Symbol-Intersecting Codes†

Ron M. Roth[1], Gadiel Seroussi
Information Theory Research
HP Laboratories Palo Alto
HPL-2004-117
July 7, 2004*

E-mail: {ronny@cs.technion.ac.il, seroussi@hpl.hp.com}

error-correcting codes, broadcast channels, codes over rings, Reed-Solomon codes, sub-field sub-codes, Kronecker sum of matrices

We consider codes consisting of arrays over an alphabet F, in which certain intersecting subsets of $n \times m$ coordinates are required to form codewords of length n in prescribed codes over the alphabet F^m. Two specific cases are studied. In the first case, referred to as a singly-intersecting coding scheme, the user data is mapped into $n \times (2m-1)$ arrays over an alphabet F, such that the $n \times m$ sub-array that consists of the left (respectively, right) m columns forms a codeword of a prescribed code of length n over F^m; in particular, the center column is shared by the left and right sub-arrays. Bounds are obtained on the achievable redundancy region of singly-intersecting coding schemes, and constructions are presented which approach--and sometimes meet--these bounds. It is shown that singly-intersecting coding schemes can be applied in a certain model of broadcast channels to guarantee reliable communication. The second setting, referred to as a fully-intersecting coding scheme, maps the user data into $n \times m \times m$ three-dimensional arrays in which parallel $n \times m$ sub-arrays are all codewords of the same prescribed code over F^m. Bounds and constructions are presented for these codes, with the analysis based on representing the $n \times m \times m$ arrays as vectors over certain algebras on $m \times m$ matrices.

* Internal Accession Date Only
†This work was supported by grants Nos. 98-199 and 2002197 from the U.S.-Israel Binational Science Foundation, Jerusalem, Israel. Part of this work was presented at the IEEE International Symposium on Information Theory (ISIT'2003), Yokohama, Japan (July 2003). [1]Computer Science Dept., Technion, Haifa 32000, Israel
Approved for External Publication

Symbol-Intersecting Codes*

Ron M. Roth[†] Gadiel Seroussi[‡]

June 25, 2004

Abstract

We consider codes consisting of arrays over an alphabet F, in which certain intersecting subsets of $n \times m$ coordinates are required to form codewords of length n in prescribed codes over the alphabet F^m. Two specific cases are studied. In the first case, referred to as a singly-intersecting coding scheme, the user data is mapped into $n \times (2m-1)$ arrays over an alphabet F, such that the $n \times m$ sub-array that consists of the left (respectively, right) m columns forms a codeword of a prescribed code of length n over F^m; in particular, the center column is shared by the left and right sub-arrays. Bounds are obtained on the achievable redundancy region of singly-intersecting coding schemes, and constructions are presented which approach—and sometimes meet—these bounds. It is shown that singly-intersecting coding schemes can be applied in a certain model of broadcast channels to guarantee reliable communication. The second setting, referred to as a fully-intersecting coding scheme, maps the user data into $n \times m \times m$ three-dimensional arrays in which parallel $n \times m$ sub-arrays are all codewords of the same prescribed code over F^m. Bounds and constructions are presented for these codes, with the analysis based on representing the $n \times m \times m$ arrays as vectors over certain algebras on $m \times m$ matrices.

Keywords: Achievable region, broadcast channels, codes over rings, Kronecker sum of matrices, Reed-Solomon codes, sub-field sub-codes.

---

*This work was supported by grants Nos. 98-199 and 2002197 from the United-States–Israel Binational Science Foundation (BSF), Jerusalem, Israel. Part of this work was presented at the *IEEE International Symposium on Information Theory (ISIT'2003)*, Yokohama, Japan (July 2003).

[†]Computer Science Department, Technion, Haifa 32000, Israel; ronny@cs.technion.ac.il.

[‡]Hewlett-Packard Laboratories, 1501 Page Mill Road, Palo Alto, CA 94304, USA; seroussi@hpl.hp.com.

1 Introduction

Let F be an alphabet and let $F^{m\times m}$ be the alphabet that consists of all $m \times m$ arrays $A = (a_{j,\ell})_{j,\ell=1}^m$ over F. Define the following projections from $F^{m\times m}$ onto the alphabet F^m:

$$\begin{aligned}
\boldsymbol{\varphi}_1^{(\ell)} : F^{m\times m} \to F^m \,, \quad \boldsymbol{\varphi}_1^{(\ell)}(A) = (a_{j,\ell})_{j=1}^m \,, \quad 1 \le \ell \le m \,, \\
\boldsymbol{\varphi}_2^{(j)} : F^{m\times m} \to F^m \,, \quad \boldsymbol{\varphi}_2^{(j)}(A) = (a_{j,\ell})_{\ell=1}^m \,, \quad 1 \le j \le m \,.
\end{aligned}$$

We regard (column) words $\Gamma \in (F^{m\times m})^n$ also as $n \times m \times m$ arrays $(\Gamma_{i,j,\ell})_{i=1}^n{}_{j,\ell=1}^m$ over F, with the ith entry (over $F^{m\times m}$) of Γ being identified as the ith *cross-section* $\Gamma^{(i)} = (\Gamma_{i,j,\ell})_{j,\ell=1}^m$. The projections $\boldsymbol{\varphi}_b^{(j)}$, $b = 1, 2$, extend in a straightforward manner to Γ by applying them to each cross-section $\Gamma^{(i)}$, thereby resulting in $n \times m$ *slices* over F, namely,

$$\boldsymbol{\varphi}_1^{(\ell)}(\Gamma) = (\Gamma_{i,j,\ell})_{i=1}^n{}_{j=1}^m \quad \text{and} \quad \boldsymbol{\varphi}_2^{(j)}(\Gamma) = (\Gamma_{i,j,\ell})_{i=1}^n{}_{\ell=1}^m \,.$$

We study the subset (code) $\mathcal{C} \subseteq (F^{m\times m})^n$ defined by

$$\mathcal{C} = \left\{ \Gamma \in (F^{m\times m})^n \;:\; \begin{array}{l} \boldsymbol{\varphi}_1^{(\ell)}(\Gamma) \in \mathbb{C}_1^{(\ell)} \text{ for } 1 \le \ell \le m \quad \text{and} \\ \boldsymbol{\varphi}_2^{(j)}(\Gamma) \in \mathbb{C}_2^{(j)} \text{ for } 1 \le j \le m \end{array} \right\} , \tag{1}$$

where $\mathbb{C}_1^{(\ell)}$ and $\mathbb{C}_2^{(j)}$ are prescribed codes of length n over F^m. Notice that the symbols of the codes over F^m resulting from the projections in (1) intersect in particular coordinates over the alphabet F; this is in contrast with the known construction of product codes, where codewords of the constituent codes intersect on whole (particular) entries over the code alphabet—F^m in our case [2, Ch. 10], [11, pp. 274–277].

We are interested in constructions that make the overall redundancy of the code $\mathcal{C}$ in (1) as small as possible for given length n and error correction capabilities of each code $\mathbb{C}_1^{(\ell)}$ and $\mathbb{C}_2^{(j)}$. In addition to minimizing the overall redundancy, we will also be interested in a finer analysis of how the redundancy is distributed among the slices, and in characterizing the region of redundancy profiles attainable by constructions of the codes in (1).

The construction (1) is useful in applications where a certain database (represented by an $n \times m \times m$ array Γ), is accessed by different users, each of whom addresses a certain slice of the database through a noisy channel that is independent of the channels of the other users. We wish each slice to be properly protected against errors, while minimizing the overall redundancy. At the same time, we wish to be able to control the distribution of the redundancy among users, or at least guarantee each user a minimum amount of information (rate) per slice.

The investigation in this paper will focus on two special cases of particular practical and mathematical interest, which are also simpler than the most general model and are therefore more amenable to analysis. In the case of *fully-intersecting coding schemes*, we

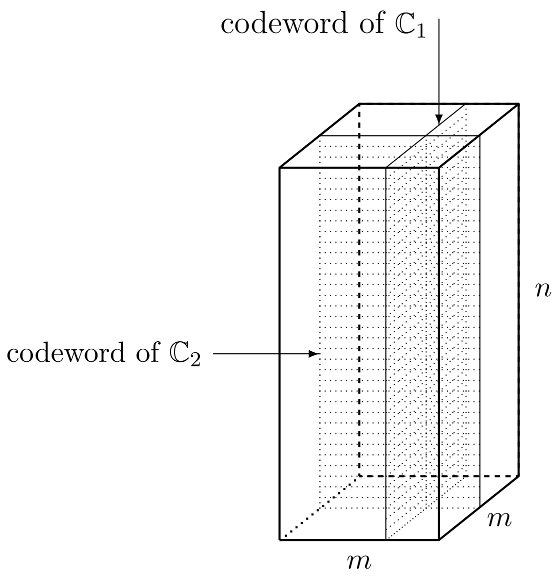

Figure 1: Fully-intersecting code array.

take $\mathbb{C}_1^{(\ell)} = \mathbb{C}_1$, independent of ℓ, and $\mathbb{C}_2^{(j)} = \mathbb{C}_2$, independent of j, $1 \le j, \ell \le m$. A typical code array in this case is shown in Figure 1.

In the case of *singly-intersecting coding schemes*, we take $\mathbb{C}_1^{(1)} = \mathbb{C}_1$, $\mathbb{C}_2^{(1)} = \mathbb{C}_2$, and $\mathbb{C}_1^{(\ell)} = \mathbb{C}_2^{(j)} = (F^m)^n$ for $1 < j, \ell \le m$. We can effectively ignore entries Γ that are indexed by (i, j, ℓ) where either $\ell > 1$ or $j > 1$, as they are unconstrained. Thus, Γ in (1) can effectively be seen as an $n \times (2m-1)$ array consisting of two $n \times m$ arrays that share one column.

Although we restrict our attention to the case where the cross-section alphabet consists of square $m \times m$ arrays, the analysis of the two cases investigated extends without difficulty, except for a more cumbersome notation, to rectangular $m_1 \times m_2$ arrays with $m_1 \neq m_2$, where each code $\mathbb{C}_1^{(\ell)}$ (respectively, $\mathbb{C}_2^{(j)}$) is now over the alphabet F^{m_1} (respectively, F^{m_2}).

The rest of the paper is organized as follows: In Section 2, we consider the simpler case of singly-intersecting coding schemes, and describe a more concrete application of these codes in a broadcast channel setting. We prove lower bounds on the overall redundancy of (1) and find trade-offs between the redundancy values along the projections $\boldsymbol{\varphi}_1^{(1)}(\Gamma)$ and $\boldsymbol{\varphi}_2^{(1)}(\Gamma)$ and the redundancy along their intersection. Then, in Section 3, we present constructions that approach, and even attain, these bounds. In Section 4, we turn to the fully-intersecting case. Here, we concentrate mainly on the overall redundancy of (1), and we show constructions based on cyclic codes. (A finer study of the attainable redundancy-per-slice regions in fully-intersecting coding schemes is an interesting topic for future work, yet it appears rather complex due to the number of parameters involved.)

2 Singly-intersecting coding schemes

2.1 Definition of the model

As mentioned in Section 1, in the case of singly-intersecting codes, we can effectively replace the alphabet $F^{m \times m}$ by F^{2m-1}. Accordingly, we regard each column word $\Gamma = (\boldsymbol{a}_i)_{i=1}^n$ as an $n \times (2m-1)$ array over F obtained when each entry $\boldsymbol{a}_i \in F^{2m-1}$ is written as a row word

$$\boldsymbol{a}_i = (a_{i,-m+1}\ a_{i,-m+2}\ \ldots\ a_{i,-1}\ a_{i,0}\ a_{i,1}\ \ldots\ a_{i,m-1}) \ , \quad a_t \in F \ .$$

Also, since the projections $\boldsymbol{\varphi}_b^{(j)}$, $b = 1, 2$, will be applied here only with $j = 1$, we will omit the superscript altogether.

For a set $\mathcal{M}$ and a function f defined over $\mathcal{M}$, we let $f(\mathcal{M})$ denote the set of images of f.

Given m, q, and a positive integer n, a *(singly-)intersecting coding scheme* of length n over F^{2m-1} is a triple $(\mathcal{E}, \mathcal{D}_1, \mathcal{D}_2)$, where $\mathcal{E}$ is an *encoding function*

$$\mathcal{E} : \mathcal{M} \rightarrow (F^{2m-1})^n \ ,$$

with the domain $\mathcal{M}$ taking the form $\mathcal{M}_0 \times \mathcal{M}_1 \times \mathcal{M}_2$ for nonempty finite sets (of *messages*) $\mathcal{M}_0$, $\mathcal{M}_1$, and $\mathcal{M}_2$, and $\mathcal{D}_1$ and $\mathcal{D}_2$ are *decoding functions*

$$\mathcal{D}_b : \boldsymbol{\varphi}_b(\mathcal{E}(\mathcal{M})) \rightarrow \mathcal{M}_0 \times \mathcal{M}_b \ , \quad b = 1, 2 \ ,$$

such that for every $(\boldsymbol{u}_0, \boldsymbol{u}_1, \boldsymbol{u}_2) \in \mathcal{M}_0 \times \mathcal{M}_1 \times \mathcal{M}_2$,

$$\mathcal{D}_b(\boldsymbol{\varphi}_b(\mathcal{E}(\boldsymbol{u}_0, \boldsymbol{u}_1, \boldsymbol{u}_2))) = (\boldsymbol{u}_0, \boldsymbol{u}_b) \ , \quad b = 1, 2 \ . \tag{2}$$

The *redundancy* of an intersecting coding scheme $(\mathcal{E}, \mathcal{D}_1, \mathcal{D}_2)$ is defined as the triple $\boldsymbol{\rho} = (\rho_0, \rho_1, \rho_2)$, where $\rho_0 = n - \log_q |\mathcal{M}_0|$ and $\rho_b = n(m-1) - \log_q |\mathcal{M}_b|$, for $b = 1, 2$. We will denote the redundancy by $\mathsf{red}(\mathcal{E}, \mathcal{D}_1, \mathcal{D}_2)$. Observe that when $\mathcal{E}(\mathcal{M})$ is regarded as a code over F, then its (conventional) redundancy—when measured in symbols of F—equals the sum $\rho_0 + \rho_1 + \rho_2$.

Remark 2.1 It follows from (2) that the mapping $\mathcal{E}$ is one-to-one over $\mathcal{M}_0 \times \mathcal{M}_1 \times \{\boldsymbol{u}_2\}$, for every fixed $\boldsymbol{u}_2 \in \mathcal{M}_2$. Hence, the sum $\rho_0 + \rho_1$ must be nonnegative. By similar arguments we get that both $\rho_0 + \rho_2$ and $\rho_0 + \rho_1 + \rho_2$ are nonnegative. On the other hand, we have the upper bounds

$$\rho_0 \leq n \quad \text{and} \quad \rho_b \leq n(m-1) \ , \quad b = 1, 2 \ . \tag{3}$$

Still, some of the individual components of $\boldsymbol{\rho} = (\rho_0, \rho_1, \rho_2)$ may be negative. □

The minimum (Hamming) distance of a code $\mathbb{C}$ over an alphabet $\mathcal{A}$ will be denoted by $\mathsf{d}_{\mathcal{A}}(\mathbb{C})$, where the subscript emphasizes the alphabet with respect to which the distance is measured.

Given q and m, let n, τ_1, and τ_2 be positive integers. We say that the real triple $\boldsymbol{\rho} = (\rho_0, \rho_1, \rho_2)$ is *achievable* if there exists an intersecting coding scheme $(\mathcal{E} : \mathcal{M} \to (F^{2m-1})^n, \mathcal{D}_1, \mathcal{D}_2)$ such that the following conditions hold:

(A1) $\mathsf{red}(\mathcal{E}, \mathcal{D}_1, \mathcal{D}_2) \le \boldsymbol{\rho}$, where the inequality holds component by component, and

(A2) $\mathsf{d}_{F^m}(\boldsymbol{\varphi}_b(\mathcal{E}(\mathcal{M}))) > \tau_b$ for $b = 1, 2$.

The set of all achievable triples $\boldsymbol{\rho}$ (for q, m, n, τ_1, and τ_2) will be called the *achievable redundancy region* and will be denoted by $\mathbb{A}_q(m, n, \tau_1, \tau_2)$.

Letting the code $\mathbb{C}_b \subseteq (F^m)^n$ be given by the set $\boldsymbol{\varphi}_b(\mathcal{E}(\mathcal{M}))$ for $b = 1, 2$, the encoding function $\mathcal{E}$ induces a one-to-one mapping $\hat{\mathcal{E}} : \mathcal{M} \to \mathbb{C}_1 \times \mathbb{C}_2$, which sends each triple $(\boldsymbol{u}_0, \boldsymbol{u}_1, \boldsymbol{u}_2) \in \mathcal{M}$ to a pair of codewords $(\boldsymbol{c}_1, \boldsymbol{c}_2) \in \mathbb{C}_1 \times \mathbb{C}_2$, where

$$\boldsymbol{c}_b = \boldsymbol{\varphi}_b(\mathcal{E}(\boldsymbol{u}_0, \boldsymbol{u}_1, \boldsymbol{u}_2)) , \quad b = 1, 2 .$$

Condition (A2) sets a lower bound on the minimum distance of the code $\mathbb{C}_b$.

