_j)^3$ equals either α or α^2. This, in turn, implies that α is a third power of an element in $\mathbb{F}_q^*$ and so 3 is a divisor of $(q-1)/\mathcal{O}(\alpha)$. On the other hand, recall that $\ell b = 3(t_j - t_i)$ and so 3 is also a divisor of b. This, however, contradicts by Theorem 2.4 our assumption that $\mathcal{U}_\alpha$ satisfies (P2). Therefore, (15) implies $t_i = t_j$ and $a_i^3 = a_j^3$. Now, when h is odd, there are no elements in $\mathbb{F}_q^*$ of order 3; so, $a_i = a_j$, i.e., $\beta_i = \beta_j$. We will treat the case of even h after the proof of Proposition 4.3 below.

Turning to the remaining two expressions in (14), the equality $\beta_i + \beta_j + \beta_\ell = 0$ translates to

$$a_i \xi^{t_i} + a_j \xi^{t_j} + a_\ell \xi^{t_\ell} \equiv 0 \pmod{(\xi^b - \alpha)} ,$$

which can hold if and only if $t_i = t_j = t_\ell$ and $a_i + a_j + a_\ell = 0$. Similarly, $\beta_i^{-1} + \beta_j^{-1} + \beta_\ell^{-1} = 0$ if and only if $t_i = t_j = t_\ell$ and $a_i^{-1} + a_j^{-1} + a_\ell^{-1} = 0$. Therefore, we select the set $\mathcal{B}$ to contain elements of $\mathcal{U}_\alpha$ of the form $a \cdot C_\alpha^t$, $0 \leq t < b$, where a ranges over a subset of $\mathbb{F}_q^*$ with the property that no three elements in the subset sum to zero, and neither do their inverses. A subset that satisfies this property is given by

$$\mathcal{A}_q = \left\{ a \in \mathbb{F}_q^* \;\middle|\; \mathrm{Tr}(a) = \mathrm{Tr}(a^{-1}) = 1 \right\} ,$$

where $\mathrm{Tr}(x) = \sum_{i=0}^{h-1} x^{2^i}$ is the absolute trace function from $\mathbb{F}_q$ to $\mathbb{F}_2$ [10, Section 3.2]. Indeed, since the trace is additive, the trace of the sum of every three elements in $\mathcal{A}_q$ is 1 and is therefore nonzero. The same applies to the inverse elements of $\mathcal{A}_q$. The code $\mathcal{C}_\mathcal{B}(4)$ thus obtained is a $[k+4, k]$ MDS code with $k = |\mathcal{B}| = b|\mathcal{A}_q|$.

We provide next an estimate on the size of $\mathcal{A}_q$. The following analysis can essentially be deduced from [9] (see also [7]) and is included here for the sake of completeness.

Lemma 4.2 [10, p. 228] *For $q = 2^m$,*

$$\left| \sum_{a \in \mathbb{F}_q^*} (-1)^{\mathrm{Tr}(a + a^{-1})} \right| \leq 2q^{1/2} .$$

Proposition 4.3 *For $q = 2^m$,*

$$\left| |\mathcal{A}_q| - \frac{q+1}{4} \right| \leq \frac{1}{2} q^{1/2} .$$

Proof. Write $|\mathcal{A}_q|$ as

$$|\mathcal{A}_q| = \frac{1}{4} \sum_{a \in \mathbb{F}_q^*} \left(1 - (-1)^{\mathrm{Tr}(a)}\right) \left(1 - (-1)^{\mathrm{Tr}(a^{-1})}\right) . \tag{16}$$

Now, $\sum_{a \in \mathbb{F}_q^*} (-1)^{\mathrm{Tr}(a)} = \sum_{a \in \mathbb{F}_q^*} (-1)^{\mathrm{Tr}(a^{-1})} = -1$; so, from (16) we obtain

$$|\mathcal{A}_q| = \frac{1}{4} \left(q + 1 + \sum_{a \in \mathbb{F}_q^*} (-1)^{\mathrm{Tr}(a+a^{-1})}\right) .$$

The result now follows from Lemma 4.2. □

The previous construction can be amended to fit also the case $q = 2^h$ when h is even. To this end, we need to avoid the equality $a_i^3 = a_j^3$ in (15) when $a_i \neq a_j$. This can be accomplished by eliminating elements from $\mathcal{A}_q$ so that it will have at most one representative of each triple $\{a, a\omega, a\omega^2\} \subseteq \mathbb{F}_q^*$, where $\mathcal{O}(\omega) = 3$. Observe that $a + a\omega + a\omega^2 = 0$, and recall that no three elements in $\mathcal{A}_q$ sum to zero; so, $\mathcal{A}_q$ can contain at most two of the elements of each triple $\{a, a\omega, a\omega^2\}$ in the first place. It follows that we need to delete at most half of the elements of $\mathcal{A}_q$ in order to guarantee that all the third powers of the elements in $\mathcal{A}_a$ are distinct. This, in turn, provides a construction of a $[k+4, k]$ MDS code with $k \geq b(q+1)(1 - 2q^{-1/2})/8$.

