Lowest-Density MDS Codes over Extension Alphabets

Erez Louidor and Ron M. Roth

***Abstract*— Let F be a finite field and b be a positive integer. A construction is presented of codes over the alphabet F^b with the following three properties: (i) the codes are MDS over F^b, (ii) they are linear over F, and (iii) they have systematic generator and parity-check matrices over F with the smallest possible number of nonzero entries. Furthermore, for the case $F = \mathbf{GF}(2)$, the construction is the longest possible among all codes that satisfy properties (i)–(iii).**

Keywords: Low-density parity-check (LDPC) codes, MDS codes.

I. Introduction

Let F denote a finite field and let b be a positive integer. In this paper, we consider codes over the extension alphabet F^b. Given such a code $\mathcal{C}$ of length n, the codewords of $\mathcal{C}$ can be transformed in a one-to-one manner into words of F^{nb} simply by concatenating the b-blocks over F that are formed by the entries (in F^b) within each codeword. The set of words thus obtained will be denoted by $(\mathcal{C})_F$.

We say that $\mathcal{C}$ is an *F-linear code* over F^b if $(\mathcal{C})_F$ is a linear code (in the traditional sense) of length nb over F. It is clear from this definition that an F-linear code is a vector space over F.

Let $\mathcal{C}$ be an F-linear code of length n over F^b and let d denote its minimum Hamming distance (measured with respect to the alphabet F^b). Note that, as in conventional linear codes, d is the minimum Hamming weight of any nonzero codeword of $\mathcal{C}$. Letting $\dim\mathcal{C}$ denote the dimension of $\mathcal{C}$ (or $(\mathcal{C})_F$) as a vector space over F, we denote by k the (rational) quantity $(\dim\mathcal{C})/b$ and refer to $\mathcal{C}$ as an F-linear $[n,k,d]$ code over F^b (we may sometimes omit the parameter d and refer to $\mathcal{C}$ simply as an F-linear $[n,k]$ code over F^b). We call k the *normalized dimension* of $\mathcal{C}$, and the *redundancy* of $\mathcal{C}$ is defined accordingly by $r{=}n{-}k$.

A matrix is said to be a parity-check (respectively, generator) matrix of $\mathcal{C}$ if it is a parity-check (respectively, generator) matrix of $(\mathcal{C})_F$. Such a matrix is called *(weakly) systematic* if it contains the $rb\times rb$ (respectively, $kb\times kb$) identity matrix as a sub-matrix. (To be consistent with the terms in [5], the qualifier 'weakly' indicates that the identity matrix does not have to be aligned with b-blocks that are formed by the symbols of F^b; yet, we will hereafter omit this qualifier, since this work does not deal with any stronger systematic properties.)

From the Singleton bound for linear and nonlinear codes [8], the parameters of every F-linear $[n,k{=}n{-}r,d]$ code over F^b must satisfy

$$d \le n - k + 1.$$

An F-linear $[n,k{=}n{-}r,d]$ code over F^b is called maximum-distance separable (in short, MDS), if it attains the Singleton bound with equality. In particular, k is an integer in this case.

F-linear MDS codes over F^b were studied in several papers, including [3], [4], [5], [13], and [14]. These codes have various applications in storage systems, where the alphabet size is typically large. In such applications, it is also desirable that the number of redundancy symbols that need to be modified for each update of an information symbol (the so-called update complexity) be as small as possible. Given an F-linear $[n,k,d]$ code $\mathcal{C}$ over F^b, consider a codeword $w \in \mathcal{C}$ and let $(w)_F$ denote the codeword of $(\mathcal{C})_F$ constructed by concatenating the b-blocks of w. The symbols of $(w)_F$ can be partitioned into kb information symbols and rb redundancy symbols. Letting $u \in F^{kb}$ denote the sub-vector of $(w)_F$ whose entries are the information symbols, we can compute $(w)_F$ by multiplying u by a suitable systematic generator matrix G of $\mathcal{C}$. Thus, for $i = 1, 2, \ldots, kb$, updating the ith information symbol of $(w)_F$ requires modification of additional $\mathrm{wt}(G_i){-}1$ redundancy symbols, where $\mathrm{wt}(G_i)$ denotes the number of nonzero entries in the ith row of G. Hence, minimizing the update complexity translates into minimizing the number of nonzero entries in some systematic generator matrix of the code (see [5] for a discussion of this in disk arrays). There is also an advantage in having low-density parity-check matrices, as the latter allow fast syndrome computation.

It was shown in [5] that each row in a parity-check (respectively, generator) matrix of an F-linear $[n,k{=}n{-}r,r{+}1]$ MDS code $\mathcal{C}$ over F^b must contain at least $k{+}1$ (respectively, $r{+}1$) nonzero entries. We say that a parity-check (respectively, generator) matrix of $\mathcal{C}$ has *lowest density* if it meets this lower bound for every row. We call $\mathcal{C}$ a *lowest-density MDS code* if it has a *systematic* lowest-density parity-check matrix; this is equivalent to requiring that $\mathcal{C}$ have a systematic lowest-density generator matrix [5, Proposition 6.1].

It was also shown in [5] that when F is the binary field $\mathrm{GF}(2)$ and $r > 1$, any lowest-density $[n, n{-}r, r{+}1]$ MDS code $\mathcal{C}$ over F^b must satisfy

$$n \le rb + 1\ .$$

Erez Louidor is with the Department of Mathematics, University of British Columbia, Vancouver, BC V6T 1Z2, Canada. This work was done while he was with the Computer Science Department, Technion, Haifa, Israel. email: erez@math.ubc.ca.

Ron M. Roth is with the Computer Science Department, Technion, Haifa 32000, Israel. email: ronny@cs.technion.ac.il

This work was supported by Grant No. 746/04 from the Israel Science Foundation. Part of this work was presented at the *2003 IEEE International Symposium on Information Theory (ISIT'2003)*, Yokohama, Japan (June 2003).

When this bound is met, we will say that $\mathcal{C}$ is a *maximum-length* lowest-density MDS code.

This work studies a certain class of F-linear codes over F^b whose length is a prime p such that b divides $p-1$ and their redundancy equals $r = (p-1)/b$. These codes are not always MDS; yet, when they are, then they are also lowest-density MDS. In addition, if $F = \mathrm{GF}(2)$ and $r > 1$, then the codes are maximum-length lowest-density MDS.

These codes, which we denote by $\mathcal{Z}_F(p,r)$ and define in Section II, were initially proposed by Zaitsev, Zinov'ev, and Semakov in [14] for the special case $r = 2$; for this value of r, these codes are always MDS (and for $F = \mathrm{GF}(2)$ they are maximum-length lowest-density MDS). A generalization of these codes to larger r was suggested in [5], yet the resulting codes are no longer necessarily MDS.

In this work, we identify a range of parameters for which the codes $\mathcal{Z}_F(p,r)$ are MDS. We first define the codes $\mathcal{Z}_F(p,r)$ in Section II and then summarize our main results in Section III. In Section IV, we associate with the code $\mathcal{Z}_F(p,r)$ certain cyclic codes over an extension field of F and show that the latter codes are MDS if and only if $\mathcal{Z}_F(p,r)$ is. Based on this relationship between $\mathcal{Z}_F(p,r)$ and its extension-field counterparts, we then show in Section V that the code $\mathcal{Z}_F(p,r)$ is MDS for $r = 3, 4$, whenever F has characteristic 2 and 2 is primitive modulo p. In Section VI, we present a sufficient condition that a given cyclic code of prime length is MDS. This condition is then applied in Section VII to show that the codes $\mathcal{Z}_F(p,r)$ are MDS when the field F is sufficiently large and $|F|$ is primitive modulo p.

Hereafter, the notation $\mathbb{F}_q$ stands for the finite field $\mathrm{GF}(q)$ and $\mathbb{F}_q^*$ for the nonzero elements of $\mathbb{F}_q$.

II. The construction

Let F be a finite field and p be a prime. Fix r to be a divisor of $p-1$ and write $b = (p-1)/r$. Define the relation $\overset{r}{\sim}$ on $\mathbb{F}_p$ as follows: for any two elements $\beta, \gamma \in \mathbb{F}_p$,

$$\beta \overset{r}{\sim} \gamma \iff \beta^r = \gamma^r \ .$$

Clearly, $\overset{r}{\sim}$ is an equivalence relation, and it partitions $\mathbb{F}_p$ into $b+1$ equivalence classes: an equivalence class C_0, which consists of the zero element only, and b equivalence classes, denoted $C_1, C_2, \ldots, C_b$, of size r. Each of the latter b classes can be expressed as $\{a\omega^t\}_{t=0}^{r-1}$, where ω is an element of multiplicative order r in $\mathbb{F}_p$ and a is an element in $\mathbb{F}_p^*$ (in other words, these classes are the cosets of the cyclic subgroup $\{\omega^t\}_{t=0}^{r-1}$ in $\mathbb{F}_p^*$).

Throughout this paper, we will find it occasionally convenient to index entries of vectors, or rows or columns of matrices, by the elements of $\mathbb{F}_p$. To express such vectors or matrices concretely, one then needs to assume some ordering on $\mathbb{F}_p$. To this end, we will assume the standard lexicographic ordering $0 < 1 < \ldots < p-1$. With each element $i \in \mathbb{F}_p$ we will associate a nonnegative rational integer $\langle i \rangle$, which is the ordinal number of i; thus, $\langle 0 \rangle = 0$, $\langle 1 \rangle = 1$, and so on.

Denote by $P_F(p,r)$ the binary $p \times (b+1)$ matrix over F whose rows are indexed by $\mathbb{F}_p$, whose columns are indexed by $j \in \{0, 1, \ldots, b\}$, and whose entries are given by

$$\left(P_F(p,r)\right)_{\ell,j} = \begin{cases} 1 & \text{if } \ell \in C_j \\ 0 & \text{otherwise} \end{cases} \ , \quad \ell \in \mathbb{F}_p \ , \quad 0 \le j \le b \ . \tag{1}$$

Note that $P_F(p,r)$ contains exactly one '1' in each row, one '1' in the first column, and r '1's in each of the other columns. Let D_p be the $p \times p$ permutation matrix over F whose rows and columns are indexed by $\mathbb{F}_p$ and

$$(D_p)_{\ell,\ell'} = \begin{cases} 1 & \text{if } \ell - 1 = \ell' \\ 0 & \text{otherwise} \end{cases} \ , \quad \ell, \ell' \in \mathbb{F}_p \ . \tag{2}$$

Thus, if we use the standard lexicographic ordering on the elements of $\mathbb{F}_p$, a left-multiplication by the matrix D_p realizes a downward-cyclic shift operator.