Our study in Sections 2 and 3 aims at determining the achievable redundancy region $\mathbb{A}_q(m, n, \tau_1, \tau_2)$. To motivate the setting, we describe first in Section 2.2 a communication problem where intersecting coding schemes can be applied.

2.2 Application to broadcast channels

A *(probabilistic) broadcast channel* $\mathbb{B}$ is defined by the quadruple $(\mathrm{I}, \Omega_1, \Omega_2, \mathsf{Prob})$, where I stands for an input alphabet, Ω_1 are Ω_2 are output alphabets, and Prob is a conditional probability distribution

$$\mathsf{Prob}\{\, (\boldsymbol{y}_1, \boldsymbol{y}_2) \text{ received} \mid \boldsymbol{x} \text{ transmitted} \,\}$$

defined for every triple $(\boldsymbol{x}, \boldsymbol{y}_1, \boldsymbol{y}_2) \in \bigcup_{\ell \ge 0} (\mathrm{I}^\ell \times \Omega_1^\ell \times \Omega_2^\ell)$.

A *broadcast coding scheme* of length n for $\mathbb{B}$ is a triple $(\mathcal{E}, \mathcal{D}_1, \mathcal{D}_2)$, where $\mathcal{E}$ is an encoding function

$$\mathcal{E} : \mathcal{M} \to \mathrm{I}^n ,$$

with the domain $\mathcal{M}$ taking the form $\mathcal{M}_0 \times \mathcal{M}_1 \times \mathcal{M}_2$ for nonempty finite sets $\mathcal{M}_0$, $\mathcal{M}_1$, and $\mathcal{M}_2$, and $\mathcal{D}_1$ and $\mathcal{D}_2$ are decoding functions

$$\mathcal{D}_b : \Omega_b^n \to \mathcal{M}_0 \times \mathcal{M}_b , \quad b = 1, 2$$

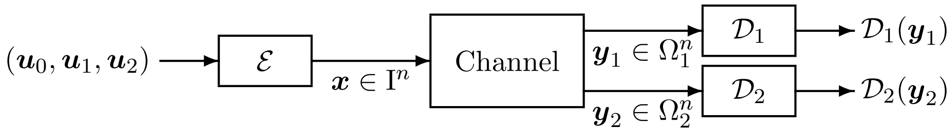

Figure 2: Broadcast channel, with encoding function $\mathcal{E}$ and decoding functions $\mathcal{D}_1$ and $\mathcal{D}_2$.

(see Figure 2).

The *rate* of a broadcast coding scheme is given by a triple (R_0, R_1, R_2), where

$$R_b = \frac{\log_2 |\mathcal{M}_b|}{n}, \quad b = 0, 1, 2 .$$

In the common application of broadcast channels, a source wishes to transmit to end user $b \in \{1, 2\}$ a message out of a finite set $\mathcal{M}_b$ and a common message to both users from $\mathcal{M}_0$. The transmission is carried out synchronously to the two end users over n time slots through the channel, which effectively consists of two sub-channels, each associated with one end user. Each user can see the output of its sub-channel only. The design goal of the broadcast coding scheme is to guarantee reliable communication between the source and each end user, at the highest possible rate.

Given a broadcast channel $\mathbb{B} = (\mathrm{I}, \Omega_1, \Omega_2, \mathsf{Prob})$ and a broadcast coding scheme $(\mathcal{E}, \mathcal{D}_1, \mathcal{D}_2)$ of length n for $\mathbb{B}$, the *decoding error probability* of the scheme is defined by the maximum probability that either $\mathcal{D}_1(\boldsymbol{y}_1) \neq (\boldsymbol{u}_0, \boldsymbol{u}_1)$ or $\mathcal{D}_2(\boldsymbol{y}_2) \neq (\boldsymbol{u}_0, \boldsymbol{u}_2)$, conditioned on $(\boldsymbol{u}_0, \boldsymbol{u}_1, \boldsymbol{u}_2)$ being transmitted, where the maximum is taken over all triples $(\boldsymbol{u}_0, \boldsymbol{u}_1, \boldsymbol{u}_2)$ in the domain $\mathcal{M}$ of $\mathcal{E}$. A real triple (R_0, R_1, R_2) is called *achievable* for $\mathbb{B}$ if there exists a sequence of broadcast coding schemes for $\mathbb{B}$ with rates (R_0, R_1, R_2) such that the decoding error probability vanishes as the code length n goes to infinity. The *capacity region* of $\mathbb{B}$ is the closure (over the reals) of the set of achievable rates. See [3]–[5] and [6, §14.6].

Let Ω denote the alphabet $F^m \cup \{\mathsf{x}\}$, and consider the following broadcast channel $\mathbb{B}_q(m, n, \tau_1, \tau_2) = (F^{2m-1}, \Omega, \Omega, \mathsf{Prob})$. The channel $\mathbb{B}_q(m, n, \tau_1, \tau_2)$ consists of $2m-1$ lines, where each line conveys one symbol of F. The input to the channel at each time slot is an element of F^{2m-1}, which is transmitted synchronously in parallel through the $2m-1$ lines. The two end users see lines $0, 1, 2, \ldots, m-1$ and $0, -1, -2, \ldots, -(m-1)$, respectively (i.e., line 0 belongs to both user sub-channels); thus, at each time slot, each user sees an element of F^m. Yet, each user may be disconnected (i.e., blacked-out) from the lines at certain time slots, independently of the other user. The special symbol 'x' will stand for an erasure: it will mark the 'output' of the channel during disconnection. The conditional probability distribution Prob is such that for prescribed nonnegative integers τ_1 and τ_2, each user b is disconnected during at most τ_b slots within a time frame of n slots (in practice, this is typically guaranteed only within a certain high probability, but we assume for simplicity that this probability is 1).

The following result makes the connection between intersecting coding schemes and the design problem of broadcast coding schemes for the channel $\mathbb{B}_q(m, n, \tau_1, \tau_2)$.

Proposition 2.1 *Suppose that a source transmits through $\mathbb{B}_q(m, n, \tau_1, \tau_2)$ messages from sets $\mathcal{M}_1$ and $\mathcal{M}_2$ to end users 1 and 2, respectively, and a common message to both users from a set $\mathcal{M}_0$. Then both users will be able to recover every transmitted message, if and only if there exists a broadcast coding scheme $(\mathcal{E}, \mathcal{D}'_1, \mathcal{D}'_2)$ of length n for $\mathbb{B}_q(m, n, \tau_1, \tau_2)$ (with $\mathcal{M} = \mathcal{M}_0 \times \mathcal{M}_1 \times \mathcal{M}_2$ being the domain of $\mathcal{E}$), such that the following two conditions hold:*

(B1) *Letting $\mathcal{D}_b$ be the restriction of $\mathcal{D}'_b$ to the domain F^n, the triple $(\mathcal{E}, \mathcal{D}_1, \mathcal{D}_2)$ is an intersecting coding scheme of length n over F^{2m-1}.*

(B2) $\mathsf{d}_{F^m}(\boldsymbol{\varphi}_b(\mathcal{E}(\mathcal{M}))) > \tau_b$ *for $b = 1, 2$.*

(The 'only if' part holds if each user b can be disconnected during no less than τ_b slots.)

Proof. Let $\boldsymbol{c}_b = \boldsymbol{\varphi}_b(\mathcal{E}(\boldsymbol{u}_0, \boldsymbol{u}_1, \boldsymbol{u}_2))$ for $b = 1, 2$. Condition (B1) is necessary and sufficient to allow each user $b \in \{1, 2\}$ to recover $\boldsymbol{u}_0$ and $\boldsymbol{u}_b$ from the (erasure-free) word $\boldsymbol{c}_b$, and condition (B2) is necessary and sufficient to correct all patterns of up to τ_b erasures that $\boldsymbol{c}_b$ may be subject to. $\square$

It follows from Proposition 2.1 that a rate triple (R_0, R_1, R_2) is achievable for the channel $\mathbb{B}_q(m, n, \tau_1, \tau_2)$ whenever $(\rho_0, \rho_1, \rho_2) \in \mathbb{A}_q(m, n, \tau_1, \tau_2)$, where $\rho_0 = n(1 - (R_0/\log_2 q))$ and $\rho_b = n((m-1 - (R_b/\log_2 q)), b = 1, 2$.

2.3 Systematic encoding schemes

Intersecting coding schemes are best visualized in the special case where a copy the encoded information $(\boldsymbol{u}_0, \boldsymbol{u}_1, \boldsymbol{u}_2)$ is embedded explicitly in the generated array $\Gamma = \mathcal{E}(\boldsymbol{u}_0, \boldsymbol{u}_1, \boldsymbol{u}_2)$. We then say that the coding scheme is *systematic*. We formalize this coding model next.

Henceforth, we index the entries of an $n \times (2m-1)$ array $\Gamma = (\Gamma_{i,j})$ in $(F^{2m-1})^n$ with pairs from the set

$$\mathcal{I}_{m,n} = \{(i, j) \,:\, 1 \le i \le n \,,\; |j| < m\} \,.$$

Given an ordered subset $\mathcal{X} \subseteq \mathcal{I}_{m,n}$, let $(\Gamma)_{\mathcal{X}}$ denote the word of length $|\mathcal{X}|$ over F that consists of the entries of Γ that are indexed by $\mathcal{X}$.

Let $\mathcal{C}$ be a subset of $(F^{2m-1})^n$ of size q^k for some integer k. We say that $\mathcal{C}$ is systematic if there exists an ordered subset $\mathcal{X}$ of $\mathcal{I}_{m,n}$ of size k such that

$$\{(\Gamma)_{\mathcal{X}}\}_{\Gamma \in \mathcal{C}} = F^k \,.$$

We call $\mathcal{X}$ an *information locator set* of $\mathcal{C}$. In particular, if $F = \mathrm{GF}(q)$ and $\mathcal{C}$ is a linear space over F then $\mathcal{C}$ is necessarily systematic.

A function $f : F^k \to (F^{2m-1})^n$ is called systematic if there is an ordered subset $\mathcal{X}$ of $\mathcal{I}_{m,n}$ of size k such that the function $F^k \to F^k$, which maps every element $\boldsymbol{u} \in F^k$ to $(f(\boldsymbol{u}))_{\mathcal{X}}$, is the identity mapping.

An encoding function $\mathcal{E} : \mathcal{M} \to (F^{2m-1})^n$ in an intersecting coding scheme $(\mathcal{E}, \mathcal{D}_1, \mathcal{D}_2)$ is called systematic if $\mathcal{M}_b = F^{k_b}$ for integers k_b, $b = 0, 1, 2$, and the mapping $F^{k_0+k_1+k_2} \to (F^{2m-1})^n$, defined by $(\boldsymbol{u}_0 \,|\, \boldsymbol{u}_1 \,|\, \boldsymbol{u}_2) \mapsto \mathcal{E}(\boldsymbol{u}_0, \boldsymbol{u}_1, \boldsymbol{u}_2)$, is systematic (hereafter $(\cdot|\cdot)$ denotes concatenation); note that in this case, the redundancy $\boldsymbol{\rho} = (\rho_0, \rho_1, \rho_2)$ is related to the values k_b by

$$\rho_0 = n - k_0 \quad \rho_b = n(m-1) - k_b \ \text{ for } \ b = 1, 2 \ .$$

The respective information locator set $\mathcal{X}$ indexes the *information symbols* in an array $\Gamma = \mathcal{E}(\boldsymbol{u}_0, \boldsymbol{u}_1, \boldsymbol{u}_2)$ in $\mathcal{E}(\mathcal{M})$, while $\mathcal{I}_{m,n} \backslash \mathcal{X}$ indexes the *check symbols*. The set $\mathcal{X}$ can be partitioned into three subsets $\mathcal{X}_0$, $\mathcal{X}_1$, and $\mathcal{X}_2$, where $|\mathcal{X}_b| = k_b$ and $(\Gamma)_{\mathcal{X}_b} = \boldsymbol{u}_b$, $b = 0, 1, 2$.

Figure 3 displays a typical array $\Gamma \in \mathcal{E}(\mathcal{M})$ for the case where $\mathcal{E}$ is systematic. The m leftmost columns in Γ form the sub-array $\boldsymbol{\varphi}_1(\Gamma)$, and the m rightmost columns form the sub-array $\boldsymbol{\varphi}_2(\Gamma)$ (both sub-arrays share the center column of Γ). The shaded area represent the locations of check symbols within Γ. From the layout of the index sets $\mathcal{X}_0$, $\mathcal{X}_1$, and $\mathcal{X}_2$ in Figure 3 we get that for $b = 1, 2$, both $\boldsymbol{u}_0$ and $\boldsymbol{u}_b$ are embedded in the sub-array $\boldsymbol{\varphi}_b(\Gamma)$, thereby guaranteeing (2). (While such embedding is sufficient to obtain (2), it is not necessary.)

Example 2.1 Suppose there exists a maximum distance separable (MDS) code $\mathcal{C}_0$ of length n and minimum distance $\tau{+}1$ (and size $q^{n-\tau}$) over F; for example, such a code exists when $F = \mathrm{GF}(q)$ and $n \le q{+}1$ [14, Ch. 11]. A MDS code always has an (ordinary) systematic encoder, where the $n{-}\tau$ information symbols can be placed in *any* prescribed locations within the generated codeword.

We next show an intersecting coding scheme $(\mathcal{E}, \mathcal{D}_1, \mathcal{D}_2)$ that satisfies conditions (A1)–(A2) with respect to the triple

$$\boldsymbol{\rho}^* = (\rho_0^*, \rho_1^*, \rho_2^*) = (\tau, (m{-}1)\tau, (m{-}1)\tau) \ .$$

Let $k_0 = n{-}\rho_0^* = n{-}\tau = \log_q |\mathcal{C}_0|$ and $\mathcal{M}_0 = F^{k_0}$, and for $b = 1, 2$ let $k_b = n(m{-}1) - \rho_b^* = (m{-}1)(n{-}\tau)$ and $\mathcal{M}_b = F^{k_b}$. The encoding function $\mathcal{E} : \mathcal{M} \to (F^{2m-1})^n$ will be systematic, with the information locator set $\mathcal{X}$ partitioned into the subsets

$$\mathcal{X}_0 = \{(i, 0) \,:\, 1 \le i \le k_0\}$$

and

$$\mathcal{X}_b = \{(i, j) \,:\, 1 \le i \le k_0 \ , \ 0 < (-1)^b j < m\} \ , \quad b = 1, 2 \ .$$

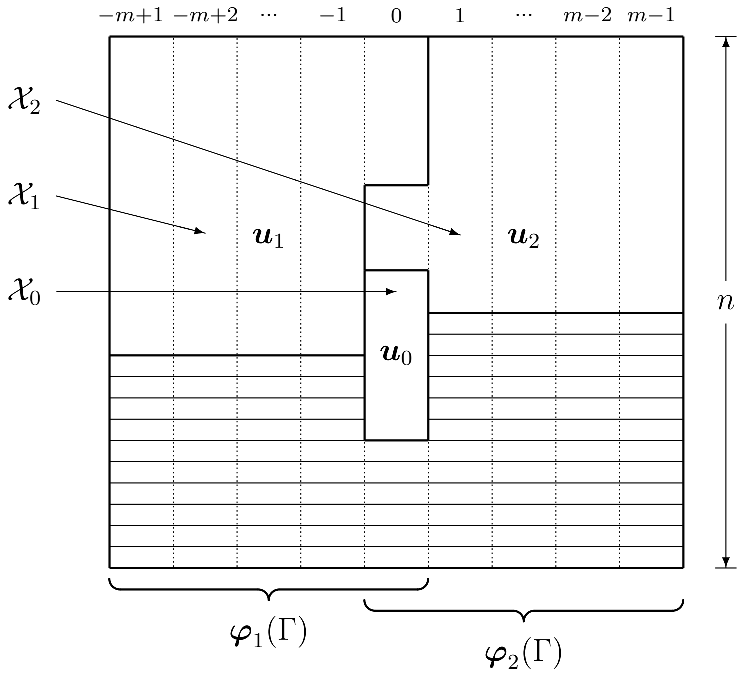

Figure 3: Array $\Gamma \in \mathcal{E}(\mathcal{M})$ in a systematic intersecting coding scheme.

