On Spectral Design Methods for Quasi-Cyclic Codes

Ron M. Roth, *Fellow, IEEE* Alexander Zeh, *Member, IEEE*

***Abstract*—A method is provided for constructing upper-triangular square matrices over the univariate polynomial ring over a finite field, under certain constraints on the eigenvalues of the matrices. In some cases of interest, the degree of the determinant of such matrices is shown to be the smallest possible. The method is then applied to construct generator polynomial matrices of quasi-cyclic codes for correcting phased burst errors. Finally, an interpolation-based list decoding algorithm is presented for these codes, which, for a wide range of code parameters, is shown to outperform existing list decoding schemes.**

***Index Terms*—List decoding, phased burst error, quasi-cyclic code, spectral analysis and design, subspace subcode.**

I. Introduction

In [19], Semenov and Trifonov presented a counterpart of the BCH bound for quasi-cyclic codes. Generalizations to (an analog of) the Hartmann–Tzeng bound for quasi-cyclic codes have since been presented in [22].

Motivated by those results, we consider here the problem of synthesizing upper-triangular square matrices over the univariate polynomial ring over a finite field, under certain constraints on their eigenvalues. Using the BCH-like bound of [19], we then illustrate how our synthesis method can be used to construct quasi-cyclic codes with prescribed error correction capabilities. We also present an interpolation-based list decoding algorithm for them.

Our formulation of the matrix synthesis problem, which could be of independent interest, is presented below. Hereafter, for integers $a \leq b$, we denote by $[a\,{:}\,b]$ the integer set $\{a, a{+}1, a{+}2, \ldots, b\}$, with $[b]$ being a shorthand notation for $[1\,{:}\,b]$.

Let $F = \mathrm{GF}(q)$ and $\Phi = \mathrm{GF}(q^h)$, and fix Γ to be a subset of Φ. Also, fix ℓ to be an integer in $[h]$. Given the quadruple (F, Φ, Γ, ℓ), we are interested in constructing an $\ell \times \ell$ matrix $\boldsymbol{G}(x) = (g_{i,j}(x))_{i,j=1}^{\ell}$ over $F[x]$ with the following properties.

(P1) $\boldsymbol{G}(x) = (g_{i,j}(x))_{i,j=1}^{\ell}$ is upper-triangular, i.e., $g_{i,j}(x) = 0$ for $i > j$.

(P2) $g_{i,i}(x) \neq 0$, for every $i \in [\ell]$.

(P3) There exists a column vector $\boldsymbol{v} \in \Phi^{\ell}$ whose entries are linearly independent over F, such that for every $\beta \in \Gamma$,

$$\boldsymbol{G}(\beta)\boldsymbol{v} = \boldsymbol{0}\ .$$

The elements of Γ will be referred to as the *(designed) eigenvalues* of $\boldsymbol{G}(x)$ [4, Ch. 1], and the vector $\boldsymbol{v}$ in (P3) will be called the *common eigenvector*. Note that the eigenvalues are roots of the polynomial $\det(\boldsymbol{G}(x)) = \prod_{i\in[\ell]} g_{i,i}(x)\ (\in F[x])$.

The degree of the polynomial $\det(\boldsymbol{G}(x))$ will be (sloppily) referred to as the degree of $\boldsymbol{G}(x)$ and will be denoted by $\deg \boldsymbol{G}(x)$; clearly, $\deg \boldsymbol{G}(x) = \sum_{i\in[\ell]} \deg g_{i,i}(x)$.

Next we state our synthesis problem.

Problem 1. *Given (F, Φ, Γ, ℓ), find an $\ell \times \ell$ matrix $\boldsymbol{G}(x)$ over $F[x]$ with the smallest degree, among all matrices that satisfy properties (P1)–(P3).*

The rest of this work is organized as follows. We start by presenting in Section II the relation of Problem 1 to the design of quasi-cyclic codes. Then, in Section III, we present lower bounds on the degree of matrices $\boldsymbol{G}(x)$ that satisfy properties (P1)–(P3), and in Section IV, we present a method for constructing such matrices, which, in certain cases of interest, attain those bounds (thereby solving Problem 1 for those cases). In Section V, we turn back to quasi-cyclic codes and illustrate an application of our method to the design of such codes. Finally in Section VI, we present a list decoding algorithm for correcting phased burst errors while using our codes, and we demonstrate that, for a wide range of code parameters, our codes outperform existing list decoding schemes.