Define the $p \times (p(b+1))$ matrix $H_F^+(p,r)$ over F by

$$H_F^+(p,r) = \left(P_F(p,r) \middle| D_p P_F(p,r) \middle| D_p^2 P_F(p,r) \middle| \ldots \middle| D_p^{p-1} P_F(p,r) \right) \ .$$

We will index the columns of $H_F^+(p,r)$ by pairs (i,j), where $i \in \mathbb{F}_p$ and $j \in \{0, 1, \ldots, b\}$. The rows of $H_F^+(p,r)$ will be indexed by $\ell \in \mathbb{F}_p$. Using this convention, the entries of $H_F^+(p,r)$ are given by

$$\left(H_F^+(p,r)\right)_{\ell,(i,j)} = \begin{cases} 1 & \text{if } \ell - i \in C_j \\ 0 & \text{otherwise} \end{cases} \ . \tag{3}$$

Next we construct the $(p-1) \times (pb)$ matrix $H_F(p,r)$ over F by deleting from $H_F^+(p,r)$ the first row and every column that contains a '1' in the (deleted) first row; that is, we delete all the columns that are indexed by

$$\left\{ (i,j) \in \mathbb{F}_p \times \{0, 1, \ldots, b\} \ : \ -i \in C_j \right\} .$$

The code $\mathcal{Z}_F(p,r)$ is now defined as the F-linear code of length p over F^b whose parity-check matrix is given by $H_F(p,r)$.

Example 2.1: Consider the case $p = 7$ and $r = 3$. Here,

$$C_0 = \{0\} \ , \quad C_1 = \{1, 2, 4\} \ , \quad \text{and} \quad C_2 = \{3, 5, 6\} \ .$$

Hence, for every field F, the matrix $H_F^+(7,3)$ is given by

$$H_F^+(7,3) = \left(\begin{array}{c|c|c|c|c|c|c} 1\,0\,0 & 0\,0\,1 & 0\,0\,1 & 0\,1\,0 & 0\,0\,1 & 0\,1\,0 & 0\,1\,0 \\ 0\,1\,0 & 1\,0\,0 & 0\,0\,1 & 0\,0\,1 & 0\,1\,0 & 0\,0\,1 & 0\,1\,0 \\ 0\,1\,0 & 0\,1\,0 & 1\,0\,0 & 0\,0\,1 & 0\,0\,1 & 0\,1\,0 & 0\,0\,1 \\ 0\,0\,1 & 0\,1\,0 & 0\,1\,0 & 1\,0\,0 & 0\,0\,1 & 0\,0\,1 & 0\,1\,0 \\ 0\,1\,0 & 0\,0\,1 & 0\,1\,0 & 0\,1\,0 & 1\,0\,0 & 0\,0\,1 & 0\,0\,1 \\ 0\,0\,1 & 0\,1\,0 & 0\,0\,1 & 0\,1\,0 & 0\,1\,0 & 1\,0\,0 & 0\,0\,1 \\ 0\,0\,1 & 0\,0\,1 & 0\,1\,0 & 0\,0\,1 & 0\,1\,0 & 0\,1\,0 & 1\,0\,0 \end{array} \right) ,$$

and the parity-check matrix $H_F(7,3)$ of $\mathcal{Z}_F(7,3)$ is given by

$$H_F(7,3) = \left(\begin{array}{c|c|c|c|c|c|c} 1\,0 & 1\,0 & 0\,0 & 0\,1 & 0\,1 & 0\,1 & 0\,0 \\ 1\,0 & 0\,1 & 1\,0 & 0\,1 & 0\,0 & 0\,0 & 0\,1 \\ 0\,1 & 0\,1 & 0\,1 & 1\,0 & 0\,0 & 0\,1 & 0\,0 \\ 1\,0 & 0\,0 & 0\,1 & 0\,0 & 1\,0 & 0\,1 & 0\,1 \\ 0\,1 & 0\,1 & 0\,0 & 0\,0 & 0\,1 & 1\,0 & 0\,1 \\ 0\,1 & 0\,0 & 0\,1 & 0\,1 & 0\,1 & 0\,0 & 1\,0 \end{array} \right)$$

(both matrices are over F). □

It can be readily verified that the matrix $H_F(p,r)$ is systematic and, so, $\text{rank}(H_F(p,r)) = p-1$. It follows that the normalized dimension of the code $\mathcal{Z}_F(p,r)$ equals

$$(pb-(p-1))/b = p-r\ ;$$

namely, $\mathcal{Z}_F(p,r)$ is an F-linear $[p{=}rb{+}1, k{=}p{-}r]$ code over F^b.

Next we turn to analyzing the density of $H_F(p,r)$. First, it is easy to see that each of the p rows of $H_F^+(p,r)$ contains p nonzero entries (all of which equal '1'). Consider the p columns that were deleted from $H_F^+(p,r)$ when constructing $H_F(p,r)$. One of these columns contains only one '1', while each of the other $p-1$ columns contains r '1's. Hence, the number of '1's in $H_F(p,r)$ is

$$p^2 - 1 - (p-1)r = (p-1)(p-r+1)\ . \tag{4}$$

Now, when the code $\mathcal{Z}_F(p,r)$ is MDS, each row in $H_F(p,r)$ must contain at least $k{+}1 = p{-}r{+}1$ nonzero entries; so, from (4) it follows that each row in $H_F(p,r)$ contains exactly $p{-}r{+}1$ nonzero entries. In fact, this property of $H_F(p,r)$ holds also when $\mathcal{Z}_F(p,r)$ is not MDS, as stated next.

Proposition 2.1: Each row of $H_F(p,r)$ contains $p{-}r{+}1$ nonzero entries.

Proposition 2.1 was mentioned in [5] yet no proof was given. We provide a proof in the appendix.

We conclude from Proposition 2.1 that when the code $\mathcal{Z}_F(p,r)$ is MDS then it is lowest-density MDS. And since the length of $Z_F(p,r)$ is $rb+1$, a stronger claim can be made for $F=\mathbb{F}_2$ and $r>1$: when $\mathcal{Z}_{\mathbb{F}_2}(p, r{>}1)$ is MDS then it is maximum-length lowest-density MDS.

The following proposition implies that the study of the MDS properties of $\mathcal{Z}_F(p,r)$ can be reduced to the case where F is a prime field.

Proposition 2.2: Let $F' \subseteq F$ denote a subfield of F. Then $\mathcal{Z}_F(p,r)$ is MDS if and only if $\mathcal{Z}_{F'}(p,r)$ is.

Proof: Write

$$H_F(p,r) = H_{F'}(p,r) = \left(\ Y^{(0)}\ \middle|\ Y^{(1)}\ \middle|\ \ldots\ \middle|\ Y^{(p-1)}\ \right)\ ,$$

where each $Y^{(i)}$ is a $(p-1)\times b$ sub-matrix. It was shown in [5] that $\mathcal{Z}_F(p,r)$ (respectively, $\mathcal{Z}_{F'}(p,r)$) is MDS if and only if for every r distinct elements $i_1, i_2, \ldots, i_r \in \mathbb{F}_p$, the matrix

$$\left(\ Y^{(i_1)}\ \middle|\ Y^{(i_2)}\ \middle|\ \ldots\ \middle|\ Y^{(i_r)}\ \right)$$

is nonsingular over F (respectively, over F'). But clearly, each such matrix is nonsingular over F if and only if it is nonsingular over F'. □

The code $\mathcal{Z}_F(p,2)$ was initially proposed by Zaitsev *et al.* in [14], and was shown to be maximum-length lowest-density MDS.[1] The generalization, $\mathcal{Z}_{\mathbb{F}_2}(p,r)$, of these codes to larger r (for $F=\mathbb{F}_2$) was suggested in [5], but the resulting codes are not necessarily MDS. The authors of [5] provide a list of pairs (p,r) for which they determined by exhaustive search whether the corresponding codes are MDS.

[1]Specifically, the paper [14] analyzes the code over F^{b+1} that is defined by the parity-check matrix $H_F^+(p,2)$ and identifies the uncorrectable single-error patterns to be those with an error value that is a multiple of the all-one vector in F^{b+1}. The transformation from $H_F^+(p,2)$ to $H_F(p,2)$ then excludes such error patterns.

III. Main results

We next state the main results of the paper. The first two theorems deal with the case where F has characteristic 2 and $r=3,4$.

Theorem 3.1: Let F be a finite field of characteristic 2 and let p be a prime of the form $3b+1$, for some positive integer b. If 2 is primitive in $\mathbb{F}_p$, then $\mathcal{Z}_F(p,3)$ is a lowest-density MDS code over F^b.

Theorem 3.2: Let F be a finite field of characteristic 2 and let $p \neq 13$ be a prime of the form $4b+1$, for some positive integer b. If 2 is primitive in $\mathbb{F}_p$, then $\mathcal{Z}_F(p,4)$ is a lowest-density MDS code over F^b.

We remark that it is still an open problem whether there are infinitely many primes p such that 2 is primitive in $\mathbb{F}_p$. Up to 10^6, there are $39,231$ primes of the form $3b+1$, of which $11,718$ have 2 as a primitive element, and $39,175$ primes of the form $4b{+}1$, of which $14,699$ have 2 as a primitive element.

The next theorem treats finite fields with large characteristic.

Theorem 3.3: Let F be a finite field of characteristic q and let p be a prime. Given a divisor r of $p{-}1$, write $b=(p{-}1)/r$ and $k=p{-}r$. Then $\mathcal{Z}_F(p,r)$ is a lowest-density MDS code over F^b when either

- $r \in \{1, 2, p{-}1\}$ or—
- q is a primitive element in $\mathbb{F}_p$ and is greater than

$$\begin{cases} \left(\dfrac{r^{p-1}}{p^{r-1}}\right)^{1/2} & \text{if } r \text{ is odd} \\ \min\left\{\dfrac{r^{p-1}}{p^{r-1}}, \left(\dfrac{k^{p-1}}{p^{k-1}}\right)^{k/(2r)}\right\} & \text{if } r \text{ is even and } b \text{ is odd} \\ \dfrac{r^{p-1}}{p^{r-1}} & \text{if } r \text{ and } b \text{ are both even} \end{cases}\ .$$

Note that by Dirichlet's Theorem [6, p. 251], there are infinitely many primes which are primitive modulo any given prime p. Hence, given p and r, there are infinitely many prime fields F for which the code $\mathcal{Z}_F(p,r)$ is lowest-density MDS over F^b.