For each possible contents $(\boldsymbol{u}_0 \,|\, \boldsymbol{u}_1 \,|\, \boldsymbol{u}_2)$ of the information symbols, the mapping $\mathcal{E}$ computes check symbols, which are indexed by $\mathcal{I}_{m,n} \setminus \mathcal{X}$, to form an $n \times (2m-1)$ array Γ in which each column is a codeword of $\mathcal{C}_0$; such computation can be implemented using an (ordinary) systematic encoder of $\mathcal{C}_0$. The existence of respective decoding functions $\mathcal{D}_1$ and $\mathcal{D}_2$ that satisfy (2) is straightforward, and it is also easy to verify that conditions (A1)–(A2) hold; specifically,

$$\mathsf{red}(\mathcal{E}, \mathcal{D}_1, \mathcal{D}_2) = \boldsymbol{\rho}^* = (\tau, (m-1)\tau, (m-1)\tau)$$

and

$$\mathsf{d}_{F^m}(\boldsymbol{\varphi}_b(\mathcal{E}(\mathcal{M}))) = \tau_b + 1 \;, \quad b = 1, 2 \;.$$

$\square$

For a subset $\mathcal{C} \subseteq (F^{2m-1})^n$, we denote by $\mathrm{red}(\mathcal{C})$ the (ordinary) redundancy of $\mathcal{C}$, when measured in symbols of F; namely,

$$\mathrm{red}(\mathcal{C}) = n(2m-1) - \log_q |\mathcal{C}| \;.$$

Proposition 2.2 *Let $\mathcal{C}$ be a systematic subset of $(F^{2m-1})^n$. There exists a systematic intersecting coding scheme $(\mathcal{E} : \mathcal{M} \to (F^{2m-1})^n, \mathcal{D}_1, \mathcal{D}_2)$ with redundancy (ρ_0, ρ_1, ρ_2) such that $\mathcal{E}(\mathcal{M}) = \mathcal{C}$ and $\rho_0 + \rho_1 + \rho_2 = \mathrm{red}(\mathcal{C})$.*

The proof of the proposition is straightforward, and is given in Appendix A for completeness. We also show in that appendix that there are cases of non-systematic sets $\mathcal{C} \subseteq (F^{2m-1})^n$ such that no (systematic or non-systematic) intersecting coding scheme $(\mathcal{E} : \mathcal{M} \to (F^{2m-1})^n, \mathcal{D}_1, \mathcal{D}_2)$ satisfies $\mathcal{E}(\mathcal{M}) = \mathcal{C}$.

2.4 Bounds

The following is a Singleton-like bound for intersecting coding schemes.

Theorem 2.3 *If $\boldsymbol{\rho} = (\rho_0, \rho_1, \rho_2)$ is in $\mathbb{A}_q(m, n, \tau_1, \tau_2)$ then*

$$\rho_0 + \rho_b \geq m\tau_b \ , \quad b = 1, 2 \tag{4}$$

and

$$\rho_0 + \rho_1 + \rho_2 \geq (2m{-}1)\tau \ , \tag{5}$$

where $\tau = (\tau_1 + \tau_2)/2$.

Proof. Given $\boldsymbol{\rho} \in \mathbb{A}_q(m, n, \tau_1, \tau_2)$, let the intersecting coding scheme $(\mathcal{E} : \mathcal{M} \to (F^{2m-1})^n, \mathcal{D}_1, \mathcal{D}_2)$ satisfy conditions (A1)–(A2). Our proof will be based on the simple observation that the (ordinary) redundancy of any given code over F must be at least the largest possible number of erased symbols of F that the code can handle.

Let $\mathcal{C}$ denote the set $\mathcal{E}(\mathcal{M})$. It follows from condition (A2) that each code $\boldsymbol{\varphi}_b(\mathcal{C})$ can recover correctly $m\tau_b$ erased symbols of F that result from τ_b erased symbols of F^m. This yields (4).

Next we turn to the code $\mathcal{C} \subseteq (F^{2m-1})^n$ and consider an $n \times (2m{-}1)$ array Γ (over F) in $\mathcal{C}$. Then τ_1 erased rows in $\boldsymbol{\varphi}_1(\Gamma)$ and τ_2 erased rows in $\boldsymbol{\varphi}_2(\Gamma)$ form a pattern that consists of at least

$$(m{-}1)(\tau_1 + \tau_2) + \max\{\tau_1, \tau_2\}$$

erased symbols of F in Γ. Therefore,

$$\rho_0 + \rho_1 + \rho_2 \geq (m{-}1)(\tau_1 + \tau_2) + \max\{\tau_1, \tau_2\} \geq (2m{-}1)\tau \ ,$$

thus yielding (5). □

Let ρ denote the sum $\rho_1 + \rho_2$. Inequalities (4)–(5) define a region in the (ρ_0, ρ) plane, as marked by the lower shaded piecewise-linear line in Figure 4. The boundary of the region is formed by the two straight lines defined by the equations

$$\rho = 2m\tau - 2\rho_0 \tag{6}$$

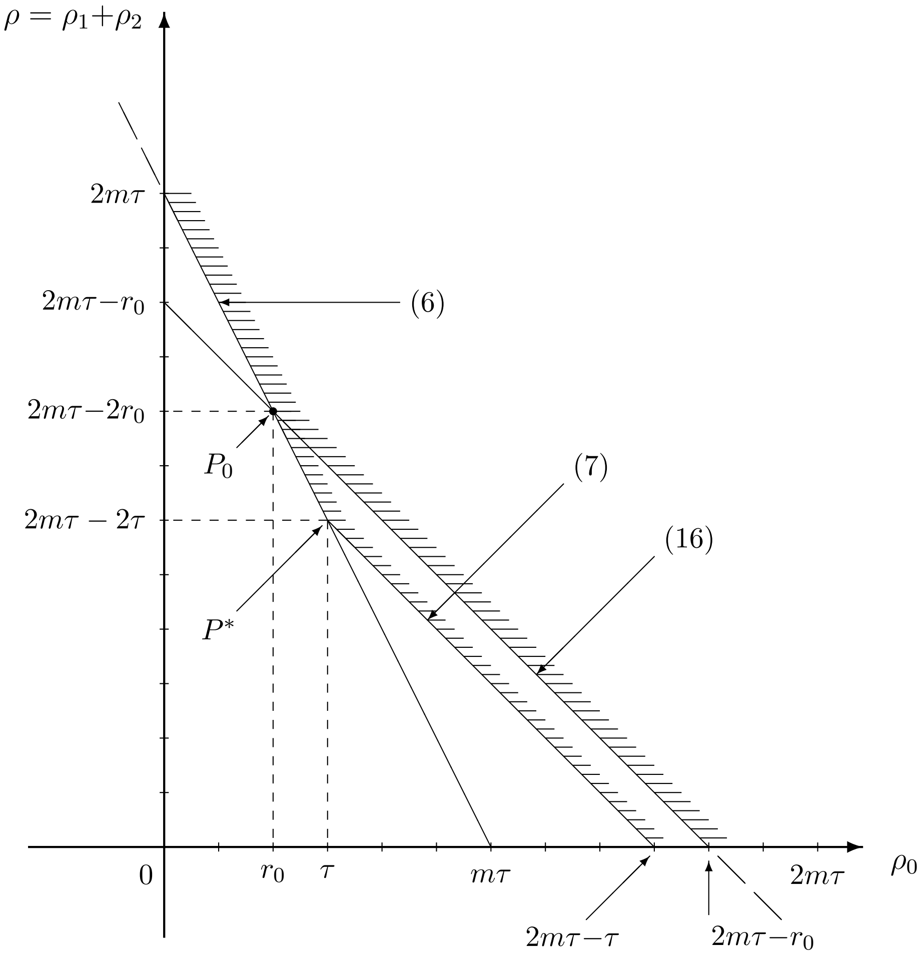

Figure 4: Bounds on the achievable redundancy region.

and

$$\rho = (2m-1)\tau - \rho_0\ . \tag{7}$$

The triple $\boldsymbol{\rho}^* = (\tau, (m-1)\tau, (m-1)\tau)$ in Example 2.1 satisfies both (4) and (5) with equality and, thus, it corresponds to the intersection point P^* of these two lines.

In the remaining part of this section, we demonstrate how the boundary defined by Equations (6) and (7) can in fact be attained for $\tau = \tau_1 = \tau_2$, whenever there exists a MDS code of length n and minimum distance τ over F. The length n of the respective intersecting coding scheme will then be bounded from above by the maximum length of any MDS code over F whose minimum distance is at least τ.

We will make use of the following lemma, the proof of which can be found in Appendix B.

Lemma 2.4 *Let $\boldsymbol{\rho} = (\rho_0, \rho_1, \rho_2)$ be an integer triple. If $\boldsymbol{\rho}$ belongs to $\mathbb{A}_q(m, n, \tau_1, \tau_2)$, then* *so do*

$$\boldsymbol{\rho}' = (\rho_0 - \theta, \rho_1 + \theta, \rho_2 + \theta)$$

and

$$\boldsymbol{\rho}'' = (\rho_0 + \theta_1 + \theta_2, \rho_1 - \theta_1, \rho_2 - \theta_2) ,$$

for any integer θ (respectively, θ_1 and θ_2) such that $\boldsymbol{\rho}'$ (respectively, $\boldsymbol{\rho}''$) satisfies (3).

The next proposition identifies a range of parameters for which the bounds of Theorem 2.3 are tight.

Proposition 2.5 *Let m, n, and τ be such that there exists a MDS code of length n and minimum distance τ over F. An integer triple $\boldsymbol{\rho} = (\rho_0, \rho_1, \rho_2)$ that satisfies (3) belongs to $\mathbb{A}_q(m, n, \tau, \tau)$ if (and only if) it satisfies both (4) and (5).*

Proof. Let $\boldsymbol{\rho} = (\rho_0, \rho_1, \rho_2)$ be an integer triple that satisfies (3), (4), and (5), and suppose that $\rho_0 \le \tau$ (i.e., the respective point $(\rho_0, \rho_1{+}\rho_2)$ lies to the left of P^* in Figure 4). Apply Lemma 2.4 to the triple $\boldsymbol{\rho}^* = (\tau, (m{-}1)\tau, (m{-}1)\tau)$ in Example 2.1, taking $\theta = \tau - \rho_0$, thereby yielding that the triple $\boldsymbol{\rho}' = (\rho_0, m\tau{-}\rho_0, m\tau{-}\rho_0)$ is achievable; hence, so is the triple $\boldsymbol{\rho} \ge \boldsymbol{\rho}'$, where the (component by component) inequality follows from (4).

Next, suppose that $\rho_0 \ge \tau$ (this corresponds to the region to the right of P^* in Figure 4). Obviously, $\boldsymbol{\rho}$ is achievable if $\boldsymbol{\rho} \ge \boldsymbol{\rho}^*$. Hence, we assume now that ρ_1 (say) is less than $(m{-}1)\tau$. Define

$$\theta_1 = (m{-}1)\tau - \rho_1 \qquad \text{and} \qquad \theta_2 = \rho_0 + \rho_1 - m\tau \ .$$

We have $\theta_1 > 0$ from assuming that $\rho_1 < (m{-}1)\tau$, and $\theta_2 \ge 0$ from (4). We now apply Lemma 2.4 to $\boldsymbol{\rho}^*$ with these values of θ_1 and θ_2 to conclude that

$$\boldsymbol{\rho} \ge \boldsymbol{\rho}'' = (\rho_0, \rho_1, (2m{-}1)\tau{-}\rho_0{-}\rho_1)$$

is achievable, where the inequality follows from (5). □

Proposition 2.5 applies only to relatively small values of n (most likely, $n \le q{+}1$ [14, Ch. 11]), as n therein is the length of some MDS code over F. In the next section, we relax the requirement on n so that it can be the length of a MDS code over (the larger alphabet) F^m, at the expense of requiring a stronger inequality in (5).

3 Construction of singly-intersecting coding schemes

Our strategy in obtaining intersecting coding schemes will be as follows. We construct systematic sets $\mathcal{C} \subseteq (F^{2m-1})^n$ (with the smallest possible redundancy $\mathrm{red}(\mathcal{C})$) such that for $b = 1, 2$, each set $\boldsymbol{\varphi}_b(\mathcal{C})$ is a (largest possible) sub-code of a MDS code over F^m with $\mathsf{d}_{F^m}(\boldsymbol{\varphi}_b(\mathcal{C})) > \tau$. We then apply Proposition 2.2 to obtain an intersecting coding scheme $(\mathcal{E} : \mathcal{M} \to (F^{2m-1})^n, \mathcal{D}_1, \mathcal{D}_2)$ such that $\mathcal{E}(\mathcal{M}) = \mathcal{C}$. Lemma 2.4 will subsequently expand this construction into a whole region of achievable triples.

3.1 Construction tools

We assume henceforth that F is the finite field $\mathrm{GF}(q)$ and identify F^m with a representation of the extension field $\Phi = \mathrm{GF}(q^m)$ with respect to some fixed basis $\boldsymbol{\omega} = (\omega_0\ \omega_1\ \ldots\ \omega_{m-1})^T$ of Φ over F. Specifically, each vector $\boldsymbol{v}$ in F^m represents the element $\boldsymbol{v} \cdot \boldsymbol{\omega}$ in Φ. Accordingly, we will find it convenient to replace the projections $\boldsymbol{\varphi}_b : F^{2m-1} \to F^m$ with the mappings $\varphi_b : F^{2m-1} \to \Phi$ defined by

$$\varphi_b(\boldsymbol{a}) = \boldsymbol{\varphi}_b(\boldsymbol{a})\boldsymbol{\omega} \ , \quad b = 1, 2 \ .$$

Denote by $\mathrm{Tr} : \Phi \to F$ the trace operator $\mathrm{Tr} : x \mapsto \sum_{\ell=0}^{m-1} x^{q^\ell}$ [10, p. 54]. We extend the definition of the operator to vectors $\boldsymbol{y} = (y_i)_{i=1}^n$ over Φ so that $\mathrm{Tr}(\boldsymbol{y}) = (\mathrm{Tr}(y_i))_{i=1}^n$, and to subsets $\mathbb{C} \subseteq \Phi^n$ by

$$\mathrm{Tr}(\mathbb{C}) = \{\mathrm{Tr}(\boldsymbol{c}) \,:\, \boldsymbol{c} \in \mathbb{C}\} \subseteq F^n \ .$$

Without real loss of generality, we will assume that the basis $\boldsymbol{\omega}$ is selected so that $\mathrm{Tr}(\omega_0) = 1$ and $\mathrm{Tr}(\omega_j) = 0$ for $1 \leq j < m$ (such a basis always exists).

Given a linear code $\mathbb{C}$ over Φ, we will use the standard notation $[n, k, d]$ to specify the parameters of $\mathbb{C}$ (length n, dimension k over Φ, and minimum distance $d = \mathsf{d}_\Phi(\mathbb{C})$). The dual code of $\mathbb{C}$ will be denoted by $\mathbb{C}^\perp$, and the dimension of an affine space $\mathcal{B}$ over F will be denoted by $\dim(\mathcal{B})$.

We will make use of the following two lemmas. The first lemma combines Problem 33 in [14, p. 26] with Corollary 1 in [13, p. 204], and the second lemma is taken from [14, p. 208].

Lemma 3.1 *For every two linear codes $\mathcal{C}_1$ and $\mathcal{C}_2$ of the same length over F,*

$$\mathrm{red}(\mathcal{C}_1^\perp \cap \mathcal{C}_2^\perp) = \dim(\mathcal{C}_1) + \dim(\mathcal{C}_2) - \dim(\mathcal{C}_1 \cap \mathcal{C}_2) \ . \tag{8}$$

Lemma 3.2 *For every linear code $\mathbb{C}$ over Φ,*

$$(\mathrm{Tr}(\mathbb{C}))^\perp = \mathbb{C}^\perp \cap F^n \ . \tag{9}$$

The code $\mathbb{C}^\perp \cap F^n$ is usually referred to in the literature as the *sub-field sub-code* of $\mathbb{C}^\perp$.