It remains open to provide a construction for general r that attains the lower bounds of Proposition 3.4 with values of k (close to) the upper bound of Theorem 3.6(ii). Due to the structure of the ring $\mathbb{F}_q[\xi]/(\xi^b - \alpha)$, the methods of [3] can be useful to find large sets $\mathcal{B}$ for which $\mathcal{C}_{\mathcal{B}}(r)$ is MDS. Of course, once we construct such a code, the dual code $\mathcal{C}_{\mathcal{B}}^{\perp}(r)$ is also an MDS code that attains the lower bounds of Proposition 3.4. Furthermore, if $\mathcal{C}_{\mathcal{B}}(r)$ attains the upper bound on k of Theorem 3.6(ii), then $(\mathcal{C}_{\mathcal{B}}(r))^{\perp}$ attains the respective bound on r.

The case $q = 2$ remains open already for $r = 3$. An attempt to substitute $B_i = Q_\alpha^{(i)}$ in $H_{\mathcal{B}}(3)$ will fail since $(Q_\alpha^{(j)})^2 - (Q_\alpha^{(i)})^2$ can be singular (the matrices in $Q_\alpha^{(i)}$ do not commute); check, for example, the matrices $Q_\alpha^{(1)}$ and $Q_\alpha^{(2)}$ in Example 2.1. (Also, the matrices $(Q_\alpha^{(i)})^2$ do not satisfy (P3'); however, if this were the only problem, we could multiply the ith block column in $H_{\mathcal{B}}(3)$ by $(Q_\alpha^{(i)})^{-1} = Q_\alpha^{(b+1-i)}$.) Still, it is worthwhile presenting the following example.

Example 4.1 Let $k = r = 3$ and $b > 1$ and let

$$A = \begin{pmatrix} D & I & I \\ I & D & I \\ I & I & D \end{pmatrix} ,$$

where $I = I_b$ and $D = (d_{\ell,m})$ is a matrix over $\mathbb{F}_2$ of the form

$$d_{\ell,m} = \begin{cases} 1 & \text{if } \ell < b \text{ and } m = \ell+1 \\ 1 & \text{if } \ell = b \text{ and } m \in \{1, t\} \text{ for some } 2 \le t \le b \\ 0 & \text{otherwise} \end{cases} , \quad 1 \le \ell, m \le b \; .$$

It is easy to check that both D and $D + I$ are nonsingular. This, in turn, implies that every square submatrix of A that consists of full $b \times b$ block submatrices D or I, is nonsingular. Hence, $\hat{H} = (\, A \; I_{3b} \,)$ is a systematic parity-check (or generator) matrix of an $\mathbb{F}_2$-linear $[6, 3]$ MDS code over $\mathbb{F}_2^b$, and the number of 1's in $\hat{H}$ is $12b + 3$. This corresponds to an average number of 1's per row equaling to $4 + \frac{1}{b}$, thus attaining lower bounds which we prove in Propositions 5.2 and 5.5 below. □

5 Stronger bounds for the binary case

We saw in Section 2 that the case $q = 2$ is unique compared to larger fields in the sense that it is the only field for which there are only finitely many values of b (in fact, only one value of b) for which properties (P1)–(P3) can be satisfied. This suggests that we may be able to improve the bounds of Section 3 for $q = 2$. We indeed do this in this section, starting with the following lemma.

Lemma 5.1 *Let $k \ge r \ge 2$ and $A = (A_{i,j})_{i,j=1}^{r\;k}$ be an $rb \times kb$ matrix over $\mathbb{F}_2$, where each $A_{i,j}$ is a $b \times b$ block submatrix of A. Furthermore, assume that every square submatrix of A consisting of full block submatrices $A_{i,j}$ is nonsingular. Then the average number of 1's in a block submatrix $A_{i,j}$ of A is at least $b + \frac{1}{2} - \frac{1}{2k}$.*