IV. Alternate representation

In this section, we show a correspondence between $\mathcal{Z}_F(p,r)$ and certain cyclic codes over extension fields of F. This correspondence, in turn, will be used in subsequent sections to prove our main results.

Let F be the field $\mathbb{F}_q$ and let p, b, and r be as in Section II. Throughout this section we assume that q is a primitive element in $\mathbb{F}_p$. In this case, the polynomial $M_p(x) = 1 + x + x^2 + \ldots + x^{p-1}$ is irreducible over F (see [7, p. 65, Theorem 2.47(ii)]). We denote by K and Φ the extension fields $\mathbb{F}_{q^b}$ and $\mathbb{F}_{q^{p-1}}$, respectively. Since b divides $p{-}1$, the field K is a subfield of Φ.

Since p divides $q^{p-1}-1$, the field Φ contains elements of multiplicative order p. Fix α to be such an element; the minimal polynomial of α with respect to F is then given by $M_p(x)$ (indeed, $M_p(\alpha) = (\alpha^p - 1)/(\alpha - 1) = 0$). We define

the code $\mathbf{Z}_K(p,r)$ over K by

$$\mathbf{Z}_K(p,r) = \left\{ c = (c_i)_{i\in\mathbb{F}_p} \in K^p \,:\, \sum_{i\in\mathbb{F}_p} c_i\alpha^i = 0 \right\} ,$$

where α^i stands for $\alpha^{\langle i\rangle}$ (since the multiplicative order of α is p, any power of α is uniquely determined by the residue class of the exponent modulo p). We will hereafter associate with each vector $c = (c_i)_{i\in\mathbb{F}_p}$ over an extension field of F the polynomial

$$c(x) = \sum_{i\in\mathbb{F}_p} c_i x^{\langle i\rangle} .$$

Using this association, the code $\mathbf{Z}_K(p,r)$ can be expressed as

$$\mathbf{Z}_K(p,r) = \{ c \in K^p \,:\, c(\alpha) = 0 \} .$$

It is easy to see that $\mathbf{Z}_K(p,r)$ is a cyclic $[p,p-r]$ code over K whose roots are given by α and its conjugates with respect to K; i.e., the set of roots of $\mathbf{Z}_K(p,r)$ is

$$\left\{ \alpha, \alpha^{q^b}, \alpha^{q^{2b}}, \ldots, \alpha^{q^{(r-1)b}} \right\} .$$

Letting ω be an element of $\mathbb{F}_p$ with multiplicative order r, this set can also be written as

$$\left\{ \alpha, \alpha^{\omega}, \alpha^{\omega^2}, \ldots, \alpha^{\omega^{r-1}} \right\} . \tag{5}$$

We next turn to analyzing the code $\mathbf{Z}_K(p,r)$, with the ultimate goal of relating it to the code $\mathcal{Z}_F(p,r)$. To this end, we will make use of the following definitions.

Let $C_0, C_1, \ldots, C_b$ be the equivalence classes defined in Section II and for $0 \le j \le b$, define the polynomial $T_j(x) \in F[x]$ by

$$T_j(x) = \sum_{i\in C_j} x^{\langle i\rangle} . \tag{6}$$

Consider the value

$$T_j(\alpha) = \sum_{i\in C_j} \alpha^i .$$

Raising $T_j(\alpha)$ to the q^bth power, we obtain

$$(T_j(\alpha))^{q^b} = \left(\sum_{i\in C_j} \alpha^i \right)^{q^b} = \sum_{i\in C_j} \alpha^{iq^b} . \tag{7}$$

Now, since $q^b \overset{r}{\sim} 1$, the set $\{ i\cdot q^b \,:\, i \in C_j \}$ is equal to C_j and, therefore, the rightmost sum in (7) equals $T_j(\alpha)$. Hence, $T_j(\alpha) \in K$.

Lemma 4.1: Let $\varphi : F^{b+1} \to K$ be the linear transformation over F that is defined by

$$\varphi(a_0\ a_1\ \ldots\ a_b) = \sum_{j=0}^{b} a_j T_j(\alpha) , \quad (a_0\ a_1\ \ldots\ a_b) \in F^{b+1} .$$

The kernel of φ is given by

$$\left\{ (a_0\ a_1\ \ldots\ a_b) \in F^{b+1} \,:\, a_0 = a_1 = a_2 = \ldots = a_b \right\} .$$

Proof: Let $(a_0\ a_1\ \ldots\ a_b)$ be an element in F^{b+1} and define the polynomial $T(x)$ over F by

$$T(x) = \sum_{j=0}^{b} a_j T_j(x) .$$

Then

$$\varphi(a_0\ a_1\ \ldots\ a_b) = \sum_{i=0}^{b} a_j T_j(\alpha) = T(\alpha) .$$

Recalling that $M_p(x)$ is the minimal polynomial of α with respect to F, we get

$$\varphi(a_0\ a_1\ \ldots\ a_b) = 0 \iff T(\alpha) = 0 \iff M_p(x)\,|\,T(x) .$$

But $\deg T(x) < p$; so, $M_p(x)$ divides $T(x)$ if and only if there exists some scalar $a \in F$ such that

$$aM_p(x) = T(x) = \sum_{j=0}^{b} a_j T_j(x) . \tag{8}$$

Now, from the definition (6) we see that for every $i \in \mathbb{F}_p$, the monomial $x^{\langle i\rangle}$ appears in exactly one polynomial $T_j(x)$, which is identified by the unique index j for which $i \in C_j$. Hence, (8) holds if and only if $a_0 = a_1 = \ldots = a_b = a$. □

Given a word $w = (w_i)_{i\in\mathbb{F}_p}$ in $(F^b)^p$, let $w^+ = (w_i^+)_{i\in\mathbb{F}_p}$ be the following word in $(F^{b+1})^p$: for every $i \in \mathbb{F}_p$, the $(b+1)$-block w_i^+ (over F) contains a zero entry at the (unique) index j for which $-i \in C_j$, whereas the remaining entries of w_i^+ form a b-block which equals w_i.

Next we define the mapping $f : (F^b)^p \to K^p$ whose value for every word $w = (w_i)_{i\in\mathbb{F}_p}$ is given by

$$f(w) = \left(\varphi(w_0^+)\ \varphi(w_1^+)\ \ldots\ \varphi(w_{p-1}^+) \right) ,$$

where φ is the mapping in Lemma 4.1.

Lemma 4.2: The mapping $f : (F^b)^p \to K^p$ is linear over F and it is weight-preserving: for every word $w \in (F^b)^p$, the Hamming weight of w (over F^b) is equal to the Hamming weight of $f(w)$ (over K).

Proof: The linearity of f follows from the linearity of φ. To see why f is weight-preserving, notice that for every $i \in \mathbb{F}_p$, the $(b+1)$-block w_i^+ contains a zero entry. Thus, by Lemma 4.1, $\varphi(w_i^+) = 0$ only if $w_i = 0$. □

Since f is weight-preserving, its kernel contains only the all-zero word; hence, f is one-to-one and onto K.

We next state the main result of this section.

Proposition 4.3: Assuming that q is primitive in $\mathbb{F}_p$, the codes $\mathcal{Z}_F(p,r)$ and $\mathbf{Z}_K(p,r)$ are related by

$$\mathbf{Z}_K(p,r) = \{ f(w) \,:\, w \in \mathcal{Z}_F(p,r) \} ,$$

and the minimum Hamming distance of $\mathbf{Z}_K(p,r)$ (over K) is the same as that of $\mathcal{Z}_F(p,r)$ (over F^b).

Our proof of Proposition 4.3 involves operations in the extension field $\Phi = \mathbb{F}_{q^{p-1}}$ and, to this end, we select the following representation of this field: elements are represented as column vectors in F^p, where the column vector $v = (v_\ell)_{\ell\in\mathbb{F}_p}$ represents the element $v(\alpha) = \sum_{\ell\in\mathbb{F}_p} v_\ell \alpha^\ell$ of Φ. Now, every element of Φ can be expressed as a polynomial in α of degree less than $p-1$, and, so, every element of Φ

has at least one representation. In fact, such an element has exactly q distinct representations: recalling that $M_p(\alpha) = 0$, the q vectors

$$(v_\ell + a)_{\ell \in \mathbb{F}_p} , \quad a \in F ,$$

all represent the same element $v(\alpha) = \sum_{\ell \in \mathbb{F}_p} v_\ell \alpha^\ell$, and it can be easily verified that these are all the representations of $v(\alpha)$.

While this representation of Φ is not one-to-one, it does possess two useful properties. First, observe that multiplication and division by α can be carried out by applying cyclic shifts to the representation: for any element $v(\alpha) \in \Phi$ (whose representation is $v \in F^p$) and any integer t, we have

$$(D_p^t v)(\alpha) = \alpha^t v(\alpha) , \tag{9}$$

where D_p is given by (2).

Secondly, there exists a simple characterization of the representations of elements of K within Φ, as we show in the next lemma. A column vector $v = (v_\ell)_{\ell \in \mathbb{F}_p}$ in F^p is called *coset-equal* if for every $\ell, \ell' \in \mathbb{F}_p$,

$$\ell \overset{r}{\sim} \ell' \implies v_\ell = v_{\ell'} .$$

In other words, for every class C_j, the sub-vector of v that is indexed by C_j is a constant vector. Clearly, the set of all coset-equal vectors is a subspace of F^p. Moreover, it follows from the definition of the matrix $P_F(p,r)$ in (1) that the columns of $P_F(p,r)$ form a basis of this subspace.

Lemma 4.4: Let $v = (v_\ell)_{\ell \in \mathbb{F}_p}$ be a column vector in F^p. Then $v(\alpha) \in K$ if and only if v is coset-equal. Furthermore, if v is coset-equal then

$$v(\alpha) = \varphi(u) ,$$

where u is the unique column vector in F^{b+1} such that $v = P_F(p,r)u$.

Proof: We start with the "if" part. Let $v = (v_\ell)_{\ell \in \mathbb{F}_p}$ be a coset-equal vector and write $v = P_F(p,r)u$, where $u = (u_j)_{j=0}^b \in F^{b+1}$. From the definition of the matrix $P_F(p,r)$ in (1) we see that for every $\ell \in \mathbb{F}_p$, the entry v_ℓ equals u_j, where j is the unique index for which $\ell \in C_j$. Therefore,

$$v(\alpha) = \sum_{\ell \in \mathbb{F}_p} v_\ell \alpha^\ell = \sum_{j=0}^{b} u_j \sum_{\ell \in C_j} \alpha^\ell = \sum_{j=0}^{b} u_j T_j(\alpha) = \varphi(u) .$$

In particular, $v(\alpha) \in K$.