II. Application to quasi-cyclic codes

A quasi-cyclic $[\ell \times n, k]$ code (or an ℓ-quasi-cyclic $[\ell n, k]$ code) over $F = \mathrm{GF}(q)$ is a linear $[\ell n, k]$ code $\mathbb{C}$ over F with the additional property that when the entries in a codeword are arranged (in a prescribed order) to form an $\ell \times n$ array over F, then re-ordering of the columns through a cyclic shift results in another codeword of $\mathbb{C}$. If we represent each row in a codeword array as a polynomial in the set $F_n[x]$ of all polynomials of degree less than n over F, then the code $\mathbb{C}$ can be written as (see [11]):

$$\mathbb{C} = \Big\{ \boldsymbol{c}(x) \in (F_n[x])^{\ell}\ :\ \boldsymbol{c}(x) = \boldsymbol{u}(x)\boldsymbol{G}(x) \ \textsc{mod}\ ((x^n - 1)\cdot \boldsymbol{1})\ ,\ \text{for some}\ \ \boldsymbol{u}(x) \in (F[x])^{\ell} \Big\}\ ,$$

where $\boldsymbol{1}$ is the all-1 row vector in F^{ℓ}, the operation "MOD" stands for taking the remainder component-by-component, and

This work was supported in part by Grant No. 1396/16 from the Israel Science Foundation. A. Zeh was supported by the German research council (Deutsche Forschungsgemeinschaft, DFG) under grant Ze1016/1-1.Parts of this work were presented at the *IEEE International Symposium on Information Theory (ISIT)*, in 2015 and 2016.

Ron M. Roth is with the Computer Science Department, Technion, Haifa 3200003, Israel. Email: ronny@cs.technion.ac.il

Alexander Zeh is with the Automotive Cybersecurity Research and Development Center, Infineon Technologies AG, 85579 Munich (Neubiberg), Germany. This work was done while A. Zeh was with the Computer Science Dept., Technion, Haifa, Israel. Email: alexzeh@gmx.de

$\boldsymbol{G}(x) = (g_{i,j}(x))_{i,j=1}^{\ell}$ is an $\ell \times \ell$ *generator polynomial matrix* over $F[x]$.[1] As shown in [11], there is always such a generator polynomial matrix $\boldsymbol{G}(x)$ for $\mathbb{C}$ that satisfies properties (P1)–(P2); in fact, it satisfies the following stronger property (which implies (P1)–(P2)).

(P4) There exists an upper-triangular $\ell \times \ell$ matrix $\boldsymbol{H}(x)$ over $F[x]$ such that, over $F[x]$,

$$\boldsymbol{H}(x)\boldsymbol{G}(x) = (x^n - 1) \cdot \boldsymbol{I}_\ell$$

(where $\boldsymbol{I}_\ell$ is the identity matrix of order ℓ). In particular, $g_{i,i}(x)$ divides $x^n - 1$, for every $i \in [\ell]$.

When $\boldsymbol{G}(x)$ is such a generator polynomial matrix, the redundancy of $\mathbb{C}$, as a linear code over F, equals $\deg \boldsymbol{G}(x)$, namely, the dimension is[2]

$$k = \ell n - \deg \boldsymbol{G}(x) \ . \tag{1}$$

Conversely, if $\boldsymbol{G}(x)$ is an $\ell \times \ell$ matrix over $F[x]$ that satisfies property (P4), then it generates a quasi-cyclic $[\ell \times n, k]$ code over F.

For systematic encoding of generalized quasi-cyclic codes (which include ℓ-quasi-cyclic codes as a special case), see [14, Section 2.5] and references therein.

Proposition 1 below is (a modified version of) the BCH-like bound of [19]. In our setting, the minimum (Hamming) distance of a quasi-cyclic $[\ell \times n, k]$ code $\mathbb{C}$ over F is measured in symbols of F^ℓ; namely, we regard $\mathbb{C}$ as having length n over F^ℓ, and the minimum distance is then the smallest number of nonzero columns in any nonzero $\ell \times n$ array of $\mathbb{C}$.[3] This definition of minimum distance determines the correction capability of $\mathbb{C}$ when handling *ℓ-phased burst errors*, i.e., bursts of length ℓ (or less) that are aligned with the columns of the transmitted $\ell \times n$ array.