Proof. Suppose to the contrary that the lemma does not hold. Then there are two rows of block submatrices $A_{i,j}$ in A that form a $2b \times kb$ submatrix $\hat{A}$ in which the average number of 1's per block submatrix is less than $b + \frac{1}{2} - \frac{1}{2k}$; without loss of generality we assume that those rows are $i = 1, 2$. It follows that the total number of 1's in $\hat{A}$ must be $2kb + k - 2$ or less. Since each block submatrix $A_{i,j}$ in $\hat{A}$ is nonsingular, the number of 1's in each such block submatrix must be at least b. Thus, there are $k+2$ block submatrices $A_{i,j}$ in $\hat{A}$ in which the number of 1's is exactly b; each such block submatrix must be a $b \times b$ permutation matrix. It follows that there must be indexes $j_1 < j_2$ such that all four block submatrices, A_{1,j_1}, A_{1,j_2}, A_{2,j_1}, and A_{2,j_2}, are permutation matrices. Hence, the columns of the $2b \times 2b$ submatrix

$$\begin{pmatrix} A_{1,j_1} & A_{1,j_2} \\ A_{2,j_1} & A_{2,j_2} \end{pmatrix}$$

of A sum to zero, contradicting our assumption on A. □

The following improves on Proposition 3.4 for $q = 2$.

Proposition 5.2 *Let $\mathcal{C}$ be an $\mathbb{F}_2$-linear $[n, k{=}n{-}r]$ MDS code over $\mathbb{F}_2^b$ and assume that $k \geq r \geq 2$.*

(a) The average number of 1's per row in every systematic parity-check matrix of $\mathcal{C}$ is at least $k + 1 + \frac{k-1}{2b}$.

(b) The average number of 1's per row in every systematic generator matrix of $\mathcal{C}$ is at least $r + 1 + \frac{r}{2b}(1 - \frac{1}{k})$.

Proof. Part (a) follows from Proposition 3.2 and Lemma 5.1. Part (b) follows from part (a), combined with the fact that $(\, A \;\; I_{rb} \,)$ is a parity-check matrix of an $\mathbb{F}_q$-linear $[n, k{=}n{-}r]$ code $\mathcal{C}$ over $\mathbb{F}^b$ if and only if $(\, I_{kb} \;\; -A^T \,)$ is a generator matrix of $\mathcal{C}$. □

When $r > k$ we can apply Proposition 5.2 to the dual code. The statement of Proposition 3.5 holds also with respect to the bounds of Proposition 5.2.

The following theorem is an improvement of a result in [3]. It tightens the bound on k of Theorem 3.6 for $q = r = 2$.

Theorem 5.3 *Let $\mathcal{C}$ be an $\mathbb{F}_2$-linear $[k{+}2, k]$ MDS code over $\mathbb{F}_2^b$ and suppose that $\mathcal{C}$ has a systematic parity-check matrix that attains the bound of Proposition 5.2(a). Then*

$$k \;\leq\; b + 1 \;.$$

Proof. Let $(\, A \;\; I_{2b} \,)$ be a parity-check matrix that attains the bound of Proposition 5.2(a), and write $A = (A_{i,j})_{i,j=1}^{2\;k}$, where each $A_{i,j}$ is a $b \times b$ block submatrix of A. In order to attain the required average, the matrix A must consist of exactly $k{+}1$ block submatrices $A_{i,j}$ that are permutation matrices. Hence, there must be an index j (say, $j = 1$), such that both $A_{1,j}$ and $A_{2,j}$ are permutation matrices. Furthermore, for every $j = 2, 3, \ldots, k$, exactly one out of the two block submatrices, $A_{1,j}$ and $A_{2,j}$, is a permutation matrix. Each of the remaining $k{-}1$ block submatrices must have exactly $b{+}1$ entries equaling 1, and, as such, each of those block submatrices can be regarded as a permutation matrix with an extra entry equaling 1.

Next we claim that we can assume that for every $j = 2, 3, \ldots, k$, the block submatrix $A_{1,j}$ is a (proper) permutation matrix whereas $A_{2,j}$ has $b{+}1$ entries equaling 1. Otherwise, if $A_{2,j}$ were a permutation matrix and $A_{1,j}$ had $b{+}1$ entries equaling 1, we could right-multiply both matrices by $A_{1,j}^{-1}$. Now, it is easy to see that $A_{1,j}^{-1}$ also has exactly $b{+}1$ entries equaling 1. Therefore, multiplying by $A_{1,j}^{-1}$ would still maintain a $2b \times kb$ matrix A that would satisfy the conditions of the proposition.

Hence, we assume that each of the $k{-}1$ block submatrices $A_{2,2}$, $A_{2,3}$, …, $A_{2,k}$ is a permutation matrix with an extra entry equaling 1. So, the set $\{A_{2,j}\}_{j=1}^{k}$ satisfies properties

(P1)–(P3'), and the theorem follows from Proposition 2.2 (the cases $b = 1, 2$ can be individually checked to hold). □

The following lemma is used to improve on the lower bound of Proposition 5.2 for $r = 3$ (and, therefore, for any $k \geq r \geq 3$).