The "only if" direction follows from a simple counting argument: on the one hand, there are q^{b+1} $(= q \cdot |K|)$ coset-equal vectors in F^p, and on the other hand, each element of K has q different representations in F^p. □

We are now in a position to prove Proposition 4.3.

Proof of Proposition 4.3: Let $w = (w_i)_{i \in \mathbb{F}_p}$ be a codeword in $\mathcal{Z}_F(p,r)$; as such, w satisfies

$$H_F(p,r)(w_0 \,|\, w_1 \,|\, \ldots \,|\, w_{p-1})^{\mathrm{tr}} = 0 ,$$

where $(\cdot|\cdot)$ denotes concatenation and $(\cdot)^{\mathrm{tr}}$ denotes transposition. Recalling the definition of $w^+ = (w_i^+)_{i \in \mathbb{F}_p}$ and the relationship between $H_F(p,r)$ and $H_F^+(p,r)$, we obtain

$$H_F^+(p,r)(w_0^+ \,|\, w_1^+ \,|\, \ldots \,|\, w_{p-1}^+)^{\mathrm{tr}} = 0 ,$$

i.e.,

$$\sum_{i \in \mathbb{F}_p} D_p^{\langle i \rangle} P_F(p,r)(w_i^+)^{\mathrm{tr}} = 0 .$$

We denote the vector $P_F(p,r)(w_i^+)^{\mathrm{tr}}$ (which is in F^p) by $y_i = (y_{i,\ell})_{\ell \in \mathbb{F}_p}$ and, as before, use the notation $y_i(\alpha)$ for $\sum_{\ell \in \mathbb{F}_p} y_{i,\ell} \alpha^\ell$. The last equation can then be rewritten as

$$\sum_{i \in \mathbb{F}_p} D_p^{\langle i \rangle} y_i = 0 . \tag{10}$$

Combining (9) with (10) we get that

$$\sum_{i \in \mathbb{F}_p} \alpha^i y_i(\alpha) = \sum_{i \in \mathbb{F}_p} (D_p^{\langle i \rangle} y_i)(\alpha) = 0 .$$

Hence, by Lemma 4.4,

$$\sum_{i \in \mathbb{F}_p} \varphi(w_i^+) \alpha^i = 0 ,$$

namely, the word $f(w) = \big(\varphi(w_0^+)\ \varphi(w_1^+)\ \ldots\ \varphi(w_{p-1}^+)\big)$ is a codeword of $\mathbf{Z}_K(p,r)$.

We have thus proved the containment $\{f(w) : w \in \mathcal{Z}_F(p,r)\} \subseteq \mathbf{Z}_K(p,r)$. In fact, this containment holds with equality: both $\mathcal{Z}_F(p,r)$ and $\mathbf{Z}_K(p,r)$ are of the same size (namely, $q^{b(p-r)}$) and, by Lemma 4.2, the mapping f is one-to-one. Furthermore, since f is weight-preserving, the minimum Hamming distances of $\mathcal{Z}_F(p,r)$ and $\mathbf{Z}_K(p,r)$ must be the same. □

Corollary 4.5: Assuming that q is primitive in $\mathbb{F}_p$, the minimum Hamming distance of $\mathcal{Z}_F(p,r)$ is at least 3, for any divisor $r \geq 2$ of $p-1$.

Proof: Write $\beta = \alpha^{\omega-1}$ and let ν be the multiplicative inverse of $\omega-1$ in $\mathbb{F}_p$. Then β^ν $(= \alpha)$ and $\beta^{\nu+1}$ $(= \alpha^\omega)$ are two roots of $\mathbf{Z}_K(p,r)$ that form consecutive powers of an element β of multiplicative order p in Φ. The result now follows from Proposition 4.3 and the BCH bound [8, p. 201]. □

Notice that by the result of Zaitsev *et al.* in [14], Corollary 4.5 holds for $r = 2$ even if q is not primitive in $\mathbb{F}_p$.

We point out that there is a simple decoding algorithm that corrects one error in codewords of $\mathcal{Z}_F(p,r)$. As a first decoding step, we compute the syndrome of the received word with respect to the parity-check matrix $H_F(p,r)$; this computation requires $(p-1)(p-r)$ additions in F. In the second decoding step, we enumerate over the p possible locations of the error and, for each location, we check whether there is a respective error value (in F^b) which is consistent with the computed syndrome. Due to the structure of $H_F(p,r)$, the check for each location requires at most $p-1$ comparisons between elements of F. Therefore, the overall decoding complexity is $O(p^2)$ additions and comparisons in F.

We end this section with the following definition, which will turn out to be useful in the next section. Define the extension-field code $\mathbf{Z}_\Phi(p,r)$ as the cyclic code of length p over Φ whose set of roots is (5). Clearly, $\mathbf{Z}_K(p,r) = \mathbf{Z}_\Phi(p,r) \cap K^p$, i.e., $\mathbf{Z}_K(p,r)$ is a subfield sub-code of $\mathbf{Z}_\Phi(p,r)$. Since both $\mathbf{Z}_K(p,r)$ and $\mathbf{Z}_\Phi(p,r)$ have the same check polynomial, they also share a common parity-check matrix over K. Therefore, $\mathbf{Z}_K(p,r)$ (as a code over K) and $\mathbf{Z}_\Phi(p,r)$ (as a code over

Φ) are cyclic $[p, p-r]$ codes with the same minimum Hamming distance. The next corollary immediately follows from Proposition 4.3.

Corollary 4.6: Assuming that q is primitive in $\mathbb{F}_p$, the following three conditions are equivalent:

(i) The code $\mathcal{Z}_F(p,r)$ is MDS over F^b.
(ii) The code $\mathbf{Z}_K(p,r)$ is MDS over K.
(iii) The code $\mathbf{Z}_\Phi(p,r)$ is MDS over Φ.

V. Fields with characteristic 2

In this section, we prove Theorems 3.1 and 3.2. By Proposition 2.2, it suffices to prove these theorems only for the field $F = \mathbb{F}_2$. From Corollary 4.6 we get that $\mathcal{Z}_F(p,r)$ is MDS (over $\mathbb{F}_2^b$) if and only if $\mathbf{Z}_\Phi(p,r)$ is (over $\Phi = \mathbb{F}_{2^{p-1}}$). Now, since the code $\mathbf{Z}_\Phi(p,r)$ is linear over Φ, it is MDS if and only if every $r \times r$ sub-matrix in a parity-check matrix of $\mathbf{Z}_\Phi(p,r)$ is nonsingular [8, p. 318, Theorem 1]. It turns out that over $\mathbb{F}_2$, the latter condition of the MDS property reduces to another criterion, which, in turn, is more easily checked for small values of r. We present this criterion in the next lemma.

For two integers $m \le n$, we denote by $S[m,n]$ the set of $(n-m+1)!$ permutations over $\{m, m+1, \ldots, n\}$.

Lemma 5.1: Let F be the field $\mathbb{F}_2$ and let p be a prime such that 2 is primitive in $\mathbb{F}_p$. Fix $r > 2$ to be a divisor of $p-1$ and write $b = (p-1)/r$. The following two conditions are equivalent:

1) The code $\mathcal{Z}_F(p,r)$ is MDS over F^b.
2) Letting ω be an element of multiplicative order r in $\mathbb{F}_p$, there exist no $r-1$ distinct elements $i_1, i_2, \ldots, i_{r-1} \in \mathbb{F}_p^*$ for which the multi-set

$$\mathcal{X} = \Big\{ i_1\omega^{\pi(1)} + i_2\omega^{\pi(2)} + \ldots + i_{r-1}\omega^{\pi(r-1)} \; : \; \pi \in S[1, r-1] \Big\} \quad (11)$$

(of $(r-1)!$ elements in $\mathbb{F}_p$) can be partitioned into $\frac{1}{2}((r-1)!)$ multi-subsets of the form $\{\beta, \gamma\}$ where $\beta \overset{r}{\sim} \gamma$.

Proof: We show that condition 2 implies condition 1; the implication in the other direction can be obtained by essentially reversing the steps of the proof. We will make use of Corollary 4.6 by considering the code $\mathbf{Z}_\Phi(p,r)$ instead of $\mathcal{Z}_F(p,r)$.

Recall that the set of roots of $\mathbf{Z}_\Phi(p,r)$ is given by (5). Hence, the $r \times p$ matrix $\mathbf{H}_\Phi(p,r)$ over Φ, whose entries are

$$\left(\mathbf{H}_\Phi(p,r)\right)_{m,i} = \alpha^{i\omega^m} \;, \quad 0 \le m < r \;, \quad i \in \mathbb{F}_p \;,$$

is a parity-check matrix of $\mathbf{Z}_\Phi(p,r)$. Given a subset $\mathcal{I} \subseteq \mathbb{F}_p$ of size r, denote by $\Delta_\mathcal{I}$ the determinant of the $r \times r$ sub-matrix that is formed by the columns of $\mathbf{H}_\Phi(p,r)$ that are indexed by $\mathcal{I}$. Then $\mathbf{Z}_\Phi(p,r)$ is MDS if and only if $\Delta_\mathcal{I} \neq 0$ for every subset $\mathcal{I} \subseteq \mathbb{F}_p$ of size r.

Suppose that condition 1 does not hold, namely, that $\mathbf{Z}_\Phi(p,r)$ is not MDS over Φ. Then there is a subset $\mathcal{I} = \{i_0, i_1, \ldots, i_{r-1}\}$ of $\mathbb{F}_p$ such that $\Delta_\mathcal{I} = 0$. Now,

$$\Delta_\mathcal{I} = \alpha^{i_0(1+\omega+\omega^2+\ldots+\omega^{r-1})} \cdot \Delta_{\mathcal{I}-i_0} = \Delta_{\mathcal{I}-i_0} \;,$$

where $\mathcal{I} - i_0$ stands for the set $\{0, i_1 - i_0, \ldots, i_{r-1} - i_0\}$. Therefore, we can assume without loss of generality that $i_0 = 0$. Under this assumption,

$$\begin{aligned} \Delta_\mathcal{I} &= \sum_{\pi \in S[0,r-1]} \alpha^{0\cdot\omega^{\pi(0)} + i_1\omega^{\pi(1)} + i_2\omega^{\pi(2)} + \ldots + i_{r-1}\omega^{\pi(r-1)}} \\ &= \sum_{\pi \in S[1,r-1]} \sum_{m=0}^{r-1} \alpha^{\omega^m(i_1\omega^{\pi(1)} + i_2\omega^{\pi(2)} + \ldots + i_{r-1}\omega^{\pi(r-1)})} \;. \end{aligned}$$

Define the polynomial $T(x)$ over F by

$$T(x) = \sum_{\pi \in S[1,r-1]} \sum_{m=0}^{r-1} x^{\langle \omega^m(i_1\omega^{\pi(1)} + i_2\omega^{\pi(2)} + \ldots + i_{r-1}\omega^{\pi(r-1)}) \rangle} \;.$$

Clearly, $T(\alpha) = \Delta_\mathcal{I} = 0$. Since $M_p(x)$ is the minimal polynomial of α with respect to F, it follows that $M_p(x) \,|\, T(x)$. On the other hand, $\deg T(x) < p$; therefore, $T(x)$ is a scalar multiple of $M_p(x)$, i.e., $T(x) \in \{0, M_p(x)\}$.