Proposition 1. *Let $\mathbb{C}$ be a quasi-cyclic $[\ell \times n, k]$ code over $F = \mathrm{GF}(q)$ where $\gcd(n, q) = 1$, and let $\boldsymbol{G}(x)$ be a generator polynomial matrix of $\mathbb{C}$ that satisfies property (P4). Suppose, in addition, that $\boldsymbol{G}(x)$ satisfies property (P3) with respect to the set*

$$\Gamma = \Gamma_{\alpha,b,d} = \left\{ \alpha^b, \alpha^{b+1}, \ldots, \alpha^{b+d-2} \right\} \ , \tag{2}$$

where $d \in \mathbb{Z}^+$, $b \in \mathbb{Z}$, and α is a primitive nth root of unity in the splitting field, $\Phi = \mathrm{GF}(q^h)$, of $x^n - 1$. Then the minimum distance of $\mathbb{C}$ (over F^ℓ) is at least d.

Proposition 1 follows essentially from [19] (for completeness, we will include a proof based on Proposition 2 below). Proposition 1 can serve as a design tool for quasi-cyclic codes.[4] Specifically, we seek a generator polynomial matrix $\boldsymbol{G}(x)$ that satisfies properties (P3)–(P4) for $\Gamma = \Gamma_{\alpha,b,d}$, thereby guaranteeing a minimum distance (over F^ℓ) of at least d; and, by (1), we would like $\deg \boldsymbol{G}(x)$ to be as small as possible.

In fact, when $\deg \boldsymbol{G}(x)$ is the smallest, the respective quasi-cyclic code is a subspace subcode of a Reed–Solomon code [7]. We state this in the next proposition.

Proposition 2. *Let F, n, d, b, h, Φ, and α be as in Proposition 1 and let C_{RS} be the $[n, n-d+1, d]$ Reed–Solomon code C_{RS} over Φ whose set of roots is given by $\Gamma_{\alpha,b,d}$ as defined by (2). Given $\ell \in [h]$ and a column vector $\boldsymbol{v} \in \Phi^\ell$ whose entries are linearly independent over F, define the code $\mathbb{C}$ by*

$$\mathbb{C} = \mathbb{C}_{\mathrm{RS}}(\boldsymbol{v}) = \left\{ \boldsymbol{c}(x) \in (F_n[x])^\ell \ : \ \boldsymbol{c}(x) \cdot \boldsymbol{v} \in \mathsf{C}_{\mathrm{RS}} \right\} \ . \tag{3}$$

Then $\mathbb{C}$ is a quasi-cyclic $[\ell \times n, k]$ code over F which is generated by a polynomial matrix that has the smallest degree among all polynomial matrices that satisfy properties (P3)–(P4) with respect to the set $\Gamma_{\alpha,b,d}$ and the common eigenvector $\boldsymbol{v}$.

Proof. Since C_{RS} is cyclic over Φ, the code $\mathbb{C}$ is quasi-cyclic over F. Let $\boldsymbol{G}(x)$ be a generator polynomial matrix of $\mathbb{C}$ that satisfies property (P4). For every $\boldsymbol{u}(x) \in (F[x])^\ell$ we have

$$\boldsymbol{u}(x)\boldsymbol{G}(x) \ \mathrm{MOD}\ ((x^n - 1) \cdot \boldsymbol{1}) \in \mathbb{C}$$

and, so,

$$\boldsymbol{u}(x)\boldsymbol{G}(x)\boldsymbol{v} \ \mathrm{MOD}\ (x^n - 1) \in \mathsf{C}_{\mathrm{RS}} \ .$$

It follows that for every $\boldsymbol{u}(x) \in (F[x])^\ell$ and $\beta \in \Gamma_{\alpha,b,d}$:

$$\boldsymbol{u}(\beta)\boldsymbol{G}(\beta)\boldsymbol{v} = 0 \ ,$$

which implies that $\boldsymbol{G}(\beta)\boldsymbol{v} = \boldsymbol{0}$ for every $\beta \in \Gamma_{\alpha,b,d}$, i.e., $\boldsymbol{G}(x)$ satisfies property (P3) with respect to $\Gamma_{\alpha,b,d}$ and $\boldsymbol{v}$.