Lemma 5.4 *Let $k \geq 3$ and $A = (A_{i,j})_{i,j=1}^{3\ k}$ be as in Lemma 5.1. Then the average number of 1's in a block submatrix $A_{i,j}$ of A is at least $b + \frac{2}{3} - \frac{1}{k}$.*

Proof. For $j = 1, 2, \ldots, k$, denote by ℓ_j the number of permutation matrices among the block submatrices $A_{1,j}$, $A_{2,j}$, and $A_{3,j}$. Without loss of generality we can assume that ℓ_j is non-increasing with j.

If $\ell_1 = 3$, then $\ell_j \leq 1$ for every $j \geq 2$, or else we would have four block permutation submatrices $A_{i,j}$ that form a $2b \times 2b$ singular submatrix of A. Therefore, if $\ell_1 = 3$, the number of 1's in A is at least $3kb + 2(k-1)$; so, the average number of 1's in a block submatrix $A_{i,j}$ is at least $b + \frac{2}{3} - \frac{2}{3k}$.

Now assume that $\ell_1 \leq 2$. Recalling that ℓ_j is non-increasing, we show that $\ell_j \leq 1$ for every $j \geq 4$. Otherwise, we would have $\ell_1 = \ell_2 = \ell_3 = \ell_4 = 2$, in which case we could find a $2b \times 2b$ singular submatrix of A consisting of four block permutation submatrices $A_{i,j}$ in $(A_{i,j})_{i,j=1}^{3\ 4}$. Therefore, we must have $\ell_j \leq 1$ for every $j \geq 4$; so, when $\ell_1 \leq 2$, the number of 1's in A is at least $3kb + 3 + 2(k-3) = 3kb + 2k - 3$, in which case the average number of 1's in a block submatrix $A_{i,j}$ is at least $b + \frac{2}{3} - \frac{1}{k}$. □

Proposition 5.5 *Let $\mathcal{C}$ be an $\mathbb{F}_2$-linear $[n, k{=}n{-}r]$ MDS code over $\mathbb{F}_2^b$ and assume that $k \geq r \geq 3$.*

(a) The average number of 1's per row in every systematic parity-check matrix of $\mathcal{C}$ is at least $k + 1 + \frac{2k-3}{3b}$.

(b) The average number of 1's per row in every systematic generator matrix of $\mathcal{C}$ is at least $r + 1 + \frac{r}{b}(\frac{2}{3} - \frac{1}{k})$.

Proof. The lower bound of Lemma 5.4 holds for every block submatrix $A_{i,j}$ of $A = (A_{i,j})_{i,j=1}^{r\ k}$ whenever $k \geq r \geq 3$. The result now follows from Proposition 3.2. □

It follows from Proposition 5.5(a) that when $k \geq r \geq 3$, the lower bounds of Proposition 5.2 can be attained only when $\frac{2k-3}{3b} \leq \frac{k-1}{2b}$. This occurs when $k \leq 3$, and an attaining construction for $k = 3$ is given by Example 4.1.

6 Relaxing the systematic condition

In this section, we consider MDS constructions over $\mathbb{F}_2^b$ in which the systematic condition of Definition 1.1 on the parity-check or generator matrices is relaxed. Specifically, we allow the check bits to be distributed among the various coordinates, over $\mathbb{F}_2^b$, in a codeword. This model has been studied in [13], and we describe in Section 6.1 a construction of $\mathbb{F}_2$-linear $[k+2, k]$ MDS codes over $\mathbb{F}_2^b$ which is equivalent to the one obtained in [13]. Our presentation here uses somewhat different terms compared with [13], as our alternate description suggests a way to generalize the construction to redundancy values greater than 2. The generalization of the construction is discussed in Section 6.2.

We will consider here binary codes only (namely, codes over $\mathbb{F}_2^b$).

6.1 Weakly-systematic construction

Let p be a fixed odd prime and let $b = (p-1)/2$. For $0 \le i < p$ define the $2b \times (b+1)$ matrix $Y_i = (y_{\ell,m})$ by

$$y_{\ell,m} \;=\; \begin{cases} 1 & \text{if } \ell \in \{\langle i+m\rangle, \langle i-m\rangle\} \\ 0 & \text{otherwise} \end{cases} \quad , \quad 1 \le \ell \le 2b \;, \;\; 0 \le m \le b$$

(refer to Section 2.2 for the definition of $\langle\cdot\rangle$; notice that the columns of Y_i are indexed starting with $m = 0$). Let $\hat{Y}_i$ be the $2b \times b$ matrix obtained from Y_i by deleting the column indexed by $\min\{i, p-i\}$. It is easy to see that for $0 < i < p$, the column indexed by $m = 0$ in $\hat{Y}_i$ is a unit vector whose nonzero value is located at the ith entry of that column. Each of the remaining $b-1$ columns in $\hat{Y}_i$ (and each of the b columns in $\hat{Y}_0$) contains two 1's.