For $1 \le j \le b$, let $T_j(x)$ be the polynomial over F defined in (6). We can express $M_p(x)$ and $T(x)$ as

$$M_p(x) = 1 + \sum_{j=1}^{b} T_j(x)$$

and

$$T(x) = \kappa_0 r + \sum_{j=1}^{b} \kappa_j T_j(x) \;,$$

where, for $0 \le j \le b$,

$$\kappa_j = \big|\big\{\pi \in S[1,r-1] \; : \; i_1\omega^{\pi(1)} + i_2\omega^{\pi(2)} + \ldots + i_{r-1}\omega^{\pi(r-1)} \in C_j\big\}\big| \;.$$

Recalling that $T(x) \in \{0, M_p(x)\}$ we thus obtain

$$\kappa_j \equiv \kappa_0 r \pmod 2 \;, \quad 1 \le j \le b \;, \qquad (12)$$

and summing over j yields

$$\sum_{j=1}^{b} \kappa_j \equiv \kappa_0 r b \equiv \kappa_0(p-1) \equiv 0 \pmod 2 \;.$$

On the other hand, from the condition $r > 2$ we also have

$$\sum_{j=0}^{b} \kappa_j = (r-1)! \equiv 0 \pmod 2 \;.$$

The last two equations imply that κ_0 is even, and from (12) we get that κ_j is even for every $1 \le j \le b$.

Yet, having all the κ_j's even is equivalent to saying that the multi-set $\mathcal{X}$ in (11) can be partitioned into multi-subsets of the form $\{\beta, \gamma\}$ where $\beta \overset{r}{\sim} \gamma$. This, however, means that condition 2 of the lemma does not hold. □

We can use Lemma 5.1 to check for small values of r whether the code $\mathcal{Z}_F(p,r)$ is MDS. This is how we are now going to prove Theorems 3.1 and 3.2.

Proof of Theorem 3.1: Based on Proposition 2.2, we assume that $F = \mathbb{F}_2$. For any two elements $i_1, i_2 \in \mathbb{F}_p^*$, the multiset $\mathcal{X}$ in (11) contains only two elements,

$$i_1\omega + i_2\omega^2 \quad \text{and} \quad i_1\omega^2 + i_2\omega \;,$$

where ω has multiplicative order 3 in $\mathbb{F}_p$. By Lemma 5.1 we deduce that $\mathcal{Z}_F(p,3)$ is MDS unless

$$(i_1\omega + i_2\omega^2) \overset{3}{\sim} (i_1\omega^2 + i_2\omega)$$

for some distinct $i_1, i_2 \in \mathbb{F}_p^*$. Now,

$$(i_1\omega + i_2\omega^2)^3 - (i_1\omega^2 + i_2\omega)^3 = 3i_1i_2(\omega - \omega^2)(i_1 - i_2) \ ,$$

and the right-hand side is nonzero whenever i_1 and i_2 are nonzero and distinct. Hence, the code $\mathcal{Z}_F(p,3)$ is MDS over F^b. □

Proof of Theorem 3.2: For $p = 5$, the construction $\mathcal{Z}_F(p,4)$ becomes the binary repetition code, which is obviously MDS. Hence, we assume hereafter in the proof that $p > 13$.

Let ω be an element of multiplicative order 4 in $\mathbb{F}_p$. We again use Proposition 2.2 and Lemma 5.1 to reduce the problem to showing that there are no three distinct elements $i_1, i_2, i_3 \in \mathbb{F}_p^*$ such that the multi-set

$$\mathcal{X} = \left\{ i_1\omega^{\pi(1)} + i_2\omega^{\pi(2)} + i_3\omega^{\pi(3)} \ : \ \pi \in S[1,3] \right\}$$

(of size 6) can be partitioned into three multi-subsets of the form $\{\beta, \gamma\}$ where $\beta \overset{4}{\sim} \gamma$. Equivalently, it suffices to show that for every partition of $S[1,3]$ into three pairs of permutations,

$$\{\pi_1, \pi_1'\} \ , \quad \{\pi_2, \pi_2'\} \ , \quad \text{and} \quad \{\pi_3, \pi_3'\} \ ,$$

one cannot find integers $m_1, m_2, m_3 \in \{0,1,2,3\}$ for which the following set of three linear homogeneous equations over $\mathbb{F}_p$ can be solved for distinct nonzero unknowns i_1, i_2, and i_3:

$$\begin{aligned}
&i_1\omega^{\pi_1(1)} + i_2\omega^{\pi_1(2)} + i_3\omega^{\pi_1(3)} \\
&\qquad = \ \omega^{m_1}(i_1\omega^{\pi_1'(1)} + i_2\omega^{\pi_1'(2)} + i_3\omega^{\pi_1'(3)}) \\
&i_1\omega^{\pi_2(1)} + i_2\omega^{\pi_2(2)} + i_3\omega^{\pi_2(3)} \\
&\qquad = \ \omega^{m_2}(i_1\omega^{\pi_2'(1)} + i_2\omega^{\pi_2'(2)} + i_3\omega^{\pi_2'(3)}) \\
&i_1\omega^{\pi_3(1)} + i_2\omega^{\pi_3(2)} + i_3\omega^{\pi_3(3)} \\
&\qquad = \ \omega^{m_3}(i_1\omega^{\pi_3'(1)} + i_2\omega^{\pi_3'(2)} + i_3\omega^{\pi_3'(3)})
\end{aligned}$$

Using matrix notation, this set of equations can be written as

$$A(\omega) \begin{pmatrix} i_1 \\ i_2 \\ i_3 \end{pmatrix} = \mathbf{0} \ , \tag{13}$$

where $A(\xi)$ is the following 3×3 matrix over the polynomial ring $\mathbb{F}_p[\xi]$:

$$A(\xi) = \begin{pmatrix}
\xi^{\pi_1(1)} - \xi^{m_1+\pi_1'(1)} & \xi^{\pi_1(2)} - \xi^{m_1+\pi_1'(2)} & \xi^{\pi_1(3)} - \xi^{m_1+\pi_1'(3)} \\
\xi^{\pi_2(1)} - \xi^{m_2+\pi_2'(1)} & \xi^{\pi_2(2)} - \xi^{m_2+\pi_2'(2)} & \xi^{\pi_2(3)} - \xi^{m_2+\pi_2'(3)} \\
\xi^{\pi_3(1)} - \xi^{m_3+\pi_3'(1)} & \xi^{\pi_3(2)} - \xi^{m_3+\pi_3'(2)} & \xi^{\pi_3(3)} - \xi^{m_3+\pi_3'(3)}
\end{pmatrix}.$$

Now, there are 15 possible partitions of $S[1,3]$ into three pairs and $4^3 = 64$ possible assignments to m_1, m_2, and m_3. This totals to $64 \times 15 = 960$ sets of linear equations of the form (13), and we need to show that none of these sets has a solution $(i_1 \ i_2 \ i_3) \in \mathbb{F}_p^3$ whose components are nonzero and distinct. We next show that, indeed, every solution of (13) has either a zero component or repeating entries; such solutions will be called *invalid*.

Since ω is an element of multiplicative order 4 in $\mathbb{F}_p$, it is a root of the polynomial $\xi^2 + 1 = 0$. Therefore, in determining whether (13) has a nontrivial solution, we can first compute the determinant of $A(\xi)$—denoted hereafter by $\det(A(\xi))$—as if the latter matrix were over the integer polynomial residue ring $\mathcal{J} = \mathbb{Z}[\xi]/(\xi^2+1)$, and then substitute $\xi = \omega$ and complete the arithmetic in $\mathbb{F}_p$. The value of $\det(A(\xi))$ in $\mathcal{J}$ will take the form $c_0 + c_1\xi$ for some integers c_0 and c_1. Since

$$\det(A(\omega)) = \det(A(\xi))\big|_{\xi=\omega} = c_0 + c_1\omega \ ,$$

it follows that, in $\mathbb{F}_p$,

$$\det(A(\omega)) = 0 \quad \Longrightarrow \quad (c_0 + c_1\omega)(c_0 - c_1\omega) = c_0^2 + c_1^2 = 0 \ .$$

Consequently, $A(\omega)$ is zero in $\mathbb{F}_p$ only if p divides the rational integer $c_0^2 + c_1^2$. This integer is known as the *norm* of $\det(A(\xi))$ in $\mathcal{J}$ [6, pp.172–173] and we will denote it here by $\mathcal{N}(\det(A(\xi)))$ (we will mention some of the properties of norms in Section VI; these properties, however, are not required in this proof).

Using a computer, we have computed $\det(A(\xi))$ in $\mathcal{J}$ for each of the 960 sets of equations. It turns out that each set belongs to one of the following three categories:

1) $\det(A(\xi)) \neq 0$ and the largest prime divisor of $\mathcal{N}(\det(A(\xi)))$ is at most 13. In this case, $A(\omega)$ is nonsingular in $\mathbb{F}_p$ if $p > 13$, and (13) is solved then only by $i_1 = i_2 = i_3 = 0$. Obviously, this solution is invalid.
2) $\det(A(\xi)) = 0$ and there is a linear combination of the rows of $A(\xi)$ over $\mathcal{J}$ that yields a vector of the form $(c\ 0\ 0)$, $(0\ c\ 0)$ or $(0\ 0\ c)$, where c is a nonzero integer whose largest prime divisor is at most 13. This implies that when $p > 13$, every solution $(i_1 \ i_2 \ i_3)$ of (13) must contain at least one zero entry; such a solution is therefore invalid.
3) The same as in category 2, except that the linear combination yields a vector of the form $(c\ -c\ 0)$, $(0\ c\ -c)$ or $(c\ 0\ -c)$. Therefore, when $p > 13$, every solution of (13) must contain repeating entries, thus making it invalid.