Proposition 3.3 *For $b = 1, 2$, let $\mathbb{C}_b$ be a linear $[n, n-r_b]$ code over Φ and let $\mathcal{C} \subseteq (F^{2m-1})^n$ be the linear space over F defined by*

$$\mathcal{C} = \left\{ \Gamma \in (F^{2m-1})^n \;:\; \varphi_b(\Gamma) \in \mathbb{C}_b \;,\; b = 1, 2 \right\} \;. \tag{10}$$

Then

$$\mathrm{red}(\mathcal{C}) = m(r_1 + r_2) - r_0 \;,$$

where

$$r_0 = \dim\left(\mathbb{C}_1^\perp \cap \mathbb{C}_2^\perp \cap F^n\right) \;.$$

Proof. Let

$$\Gamma = (\Gamma_{-m+1}\, \Gamma_{-m+2}\; \ldots\; \Gamma_0\, \Gamma_1\; \ldots\; \Gamma_{m-1})$$

be an array in $(F^{2m-1})^n$, where Γ_j denotes the column of Γ that is indexed by j. Clearly,

$$\varphi_1(\Gamma) = \sum_{j=0}^{m-1} \Gamma_{-j}\omega_j \quad \text{and} \quad \varphi_2(\Gamma) = \sum_{j=0}^{m-1} \Gamma_j\omega_j \;.$$

By the linearity of the trace operator over F and the choice of the basis $\boldsymbol{\omega}$ we have,

$$\mathrm{Tr}\left(\varphi_1(\Gamma)\right) = \mathrm{Tr}\left(\varphi_2(\Gamma)\right) = \Gamma_0 \;. \tag{11}$$

For $b = 1, 2$ and an element $\boldsymbol{z} \in \mathrm{Tr}(\mathbb{C}_b)$, define the affine spaces

$$\mathbb{C}_b(\boldsymbol{z}) = \{\boldsymbol{c} \in \mathbb{C}_b \;:\; \mathrm{Tr}(\boldsymbol{c}) = \boldsymbol{z}\} \tag{12}$$

and

$$\mathcal{B}_b(\boldsymbol{z}) = \left\{ \Gamma \in (F^{2m-1})^n \;:\; \varphi_b(\Gamma) \in \mathbb{C}_b(\boldsymbol{z}) \right\} \tag{13}$$

over F (note that the center column of every array in $\mathcal{B}_b(\boldsymbol{z})$ equals $\boldsymbol{z}$). Now, $\mathbb{C}_b(\mathbf{0})$ is the kernel of the mapping $\mathrm{Tr} : \mathbb{C}_b \to F^n$ obtained when restricting $\mathrm{Tr} : \Phi^n \to F^n$ to the domain $\mathbb{C}_b$; therefore, for every $\boldsymbol{z} \in \mathrm{Tr}(\mathbb{C}_b)$, the dimension of $\mathbb{C}_b(\boldsymbol{z})$ is given by

$$\dim(\mathbb{C}_b(\boldsymbol{z})) = \dim(\mathbb{C}_b(\mathbf{0})) = \dim(\mathbb{C}_b) - \dim\left(\mathrm{Tr}(\mathbb{C}_b)\right) \;, \tag{14}$$

and for every $\boldsymbol{z} \in \mathrm{Tr}(\mathbb{C}_1) \cap \mathrm{Tr}(\mathbb{C}_2)$,

$$\dim\left(\mathcal{B}_1(\boldsymbol{z}) \cap \mathcal{B}_2(\boldsymbol{z})\right) = \dim(\mathbb{C}_1(\mathbf{0})) + \dim(\mathbb{C}_2(\mathbf{0})) \;. \tag{15}$$

If follows from the definitions of $\mathcal{C}$ and $\mathcal{B}_b(\boldsymbol{z})$ in (10) and (13) that when $\boldsymbol{z}$ ranges over the elements of $\mathrm{Tr}(\mathbb{C}_1) \cap \mathrm{Tr}(\mathbb{C}_2)$, the respective sets $\mathcal{B}_1(\boldsymbol{z}) \cap \mathcal{B}_2(\boldsymbol{z})$ form a partition of $\mathcal{C}$. Therefore,

$$\begin{aligned}
\dim(\mathcal{C}) &\overset{(15)}{=} \dim(\mathrm{Tr}(\mathbb{C}_1) \cap \mathrm{Tr}(\mathbb{C}_2)) + \dim(\mathbb{C}_1(\mathbf{0})) + \dim(\mathbb{C}_2(\mathbf{0})) \\
&\overset{(14)}{=} \dim(\mathrm{Tr}(\mathbb{C}_1) \cap \mathrm{Tr}(\mathbb{C}_2)) + \dim(\mathbb{C}_1) - \dim\left(\mathrm{Tr}(\mathbb{C}_1)\right) + \dim(\mathbb{C}_2) - \dim\left(\mathrm{Tr}(\mathbb{C}_2)\right) \\
&\overset{(8)}{=} \dim(\mathbb{C}_1) + \dim(\mathbb{C}_2) - \mathrm{red}\left((\mathrm{Tr}(\mathbb{C}_1))^\perp \cap (\mathrm{Tr}(\mathbb{C}_2))^\perp\right) \;,
\end{aligned}$$

and, so,

$$\begin{aligned}
\mathrm{red}(\mathcal{C}) &= n(2m-1) - \dim(\mathcal{C}) \\
&\overset{(9)}{=} n(2m-1) - \dim(\mathbb{C}_1) - \dim(\mathbb{C}_2) + \mathrm{red}\left((\mathbb{C}_1^\perp \cap F^n) \cap (\mathbb{C}_2^\perp \cap F^n)\right) \\
&= \mathrm{red}(\mathbb{C}_1) + \mathrm{red}(\mathbb{C}_2) - \dim\left(\mathbb{C}_1^\perp \cap \mathbb{C}_2^\perp \cap F^n\right) \\
&= m(r_1 + r_2) - r_0 \ ,
\end{aligned}$$

as claimed. $\square$

3.2 Construction based on MDS codes over GF(q^m)

In applying Proposition 3.3, we will select the codes $\mathbb{C}_b$ so that $\mathsf{d}_\Phi(\mathbb{C}_b) > \tau_b$; this, in turn, will guarantee condition (A2). In addition, to minimize $\mathrm{red}(\mathcal{C})$, we should select the codes $\mathbb{C}_b$ so that $m(r_1 + r_2) - r_0$ is minimized; from the definition of r_0 one can see that

$$0 \le r_0 \le \min\{r_1, r_2\} \ .$$

Hereafter, we restrict ourselves to the symmetric case where $\tau_1 = \tau_2 = \tau$. For $b = 1, 2$, let $\mathbb{C}_b$ be a linear $[n, n{-}r_b, {>}\tau]$ code over Φ and suppose that $r_1 \le r_2$. Clearly, we can re-define $\mathbb{C}_2$ to be equal to $\mathbb{C}_1$, while still satisfying the required erasure-correction capabilities. Also, the value $r_0 = \dim\left(\mathbb{C}_1^\perp \cap \mathbb{C}_2^\perp \cap F^n\right)$ will not decrease, and $\mathrm{red}(\mathcal{C}) = m(r_1 + r_2) - r_0$ will not increase with the change. Hence, in the symmetric case, we can assume without loss of optimality that $\mathbb{C}_1 = \mathbb{C}_2 = \mathbb{C}$, where $\mathbb{C}$ is a linear $[n, n{-}r, {>}\tau]$ code over Φ. In this case,

$$\mathrm{red}(\mathcal{C}) = 2mr - r_0 \ ,$$

where

$$r_0 = \dim(\mathbb{C}^\perp \cap F^n) \overset{(9)}{=} \mathrm{red}(\mathrm{Tr}(\mathbb{C})) \ .$$

Suppose that $\mathbb{C}_1 = \mathbb{C}_2 = \mathbb{C}$ where $\mathbb{C}$ is a linear $[n, n{-}r, {>}\tau]$ code over Φ, and let $\mathcal{C} \subseteq (F^{2m-1})^n$ be defined accordingly by (10). At this point, we can obtain an intersecting coding scheme $(\mathcal{E}, \mathcal{D}_1, \mathcal{D}_2)$ with an onto encoding function $\mathcal{E} : \mathcal{M} \to \mathcal{C}$ directly from Proposition 2.2, thereby attaining redundancy (ρ_0, ρ_1, ρ_2) such that

$$\rho_0 + \rho_1 + \rho_2 = \mathrm{red}(\mathcal{C}) = 2mr - r_0 \ .$$

Furthermore, if $\mathbb{C}$ can be taken as a MDS code (and this is possible whenever $n \le q^m + 1$), then $r = \tau$ and, so,

$$\rho_0 + \rho = \mathrm{red}(\mathcal{C}) = 2m\tau - r_0 \ ,$$

where $\rho = \rho_1 + \rho_2$; i.e., we are on the straight line defined by

$$\rho = (2m\tau{-}r_0) - \rho_0 \ , \tag{16}$$

which parallels line (7) with an offset of $\tau - r_0$ (see Figure 4). Yet, we would also like to show that the particular values of ρ_0 and ρ can be chosen so that the point (ρ_0, ρ) lies on the line (6). To this end, we will make use of the analysis in the proof of Proposition 3.3.

For $b = 1, 2$ and $\boldsymbol{z} \in \mathrm{Tr}(\mathbb{C})$, let $\mathbb{C}_b(\boldsymbol{z})$ and $\mathcal{B}_b(\boldsymbol{z})$ be defined by (12) and (13) taking $\mathbb{C}_1 = \mathbb{C}_2 = \mathbb{C}$. The set $\mathcal{B}_b(\boldsymbol{z})$ can be written in the form

$$\mathcal{B}_b(\boldsymbol{z}) = \left\{ \Gamma \in (F^{2m-1})^n \; : \; \Gamma_0 = \boldsymbol{z} \; , \; \textstyle\sum_{j=1}^{m-1} B_j \Gamma_{(-1)^b j} = -B_0 \boldsymbol{z} \right\} \; , \quad b = 1, 2 \; ,$$

where $B_0, B_1, \ldots, B_{m-1}$ are matrices over F, derived from the parity check constraints of $\mathbb{C}$, and of dimensions $\sigma \times n$ such that

$$\begin{aligned} \mathrm{rank}(B_1 \,|\, B_2 \,|\, \ldots \,|\, B_{m-1}) = \sigma &\stackrel{(13)}{=} n(m-1) - \dim(\mathbb{C}_b(\boldsymbol{z})) \\ &\stackrel{(14)}{=} n(m-1) - \dim(\mathbb{C}) + \dim(\mathrm{Tr}(\mathbb{C})) \\ &\stackrel{(9)}{=} \mathrm{red}(\mathbb{C}) - \dim(\mathbb{C}^\perp \cap F^n) \\ &= mr - r_0 \; . \end{aligned}$$

Let H_0 be an $r_0 \times n$ parity-check matrix of the code $\mathrm{Tr}(\mathbb{C})$ over F (recall that $r_0 = \dim(\mathbb{C}^\perp \cap F^n) = \mathrm{red}(\mathrm{Tr}(\mathbb{C}))$), and define the $(2mr - r_0) \times n(2m-1)$ matrix H over F by

$$H = \left(\begin{array}{ccc|c|ccc} B_{m-1} & \cdots & B_1 & B_0 & & 0 & \\ \hline & 0 & & H_0 & & 0 & \\ \hline & 0 & & B_0 & B_1 & \cdots & B_{m-1} \end{array} \right) \; ;$$

note that $\mathrm{rank}(H) = 2mr - r_0$. Associate with every array $\Gamma = (\Gamma_{-m+1} \; \Gamma_{-m+2} \; \ldots \; \Gamma_{m-1})$ in $(F^{2m-1})^n$ the column vector $\mathsf{col}(\Gamma) \in F^{n(2m-1)}$ resulting from the concatenation of the columns of Γ, namely,

$$\mathsf{col}(\Gamma) = \begin{pmatrix} \Gamma_{-m+1} \\ \Gamma_{-m+2} \\ \vdots \\ \Gamma_{m-1} \end{pmatrix} \; .$$

From (10), (12), and (13) we get that

$$\begin{aligned} \mathcal{C} &= \{ \Gamma \in \mathcal{B}_1(\boldsymbol{z}) \cap \mathcal{B}_2(\boldsymbol{z}) \; : \; \boldsymbol{z} \in \mathrm{Tr}(\mathbb{C}) \} \\ &= \left\{ \Gamma \in (F^{2m-1})^n \; : \; H \, \mathsf{col}(\Gamma) = \mathbf{0} \right\} \; . \end{aligned}$$

This characterization of $\mathcal{C}$ leads to an encoding function

$$\mathcal{E} : F^{k_0} \times F^{k_1} \times F^{k_2} \to \mathcal{C} \; ,$$

1. Map $\boldsymbol{u}_0 \in F^{k_0}$ one-to-one into a codeword $\Gamma_0 \in \mathrm{Tr}(\mathbb{C})$.

2. Map $\boldsymbol{u}_1 \in F^{k_1}$ one-to-one to an element in the set

$$\left\{ (\Gamma_{-1}\, \Gamma_{-2}\, \ldots\, \Gamma_{-m+1}) \,:\, \Gamma_{-j} \in F^n \,,\, \textstyle\sum_{j=1}^{m-1} B_j \Gamma_{-j} = -B_0 \Gamma_0 \right\} .$$

3. Map $\boldsymbol{u}_2 \in F^{k_2}$ one-to-one to an element in the set

$$\left\{ (\Gamma_1\, \Gamma_2\, \ldots\, \Gamma_{m-1}) \,:\, \Gamma_j \in F^n \,,\, \textstyle\sum_{j=1}^{m-1} B_j \Gamma_j = -B_0 \Gamma_0 \right\} .$$

Figure 5: Computation of encoding function $\mathcal{E} : (\boldsymbol{u}_0, \boldsymbol{u}_1, \boldsymbol{u}_2) \mapsto (\Gamma_j)_{j=-m+1}^{m-1}$.

where $k_0 = n - r_0$ and $k_1 = k_2 = n(m-1) - \sigma = n(m-1) - mr + r_0$, through the algorithm in Figure 5.

The respective decoding functions $\mathcal{D}_1$ and $\mathcal{D}_2$ are readily obtained using a standard decoder for $\mathbb{C}$, and it is easily seen that

$$\mathsf{red}(\mathcal{E}, \mathcal{D}_1, \mathcal{D}_2) = (\rho_0, \rho_1, \rho_2) = (\mathrm{red}(\mathrm{Tr}(\mathbb{C})), \sigma, \sigma) = (r_0, mr - r_0, mr - r_0) .$$

We have the relation

$$\rho_0 + \rho_1 + \rho_2 = 2mr - r_0 = \mathrm{red}(\mathcal{C}) ,$$

which readily implies that $\mathcal{E}$ is onto $\mathcal{C}$. Furthermore, since $\rho_0 + \rho_b = mr$ for $b = 1, 2$, we have $\varphi_1(\mathcal{C}) = \varphi_2(\mathcal{C}) = \mathbb{C}$.

When $n \le q^m + 1$, we can take $\mathbb{C}$ to be MDS. The next result covers this case.

Proposition 3.4 *Let $\mathbb{C}$ be a linear $[n, n-\tau, \tau+1]$ MDS code over Φ. There exists a systematic intersecting coding scheme $(\mathcal{E} : \mathcal{M} \to (F^{2m-1})^n, \mathcal{D}_1, \mathcal{D}_2)$ such that*

$$\varphi_1(\mathcal{E}(\mathcal{M})) = \varphi_2(\mathcal{E}(\mathcal{M})) = \mathbb{C}$$

and

$$\mathsf{red}(\mathcal{E}, \mathcal{D}_1, \mathcal{D}_2) = (r_0, m\tau - r_0, m\tau - r_0) ,$$

where

$$r_0 = \dim(\mathbb{C}^\perp \cap F^n) = \mathrm{red}(\mathrm{Tr}(\mathbb{C})) .$$

In particular, $(\mathcal{E}, \mathcal{D}_1, \mathcal{D}_2) \in \mathbb{A}_q(m, n, \tau, \tau)$.

The point $P_0 = (\rho_0, \rho) = (r_0, 2(m\tau - r_0))$ attained by Proposition 3.4 is the intersection of the straight lines (6) and (16). These lines form the upper shaded boundary in Figure 4.

The next result shows that all integer points to the left of P_0 along the line (6) are achievable, as well as all integer points to the right of P_0 along the line (16).

Theorem 3.5 *Let $\mathbb{C}$ be a linear $[n, n-\tau, \tau+1]$ MDS code over Φ. An integer triple $\boldsymbol{\rho} = (\rho_0, \rho_1, \rho_2)$ that satisfies (3) belongs to $\mathbb{A}_q(m, n, \tau, \tau)$ if*

$$\rho_0 + \rho_b \geq m\tau_b \ , \quad b = 1, 2 \ ,$$

and

$$\rho_0 + \rho_1 + \rho_2 \geq 2m\tau - r_0 \ ,$$

where

$$r_0 = \dim(\mathbb{C}^\perp \cap F^n) = \mathrm{red}(\mathrm{Tr}(\mathbb{C})) \ .$$

Proof. Follow the steps of the proof of Proposition 2.5, except that now apply Lemma 2.4 to the achievable triple $(r_0, m\tau-r_0, m\tau-r_0)$. □

Looking at the offset, $\tau-r_0$, between the lines (7) and (16), we face the problem of selecting the 'best' MDS code $\mathbb{C}$ over Φ that maximizes $r_0 = \dim(\mathbb{C}^\perp \cap F^n)$. In Section 3.3, we compute lower bounds on the values of r_0 that are attainable when $\mathbb{C}$ is a Reed-Solomon (RS) code.