Turning now to showing the minimality of $\deg \boldsymbol{G}(x)$, let $\boldsymbol{G}'(x)$ be an $\ell \times \ell$ polynomial matrix that satisfies properties (P3)–(P4) with respect to $\Gamma_{\alpha,b,d}$ and $\boldsymbol{v}$, and let $\mathbb{C}'$ be the quasi-cyclic $[\ell \times n, k']$ code over F that is generated by $\boldsymbol{G}'(x)$. We show that $\mathbb{C}' \subseteq \mathbb{C}$.

Let $\boldsymbol{c}(x) \in (F_n[x])^\ell$ be a codeword of $\mathbb{C}'$. Then, for some $\boldsymbol{u}(x) \in (F[x])^\ell$,

$$\boldsymbol{c}(x) = \boldsymbol{u}(x)\boldsymbol{G}'(x) \ \mathrm{MOD}\ ((x^n - 1) \cdot \boldsymbol{1})$$

and, so,

$$\boldsymbol{c}(\beta) = \boldsymbol{u}(\beta)\boldsymbol{G}'(\beta) \ , \quad \text{for every } \beta \in \Gamma_{\alpha,b,d} \ .$$

Hence,

$$\boldsymbol{c}(\beta) \cdot \boldsymbol{v} = \boldsymbol{u}(\beta)\boldsymbol{G}'(\beta)\boldsymbol{v} = 0 \ , \quad \text{for every } \beta \in \Gamma_{\alpha,b,d} \ ,$$

namely, $\boldsymbol{c}(x) \cdot \boldsymbol{v} \in \mathsf{C}_{\mathrm{RS}}$. We conclude that $\boldsymbol{c}(x)$ must be a codeword of $\mathbb{C}$. □

Proof of Proposition 1. Let $\boldsymbol{v}$ be a common eigenvector of $\boldsymbol{G}(x)$ with respect to the set $\Gamma_{\alpha,b,d}$. Then $\mathbb{C}$ plays the role of $\mathbb{C}'$ in the last proof and is therefore a subcode of the code $\mathbb{C}_{\mathrm{RS}}(\boldsymbol{v})$ defined in (3). The code $\mathbb{C}_{\mathrm{RS}}(\boldsymbol{v})$, in turn, is a subspace subcode of a Reed–Solomon code with minimum distance d, thereby yielding the result. □

[1] To simplify the notation, the codewords $\boldsymbol{c}(x)$ are defined here to be (row) ℓ-tuples over $F_n[x]$, rather than elements of the module $(F[x]/\langle x^n - 1 \rangle)^\ell$ and, so, $\boldsymbol{G}(x)$ is seen as a matrix over $F[x]$. In that regard, we are inconsistent with the notation in [11].

[2] As shown in [11], by elementary operations on rows, the matrix $\boldsymbol{G}(x)$ can be further brought into a reduced form where $\deg g_{j,i}(x) < \deg g_{i,i}(x)$, for every $j < i$. Yet this reduction does not affect the diagonal entries and therefore does not change $\deg \boldsymbol{G}(x)$.

[3] On the other hand, the goal in [19] is to find a lower bound on the minimum distance of $\mathbb{C}$ when $\mathbb{C}$ is seen as a code of length ℓn over F. See Appendix A for the adaptation of the setting of [19] to ours.

[4] So can the Hartmann–Tzeng-like improvement obtained in [22], yet for the sake of simplicity, we will refer here only to Proposition 1.

In view of the connection with subspace subcodes of Reed–Solomon codes, the lower bounds on $\deg \boldsymbol{G}(x)$ that we present in the next section are related in part to Theorem 4.4 in [7] (and Proposition 3 below can also be proved using that theorem). The paper [7], however, does not present a general strategy for obtaining constructions that attain those bounds.

III. Lower bounds on the degree

Let F, Φ, Γ, and ℓ be as in Section I, and let $\boldsymbol{G}(x)$ satisfy properties (P1)–(P3) therein. We obtain here lower bounds on $\deg \boldsymbol{G}(x)$, which apply when $\ell = h$ or when Γ has a certain structure which will be of interest (e.g., for our quasi-cyclic application).

Let $\mathcal{P} = \mathcal{P}(\Gamma) = \{\pi_1, \pi_2, \ldots\}$ be a partition of Γ, such that any two elements $\beta, \gamma \in \Gamma$ are in the same subset $\pi \in \mathcal{P}$, if and only if they are conjugate with respect to F (namely, $\gamma = \beta^{q^j}$ for some $j \in \mathbb{Z}^+$). For each $\pi \in \mathcal{P}$, let $M_\pi(x)$ be the minimal polynomial (with respect to F) of the elements of π and let $m_\pi = \deg M_\pi(x)$ (thus, $|\pi| \le m_\pi$).