We conclude that each of the 960 sets of equations obtained by (13) has only invalid solutions. □

We remark that the exclusion of the case $p = 13$ from Theorem 3.2 is necessary, as it was verified in [5, p. 57] that the code $\mathcal{Z}_{\mathbb{F}_2}(13,4)$ is not MDS over $\mathbb{F}_2^3$.

VI. Cyclic MDS codes of prime length

In this section, we derive a sufficient condition that a given cyclic code of prime length be MDS. Then, in Section VII, we apply this condition to the codes $\mathbf{Z}_K(p,r)$ and their dual codes over K.

Let K be a finite field with characteristic q and let $\mathbf{C}_K$ denote a cyclic $[p, p-r]$ code over K, where p is a prime and $0 \leq r < p$ (we do not require in this section that r be a divisor of $p-1$, neither do we assume that q is primitive in $\mathbb{F}_p$). We index the coordinates of $\mathbf{C}_K$ by the elements of $\mathbb{F}_p$.

It is known that $\mathbf{C}_K$ is MDS when either $r \in \{0, 1, p-1\}$ or $q = p$ (see [12]). Hence, we assume hereafter in this section

that $q \neq p$, in which case there exists an extension field Φ of K that contains an element α of multiplicative order p. And since the generator polynomial of $\mathbf{C}_K$ divides x^p-1, the roots of $\mathbf{C}_K$ are all simple and are powers of α. Let

$$\{\alpha^{\varepsilon_0}, \alpha^{\varepsilon_1}, \ldots, \alpha^{\varepsilon_{r-1}}\} \tag{14}$$

be the set of roots of $\mathbf{C}_K$. We have,

$$\mathbf{C}_K = \{c \in K^p \,:\, c(\alpha^{\varepsilon_m}) = 0\,, \quad 0 \leq m < r\}\ .$$

By the BCH bound it follows that $\mathbf{C}_K$ is MDS when $r = 2$, and since the cyclic MDS property is preserved under duality, it is MDS also when $r = p-2$. Therefore, we will focus from now on in this section on the range $2 < r < p-2$.

Following arguments similar to those made at the end of Section IV, we can conclude that $\mathbf{C}_K$ is MDS over K if and only if the cyclic $[p, p-r]$ code $\mathbf{C}_\Phi$ over Φ, whose set of roots is given by (14), is MDS over Φ. An $r \times p$ parity-check matrix of $\mathbf{C}_\Phi$ over Φ, in turn, is given by

$$\mathbf{H} = \left(\, \alpha^{\varepsilon_m i}\,\right)_{m=0,\ i\in\mathbb{F}_p}^{r-1}\ . \tag{15}$$

Thus, we can check whether $\mathbf{C}_K$ is MDS by analyzing the $r \times r$ sub-matrices of $\mathbf{H}$. Similarly to what we have done in the proof of Theorem 3.2, we do this analysis by lifting the computations to an extension ring of $\mathbb{Z}$, as we describe next.

Let ζ denote a primitive pth root of unity in the complex field and let $\mathbb{Q}_p(\zeta) \cong \mathbb{Q}[x]/M_p(x)$ denote the pth cyclotomic extension of the rational field $\mathbb{Q}$, where $M_p(x) = 1+x+\ldots+x^{p-1}$ is regarded here as a polynomial over $\mathbb{Q}$. That is, $\mathbb{Q}_p(\zeta)$ is the smallest field containing both $\mathbb{Q}$ and ζ and its elements are all the rational polynomials in ζ of degree less than $p-1$; multiplication in $\mathbb{Q}_p(\zeta)$ is carried out modulo $M_p(x)$.

We briefly summarize here several properties of $\mathbb{Q}_p(\zeta)$. Let g be a primitive element of $\mathbb{F}_p$. The mapping $\psi : \mathbb{Q}_p(\zeta) \to \mathbb{Q}_p(\zeta)$, defined by

$$\psi\left(\textstyle\sum_{\ell=0}^{p-2} a_\ell \zeta^\ell\right) = \sum_{\ell=0}^{p-2} a_\ell \zeta^{g\ell}\ , \tag{16}$$

is a generator of the automorphism group $\{\psi^t\}_{t=0}^{p-2}$ of $\mathbb{Q}_p(\zeta)$, where

$$\psi^t\left(\textstyle\sum_{\ell=0}^{p-2} a_\ell \zeta^\ell\right) = \sum_{\ell=0}^{p-2} a_\ell \zeta^{\ell g^t}\ , \quad t \geq 0\ .$$

The conjugacy class of an element $\gamma \in \mathbb{Q}_p(\zeta)$ with respect to $\mathbb{Q}$ is given by

$$\left\{\gamma, \psi(\gamma), \psi^2(\gamma), \ldots, \psi^{\mu-1}(\gamma)\right\}\ ,$$

where μ is the smallest positive integer such that $\psi^\mu(\gamma) = \gamma$. The minimal polynomial of γ is given by $\prod_{m=0}^{\mu-1}(x-\psi^m(\gamma))$, and this polynomial is an irreducible polynomial over $\mathbb{Q}$. The norm of γ over $\mathbb{Q}$, denoted $\mathcal{N}(\gamma)$, is given by $\prod_{t=0}^{p-2}\psi^t(\gamma)$, and is a rational number. The norm is multiplicative: for every two elements γ_1, γ_2 in $\mathbb{Q}_p(\zeta)$ we have $\mathcal{N}(\gamma_1\gamma_2) = \mathcal{N}(\gamma_1)\mathcal{N}(\gamma_2)$. An element such that the coefficients of its minimal polynomial are all integers, is called an algebraic integer. An element $a_0 + a_1\zeta + \ldots + a_{p-2}\zeta^{p-2} \in \mathbb{Q}_p(\zeta)$ is an algebraic integer if and only if $a_0, a_1, \ldots, a_{p-2}$ are integers. The norm of an algebraic integer is an integer. The set of algebraic integers of $\mathbb{Q}_p(\zeta)$ is a ring, and is denoted here by $\mathcal{O}_p$. The mapping $\delta_\Phi : \mathcal{O}_p \to \Phi$, which is defined by

$$\begin{aligned}\delta_\Phi\left(a_0 + a_1\zeta + \ldots + a_{p-2}\zeta^{p-2}\right)& \\ = \quad a_0 + a_1\alpha + \ldots + a_{p-2}\alpha^{p-2},&\end{aligned} \tag{17}$$

is a homomorphism from $\mathcal{O}_p$ to Φ. See [9] for a discussion of cyclotomic and general number fields.

Turning back to the analysis of $\mathbf{C}_K$, let $\mathit{\Gamma}(p,r)$ denote the collection of all the subsets of $\mathbb{F}_p$ of size r. Given a subset $\mathcal{I} = \{i_0, i_1, \ldots, i_{r-1}\}$ in $\mathit{\Gamma}(p,r)$, define the $r \times r$ matrix $\Lambda_\mathcal{I}(x)$ over $\mathbb{Z}[x]$ by

$$\Lambda_\mathcal{I}(x) = \left(\, x^{\langle \varepsilon_m i_s\rangle}\,\right)_{m,s=0}^{r-1}$$

(here we assume some ordering on the elements of $\mathcal{I}$, say, the lexicographic ordering on $\mathbb{F}_p$). The determinant of $\Lambda_\mathcal{I}(x)$, which we denote by $\Delta_\mathcal{I}(x)$, is a polynomial in $\mathbb{Z}[x]$. Observe that the value $\Delta_\mathcal{I}(\alpha)$ (in Φ) is the determinant of the $r \times r$ matrix $\Lambda_\mathcal{I}(\alpha)$ over Φ; this matrix, in turn, is the $r \times r$ sub-matrix that is formed by the columns of $\mathbf{H}$ in (15) that are indexed by $\mathcal{I}$. Thus, $\mathbf{C}_K$ is MDS if and only if $\Delta_\mathcal{I}(\alpha)$ is nonzero for all $\mathcal{I} \in \mathit{\Gamma}(p,r)$.

For a subset $\mathcal{I} = \{i_s\}_{s=0}^{r-1}$ in $\mathit{\Gamma}(p,r)$ and an element $y \in \mathbb{F}_p^*$, denote by $y\mathcal{I}$ the set $\{y \cdot i_s \,:\, i_s \in \mathcal{I}\}$; clearly, $y\mathcal{I} \in \mathit{\Gamma}(p,r)$. Consider the polynomial

$$B_\mathcal{I}(x) = \prod_{y\in\mathbb{F}_p^*} \Delta_{y\mathcal{I}}(x)$$

in $\mathbb{Z}[x]$. It follows that $\mathbf{C}_K$ is MDS if and only if $B_\mathcal{I}(\alpha)$ is nonzero (in Φ) for all $\mathcal{I} \in \mathit{\Gamma}(p,r)$. On the other hand, by the homomorphism (17) we have

$$B_\mathcal{I}(\alpha) = \delta_\Phi\left(B_\mathcal{I}(\zeta)\right)\ .$$

We next analyze the value $B_\mathcal{I}(\zeta)$ (in $\mathbb{Q}_p(\zeta)$).

Letting g be a primitive element in $\mathbb{F}_p$, we have

$$B_\mathcal{I}(\zeta) = \prod_{y\in\mathbb{F}_p^*} \Delta_{y\mathcal{I}}(\zeta) = \prod_{t=0}^{p-2} \Delta_{g^t\mathcal{I}}(\zeta)\ .$$

Now, the matrix $\Lambda_{g^t\mathcal{I}}(\zeta)$ (over $\mathbb{Q}_p(\zeta)$) can be obtained by applying the automorphism ψ^t to each entry in $\Lambda_\mathcal{I}(\zeta)$, possibly with re-ordering of columns. Therefore,

$$\Delta_{g^t\mathcal{I}}(\zeta) = \pm\psi^t\left(\Delta_\mathcal{I}(\zeta)\right)\ , \quad 0 \leq t < p-1\ ,$$

and, so,

$$B_\mathcal{I}(\zeta) = \pm\prod_{t=0}^{p-2}\psi^t\left(\Delta_\mathcal{I}(\zeta)\right) = \pm\mathcal{N}(\Delta_\mathcal{I}(\zeta))\ . \tag{18}$$

The next proposition presents a property of the norm $\mathcal{N}(\Delta_\mathcal{I}(\zeta))$.