3.3 Construction based on RS codes

In this section, we consider the case where $\mathbb{C}$ is a cyclic $[n, n-r, \tau+1]$ code over Φ, where $n \,|\, q^m-1$. Such a code has r distinct roots in Φ, all of which belong to the subset $\{\beta \in \Phi : \beta^n = 1\}$. RS codes are examples of such codes, where $r = \tau$ and the set of roots is given by

$$S = \left\{\alpha^\Delta, \alpha^{\Delta+1}, \ldots, \alpha^{\Delta+\tau-1}\right\} \ , \tag{17}$$

for some integer Δ and an element $\alpha \in \Phi$ of multiplicative order n.

Recall that a conjugacy class in Φ over F is a subset

$$\left\{\gamma, \gamma^q, \ldots, \gamma^{q^{s-1}}\right\} \subseteq \Phi \ ,$$

where s is the smallest positive integer j such that $\gamma^{q^j} = \gamma$. We denote by $\mathcal{J}(\Phi/F)$ the set of all conjugacy classes in Φ over F.

The next proposition follows from known properties of sub-field sub-codes of cyclic codes; namely, if $\mathbb{C}$ is a cyclic code over Φ, then $\mathbb{C}^\perp \cap F^n$ is a cyclic code over F, whose set of roots is the union of the conjugacy classes of the roots of (the cyclic code) $\mathbb{C}^\perp$ (see [1, Ch. 12] for the case where $\mathbb{C}$ is a primitive RS code).

Proposition 3.6 *Let $\mathbb{C}$ be an $[n, n-r]$ cyclic code over Φ where $n \,|\, q^m-1$, and let S denote the set of roots of $\mathbb{C}$ (in Φ). Then*

$$r_0 = \dim(\mathbb{C}^\perp \cap F^n) = \mathrm{red}(\mathrm{Tr}(\mathbb{C})) = \sum_{\substack{J \in \mathcal{J}(\Phi/F) : \\ J \subseteq S}} |J| \ . \tag{18}$$

Example 3.1 Consider $[n, n-\tau]$ RS codes over $\Phi = \mathrm{GF}(q^m)$ where $m = 2$, $q = 4$, and $n = 15$. For every $\tau \in \{1, 2, \ldots, n-1\}$, we can apply Proposition 3.6 to find the largest attainable value of r_0 by enumerating over the parameter Δ in (17). The results are summarized in Table 1. $\square$

τ	1	2	3	4	5	6	7	8	9	10	11	12	13	14
r_0	1	1	1	2	3	4	4	5	7	8	9	10	12	14
Δ	0	0	0	1	0	0	0	1	1	0	0	1	1	1

Table 1: Largest attainable values of r_0 for RS codes of length 15 over $\mathrm{GF}(4^2)$.

Example 3.2 Take $n = q^m - 1$ and $\tau = \lambda q^{m-1} + 1$ for some nonnegative integer $\lambda < q$, and let $\mathbb{C}$ be an $[n, n-\tau]$ RS code over Φ whose set of roots is $S = \{\alpha^i \,:\, 0 \le i < \tau\}$, where α has multiplicative order n in Φ. Then the following λ conjugacy classes

$$\left\{\alpha^{eq^j} \,:\, 0 \le j < m\right\} \;, \quad 1 \le e \le \lambda \;,$$

are wholly contained in S, and so are the λ singleton conjugacy classes

$$\left\{\alpha^{en/(q-1)}\right\} \;, \quad 0 \le e < \lambda \;.$$

By Proposition 3.6 we thus get that

$$r_0 \ge \lambda(m+1) \;.$$

$\square$

4 Fully-intersecting codes

In this section, we study the problem of constructing three-dimensional, $n \times m \times m$ arrays over F where each $n \times m$ slice in one direction contains a codeword of a code $\mathbb{C}_1$ over F^m, while an $n \times m$ slice in the perpendicular direction contains a codeword of $\mathbb{C}_2$ over F^m (see Figure 1).

As in Section 3.1, we assume that F is the finite field $\mathrm{GF}(q)$ and identify F^m with a representation of the extension field $\Phi = \mathrm{GF}(q^m)$ with respect to some fixed basis $\boldsymbol{\omega} = (\omega_0\, \omega_1\, \ldots\, \omega_{m-1})^T$ of Φ over F. Thus, Equation (1) takes the form

$$\mathcal{C} = \left\{ \Gamma \in (F^{m\times m})^n \;:\; \begin{array}{l} \boldsymbol{\varphi}_1^{(\ell)}(\Gamma)\boldsymbol{\omega} \in \mathbb{C}_1 \text{ for } 1 \le \ell \le m \quad \text{and} \\ \boldsymbol{\varphi}_2^{(j)}(\Gamma)\boldsymbol{\omega} \in \mathbb{C}_2 \text{ for } 1 \le j \le m \end{array} \right\} . \tag{19}$$

We focus on constructions where $\mathbb{C}_1$ and $\mathbb{C}_2$ are linear codes over Φ and, as in Section 3.2, the preferred constructions will be based on MDS codes of parameters $[n, n-r_1, r_1+1]$ and $[n, n-r_2, r_2+1]$, respectively.

4.1 Basic tools

We first recall the notions of direct product and Kronecker sum (or, rather, difference) of matrices. Let $A = (a_{k,h})$ and $B = (b_{k',h'})$ be matrices over F of orders $m \times t$ and $m' \times t'$, respectively. The *direct product* of A and B, denoted $A \otimes B$, is the $mm' \times tt'$ matrix over F whose entries are given by

$$(A \otimes B)_{m'k+k',t'h+h'} = a_{k,h} b_{k',h'} \ , \quad 0 \le k < m \ , \ 0 \le h < t \ , \ 0 \le k' < m' \ , \ 0 \le h' < t' \ .$$

When $t = m$ and $t' = m'$, we define the *Kronecker difference* of A and B as the $mm' \times mm'$ matrix over F that is given by

$$A \ominus B = (A \otimes I_{m'}) - (I_m \otimes B) \ ,$$

where hereafter I_k stands for the $k \times k$ identity matrix.

The next lemma presents a known property of Kronecker difference of matrices (see, for example, Theorem 43.8 in [12]).

Lemma 4.1 *Let A and B be square matrices over F. The eigenvalues of $A \ominus B$ are given by $\lambda_A - \lambda_B$, where λ_A (respectively, λ_B) ranges over all eigenvalues of A (respectively, B), each with its respective algebraic multiplicity.*

Denote by $\boldsymbol{v}_\gamma$ the unique row vector in F^m such that $\gamma = \boldsymbol{v}_\gamma \cdot \boldsymbol{\omega}$. For every element $\gamma \in \Phi$, we can associate an $m \times m$ matrix L_γ over F that represents (the linear transformation of) multiplication by γ with respect to the basis $\boldsymbol{\omega}$; i.e., for every $\beta \in \Phi$,

$$\boldsymbol{v}_{\beta\gamma} = \boldsymbol{v}_\beta L_\gamma \ .$$

If $\boldsymbol{\omega}$ is taken as the standard basis $\boldsymbol{\alpha} = (1 \ \alpha \ \alpha^2 \ \ldots \ \alpha^{m-1})^T$ for some primitive element $\alpha \in \Phi$, then L_α is the companion matrix, C_α, of the minimal polynomial of α, and $L_{\alpha^t} = C_\alpha^t$ [10, p. 68]. Consequently, for any arbitrary basis $\boldsymbol{\omega}$, the respective matrix L_{α^t} will be similar to C_α^t. Hence, we get from [10, p. 102] the following property of the eigenvalues of L_γ.

Lemma 4.2 *Let γ be an element of Φ and let J be the conjugacy class in Φ over F that contains γ. The eigenvalues of L_γ are the elements of J, each having algebraic multiplicity $m/|J|$.*

A finite-dimensional vector space $\mathcal{A}$ over F that is also endowed with a vector multiplication ($\bullet$) operation that (together with vector addition) makes it a ring, and such that

$$(au) \bullet v = u \bullet (av) = a(u \bullet v), \quad a \in F, \ u, v \in \mathcal{A},$$

is called an *associative algebra* over F (or, in our context, simply an F-*algebra*) [16, Ch. 13]. In the next lemma, we characterize a commutative sub-algebra of the matrix F-algebra $F^{m^2 \times m^2}$ that contains all matrices of the form $L_\gamma \otimes I_m$ and $I_m \otimes L_\gamma$; this sub-algebra will be used in our analysis in subsequent sections.

Recall that there is a unique $m^2 \times m$ matrix M over F that satisfies

$$\boldsymbol{\omega} \otimes \boldsymbol{\omega} = M\boldsymbol{\omega} \ . \tag{20}$$

(The matrix M is equal to $\left(L_{\omega_j}\right)_{j=0}^{m-1}$, and it describes the multiplication table of the elements of $\boldsymbol{\omega}$; namely, for $0 \leq j, j' < m$, the representation of $\omega_j \omega_{j'}$ with respect to the basis $\boldsymbol{\omega}$ is given by $\sum_{h=0}^{m-1} (M)_{mj+j',h}\omega_h$; when re-arranged as an $m \times m \times m$ array, M is also referred to as the *tensor of multiplication* of Φ.) For a matrix $A \in F^{m\times m}$, let $\mathsf{row}(A)$ denote the row vector in F^{m^2} obtained by concatenating the m rows of A, i.e.

$$\mathsf{row}(A) = \left(\boldsymbol{\varphi}_2^{(0)}(A) \mid \boldsymbol{\varphi}_2^{(1)}(A) \mid \ \ldots \ \mid \boldsymbol{\varphi}_2^{(m-1)}(A)\right) \ . \tag{21}$$

Lemma 4.3 *Let $\Phi \otimes \Phi$ denote the linear sub-space of $F^{m^2 \times m^2}$ over F that is spanned by the set*

$$\left\{L_{\omega_j} \otimes L_{\omega_\ell}\right\}_{j,\ell=0}^{m-1} \ . \tag{22}$$

Then the following holds.

(i) $\Phi \otimes \Phi$ is a commutative F-algebra under ordinary matrix addition and matrix multiplication in $F^{m^2 \times m^2}$, with a multiplicative identity element given by $L_1 \otimes L_1 = I_{m^2}$.

(ii) $\Phi \otimes \Phi$ is the smallest sub-ring of $F^{m^2 \times m^2}$ that contains all elements of the set

$$\{L_\beta \otimes I_m \ : \ \beta \in \Phi\} \cup \{I_m \otimes L_\gamma \ : \ \gamma \in \Phi\} \ .$$

(iii) $\Phi \otimes \Phi$ is isomorphic to the F-algebra $(F^{m\times m}, +, \odot)$, where $+$ is the ordinary matrix addition in $F^{m\times m}$ and $\odot$ is a product defined by

$$A \odot B = M^T(A \otimes B)M \ , \quad A, B \in F^{m\times m} \ ;$$

the isomorphism $(\Phi \otimes \Phi) \cong (F^{m\times m}, +, \odot)$ is given by

$$A = (a_{j,\ell})_{j,\ell=0}^{m-1} \quad \cong \quad \sum_{j,\ell} a_{j,\ell}(L_{\omega_j} \otimes L_{\omega_\ell}) \ , \quad a_{j,\ell} \in F \ . \tag{23}$$

(iv) For every $A, B \in F^{m\times m}$,

$$\mathsf{row}(A \odot B) = \mathsf{row}(A)\, \mathbf{B} \ ,$$

where $\mathbf{B}$ is the element in $\Phi \otimes \Phi$ that is associated with B by (23).

The proof of Lemma 4.3 is given in Appendix C.

The F-algebra $\Phi \otimes \Phi$ (or $(F^{m\times m}, +, \odot)$) can be identified with the tensor product (or product algebra [16, Ch. 13]) of Φ with itself, when Φ is regarded as an F-algebra.

4.2 Bounds on the redundancy

Recall that the (ordinary) redundancy of a code $\mathcal{C} \subseteq (F^{m\times m})^n$ is defined by

$$\mathrm{red}(\mathcal{C}) = m^2 n - \log_q |\mathcal{C}| \ .$$

In this section, we obtain upper bounds on the redundancy of the code $\mathcal{C}$ in (19), in terms of the constituent codes $\mathbb{C}_1$ and $\mathbb{C}_2$. While general bounds can be stated that depend only on the parameters of $\mathbb{C}_1$ and $\mathbb{C}_2$, our sharper bounds will also depend on finer structural properties of these codes.

For $b = 1, 2$, let $\mathbb{C}_b$ be a linear $[n, n{-}r_b]$ code over Φ and let $\mathbb{H}_b$ be an $r_b \times n$ parity-check matrix of $\mathbb{C}_b$ over Φ. For $0 \le \ell < r_b$ and $0 \le i < n$, we let $(\mathbb{H}_b)_{\ell,i}$ stand for the entry in $\mathbb{H}_b$ that is indexed by (ℓ, i). Define the $m^2 r_b \times m^2 n$ matrices $\mathbf{H}_b$ over F by

$$\mathbf{H}_1^T = \begin{pmatrix} L_{(\mathbb{H}_1)_{0,0}} \otimes I & L_{(\mathbb{H}_1)_{1,0}} \otimes I & \ldots & L_{(\mathbb{H}_1)_{r_1-1,0}} \otimes I \\ L_{(\mathbb{H}_1)_{0,1}} \otimes I & L_{(\mathbb{H}_1)_{1,1}} \otimes I & \ldots & L_{(\mathbb{H}_1)_{r_1-1,1}} \otimes I \\ \vdots & \vdots & \vdots & \vdots \\ L_{(\mathbb{H}_1)_{0,n-1}} \otimes I & L_{(\mathbb{H}_1)_{1,n-1}} \otimes I & \ldots & L_{(\mathbb{H}_1)_{r_1-1,n-1}} \otimes I \end{pmatrix} \qquad (24)$$

and

$$\mathbf{H}_2^T = \begin{pmatrix} I \otimes L_{(\mathbb{H}_2)_{0,0}} & I \otimes L_{(\mathbb{H}_2)_{1,0}} & \ldots & I \otimes L_{(\mathbb{H}_2)_{r_2-1,0}} \\ I \otimes L_{(\mathbb{H}_2)_{0,1}} & I \otimes L_{(\mathbb{H}_2)_{1,1}} & \ldots & I \otimes L_{(\mathbb{H}_2)_{r_2-1,1}} \\ \vdots & \vdots & \vdots & \vdots \\ I \otimes L_{(\mathbb{H}_2)_{0,n-1}} & I \otimes L_{(\mathbb{H}_2)_{1,n-1}} & \ldots & I \otimes L_{(\mathbb{H}_2)_{r_2-1,n-1}} \end{pmatrix} , \qquad (25)$$

respectively, where $I = I_m$.

Extend the notation $\mathsf{row}(\cdot)$ in (21) to an array $\Gamma \in (F^{m\times m})^n$ by letting $\mathsf{row}(\Gamma)$ denote the following row vector in $F^{m^2 n}$:

$$\mathsf{row}(\Gamma) = \left(\mathsf{row}(\Gamma^{(0)}) \mid \mathsf{row}(\Gamma^{(1)}) \mid \ldots \mid \mathsf{row}(\Gamma^{(n-1)}) \right) \ .$$

Proposition 4.4 *For $b = 1, 2$, let $\mathbb{C}_b$ be a linear $[n, n{-}r_b]$ code over Φ and let the code $\mathcal{C}$ over $F^{m\times m}$ be given by (19). Define the $(m^2(r_1 + r_2)) \times m^2 n$ matrix $\mathbf{H}$ over F by*

$$\mathbf{H} = \begin{pmatrix} \mathbf{H}_1 \\ \mathbf{H}_2 \end{pmatrix} ,$$

where $\mathbf{H}_1$ and $\mathbf{H}_2$ are given by (24)–(25). Then, for every $\Gamma \in (F^{m\times m})^n$,

$$\Gamma \in \mathcal{C} \quad \Longleftrightarrow \quad \mathsf{row}(\Gamma)\, \mathbf{H}^T = \mathbf{0} \ .$$

Proof. This follows from (19) and the fact that a vector $(c_0\ c_1\ \ldots\ c_{n-1}) \in \Phi^n$ is a codeword of $\mathbb{C}_b$ if and only if

$$\left(\boldsymbol{v}_{c_0} \,|\, \boldsymbol{v}_{c_1} \,|\, \ldots \,|\, \boldsymbol{v}_{c_{n-1}}\right) \left(L_{(\mathbb{H}_b)_{\ell,i}}\right)_{i,\ell} = \mathbf{0} \; .$$

$\square$

For our analysis in the sequel, we find it convenient to view the $m^2 \times m^2$ blocks of the matrices $\mathbf{H}_1$ and $\mathbf{H}_2$ in (24)–(25) as elements of the F-algebra $(F^{m\times m}, +, \odot)$ defined in Lemma 4.3.