The code of [13], which we denote by $\mathcal{Z}_p$, is an $\mathbb{F}_2$-linear $[2b+1, k=2b-1]$ code over $\mathbb{F}_2^b$ defined by the parity-check matrix

$$H \;=\; (\,\hat{Y}_0\;\hat{Y}_1\;\ldots\;\hat{Y}_{p-1}\,)\;. \tag{17}$$

It is shown in [13] that $\mathcal{Z}_p$ is MDS. Now, the number of 1's in the matrix (17) is $4b^2$, thus making the average number of 1's per row equal to $2b = k+1$. Obviously, this average is smaller than the lower bound of Proposition 5.2(a). Furthermore, the dimension, $k = 2b-1$, of $\mathcal{Z}_p$ is greater than the upper bound of Theorem 5.3.

This paradox is resolved by observing that the matrix (17) does not satisfy Definition 1.1 of a systematic matrix. Nevertheless, (17) can be regarded as a *weakly-systematic* matrix in the sense that it contains I_{2b} as a submatrix—yet this submatrix is not aligned with symbols of $\mathbb{F}_2^b$. Since the columns of I_{2b} correspond to check bits of a codeword, it follows that the check bits of any codeword of $\mathcal{Z}_p$ are distributed among most of the $\mathbb{F}_2^b$-symbols of that codeword.

If we compute from (17) the respective weakly-systematic generator matrix, the resulting average number of 1's in every row is *exactly* three—again, smaller than the lower bound of Proposition 5.2(b).

Comparing $\mathcal{Z}_p$ with the systematic construction of Section 4 for similar block sizes b, the code $\mathcal{Z}_p$ can be longer and has a weakly-systematic parity-check (respectively, generator) matrix with an average number of 1's per row smaller by an additive term $(k-1)/(2b)$ (respectively, $(1-(1/k))/b$). However, if we shorten $\mathcal{Z}_p$ by deleting some of the $\hat{Y}_i$'s from (17), the resulting codes will typically not be MDS. So, having less flexibility in choosing the code parameters of $\mathcal{Z}_p$ is a drawback in potential applications. The codes of Section 4, being (fully) systematic, can be naturally shortened.

6.2 Generalization to redundancy values greater than 2

We can generalize the construction (17) to redundancy values greater than 2 in the following way. Let p be an odd prime, and suppose that r divides $p-1$. Let ω be an element of order r in $GF(p)$, α a primitive element in $GF(p)$ and $b = (p-1)/r$. Re-define each Y_i to be the $rb \times (b+1)$ matrix $(y_{\ell,m})$ given by

$$y_{\ell,m} \;=\; \begin{cases} 1 & \text{if } \ell \in \{\langle i + \omega^j m\rangle\}_{j=0}^{r-1} \\ 0 & \text{otherwise} \end{cases} \quad , \quad 1 \le \ell \le rb \;, \;\; m \in \{0, 1, \alpha^2, \ldots, \alpha^{b-1}\} \;.$$

Similarly, the matrix $\hat{Y}_i$ is re-defined as the $rb \times b$ matrix obtained from Y_i by deleting the column indexed by $\min_{0\le j<r}\langle -\omega^j i\rangle$. For $0 < i < p$, the column indexed by $m = 0$ in $\hat{Y}_i$ is a unit vector, and the number of 1's in each of the remaining $b-1$ columns in $\hat{Y}_i$ (and in each of the b columns in $\hat{Y}_0$) is r.

We now insert this amended definition of $\hat{Y}_i$ into (17) to obtain a parity-check matrix H of an $\mathbb{F}_2$-linear $[rb+1, k=rb-r+1]$ code over $\mathbb{F}_2^b$ which we denote by $\mathcal{Z}_p(r)$ (note that $\mathcal{Z}_p(2) = \mathcal{Z}_p$). The matrix H is weakly-systematic and the number of 1's in each row of H is $rb-r+2 = k+1$. In fact, if $\mathcal{Z}_p(r)$ is MDS, then—as we showed in Proposition 3.4—such a matrix H is optimal with respect to the number of 1's.