Proposition 6.1: Given a subset $\mathcal{I} \in \mathit{\Gamma}(p,r)$, let $\mu_\mathcal{I}$ denote the size of the conjugacy class of $\Delta_\mathcal{I}(\zeta)$ with respect to the field $\mathbb{Q}$. The following holds:

(i) The norm $\mathcal{N}(\Delta_\mathcal{I}(\zeta))$ is a nonzero (rational) integer.
(ii) Every (rational) prime factor of $\mathcal{N}(\Delta_\mathcal{I}(\zeta))$ other than p is bounded from above by

$$\left(\frac{r^{p-1}}{p^{r-1}}\right)^{r\mu_\mathcal{I}/(2p-2)}\ . \tag{19}$$

We prove Proposition 6.1 later on in this section, but first we present the following theorem and corollary, which are proved based on Proposition 6.1.

Theorem 6.2: Let K be a finite field with characteristic q and let p be a prime other than q. For an integer r in the range $0 \leq r < p$, let $\mathbf{C}_K$ be the $[p, p-r]$ cyclic code over K with roots (14), and define

$$\mu = \mu_{\max}(\mathbf{C}_K) = \max_{\mathcal{I} \in \Gamma(p,r)} \mu_{\mathcal{I}} \ ,$$

where $\mu_{\mathcal{I}}$ is as in Proposition 6.1. Then $\mathbf{C}_K$ is MDS when either $r \in \{0, 1, 2, p-2, p-1\}$ or

$$q > \left(\frac{r^{p-1}}{p^{r-1}} \right)^{r\mu/(2p-2)} \ . \tag{20}$$

Proof: The cases $r \in \{0, 1, 2, p-2, p-1\}$ have already been discussed earlier, so we only need to consider the range $2 < r < p-2$.

First, by (18) and Proposition 6.1(i) we get that for every subset $\mathcal{I} \in \Gamma(p, r)$, the value $B_{\mathcal{I}}(\zeta)$ is a nonzero integer. Secondly, it is easy to verify that $r^{p-1}/p^{r-1} > 1$ whenever $2 < r < p-2$ and, so, (19) increases with $\mu_{\mathcal{I}}$ for fixed p and r. Therefore, given that (20) holds, we conclude from Proposition 6.1(ii) that $B_{\mathcal{I}}(\zeta)$ is not divisible by q. This means that every $B_{\mathcal{I}}(\alpha)$ $(= \delta_\Phi(B_{\mathcal{I}}(\zeta)))$ is nonzero (in Φ) and, thus, $\mathbf{C}_K$ is MDS.

Corollary 6.3: Let K be a finite field with characteristic q, let p be a prime other than q, and let r be an integer in the range $0 \leq r < p$. Every cyclic $[p, k{=}p{-}r]$ code over K is MDS when either $r \in \{0, 1, 2, p-2, p-1\}$ or

$$q > \begin{cases} \left(\dfrac{r^{p-1}}{p^{r-1}} \right)^{r/2} & \text{if } r < p/2 \\ \left(\dfrac{k^{p-1}}{p^{k-1}} \right)^{k/2} & \text{otherwise} \end{cases} \ .$$

Proof: Since μ divides $p-1$, the condition (20) may only become stronger if we replace μ with $p-1$ therein. Recalling that the cyclic MDS property is preserved under duality, we thus get by Theorem 6.2 that every cyclic $[p, k]$ code over K is MDS whenever

$$q > \min \left\{ \left(\frac{r^{p-1}}{p^{r-1}} \right)^{r/2}, \left(\frac{k^{p-1}}{p^{k-1}} \right)^{k/2} \right\} \ .$$

Finally, a simple analysis reveals that $\left(r^{p-1}/p^{r-1}\right)^r < \left(k^{p-1}/p^{k-1}\right)^k$ if and only if $r < k$. □

Remark: Using the same method of lifting to the field $\mathbb{Q}_p(\zeta)$, Assmus and Mattson showed in [1] that for all primes q greater than some bound $q_0(p, k)$, each $[p, k]$ cyclic code over a field with characteristic q is MDS. They do not, however, give an estimate for $q_0(p, k)$. □

We now turn to proving Proposition 6.1, starting with two lemmas, the first of which is a direct application of Hadamard's inequality (see [2, pp. 126–130]).

Lemma 6.4: For every $\mathcal{I} \in \Gamma(p, r)$,

$$|\Delta_{\mathcal{I}}(\zeta)| \leq r^{r/2} \ ,$$

where $|\Delta_{\mathcal{I}}(\zeta)|$ denotes the absolute value (modulus) of the complex $\Delta_{\mathcal{I}}(\zeta)$.

Lemma 6.5: For every subset $\mathcal{I} = \{i_0, i_1, \ldots, i_{r-1}\}$ in $\Gamma(p, r)$,

$$\Delta_{\mathcal{I}}(\zeta) = \mathcal{S}_{\mathcal{I}}(\zeta) \prod_{\substack{s,m=0 \\ s<m}}^{r} \left(\zeta^{i_m} - \zeta^{i_s} \right) \ ,$$

where $\mathcal{S}_{\mathcal{I}}(\zeta)$ is an algebraic integer.

Proof: Consider the $r \times r$ matrix

$$\Lambda(x_0, x_1, \ldots, x_{r-1}) = \left(x_s^{\varepsilon_m} \right)_{m,s=0}^{r-1}$$

over $\mathbb{Z}[x_0, x_1, \ldots, x_{r-1}]$, and denote by

$$\Delta(x_0, x_1, \ldots, x_{r-1})$$

the determinant of $\Lambda(x_0, x_1, \ldots, x_{r-1})$. Clearly,

$$\Delta(x_0, x_1, \ldots, x_{r-1}) \in \mathbb{Z}[x_0, x_1, \ldots, x_{r-1}] \ .$$

Now, by [10, pp. 334, §339], $\Delta(x_0, x_1, \ldots, x_{r-1})$ satisfies

$$\Delta(x_0, x_1, \ldots, x_{r-1}) = \mathcal{S}(x_0, x_1, \ldots, x_{r-1}) \prod_{\substack{s,m=0 \\ s<m}}^{r} (x_s - x_m) \ ,$$

where $\mathcal{S}(x_0, x_1, \ldots, x_{r-1}) \in \mathbb{Z}[x_0, x_1, \ldots, x_{r-1}]$ is the determinant of a certain $r \times r$ matrix over $\mathbb{Z}[x_0, x_1, \ldots, x_{r-1}]$. Substituting $x_s = \zeta^{i_s}$ for x_s for $0 \leq s < r$, and defining $\mathcal{S}_{\mathcal{I}}(\zeta) = \mathcal{S}(\zeta^{i_0}, \zeta^{i_1}, \ldots, \zeta^{i_{r-1}})$, we obtain the result. □

Proof of Proposition 6.1: It is known [11] that every square sub-matrix of the complex matrix $(\zeta^{i\ell})_{i,\ell \in \mathbb{F}_p}$ is nonsingular. Hence, $\Delta_{\mathcal{I}}(\zeta)$ is nonzero, and so is the norm $\mathcal{N}(\Delta_{\mathcal{I}}(\zeta))$. Furthermore, since $\Delta_{\mathcal{I}}(x) \in \mathbb{Z}[x]$, we get that $\Delta_{\mathcal{I}}(\zeta)$ is an algebraic integer and, therefore, $\mathcal{N}(\Delta_{\mathcal{I}}(\zeta))$ is in $\mathbb{Z}$. This proves part (i).

As for part (ii), write $\mathcal{I} = \{i_0, i_1, \ldots, i_{r-1}\}$. By Lemma 6.5 we have

$$\mathcal{N}(\Delta_{\mathcal{I}}(\zeta)) = \mathcal{N}\left(\mathcal{S}_{\mathcal{I}}(\zeta)\right) \prod_{\substack{s,m=0 \\ s<m}}^{r-1} \mathcal{N}\left(\zeta^{i_m} - \zeta^{i_s}\right) \ , \tag{21}$$

where

$$\begin{aligned} \mathcal{N}\left(\zeta^{i_m} - \zeta^{i_s}\right) &= \mathcal{N}(\zeta^{i_m}) \mathcal{N}(1 - \zeta^{i_s - i_m}) \\ &= \prod_{t=1}^{p-1} \zeta^{t i_m} \prod_{t=1}^{p-1} (1 - \zeta^t) \\ &= (-1)^{(p-1) i_m} M_p(1) = \pm p \ . \end{aligned}$$

Recalling that $\mathcal{S}_{\mathcal{I}}(\zeta)$ is an algebraic integer, it follows from (21) that

$$\mathcal{N}(\Delta_{\mathcal{I}}(\zeta)) = \pm N_{\mathcal{I}} \cdot p^{r(r-1)/2} \ , \tag{22}$$

where $N_{\mathcal{I}} = \mathcal{N}\left(\mathcal{S}_{\mathcal{I}}(\zeta)\right)$ is in $\mathbb{Z}$.

Let $\tau_{\mathcal{I}}$ be defined by

$$\tau_{\mathcal{I}} = \prod_{t=0}^{\mu_{\mathcal{I}}-1} \psi^t(\Delta_{\mathcal{I}}(\zeta)) = \pm \prod_{t=0}^{\mu_{\mathcal{I}}-1} \Delta_{g^t \mathcal{I}}(\zeta) \ .$$

Up to a sign change, $\tau_{\mathcal{I}}$ is the free coefficient of the minimal polynomial of (the algebraic integer) $\Delta_{\mathcal{I}}(\zeta)$ with respect to $\mathbb{Q}$.

As such, $\tau_{\mathcal{I}}$ must be an integer and it is related to the norm $\mathcal{N}(\Delta_{\mathcal{I}}(\zeta))$ by

$$\mathcal{N}(\Delta_{\mathcal{I}}(\zeta)) = (\tau_{\mathcal{I}})^{(p-1)/\mu_{\mathcal{I}}} \ .$$

Therefore, we get from (22) that the multiplicity of p in the prime factorization of $\tau_{\mathcal{I}}$ (in $\mathbb{Z}$) is bounded from below by

$$\frac{r(r-1)/2}{(p-1)/\mu_{\mathcal{I}}} = \frac{r(r-1)\mu_{\mathcal{I}}}{2p-2} \ .$$

On the other hand, by Lemma 6.4 we have

$$|\tau_{\mathcal{I}}| \le r^{r\mu_{\mathcal{I}}/2} \ .$$

We conclude that every prime factor of $\tau_{\mathcal{I}}$ other than p is bounded from above by

$$\frac{|\tau_{\mathcal{I}}|}{p^{r(r-1)\mu_{\mathcal{I}}/(2p-2)}} \le \frac{r^{r\mu_{\mathcal{I}}/2}}{p^{r(r-1)\mu_{\mathcal{I}}/(2p-2)}} = \left(\frac{r^{p-1}}{p^{r-1}}\right)^{r\mu_{\mathcal{I}}/(2p-2)} ,$$

as claimed. □

VII. Finite fields with large characteristic

In this section, we prove Theorem 3.3 by applying the results of Section VI. We let F be the field $\mathbb{F}_q$ and let p, b, and r be as in Section II. As we will also use the results of Section IV, we assume that q is a primitive element in $\mathbb{F}_p$; this, in turn, implies that the characteristic of F is also primitive in $\mathbb{F}_p$. Based on Proposition 2.2, we can replace F with its prime subfield. Thus, we assume throughout this section that q is both primitive in $\mathbb{F}_p$ and prime.