For an element $\gamma \in \Phi$, let $\langle\gamma]$ and $[\gamma\rangle$ denote (the representation by (23) in $(F^{m\times m}, +, \odot)$ of) the elements $L_\gamma \otimes I_m$ and $I_m \otimes L_\gamma$, respectively. It is easy to see that each of the mappings $\langle\cdot] : \Phi \to (F^{m\times m}, +, \odot)$ and $[\cdot\rangle : \Phi \to (F^{m\times m}, +, \odot)$ defines an isomorphism from Φ to the set of images of the mapping. We extend the definitions of $\langle\cdot]$ and $[\cdot\rangle$ (and, respectively, $\odot$) in the natural way to vectors and matrices over Φ (respectively, over $F^{m\times m}$). When viewing an array $\Gamma \in (F^{m\times m})^n$ as a column vector of length n over the F-algebra $(F^{m\times m}, +, \odot)$, the product $H \odot \Gamma$ is well-defined for every matrix H with n columns over that algebra.

Combining Lemma 4.3(iv) with Proposition 4.4 yields the following result.

Proposition 4.5 *For $b = 1, 2$, let $\mathbb{C}_b$ be a linear $[n, n-r_b]$ code with an $r_b \times n$ parity-check matrix $\mathbb{H}_b$ over Φ, and define the code $\mathcal{C}$ over $F^{m\times m}$ by (19). Then, for every $\Gamma \in (F^{m\times m})^n$,*

$$\Gamma \in \mathcal{C} \quad \Longleftrightarrow \quad \begin{pmatrix} \langle\mathbb{H}_1] \\ [\mathbb{H}_2\rangle \end{pmatrix} \odot \Gamma = \mathbf{0} \; .$$

The redundancy of the code $\mathcal{C}$ in Propositions 4.4–4.5, is obviously bounded by

$$m^2 \max\{r_1, r_2\} \le \mathrm{red}(\mathcal{C}) \le m^2 \min\{r_1 + r_2, n\} \; . \tag{26}$$

The upper bound can be sharpened when $\dim(\mathbb{C}_1^\perp \cap \mathbb{C}_2^\perp) > 0$, in which case we can assume without loss of generality that the parity-check matrices $\mathbb{H}_1$ and $\mathbb{H}_2$ share $r > 0$ rows. For example, if the first row in these two matrices is the all-one row, then the first m^2 rows in $\mathbf{H}_1$ and $\mathbf{H}_2$ are identical, as both $L_1 \otimes I_m$ and $I_m \otimes L_1$ are equal to the $m^2 \times m^2$ identity matrix. Thus, in such a case, $\mathrm{red}(\mathcal{C}) = \mathrm{rank}(\mathbf{H}) \le m^2(r_1 + r_2 - 1)$. This is a special case of Theorem 4.7 below.

We next focus on the common $r \times n$ sub-matrix $\mathbb{H}$ of $\mathbb{H}_1$ and $\mathbb{H}_2$ and on the rank of the respective sub-matrix in $\mathbf{H}$; the latter sub-matrix, in turn, is given by (24)–(25), with $\mathbb{H}_1$ and $\mathbb{H}_2$ replaced by $\mathbb{H}$.

Proposition 4.6 *Let $\mathbb{H}$ be an $r \times n$ matrix over Φ and let $\mathbf{H}_1$ and $\mathbf{H}_2$ be $m^2 r \times m^2 n$ matrices over F that are given by (24)–(25), with $\mathbb{H}_1 = \mathbb{H}_2 = \mathbb{H}$ and $r_1 = r_2 = r$. For*

$\ell = 0, 1, \ldots, r{-}1$, *let the entries of row* ℓ *in* $\mathbb{H}$ *all belong to the sub-field* $\mathrm{GF}(q^{s_\ell})$ *of* Φ*. Then,*

$$\mathrm{rank} \begin{pmatrix} \mathbf{H}_1 \\ \mathbf{H}_2 \end{pmatrix} \le m^2 \Big(2r - \sum_{\ell=0}^{r-1} \frac{1}{s_\ell} \Big) .$$

Proof. Clearly,

$$\mathrm{rank} \begin{pmatrix} \mathbf{H}_1 \\ \mathbf{H}_2 \end{pmatrix} = \mathrm{rank} \begin{pmatrix} \mathbf{H}_1 \\ \mathbf{H}_1{-}\mathbf{H}_2 \end{pmatrix} \le m^2 r + \mathrm{rank}\left(\mathbf{H}_1{-}\mathbf{H}_2\right) . \tag{27}$$

Associate $\mathbf{H}_1{-}\mathbf{H}_2$ by (23) with an $r \times n$ matrix $(\xi_{\ell,i})_{\ell=0}^{r-1}{}_{i=0}^{n-1}$ over $F^{m\times m}$, where

$$\xi_{\ell,i} = \langle (\mathbb{H})_{\ell,i}] - [(\mathbb{H})_{\ell,i}\rangle .$$

Letting α_ℓ denote a primitive element in the sub-field, $\mathrm{GF}(q^{s_\ell})$, which contains $(\mathbb{H})_{\ell,i}$, it follows that

$$\xi_{\ell,i} = \langle \alpha_\ell^t] - [\alpha_\ell^t\rangle = \langle \alpha_\ell]^t - [\alpha_\ell\rangle^t$$

for some $t = t(\ell, i)$, where we use the fact that $\langle\cdot]$ and $[\cdot\rangle$ preserve multiplication. Hence, in $(F^{m\times m}, +, \odot)$,

$$\xi_{\ell,i} = (\langle\alpha_\ell] - [\alpha_\ell\rangle) \sum_{j=0}^{t-1} \Big(\langle\alpha_\ell]^j \odot [\alpha_\ell\rangle^{t-j-1} \Big) .$$

Observing that $\langle\alpha_\ell] - [\alpha_\ell\rangle \overset{(23)}{\cong} L_{\alpha_\ell} \ominus L_{\alpha_\ell}$, we thus obtain,

$$\mathrm{rank}(\mathbf{H}_1{-}\mathbf{H}_2) \le \sum_{\ell=0}^{r-1} \mathrm{rank}(L_{\alpha_\ell} \ominus L_{\alpha_\ell}) = m^2 r - \sum_{\ell=0}^{r-1} \dim\ker(L_{\alpha_\ell} \ominus L_{\alpha_\ell}) . \tag{28}$$

On the other hand, by Lemmas 4.1 and 4.2 we get that

$$\dim\ker(L_{\alpha_\ell} \ominus L_{\alpha_\ell}) = \frac{m^2}{s_\ell} .$$

The result follows by combining the last inequality with (27) and (28). $\square$

We next turn to the main result of this section.

Theorem 4.7 *For* $b = 1, 2$*, let* $\mathbb{C}_b$ *be a linear* $[n, n{-}r_b]$ *code over* Φ *and let the code* $\mathcal{C}$ *over* $F^{m\times m}$ *be given by (19). For every positive integer divisor* s *of* m*, let* Φ_s *denote the field* $\mathrm{GF}(q^s)$ *and let* k_s *be the dimension of the linear code*

$$W_s = \mathbb{C}_1^\perp \cap \mathbb{C}_2^\perp \cap \Phi_s^n$$

over Φ_s*. Then,*

$$\mathrm{red}(\mathcal{C}) \le m^2(r_1 + r_2) - m \sum_{s\,|\,m} k_s \cdot \phi(m/s) ,$$

where $\phi : \mathbb{N} \to \mathbb{N}$ *is Euler's totient function.*

Proof. For a positive divisor s of m, let U_s denote the linear span over Φ_s of the set $\bigcup_d W_d$, where d ranges over all proper divisors of s; clearly, U_s is a linear sub-space of W_s over Φ_s. We construct a generator matrix $\mathbb{H}$ of $W_m = \mathbb{C}_1^\perp \cap \mathbb{C}_2^\perp$, by successively adding the basis elements of the quotient space W_s/U_s over Φ_s, for increasing values of divisors s of m. Denote by f_s the dimension of W_s/U_s as a vector space over Φ_s. For every divisor s of m we have

$$k_s = \sum_{d \,|\, s} f_d \; . \tag{29}$$

As our next step, we select for $b = 1, 2$ an $r_b \times n$ parity-check matrix $\mathbb{H}_b$ of $\mathbb{C}_b$ such that $\mathbb{H}$ is a sub-matrix of both $\mathbb{H}_1$ and $\mathbb{H}_2$; indeed, this is always possible, since $\mathbb{H}$ generates $\mathbb{C}_1^\perp \cap \mathbb{C}_2^\perp$. By Propositions 4.4 and 4.6 we obtain,

$$\mathrm{red}(\mathcal{C}) \le m^2 \Bigl(r_1 + r_2 - \sum_{s \,|\, m} \frac{f_s}{s} \Bigr) \; . \tag{30}$$

Now, for every positive integer a we have,

$$\sum_{t \,|\, a} \phi(t) = \sum_{t \,|\, a} \phi(a/t) = a \tag{31}$$

(see, for example, [14, p. 114]). Therefore,

$$m \sum_{d \,|\, m} \frac{f_d}{d} \overset{(31)}{=} \sum_{d \,|\, m} f_d \sum_{t \,|\, m/d} \phi(m/(dt)) \overset{s=dt}{=} \sum_{s \,|\, m} \phi(m/s) \sum_{d \,|\, s} f_d \overset{(29)}{=} \sum_{s \,|\, m} \phi(m/s) \cdot k_s \; . \tag{32}$$

The result follows by combining (30) with (32). $\square$

Example 4.1 Let $F = \mathrm{GF}(2)$ and $\Phi = \mathrm{GF}(2^4)$, and select both $\mathbb{C}_1$ and $\mathbb{C}_2$ to be a $[15, 8, 8]$ RS code $\mathbb{C}$ over Φ with a set of roots $S = \{\alpha^i \,:\, 0 \le i < 7\}$, where α is primitive in Φ. Clearly, the code $W_4 = \mathbb{C}^\perp$ has dimension

$$k_4 = 15 - 8 = 7$$

over $\Phi_4 = \Phi$. The dimension of $W_1 = \mathbb{C}^\perp \cap \Phi_1^{15}$ over $\Phi_1 = F$ can be computed using Proposition 3.6 to yield

$$k_1 = \sum_{\substack{J \in \mathcal{J}(\Phi/F) : \\ J \subseteq S}} |J| = |\{1\}| = 1 \; .$$

Replacing F by $\Phi_2 = \mathrm{GF}(2^2)$ in that proposition, we can also compute the dimension of $W_2 = \mathbb{C}^\perp \cap \Phi_2^{15}$ over Φ_2 as follows:

$$k_2 = \sum_{\substack{J \in \mathcal{J}(\Phi/\Phi_2) : \\ J \subseteq S}} |J| = |\{1\}| + |\{\alpha, \alpha^4\}| + |\{\alpha^5\}| = 4 \; .$$

Finally, by Theorem 4.7 we obtain,

$$\mathrm{red}(\mathcal{C}) \leq 4^2 \cdot 14 - 4 \cdot (1 \cdot \phi(4) + 4 \cdot \phi(2) + 7 \cdot \phi(1)) = 224 - 4 \cdot (1{\cdot}2 + 4{\cdot}1 + 7{\cdot}1) = 172 \; .$$

In comparison, the lower and upper bounds in (26) equal 112 and 224, respectively. □

4.3 Construction based on shortened cyclic codes

The upper bound in Theorem 4.7 is minimized when $\mathbb{C}_1$ (say) is a subset of $\mathbb{C}_2$. If the minimum distance requirements are the same for the two directions of the $n \times m$ slices of Γ, then we may as well take $\mathbb{C}_1 = \mathbb{C}_2$.

In this section, we consider the case where $\mathbb{C}_1$ and $\mathbb{C}_2$ are taken to be the same shortened cyclic code $\mathbb{C}$ over Φ whose roots are all in Φ. We will make use of the following lemma.

Lemma 4.8 *Let $\xi_1, \xi_2, \ldots$ be elements in a commutative ring $\mathcal{R}$ with unity. Fix a positive integer N, and for $t \geq 1$, denote by V_t the following $t \times (N{+}t)$ matrix over $\mathcal{R}$:*

$$V_t = \begin{pmatrix} 1 & \xi_1 & \xi_1^2 & \ldots & \xi_1^{N+t-1} \\ 1 & \xi_2 & \xi_2^2 & \ldots & \xi_2^{N+t-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \xi_t & \xi_t^2 & \ldots & \xi_t^{N+t-1} \end{pmatrix} .$$

Then, for $t \geq 1$,

$$V_{t+1} = E_t^{(1)} \left(\begin{array}{c|c} 0 & D_t V_t \\ \hline 1 & \boldsymbol{w}_t \end{array} \right) E_t^{(2)} \; ,$$

where D_t is the following $t \times t$ diagonal matrix over $\mathcal{R}$,

$$D_t = \begin{pmatrix} \xi_1{-}\xi_{t+1} & & & \\ & \xi_2{-}\xi_{t+1} & & \\ & & \ddots & \\ & & & \xi_t{-}\xi_{t+1} \end{pmatrix} ,$$

$E_t^{(1)}$ and $E_t^{(2)}$ are invertible upper-triangular square matrices over $\mathcal{R}$, and $\boldsymbol{w}_t$ is a row vector in $\mathcal{R}^{N+t}$.

Proof. Take

$$E_t^{(1)} = \begin{pmatrix} 1 & & & & 1 \\ & 1 & & & 1 \\ & & \ddots & & \vdots \\ & & & 1 & 1 \\ & & & & 1 \end{pmatrix}, \quad E_t^{(2)} = \begin{pmatrix} 1 & 0 & 0 & 0 & \cdots & 0 \\ & 1 & \xi_{t+1} & \xi_{t+1}^2 & \cdots & \xi_{t+1}^{N+t-1} \\ & & 1 & \xi_{t+1} & \cdots & \xi_{t+1}^{N+t-2} \\ & & & 1 & \cdots & \xi_{t+1}^{N+t-3} \\ & & & & \ddots & \vdots \\ & & & & & 1 \end{pmatrix},$$

and $\boldsymbol{w}_t = (\xi_{t+1}, 0, \ldots, 0)$. $\square$

Proposition 4.9 *Let $S = \{\beta_1, \beta_2, \ldots, \beta_r\}$ be a set of r distinct nonzero elements of Φ, and for $n \geq 2r$, let the $2r \times n$ matrix $\mathbf{H}$ over $F^{m\times m}$ be defined by*

$$\mathbf{H} = \left(\begin{array}{ccccc} 1 & \langle\beta_1] & \langle\beta_1]^2 & \ldots & \langle\beta_1]^{n-1} \\ 1 & \langle\beta_2] & \langle\beta_2]^2 & \ldots & \langle\beta_2]^{n-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \langle\beta_r] & \langle\beta_r]^2 & \ldots & \langle\beta_r]^{n-1} \\ \hline 1 & [\beta_1\rangle & [\beta_1\rangle^2 & \ldots & [\beta_1\rangle^{n-1} \\ 1 & [\beta_2\rangle & [\beta_2\rangle^2 & \ldots & [\beta_2\rangle^{n-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & [\beta_r\rangle & [\beta_r\rangle^2 & \ldots & [\beta_r\rangle^{n-1} \end{array} \right). \tag{33}$$

Regarding $\mathbf{H}$ as an $2m^2r \times m^2n$ matrix over F, its rank is given by

$$\mathrm{rank}(\mathbf{H}) = m^2 \left(2r - \sum_{J \in \mathcal{J}(\Phi/F)} \frac{|J \cap S|^2}{|J|} \right). \tag{34}$$

Proof. For $t = 1, 2, \ldots, 2r$, denote by $\mathbf{H}^{(t)}$ the $t \times (n{-}2r{+}t)$ upper-left sub-matrix of $\mathbf{H}$ (over $F^{m\times m}$) and by $\mathrm{rank}(\mathbf{H}^{(t)})$ the rank of $\mathbf{H}^{(t)}$, when $\mathbf{H}^{(t)}$ is regarded as an $m^2t \times m^2(n{-}2r{+}t)$ matrix over F.

For $k = 1, 2, \ldots, r$, let J_k be the conjugacy class over F that contains β_k and let X_k denote the intersection $J_k \cap S$. We prove by induction on $k = 0, 1, 2, \ldots, r$ that

$$\mathrm{rank}(\mathbf{H}^{(r+k)}) = m^2 \left(r + k - \sum_{\ell=1}^{k} \frac{|X_\ell|}{|J_\ell|} \right). \tag{35}$$

Note that for $k = r$, the right-hand sides of (34) and (35) are equal.