The problem however is that, unlike the case $r = 2$, the code $\mathcal{Z}_p(r)$ is not necessarily MDS. An exhaustive search has shown that when $r = 3$, the code $\mathcal{Z}_p(3)$ is MDS for 18 values of p out of the 21 primes less than 200 that have the form $3b+1$ (in this case b must be even); the three exceptions are 7, 73, and 151 (the exception 7 follows from the known fact that there are no MDS codes of length 7 and redundancy 3 over an alphabet of four elements [1, Section 2.4]). When $r = 4$, the code $\mathcal{Z}_p(4)$ is MDS for the following nine values of p out of the 18 primes up to 153 that have the form $4b+1$: 5, 29, 37, 53, 61, 97, 101, 137, and 149.

We point out that in those cases where $\mathcal{Z}_p(r)$ is MDS, it attains an upper bound on the length of MDS codes with the sparsest possible weakly-systematic parity-check matrices. We

show this in Theorem 6.2 below.

6.3 Bounds for the weakly-systematic case

This section is in essence a counterpart of Sections 3 and 5 for the case where we replace the condition of Definition 1.1 on the parity-check or generator matrices with the weakly-systematic condition.

Proposition 6.1 *Let $\mathcal{C}$ be an $\mathbb{F}_q$-linear MDS code over $\mathbb{F}_q^b$. The bound in Proposition 3.4(a) is attained by some weakly-systematic parity-check matrix H if and only the bound in Proposition 3.4(b) is attained by some weakly-systematic generator matrix G.*

Proof. The proof is the same as that of Proposition 3.5. □

The following is a counterpart of Theorems 3.6 and 5.3 for the weakly-systematic case (and general redundancy values).

Theorem 6.2 *Let $\mathcal{C}$ be an $\mathbb{F}_2$-linear $[n, k{=}n{-}r]$ MDS code over $\mathbb{F}_2^b$ and suppose that $\mathcal{C}$ has a weakly-systematic parity-check matrix that attains the bound of Proposition 3.4(a).*

(i) If $k \leq 1$ or $r \leq 1$, then $n = k{+}r$ can take any positive integer value.

(ii) Otherwise,

$$\frac{r-1}{b-1} \;\leq\; k \;\leq\; r(b-1) \;+\; 1\,.$$

Proof. Part (i) follows from Theorem 3.6(i). As for part (ii), let $H = (\, H_1\, H_2\, \ldots\, H_n\,)$ be an $rb \times nb$ weakly-systematic parity-check matrix of $\mathcal{C}$ that attains the bound of Proposition 3.4(a), where each H_i is an $rb \times b$ submatrix of H. Each row in H, when divided into n non overlapping blocks of length b over $\mathbb{F}_2$ (each block being an element of the symbol alphabet $\mathbb{F}_2^b$), is a codeword of $\mathcal{C}^\perp$ of Hamming weight $k{+}1$, where the weight is measured over $\mathbb{F}_2^b$. It follows that each nonzero coordinate (over $\mathbb{F}_2^b$) of such a codeword must be a block (over $\mathbb{F}_2$) containing exactly one 1. Hence, the nonzero rows in each submatrix H_i must be unit vectors of $\mathbb{F}_2^b$. Recall also that by permuting the columns of H we can obtain an $rb \times nb$ matrix of the form $(\, I_{rb}\; A\,)$, where the number of 1's in each column of A is exactly r (see the proof of Proposition 3.5).

Now, suppose that $k \geq r(b{-}1) + 2$, i.e., $n \geq rb + 2$. There must be at least two $rb \times b$ submatrices H_{i_1} and H_{i_2} of H that do not contain any of the columns of the identity matrix I_{rb} which is assumed to be embedded in H; namely, the columns of $\tilde{H} = (\, H_{i_1}\; H_{i_2}\,)$ are all columns of A. It follows that the number of 1's in each of the submatrices H_{i_1} and H_{i_2} is

exactly rb. On the other hand, we have shown that the nonzero rows of H_{i_1} and H_{i_2} must be unit vectors of $\mathbb{F}_2^b$. Hence, none of these two submatrices contains any zero rows, and, so, each row of $\tilde{H}$ contains exactly two 1's. This, in turn, implies that the columns of $\tilde{H}$ sum to zero; therefore, the columns of $\tilde{H}$ are linearly dependent over $\mathbb{F}_2$. By Proposition 3.1 we conclude that the code $\mathcal{C}$ is MDS only when $r \leq 1$, thus bringing us back to part (i). Hence, when $r \geq 2$ we must have

$$n \ \leq \ rb + 1 \ ,$$

implying the upper bound on k claimed in (ii).