In applying the results of Section VI, we take the fields K and Φ as $\mathbb{F}_{q^b}$ and $\mathbb{F}_{q^{p-1}}$, respectively, and the code $\mathbf{C}_K$ is selected to be either $\mathbf{Z}_K(p,r)$ or the dual code $\mathbf{Z}_K^{\perp}(p,r)$ over K. Letting ω be an element of multiplicative order r in $\mathbb{F}_p$, the set of roots of $\mathbf{Z}_K(p,r)$ is given by (5) while that of the dual code $\mathbf{Z}_K^{\perp}(p,r)$ is

$$\{1\} \cup \left\{ \alpha^{-q^j \omega^t} \ : \ 0 \le t < r \ , \ 1 \le j < b \right\} \qquad (23)$$

(see [8, p. 199]).

Lemma 7.1: Using the notations of Theorem 6.2, let μ and $\mu^{\perp}$ be defined by

$$\mu = \mu_{\max}(\mathbf{Z}_K(p,r)) \quad \text{and} \quad \mu^{\perp} = \mu_{\max}(\mathbf{Z}_K^{\perp}(p,r)) \ .$$

Then the following holds:

(i) $\mu \,|\, b$ if r is odd, and $\mu \,|\, 2b$ if r is even.
(ii) $\mu^{\perp} \,|\, b$ if either r or b is odd, and $\mu^{\perp} \,|\, 2b$ if r and b are both even.

Proof: Let $\mathcal{I} = \{i_0, i_2, \ldots, i_{r-1}\}$ be a subset in $\Gamma(p,r)$ such that $\mu_{\mathcal{I}} = \mu$. Define $\Lambda_{\mathcal{I}}(\zeta)$ and its determinant $\Delta_{\mathcal{I}}(\zeta)$ as in Section VI, taking $\varepsilon_m = \omega^m$ for $0 \le m < r$, that is,

$$\Lambda_{\mathcal{I}}(\zeta) = \left(\zeta^{i_s \omega^m} \right)_{m,s=0}^{r-1} \ .$$

Denote by $\Lambda_{\mathcal{I}}^*(\zeta)$ the $r \times r$ matrix that is obtained by raising each entry of $\Lambda_{\mathcal{I}}(\zeta)$ to the ωth power. Raising to this power, in turn, is equivalent to applying the automorphism ψ^b (assuming with no loss of generality that ω is the bth power of the primitive element g used in the definition of ψ in (16)). Hence,

$$\det(\Lambda_{\mathcal{I}}^*(\zeta)) = \psi^b(\Delta_{\mathcal{I}}(\zeta)) \ .$$

On the other hand, we can get the same matrix $\Lambda_{\mathcal{I}}^*(\zeta)$ also by shifting the rows of $\Lambda_{\mathcal{I}}(\zeta)$ cyclically one position down; namely, $\Lambda_{\mathcal{I}}^*(\zeta)$ is obtained from $\Lambda_{\mathcal{I}}(\zeta)$ by $r-1$ interchanges of rows. Thus, the determinant of $\Lambda_{\mathcal{I}}^*(\zeta)$ is related to that of $\Lambda_{\mathcal{I}}(\zeta)$ by

$$\det(\Lambda_{\mathcal{I}}^*(\zeta)) = (-1)^{r-1} \Delta_{\mathcal{I}}(\zeta) \ .$$

From the last two equations we obtain that

$$\psi^b(\Delta_{\mathcal{I}}(\zeta)) = (-1)^{r-1} \Delta_{\mathcal{I}}(\zeta) \ .$$

Hence, when r is odd we get that $\psi^b(\Delta_{\mathcal{I}}(\zeta)) = \Delta_{\mathcal{I}}(\zeta)$, which readily implies that $\mu_{\mathcal{I}} \,|\, b$. For even r we have

$$\psi^{2b}(\Delta_{\mathcal{I}}(\zeta)) = \psi^b(\psi^b(\Delta_{\mathcal{I}}(\zeta))) = \psi^b(-\Delta_{\mathcal{I}}(\zeta)) = \Delta_{\mathcal{I}}(\zeta) \ ,$$

which means that $\mu_{\mathcal{I}} \,|\, 2b$. This completes the proof of part (i).

The proof of part (ii) is similar, except that now $\mathcal{I}$ is a subset in $\Gamma(p,p-r)$ and $\Lambda_{\mathcal{I}}(\zeta)$ is a $(p-r) \times (p-r)$ matrix defined with respect to the $p-r$ roots in (23). We again obtain $\Lambda_{\mathcal{I}}^*(\zeta)$ by raising each entry of $\Lambda_{\mathcal{I}}(\zeta)$ to the ωth power, and it can be verified that the same matrix $\Lambda_{\mathcal{I}}^*(\zeta)$ can be obtained also by $(b-1)(r-1)$ interchanges of rows in $\Lambda_{\mathcal{I}}(\zeta)$. □

Proof of Theorem 3.3: The cases $r = 1$ and $r = p-1$ correspond, respectively, to the parity code over $F^{\,p-1}$ and to (a code equivalent to) the repetition code over F, and the case $r = 2$ is proved in [14]. We assume from now on that $2 < r \le (p-1)/2$.

Using Proposition 2.2, we first reduce to the case where F is the prime field $\mathbb{F}_q$. Then, recalling that the MDS property is preserved under duality, we apply Corollary 4.6 to claim that it suffices to find sufficient conditions as to when either $\mathbf{Z}_K(p,r)$ or $\mathbf{Z}_K^{\perp}(p,r)$ is MDS over $K = \mathbb{F}_{q^b}$. Next we apply Theorem 6.2 to $\mathbf{Z}_K(p,r)$ and $\mathbf{Z}_K^{\perp}(p,r)$, similarly to the proof of Corollary 6.3, except that now we replace μ in the right-hand side of (20) by the upper bounds on μ and $\mu^{\perp}$ which are implied by Lemma 7.1. □

Appendix

Proof of Proposition 2.1: Fix a row index $\ell \in \mathbb{F}_p^*$ of $H_F^+(p,r)$. We count the number of '1's that were deleted from row ℓ when constructing $H_F(p,r)$. From (3) we see that a '1' was deleted from entry $(\ell,(i,j))$ of $H_F^+(p,r)$ if and only if both

$$\ell - i \in C_j \quad \text{and} \quad -i \in C_j \ .$$

It follows that the number of deleted '1's from row ℓ is given by the number of elements $i \in \mathbb{F}_p$ that satisfy

$$(\ell - i) \overset{r}{\sim} -i \ .$$

This relation can be satisfied only when $i \neq 0$ and it is therefore equivalent to

$$(1 - (\ell/i))^r = 1 \ . \qquad (24)$$

Letting ω denote an element of multiplicative order r in $\mathbb{F}_p$, the solutions of (24) for i are given by

$$i = \ell(1 - \omega^t)^{-1} \ , \quad 1 \le t < r \ .$$

Thus, $r-1$ '1's were deleted from row ℓ of $H_F^+(p,r)$, which means that the number of '1's in the respective row in $H_F(p,r)$ is $p-(r-1)$. □

REFERENCES

[1] E.F. ASSMUS, JR., H.F. MATTSON, JR., *New 5-Designs, J. of Comb. Theory*, 6 (1969), 122–151.

[2] R. BELLMAN, *Introduction to Matrix Analysis*, Second Edition, McGraw Hill, New York, 1970.

[3] 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.

[4] M. BLAUM, J. BRUCK, A. VARDY, *MDS array codes with independent parity symbols, IEEE Trans. Inform. Theory*, 42 (1996), 529–542.

[5] M. BLAUM, R.M. ROTH, *On lowest density MDS codes, IEEE Trans. Inform. Theory*, 45 (1999), 46–59.

[6] K. IRELAND, M. ROSEN, *A Classical Introduction to Modern Number Theory*, Springer, New York, 1972.

[7] R. LIDL, H. NIEDERREITER, *Finite Fields*, Second Edition, Cambridge University Press, Cambridge, UK, 1997.

[8] F.J. MACWILLIAMS, N.J.A. SLOANE, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam, 1977.

[9] R. A. MOLLIN, *Algebraic Number Theory*, CRC Press, Boca Raton, Florida, 1999.

[10] T. MUIR, *A Treatise on The Theory of Determinants*, Dover, New York, 1960.

[11] M. NEWMAN, *On a theorem of N.G. Cebotarev, Linear and Mult. Alg.*, 3 (1975/76), 259–262.

[12] R.M. ROTH, G. SEROUSSI, *On cyclic MDS codes of length q over GF(q), IEEE Trans. Inform. Theory*, 32 (1986), 284–285.

[13] L. XU, J. BRUCK, *X-Code: MDS array codes with optimal encoding, IEEE Trans. Inform. Theory*, 45 (1999), 272–276.

[14] G.V. ZAITSEV, V.A. ZINOV'EV, N.V. SEMAKOV *Minimum-check-density codes for correcting bytes of errors, erasures, or defects, Problems Inform. Transm.*, 19 (1981), 197–204.

Erez Louidor add biography here

Ron M. Roth was born in Ramat Gan, Israel, in 1958. He received the B.Sc. degree in computer engineering, the M.Sc. in electrical engineering and the D.Sc. in computer science from Technion—Israel Institute of Technology, Haifa, Israel, in 1980, 1984 and 1988, respectively. Since 1988 he has been with the Computer Science Department at Technion, where he now holds the General Yaakov Dori Chair in Engineering. During the academic years 1989–91 he was a Visiting Scientist at IBM Research Division, Almaden Research Center, San Jose, California, and during 1996–97 and 2004–05 he was on sabbatical leave at Hewlett-Packard Laboratories, Palo Alto, California. He is the author of the book *Introduction to Coding Theory*, published by Cambridge University Press in 2006. Dr. Roth was an associate editor for coding theory in IEEE TRANSACTIONS ON INFORMATION THEORY from 1998 till 2001. His research interests include coding theory, information theory, and their application to the theory of complexity.