Starting with the induction base $k = 0$, we observe that for $1 \leq j < \ell \leq r$,

$$\langle\beta_j] - \langle\beta_\ell] = \langle\beta_j{-}\beta_\ell] \overset{(23)}{\cong} L_{\beta_j-\beta_\ell} \otimes I_m$$

and, so, the element $\langle\beta_j] - \langle\beta_\ell]$ is invertible in $(F^{m\times m}, +, \odot)$ (and so is $[\beta_j\rangle - [\beta_\ell\rangle$). Applying Lemma 4.8 to $\mathcal{R} = (F^{m\times m}, +, \odot)$ and $V_t = \mathbf{H}^{(t)}$ for $t = 0, 1, 2, \ldots, r-1$, we thus obtain that

$$\operatorname{rank}(\mathbf{H}^{(r)}) = m^2 r .$$

Turning to the induction step, we apply Lemma 4.8 to $V_{r+k} = \mathbf{H}^{(r+k)}$, and distinguish between two types of elements which appear along the main diagonal of D_{r+k}. The first type consists of the elements $[\beta_j\rangle - [\beta_{k+1}\rangle$, for $1 \le j \le k$. Clearly, these elements are all invertible in $(F^{m\times m}, +, \odot)$. The second type consists of the elements $\langle\beta_j] - [\beta_{k+1}\rangle$, for $1 \le j \le r$. Here

$$\langle\beta_j] - [\beta_{k+1}\rangle = (L_{\beta_j} \otimes I_m) - (I_m \otimes L_{\beta_{k+1}}) = L_{\beta_j} \ominus L_{\beta_{k+1}}$$

and, so, from Lemmas 4.1 and 4.2 we get that $\langle\beta_j] - [\beta_{k+1}\rangle$ is a zero divisor in $(F^{m\times m}, +, \odot)$ if and only if $\beta_j \in X_{k+1}$. Furthermore, by these lemmas we get that when $\beta_j \in X_{k+1}$,

$$\dim\ker(L_{\beta_j} \ominus L_{\beta_{k+1}}) = \frac{m^2}{|J_{k+1}|} . \tag{36}$$

Now, these zero divisors are confined to the first r entries along the main diagonal of D_{r+k}, while the first r rows in $\mathbf{H}^{(r+k)}$, when translated into $m^2 r$ rows over F, have full rank. Thus, from Lemma 4.8 we obtain,

$$\begin{aligned}
\operatorname{rank}(\mathbf{H}^{(r+k+1)}) &= \operatorname{rank}(\mathbf{H}^{(r+k)}) + m^2 - \sum_{\beta\in X_{k+1}} \dim\ker(L_\beta \ominus L_{\beta_{k+1}}) \\
&\overset{(36)}{=} \operatorname{rank}(\mathbf{H}^{(r+k)}) + m^2\left(1 - \frac{|X_{k+1}|}{|J_{k+1}|}\right) \\
&\overset{(35)}{=} m^2\left(r + k + 1 - \sum_{\ell=1}^{k+1} \frac{|X_\ell|}{|J_\ell|}\right) .
\end{aligned}$$

$\square$

We now reach the main result of this section.

Theorem 4.10 *Let $S = \{\beta_1, \beta_2, \ldots, \beta_r\}$ be a set of r distinct nonzero elements of Φ and let $\mathbb{C}$ be an $[n, n-r]$ shortened cyclic code over Φ with an $r \times n$ parity-check matrix*

$$\mathbb{H} = \begin{pmatrix} 1 & \beta_1 & \beta_1^2 & \ldots & \beta_1^{n-1} \\ 1 & \beta_2 & \beta_2^2 & \ldots & \beta_2^{n-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \beta_r & \beta_r^2 & \ldots & \beta_r^{n-1} \end{pmatrix} .$$

Construct the code $\mathcal{C}$ by (19) with $\mathbb{C}_1 = \mathbb{C}_2 = \mathbb{C}$. Then,

$$\operatorname{red}(\mathcal{C}) \le m^2\left(2r - \sum_{J\in\mathcal{J}(\Phi/F)} \frac{|J\cap S|^2}{|J|}\right) ,$$

with equality holding if either $n \ge 2r$ or $\mathbb{C}$ is a cyclic code.

Proof. By Proposition 4.5, a $2r \times n$ parity-check matrix of $\mathcal{C}$ over $(F^{m\times m}, +, \odot)$ is given by (33). When $n < 2r$, we append to $\mathbf{H}$ the column vectors

$$\left(\langle\beta_1]^i \;\; \langle\beta_2]^i \;\; \ldots \;\; \langle\beta_r] \;\; [\beta_1\rangle^i \;\; [\beta_2\rangle^i \;\; \ldots \;\; [\beta_r\rangle \right)^T \;, \quad n \le i < 2r \;,$$

and redefine n to be $2r$. This change does not affect the rank of $\mathbf{H}$ when $\mathbb{C}$ is cyclic, and may only increase it otherwise. The result now follows from Proposition 4.9. $\square$

Example 4.2 Let F, Φ, and $\mathbb{C}$ be as in Example 4.1. The intersection of the set of roots S with the elements of $\mathcal{J}(\Phi/F)$ is shown in Table 2. By Theorem 4.10 we get,

$$\mathrm{red}(\mathcal{C}) = 4^2 \cdot \left(2 \cdot 7 - \left(\tfrac{0^2}{1} + \tfrac{1^2}{1} + \tfrac{3^2}{4} + \tfrac{2^2}{4} + \tfrac{1^2}{4} + \tfrac{0^2}{4}\right)\right) = 148 \;.$$

J	$\{0\}$	$\{1\}$	$\{\alpha, \alpha^2, \alpha^4, \alpha^8\}$	$\{\alpha^3, \alpha^6, \alpha^{12}, \alpha^9\}$	$\{\alpha^5, \alpha^{10}\}$	$\{\alpha^7, \alpha^{14}, \alpha^{13}, \alpha^{11}\}$
$J \cap S$	$\emptyset$	$\{1\}$	$\{\alpha, \alpha^2, \alpha^4\}$	$\{\alpha^3, \alpha^6\}$	$\{\alpha^5\}$	$\emptyset$
$\lvert J \cap S\rvert$	0	1	3	2	1	0
$\lvert J\rvert$	1	1	4	4	2	4

Table 2: Distribution of roots among the conjugacy classes for the code in Example 4.1.

Ranging now over all values $r \in \{1, 2, \ldots, 14\}$, we have summarized in Table 3 the redundancy values of $\mathcal{C}$ obtained when $\mathbb{C}$ is taken as a $[15, 15-r, r+1]$ RS code over $\mathrm{GF}(2^4)$ with a set of roots $S = \{\alpha^{\Delta+i} \,:\, 0 \le i < r\}$, where we have chosen the value Δ that minimizes the redundancy. The table also shows the difference between $\mathrm{red}(\mathcal{C})$ and the lower bound, $m^2 r$, in (26). The upper bound of Theorem 4.7 turns out to be the loosest when $r = 7$ (see Example 4.1). $\square$

r	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$\mathrm{red}(\mathcal{C})$	16	44	64	88	104	128	148	164	176	184	200	208	220	224
$\mathrm{red}(\mathcal{C}) - m^2 r$	0	12	16	24	24	32	36	36	32	24	24	16	12	0
Δ	0	0	0	1	0	0	0	1	1	1	0	1	1	1

Table 3: Smallest possible values of $\mathrm{red}(\mathcal{C})$ for RS codes of length 15 over $\mathrm{GF}(2^4)$.

Remark 4.1 It is interesting to compare the bound in Theorem 4.10 with the redundancy of sub-field sub-codes. Specifically, let $\mathbb{C}$ be an $[n, n{-}r]$ cyclic code over Φ whose set of roots, S, is contained in Φ. On the one hand,

$$\mathrm{red}(\mathbb{C} \cap F^n) = \sum_{\substack{J \in \mathcal{J}(\Phi/F):\\ J \cap S \neq \emptyset}} |J| \;=\; r + \sum_{\substack{J \in \mathcal{J}(\Phi/F):\\ J \cap S \neq \emptyset}} \left(|J| - |J \cap S|\right) \;, \tag{37}$$

where the last sum in (37) represents the 'conjugate penalty' in the redundancy of the sub-field subcode $\mathbb{C} \cap F^n$, compared to the underlying code $\mathbb{C}$. On the other hand, from Theorem 4.10 we obtain,

$$\mathrm{red}(\mathcal{C}) = m^2 \Biggl(r + \sum_{\substack{J \in \mathcal{J}(\Phi/F):\\ J \cap S \neq \emptyset}} \frac{|J \cap S|}{|J|} \cdot \left(|J| - |J \cap S|\right) \Biggr) \;, \tag{38}$$

where the sum now expresses the redundancy penalty with respect to the lower bound in (26). In both (37) and (38), conjugacy classes that are wholly contained in either S or $\Phi \setminus S$ carry no redundancy penalty. Otherwise, the penalty due to a given conjugacy class J increases in (37) as the size of the intersection $J \cap S$ becomes smaller; in contrast, the penalty increases in (38) as the size of that intersection becomes closer to $\frac{1}{2}|J|$. $\square$

Example 4.3 Suppose that the basis $\boldsymbol{\omega}$ has the form $(1 \;\alpha\; \alpha^2 \;\ldots\; \alpha^{m-1})^T$, where α belongs to a conjugacy class in Φ of size m over F. Let $n = m$ and select $\mathbb{C}$ to be the $[m, m{-}r]$ code over Φ with a parity-check matrix

$$\mathbb{H} = \begin{pmatrix} 1 & \alpha & \alpha^2 & \ldots & \alpha^{m-1} \\ 1 & \alpha^q & \alpha^{2q} & \ldots & \alpha^{(m-1)q} \\ 1 & \alpha^{q^2} & \alpha^{2q^2} & \ldots & \alpha^{(m-1)q^2} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha^{q^{r-1}} & \alpha^{2q^{r-1}} & \ldots & \alpha^{(m-1)q^{r-1}} \end{pmatrix} . \tag{39}$$

The code $\mathbb{C}$ is known to be MDS over Φ, and so is the *transpose code*

$$\mathbb{C}^T = \left\{ A^T \boldsymbol{\omega} \,:\, A \in F^{m \times m},\; A\boldsymbol{\omega} \in \mathbb{C} \right\} \;,$$

whose parity-check matrix is obtained from $\mathbb{H}$ by replacing α with $\alpha^{q^{m-r+1}}$ in (39); see [7], [8]–[9], and [15]. In this case, we get by Theorem 4.10 that

$$\mathrm{red}(\mathcal{C}) \le 2m^2 r - mr^2 = mr(2m - r) \;.$$

$\square$

Appendix A

Proof of Proposition 2.2. Let $\mathcal{X}$ be an information locator set of $\mathcal{C}$ and define the subsets

$$\mathcal{X}_0 = \mathcal{X} \cap \{(i,0) \,:\, 1 \leq i \leq n\}$$

and

$$\mathcal{X}_b = \mathcal{X} \cap \{(i,j) \,:\, 1 \leq i \leq n \;,\; 0 < (-1)^b j < m\} \;, \quad b = 1, 2 \;.$$

Clearly, $\mathcal{X}_0$, $\mathcal{X}_1$, and $\mathcal{X}_2$ form a partition of $\mathcal{X}$. For $b = 0, 1, 2$, let $k_b = |\mathcal{X}_b|$ and $\mathcal{M}_b = F^{k_b}$. Consider the encoding function $\mathcal{E} : \mathcal{M}_0 \times \mathcal{M}_1 \times \mathcal{M}_2 \to (F^{2m-1})^n$ that maps $(\boldsymbol{u}_0, \boldsymbol{u}_1, \boldsymbol{u}_2)$ to the unique array $\Gamma \in \mathcal{C}$ such that $(\Gamma)_{\mathcal{X}_b} = \boldsymbol{u}_b$ for $b = 0, 1, 2$. The existence of the decoding functions $\mathcal{D}_1$ and $\mathcal{D}_2$ that satisfy (2) is easily verified, and

$$\mathsf{red}(\mathcal{E}, \mathcal{D}_1, \mathcal{D}_2) = (\rho_0, \rho_1, \rho_2) = (n - k_0, n(m-1) - k_1, n(m-1) - k_2) \;,$$

which readily implies that $\rho_0 + \rho_1 + \rho_2 = \mathrm{red}(\mathcal{C})$. $\square$

Next we provide an example of a non-systematic set $\mathcal{C} \subseteq (F^{2m-1})^n$ for which no intersecting coding scheme $(\mathcal{E} : \mathcal{M} \to (F^{2m-1})^n, \mathcal{D}_1, \mathcal{D}_2)$ satisfies $\mathcal{E}(\mathcal{M}) = \mathcal{C}$.

Example A.4 For $t = 0, 1, 2, 3$, let $\boldsymbol{e}_t$ denote the following column words over $F = \{0, 1\}$:

$$\boldsymbol{e}_0 = (0\;0\;0)^T \;, \quad \boldsymbol{e}_1 = (1\;0\;0)^T \;, \quad \boldsymbol{e}_2 = (0\;1\;0)^T \;, \quad \text{and} \quad \boldsymbol{e}_3 = (0\;0\;1)^T \;.$$

Select $m = 1$ and $n = 3$, and consider the set $\mathcal{C} \subseteq F^3$ that is defined by

$$\mathcal{C} = \{(\boldsymbol{e}_1\;\boldsymbol{e}_0\;\boldsymbol{e}_1) \;,\; (\boldsymbol{e}_2\;\boldsymbol{e}_0\;\boldsymbol{e}_1) \;,\; (\boldsymbol{e}_3\;\boldsymbol{e}_0\;\boldsymbol{e}_2) \;,\; (\boldsymbol{e}_3\;\boldsymbol{e}_0\;\boldsymbol{e}_3)\} \;.$$

Suppose to the contrary that there exists an intersecting coding scheme $(\mathcal{E} : \mathcal{M} \to (F^3)^3, \mathcal{D}_1, \mathcal{D}_2)$ such that $\mathcal{E}(\mathcal{M}) = \mathcal{C}$. In particular,

$$|\mathcal{M}| = |\mathcal{M}_0| \cdot |\mathcal{M}_1| \cdot |\mathcal{M}_2| = |\mathcal{C}| = 4$$

and

$$|\mathcal{M}_0| \cdot |\mathcal{M}_b| \leq |\boldsymbol{\varphi}_b(\mathcal{C})| = 3 \;, \quad b = 1, 2 \;.$$

These conditions imply that $|\mathcal{M}_0| = 1$ and $|\mathcal{M}_1| = |\mathcal{M}_2| = 2$.