To prove the lower bound in (ii), we apply the upper bound we have just proved to the dual code $\mathcal{C}^\perp$ to yield

$$r \ \leq \ k(b-1) + 1 \ .$$

So, if $b = 1$ then $r \leq 1$, and if $b > 1$ then we can divide by $b-1$ to obtain the lower bound in (ii). □

The bounds of Theorem 6.2(ii) are not tight. For example, it is known that for $r \geq 2$, there exist $[n, k{=}n{-}r]$ MDS codes over $\mathbb{F}_2^b$ only when $k \leq 2^b - 1$ [1, Section 2.4]. Hence, the upper bound in Theorem 6.2(ii) is not tight when $r(b-1) \geq 2^b - 1$.

In those cases where the construction $\mathcal{Z}_p(r)$ is MDS, it attains the bounds of Proposition 3.4 and Theorem 6.2.

7 Appendix

We consider here the set $\{Q_\alpha^{(i)}\}_{i=0}^{p-1}$ of Definition 2.1 for the special case $q = 2$ and $\alpha = 1$. Specifically, We present explicit formulas for solving $(Q_1^{(j)} + Q_1^{(i)})\underline{x} = \underline{z}$ for $\underline{x}$ over $\mathbb{F}_2$.

Lemma 7.1 *Let $0 \leq i, j < p$, $i \neq j$, and define $\Delta = \langle j{-}i \rangle$, $L = \langle i/\Delta \rangle$, and $M = \langle -j/\Delta \rangle = p{-}1{-}L$. For any vector $\underline{z} = (z_\ell)_{\ell=1}^{p-1}$ over $\mathbb{F}_2$, the solution of $(Q_1^{(j)} + Q_1^{(i)})\underline{x} = \underline{z}$ for the vector $\underline{x} = (x_\ell)_{\ell=1}^{p-1}$ over $\mathbb{F}_2$ is given by*

$$x_{\langle \ell\Delta \rangle} \ = \ \begin{cases} x_\Delta \ + \ \displaystyle\sum_{t=L-\ell+1}^{L-1} z_{\langle -t\Delta \rangle} & \text{if } \ 0 < \ell \leq L \qquad \text{(a)} \\ \\ x_{p-\Delta} \ + \ \displaystyle\sum_{t=M+\ell+1}^{M-1} z_{\langle t\Delta \rangle} & \text{if } \ -M \leq \ell < 0 \qquad \text{(b)} \end{cases} \tag{18}$$

where x_Δ is given (for $i \neq 0$) by

$$x_\Delta \;=\; z_{p-i} \;+\; \begin{cases} \displaystyle\sum_{t=1}^{L/2} z_{\langle -t\Delta\rangle} & \textit{if } L \textit{ is even} \\ \displaystyle\sum_{t=(L+1)/2}^{p-1} z_{\langle -t\Delta\rangle} & \textit{if } L \textit{ is odd} \end{cases} \tag{19}$$

and $x_{p-\Delta}$ is given (for $j \neq 0$) by

$$x_{p-\Delta} \;=\; z_{p-j} \;+\; \begin{cases} \displaystyle\sum_{t=1}^{M/2} z_{\langle t\Delta\rangle} & \textit{if } M \textit{ is even} \\ \displaystyle\sum_{t=(M+1)/2}^{p-1} z_{\langle t\Delta\rangle} & \textit{if } M \textit{ is odd} \end{cases} . \tag{20}$$

Proof. The expressions in (18) are obtained from (2) by substituting $\beta = 1$. Next we turn to proving (18) and (20). Equations (4)–(6) become

$$x_i \;+\; x_{\langle i/2\rangle} \;+\; x_\Delta \;=\; z_{p-i} \;, \tag{21}$$

$$x_i \;+\; x_\Delta \;=\; \sum_{t=1}^{L-1} z_{\langle -t\Delta\rangle} \;, \tag{22}$$

and

$$x_{\langle i/2\rangle} \;+\; x_\Delta \;=\; \sum_{t=L/2+1}^{L-1} z_{\langle -t\Delta\rangle} \;, \tag{23}$$

respectively. Adding (21), (22), and (23) we obtain (19) for even L. By switching the roles of i and j we obtain (20) for even M.

Consider now the case where L and M are odd. For $q = 2$, (7) becomes

$$x_{\langle i/2\rangle} \;=\; x_{p-\Delta} \;+\; \sum_{t=(M+1)/2}^{M-1} z_{\langle t\Delta\rangle} \;.$$

Adding this with (21) and (22) we obtain

$$\begin{aligned} x_{p-\Delta} \;&=\; \sum_{t=1}^{L} z_{\langle -t\Delta\rangle} \;+\; \sum_{t=(M+1)/2}^{M-1} z_{\langle t\Delta\rangle} \;=\; \sum_{t=M+1}^{p-1} z_{\langle t\Delta\rangle} \;+\; \sum_{t=(M+1)/2}^{M-1} z_{\langle t\Delta\rangle} \\ &=\; z_{\langle M\Delta\rangle} \;+\; \sum_{t=(M+1)/2}^{p-1} z_{\langle t\Delta\rangle} \;=\; z_{p-j} \;+\; \sum_{t=(M+1)/2}^{p-1} z_{\langle t\Delta\rangle} \;. \end{aligned}$$

This proves (20) for odd M, and, thus, also (19) for odd L. □

Example 7.1 Consider the special case $i = 0$, i.e., $Q_1^{(i)} = I$. Here $\Delta = j$, $L = 0$, and $M = p-1$; so, (18)(b) becomes

$$x_{\langle \ell j \rangle} \;=\; x_{p-j} \;+\; \sum_{t=p+\ell}^{p-2} z_{\langle tj \rangle} \;, \quad -(p-1) \le \ell < 0 \;,$$

where, by (20),

$$x_{p-j} \;=\; z_{p-j} \;+\; \sum_{t=1}^{(p-1)/2} z_{\langle tj \rangle} \;=\; z_{\langle (p-1)j \rangle} \;+\; \sum_{t=1}^{(p-1)/2} z_{\langle tj \rangle} \;.$$

Writing $\ell' = p+\ell$, we thus have

$$x_{\langle \ell' j \rangle} \;=\; x_{\langle \ell j \rangle} \;=\; z_{\langle (p-1)j \rangle} \;+\; \sum_{t=1}^{(p-1)/2} z_{\langle tj \rangle} \;+\; \sum_{t=\ell'}^{p-2} z_{\langle tj \rangle} \;=\; \sum_{t=1}^{(p-1)/2} z_{\langle tj \rangle} \;+\; \sum_{t=\ell'}^{p-1} z_{\langle tj \rangle} \;, \quad 1 \le \ell' < p \;.$$

This can also be written as

$$x_{\langle \ell' j \rangle} \;=\; \sum_{t=(p+1)/2}^{p-1} z_{\langle tj \rangle} \;+\; \sum_{t=1}^{\ell'-1} z_{\langle tj \rangle} \;, \quad 1 \le \ell' < p \;.$$

□

Acknowledgment

We are grateful to Professor Simon Litsyn for pointing out Reference [13].

References

[1] I.F. Blake, R.C. Mullin, *An Introduction to Algebraic and Combinatorial Coding Theory,* Academic Press, New York, 1976.

[2] M. Blaum, J. Brady, J. Bruck, J. Menon, *EVENODD: an efficient scheme for tolerating double disk failures in RAID architectures, IEEE Trans. Comput.*, C-445 (1995), 192–202.

[3] M. Blaum, J. Bruck, A. Vardy, *MDS array codes with independent parity symbols, IEEE Trans. Inform. Theory*, 42 (1996), 529–542.

[4] M. Blaum, R.M. Roth, *New array codes for multiple phased burst correction, IEEE Trans. Inform. Theory,* 39 (1993), 66–77.

[5] G.D. Forney, Jr., *On the Hamming distance properties of group codes, IEEE Trans. Inform. Theory*, 38 (1992), 1797–1801.

[6] G.A. Gibson, *Redundant Disk Arrays,* MIT Press, 1992.

[7] D.R. Hayes, *The distribution of irreducibles in $GF[q, x]$, Trans. Am. Math. Soc.,* 117 (1965), 101–127.

[8] K. Ireland, M. Rosen, *A Classical Introduction to Modern Number Theory,* Springer, New York, 1972.

[9] R. Lidl, *An enumeration formula for certain irreducible polynomials with an application to the construction of irreducible polynomials over the binary field, AAECC,* 1 (1990), 119–124.

[10] R. Lidl, H. Niederreiter, *Finite Fields,* Cambridge University Press, Cambridge, 1997.

[11] F.J. MacWilliams, N.J.A. Sloane, *The Theory of Error-Correcting Codes,* North-Holland, Amsterdam, 1977.

[12] A.A. Zain, B. Sundar Rajan, *Algebraic characterization of MDS group codes over cyclic groups, IEEE Trans. Inform. Theory*, 41 (1995), 2052–2056.

[13] G.V. Zaitsev, V.A. Zinov'ev, N.V. Semakov, *Minimum-check-density codes for correcting bytes of errors, erasures, or defects, Probl. Inform. Transm.*, 19 (1983), 197–204.