Denote $\mathcal{M}_1 = \{\alpha, \beta\}$ and partition $\mathcal{M}$ into $\mathcal{M}_\alpha = \mathcal{M}_0 \times \{\alpha\} \times \mathcal{M}_2$ and $\mathcal{M}_\beta = \mathcal{M}_0 \times \{\beta\} \times \mathcal{M}_2$. The existence of $\mathcal{D}_1$ implies from (2) that

$$\boldsymbol{\varphi}_1(\mathcal{E}(\mathcal{M}_\alpha)) \cap \boldsymbol{\varphi}_1(\mathcal{E}(\mathcal{M}_\beta)) = \emptyset$$

and, so,

$$|\boldsymbol{\varphi}_1(\mathcal{E}(\mathcal{M}_\alpha))| + |\boldsymbol{\varphi}_1(\mathcal{E}(\mathcal{M}_\beta))| = |\boldsymbol{\varphi}_1(\mathcal{E}(\mathcal{M}))| = |\boldsymbol{\varphi}_1(\mathcal{C})| = 3 \, .$$

Without loss of generality we assume that $|\boldsymbol{\varphi}_1(\mathcal{E}(\mathcal{M}_\alpha))| = 2$ and $|\boldsymbol{\varphi}_1(\mathcal{E}(\mathcal{M}_\beta))| = 1$. On the other hand, $|\mathcal{E}(\mathcal{M}_\beta)| = |\mathcal{M}_\beta| = 2$; hence, the set $\mathcal{E}(\mathcal{M}_\beta)$ is necessarily equal to $\{(\boldsymbol{e}_3 \, \boldsymbol{e}_0 \, \boldsymbol{e}_2) \, , \, (\boldsymbol{e}_3 \, \boldsymbol{e}_0 \, \boldsymbol{e}_3)\}$. Thus,

$$\mathcal{E}(\mathcal{M}_\alpha) = \mathcal{C} \setminus \mathcal{E}(\mathcal{M}_\beta) = \{(\boldsymbol{e}_1 \, \boldsymbol{e}_0 \, \boldsymbol{e}_1) \, , \, (\boldsymbol{e}_2 \, \boldsymbol{e}_0 \, \boldsymbol{e}_1)\} \, ,$$

which readily implies that $|\boldsymbol{\varphi}_2(\mathcal{E}(\mathcal{M}_\alpha))| = 1$. Yet, this contradicts the existence of a function $\mathcal{D}_2$ that satisfies (2). □

Appendix B

Proof of Lemma 2.4. Given an integer triple $\boldsymbol{\rho} \in \mathbb{A}_q(m, n, \tau_1, \tau_2)$, let $(\mathcal{E} : \mathcal{M} \to (F^{2m-1})^n, \mathcal{D}_1, \mathcal{D}_2)$ be an intersecting coding scheme that satisfies conditions (A1)–(A2), where $\mathcal{M} = \mathcal{M}_0 \times \mathcal{M}_1 \times \mathcal{M}_2$. Since $\boldsymbol{\rho}$ is integer-valued and $\boldsymbol{\rho}'$ satisfies (3), we can assume without loss of generality that for $b = 1, 2$, the set $\mathcal{M}_b$ takes the form $\mathcal{M}'_b \times F^\theta$, where $\log_q |\mathcal{M}'_b| = n(m-1) - \rho_b - \theta$; every element $\boldsymbol{u} \in \mathcal{M}_b$ can thus be written as $(\boldsymbol{u}' \,|\, \boldsymbol{w})$, where $\boldsymbol{u}' \in \mathcal{M}'_b$ and $\boldsymbol{w} \in F^\theta$. Denote by $\mathcal{M}'_0$ the set $\mathcal{M}_0 \times F^\theta$ and let a typical element $\boldsymbol{u}'_0 \in \mathcal{M}'_0$ be written as $(\boldsymbol{u}_0 \,|\, \boldsymbol{w}_0)$, where $\boldsymbol{u}_0 \in \mathcal{M}_0$ and $\boldsymbol{w}_0 \in F^\theta$. Define the mapping

$$\mathcal{E}' : \mathcal{M}'_0 \times \mathcal{M}'_1 \times \mathcal{M}'_2 \to (F^{2m-1})^n$$

for every $(\boldsymbol{u}'_0, \boldsymbol{u}'_1, \boldsymbol{u}'_2) \in \mathcal{M}'_0 \times \mathcal{M}'_1 \times \mathcal{M}'_2$ by

$$\mathcal{E}'\left(\boldsymbol{u}'_0, \boldsymbol{u}'_1, \boldsymbol{u}'_2\right) = \mathcal{E}'\left((\boldsymbol{u}_0 \,|\, \boldsymbol{w}_0), \boldsymbol{u}'_1, \boldsymbol{u}'_2\right) = \mathcal{E}\left(\boldsymbol{u}_0, (\boldsymbol{u}'_1 \,|\, \boldsymbol{w}_0), (\boldsymbol{u}'_2 \,|\, \boldsymbol{w}_0)\right) \, .$$

Letting $\mathcal{M}'$ denote the set $\mathcal{M}'_0 \times \mathcal{M}'_1 \times \mathcal{M}'_2$, it is easily seen that $\mathcal{E}'(\mathcal{M}') = \mathcal{E}(\mathcal{M})$.

We also define for $b = 1, 2$ the mapping $\mathcal{D}'_b : \mathcal{E}'(\mathcal{M}') \to \mathcal{M}'_0 \times \mathcal{M}'_b$ by

$$\mathcal{D}'_b(\boldsymbol{c}) = ((\boldsymbol{u}_0 \,|\, \boldsymbol{w}_0), \boldsymbol{u}'_b) \; , \quad \boldsymbol{c} \in \mathcal{E}'(\mathcal{M}') \, ,$$

where the words $\boldsymbol{u}_0$, $\boldsymbol{w}_0$, and $\boldsymbol{u}'_b$ are determined by $\mathcal{D}_b(\boldsymbol{c}) = (\boldsymbol{u}_0, (\boldsymbol{u}'_b \,|\, \boldsymbol{w}_0))$. Clearly, the triple $(\mathcal{E}', \mathcal{D}'_1, \mathcal{D}'_2)$ defines an intersecting coding scheme of length n over F^{2m-1} with redundancy $(\mathcal{E}', \mathcal{D}'_1, \mathcal{D}'_2) \leq \boldsymbol{\rho}'$. Hence, this coding scheme satisfies condition (A1) with respect to the triple $\boldsymbol{\rho}'$. And from $\mathcal{E}'(\mathcal{M}') = \mathcal{E}(\mathcal{M})$ we get that condition (A2) holds as well. We therefore conclude that $\boldsymbol{\rho}' \in \mathbb{A}_q(m, n, \tau_1, \tau_2)$.

Along similar lines, we can show that $\boldsymbol{\rho}''$ is also in $\mathbb{A}_q(m, n, \tau_1, \tau_2)$. Here, we write $\mathcal{M}_0 = \mathcal{M}''_0 \times F^{\theta_1} \times F^{\theta_2}$, where $\log_q |\mathcal{M}''_0| = n - \rho_0 - \theta_1 - \theta_2$, and for $b = 1, 2$ we let $\mathcal{M}''_b$ be the set $\mathcal{M}_b \times F^{\theta_b}$. An element $\boldsymbol{u}_0 \in \mathcal{M}_0$ will be written as $(\boldsymbol{u}''_0 \,|\, \boldsymbol{w}_1 \,|\, \boldsymbol{w}_2)$, where $\boldsymbol{u}''_0 \in \mathcal{M}''_0$ and

$\boldsymbol{w}_b \in F^{\theta_b}$; similarly, for $b = 1, 2$, we break an element $\boldsymbol{u}'' \in \mathcal{M}''_b$ into $(\boldsymbol{u} \,|\, \boldsymbol{w})$, where $\boldsymbol{u} \in \mathcal{M}_b$ and $\boldsymbol{w} \in F^{\theta_b}$. Writing $\mathcal{M}'' = \mathcal{M}''_0 \times \mathcal{M}''_1 \times \mathcal{M}''_2$, the encoding function

$$\mathcal{E}'' : \mathcal{M}'' \to (F^{2m-1})^n$$

is given by

$$\mathcal{E}''\left(\boldsymbol{u}''_0, \boldsymbol{u}''_1, \boldsymbol{u}''_2\right) = \mathcal{E}''\left(\boldsymbol{u}''_0, (\boldsymbol{u}_1 \,|\, \boldsymbol{w}_1), (\boldsymbol{u}_2 \,|\, \boldsymbol{w}_2)\right) = \mathcal{E}\left((\boldsymbol{u}''_0 \,|\, \boldsymbol{w}_1 \,|\, \boldsymbol{w}_2), \boldsymbol{u}_1, \boldsymbol{u}_2\right) ,$$

and for $b = 1, 2$ we let the decoding functions $\mathcal{D}''_b : \mathcal{E}''(\mathcal{M}'') \to \mathcal{M}''_0 \times \mathcal{M}''_b$ be defined for every $\boldsymbol{c}$ in $\mathcal{E}''(\mathcal{M}'')$ $(= \mathcal{E}(\mathcal{M}))$ by

$$\mathcal{D}''_b(\boldsymbol{c}) = (\boldsymbol{u}''_0, (\boldsymbol{u}_b \,|\, \boldsymbol{w}_b)) ,$$

where $\boldsymbol{u}''_0$, $\boldsymbol{u}_b$, and $\boldsymbol{w}_b$ are determined by $\mathcal{D}_b(\boldsymbol{c}) = ((\boldsymbol{u}''_0 \,|\, \boldsymbol{w}_1 \,|\, \boldsymbol{w}_2), \boldsymbol{u}_b)$. It can be easily verified that $(\mathcal{E}'', \mathcal{D}''_1, \mathcal{D}''_2)$ is an intersecting coding scheme of length n over F^{2m-1} that satisfies conditions (A1)–(A2) with respect to $\boldsymbol{\rho}''$. $\square$

Appendix C

In our proof of Lemma 4.3, we make use of the following known property of direct product of matrices (see Theorem 43.4 in [12]).

Lemma C.11 *Let A, B, C, and D be matrices over F for which the (ordinary) products AC and BD are defined. Then,*

$$(A \otimes B)(C \otimes D) = (AC) \otimes (BD) . \tag{40}$$

Proof of Lemma 4.3. (i) By Lemma C.11 it easily follows that the matrices in (22) commute.

(ii) The sought smallest sub-ring of $F^{m^2 \times m^2}$ must contain the elements $L_{a\omega_j} \otimes I_m$ and $I_m \otimes L_{a\omega_\ell}$ for all $0 \le j, \ell < m$ and $a \in F$, as well as the sum of products

$$\sum_{j,\ell} (L_{a_{j,\ell}\omega_j} \otimes I_m)(I_m \otimes L_{a_{j,\ell}\omega_\ell}) = \sum_{j,\ell} a_{j,\ell} \left(L_{\omega_j} \otimes L_{\omega_\ell}\right) , \quad a_{j,\ell} \in F .$$

We next verify that $L_\beta \otimes I_m$ and $I_m \otimes L_\gamma$ are spanned by (22); in fact, we show that $L_\beta \otimes L_\gamma$ is in that span for every $\beta, \gamma \in \Phi$. For every $\alpha, \gamma \in \Phi$ we have,

$$\boldsymbol{v}_\alpha L_\gamma \boldsymbol{\omega} = \alpha\gamma = \alpha \cdot \boldsymbol{v}_\gamma \boldsymbol{\omega} = \sum_\ell (\boldsymbol{v}_\gamma)_\ell (\alpha\omega_\ell) = \sum_\ell (\boldsymbol{v}_\gamma)_\ell \left(\boldsymbol{v}_\alpha L_{\omega_\ell} \boldsymbol{\omega}\right) = \boldsymbol{v}_\alpha \Big(\sum_\ell (\boldsymbol{v}_\gamma)_\ell L_{\omega_\ell}\Big) \boldsymbol{\omega} ,$$

i.e.,

$$L_\gamma = \sum_\ell (\boldsymbol{v}_\gamma)_\ell L_{\omega_\ell} \ .$$

Hence,

$$L_\beta \otimes L_\gamma = \Big(\sum_j (\boldsymbol{v}_\beta)_j L_{\omega_j}\Big) \otimes \Big(\sum_\ell (\boldsymbol{v}_\gamma)_\ell L_{\omega_\ell}\Big) = \sum_{j,\ell} (\boldsymbol{v}_\beta)_j (\boldsymbol{v}_\gamma)_\ell (L_{\omega_j} \otimes L_{\omega_\ell}) \ . \tag{41}$$

(iii) Clearly, addition is preserved under the mapping (23). Since direct product is distributive with addition in $F^{m\times m}$, then so is the product $\odot$ in $F^{m\times m}$. Hence, to establish the isomorphism, it suffices to show that multiplication is preserved when the multiplicands take the form $L_\beta \otimes L_\gamma$ for $\beta, \gamma \in \Phi$ (in particular, this includes all elements in (22)).

By (41) we deduce that (23) associates the element $L_\beta \otimes L_\gamma$ ($\in \Phi \otimes \Phi$) with the element $\boldsymbol{v}_\beta^T \boldsymbol{v}_\gamma$ ($\in F^{m\times m}$). Taking the $\odot$-product of $\boldsymbol{v}_\beta^T \boldsymbol{v}_\gamma$ and $\boldsymbol{v}_{\beta'}^T \boldsymbol{v}_{\gamma'}$ we get

$$\begin{aligned}
(\boldsymbol{v}_\beta^T \boldsymbol{v}_\gamma) \odot (\boldsymbol{v}_{\beta'}^T \boldsymbol{v}_{\gamma'}) &= M^T((\boldsymbol{v}_\beta^T \boldsymbol{v}_\gamma) \otimes (\boldsymbol{v}_{\beta'}^T \boldsymbol{v}_{\gamma'}))M \\
&\overset{(40)}{=} M^T(\boldsymbol{v}_\beta^T \otimes \boldsymbol{v}_{\beta'}^T)(\boldsymbol{v}_\gamma \otimes \boldsymbol{v}_{\gamma'})M \\
&= ((\boldsymbol{v}_\beta \otimes \boldsymbol{v}_{\beta'})M)^T(\boldsymbol{v}_\gamma \otimes \boldsymbol{v}_{\gamma'})M \\
&= \boldsymbol{v}_{\beta\beta'}^T \boldsymbol{v}_{\gamma\gamma'} \ ,
\end{aligned}$$

where in the last step we have used the equality $(\boldsymbol{v}_\gamma \otimes \boldsymbol{v}'_\gamma)M = \boldsymbol{v}_{\gamma\gamma'}$, which, in turn, follows from the chain

$$(\boldsymbol{v}_\gamma \otimes \boldsymbol{v}_{\gamma'})M\boldsymbol{\omega} \overset{(20)}{=} (\boldsymbol{v}_\gamma \otimes \boldsymbol{v}_{\gamma'})(\boldsymbol{\omega} \otimes \boldsymbol{\omega}) \overset{(40)}{=} (\boldsymbol{v}_\gamma \boldsymbol{\omega}) \otimes (\boldsymbol{v}_{\gamma'} \boldsymbol{\omega}) = \gamma\gamma' = \boldsymbol{v}_{\gamma\gamma'}\boldsymbol{\omega} \ .$$

We thus conclude that the product $(\boldsymbol{v}_\beta^T \boldsymbol{v}_\gamma) \odot (\boldsymbol{v}_{\beta'}^T \boldsymbol{v}_{\gamma'})$ is associated by (23) with the element

$$L_{\beta\beta'} \otimes L_{\gamma\gamma'} = (L_\beta L_{\beta'}) \otimes (L_\gamma L_{\gamma'}) \overset{(40)}{=} (L_\beta \otimes L_\gamma)(L_{\beta'} \otimes L_{\gamma'})$$

of $\Phi \otimes \Phi$.

(iv) As in part (iii), it suffices to consider the case where $A = \boldsymbol{v}_\beta^T \boldsymbol{v}_\gamma$ and $B = \boldsymbol{v}_{\beta'}^T \boldsymbol{v}_{\gamma'}$; here,

$$A \odot B = \boldsymbol{v}_{\beta\beta'}^T \boldsymbol{v}_{\gamma\gamma'} \ ,$$

while

$$\mathsf{row}(A)\,\mathbf{B} = (\boldsymbol{v}_\beta \otimes \boldsymbol{v}_\gamma)(L_{\beta'} \otimes L_{\gamma'}) = (\boldsymbol{v}_\beta L_{\beta'}) \otimes (\boldsymbol{v}_\gamma L_{\gamma'}) = \boldsymbol{v}_{\beta\beta'} \otimes \boldsymbol{v}_{\gamma\gamma'} = \mathsf{row}(\boldsymbol{v}_{\beta\beta'}^T \boldsymbol{v}_{\gamma\gamma'}) \ .$$

$\square$

References

[1] E.R. Berlekamp, *Algebraic Coding Theory,* Revised Edition, Aegean Park Press, Laguna Hill, California, 1984.

[2] R.E. Blahut, *Theory and Practice of Error-Control Codes,* Addison-Wesley, Reading, Massachusetts, 1984.

[3] T.M. Cover, *Broadcast channels, IEEE Trans. Inform. Theory,* 18 (1972), 2–14.

[4] T.M. Cover, *An achievable rate region for the broadcast channel, IEEE Trans. Inform. Theory,* 21 (1975), 399–404.

[5] T.M. Cover, *Comments on broadcast channels, IEEE Trans. Inform. Theory,* 44 (1998), 2524–2530.

[6] T.M. Cover, J.A. Thomas, *Elements of Information Theory,* Wiley, New York, 1991.

[7] Ph. Delsarte, *Bilinear forms over a finite field, with applications to coding theory, J. Comb. Th. A,* 25 (1978), 226–241.

[8] E.M. Gabidulin, *Theory of codes with maximum rank distance, Probl. Peredach. Inform.,* 21 (1985), 3–16 (in Russian; pp. 1–12 in the English translation).

[9] E.M. Gabidulin, *Optimal array error-correcting codes, Probl. Peredach. Inform.,* 21 (1985), 102–106 (in Russian).

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

[11] S. Lin, D.J. Costello, Jr., *Error Control Coding: Fundamentals and Applications,* Prentice Hall, Englewood Cliffs, 1983.

[12] C.C. MacDuffee, *The Theory of Matrices,* Chelsea, New York, 1946.

[13] S. MacLane, G. Birkhoff, *Algebra,* Third Edition, Chelsea Publishing Company, New York, 1967.

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

[15] R.M. Roth, *Maximum-rank array codes and their application to crisscross error correction, IEEE Trans. Inform. Theory,* 37 (1991), 328–336.

[16] B.L. van der Waerden, *Algebra,* Volume II, Springer-Verlag, New York, 1991.