We prove in this section the next two propositions. Hereafter, a sum (respectively, product) over an empty set is defined as 0 (respectively, 1).

Proposition 3. *When $\ell = h$,*

$$\deg \boldsymbol{G}(x) \ge |\Gamma| \cdot h \ .$$

Proposition 4. *For each $\pi \in \mathcal{P}$, let ρ_π be the largest integer (possibly ∞) such that, for some $\beta_\pi \in \pi$,*

$$\beta_\pi^{q^j} \in \pi \quad \textit{for} \quad 0 \le j < \rho_\pi \ .$$

Then,

$$\begin{aligned} \deg \boldsymbol{G}(x) \quad &\ge \quad \sum_{\pi \in \mathcal{P}} \min(\ell, \rho_\pi) \cdot m_\pi &(4)\\ &= \quad \Bigl(\ell \cdot \sum_{\pi \,:\, \rho_\pi \ge \ell} m_\pi\Bigr) + \sum_{\pi \,:\, \rho_\pi < \ell} \rho_\pi \cdot m_\pi \ . &(5)\end{aligned}$$

Remark 1. The first term in (5) suggests that a minimum-degree matrix $\boldsymbol{G}(x)$ can be obtained by

$$\boldsymbol{G}(x) = \Bigl(\prod_{\pi \,:\, \rho_\pi \ge \ell} M_\pi(x)\Bigr) \cdot \boldsymbol{G}^*(x) \ ,$$

where $\boldsymbol{G}^*(x)$ is an $\ell \times \ell$ minimum-degree matrix for the set $\Gamma^* = \cup_{\pi \,:\, \rho_\pi < \ell} \pi$. □

The proofs of both propositions make use of the following lemma.

Lemma 5. *Let $\pi \in \mathcal{P}$ and let $J \subseteq [0\,{:}\,h{-}1]$ be of size $|J| \le \ell$ such that, for some $\beta \in \pi$,*

$$\Bigl\{\gamma \ : \ \gamma = \beta^{q^j} \ \textit{ for some } \ j \in J\Bigr\} \subseteq \pi \ . \qquad (6)$$

Then

$$(M_\pi(x))^{|J|} \ \Bigm| \ \det(\boldsymbol{G}(x))$$

when either $\ell = h$ or $J = [0\,{:}\,|J|{-}1]$.

Remark 2. A given element γ in (6) may correspond to more than one $j \in J$. For example, we may have $\pi = \{1\}$, $\beta = 1$, and $J = [0\,{:}\,\ell{-}1]$. □

Proof of Lemma 5. By properly selecting β, we can assume without loss of generality that $0 \in J$. Let $\boldsymbol{v} = (v_1\ v_2\ \ldots\ v_\ell)^T$ be a common eigenvector as in property (P3). For $j \in J$, define

$$\boldsymbol{v}_j = \Bigl(v_1^{q^{h-j}}\ v_2^{q^{h-j}}\ \ldots\ v_\ell^{q^{h-j}}\Bigr)^T$$

(where $\boldsymbol{v}_0 = \boldsymbol{v}$). From the definition of a common eigenvector, we have

$$\boldsymbol{G}(\beta^{q^j})\boldsymbol{v} = \boldsymbol{0} \ , \quad j \in J \ ,$$

and, raising to the q^{h-j}th power, we get

$$\boldsymbol{G}(\beta)\boldsymbol{v}_j = \boldsymbol{0} \ , \quad j \in J \ . \qquad (7)$$

Now, when $\ell = h$ or when $J = [0\,{:}\,|J|{-}1]$, the $\ell \times |J|$ matrix

$$\Bigl(\ \boldsymbol{v}_1 \mid \boldsymbol{v}_2 \mid \ldots \mid \boldsymbol{v}_{|J|}\ \Bigr) = \Bigl(\ v_i^{q^{h-j}}\ \Bigr)_{i \in [\ell], j \in J}$$

has full rank, $|J|$ $(\le \ell)$, over Φ [13, pp. 109–110], i.e., the set $\{\boldsymbol{v}_j\}_{j \in J}$ spans a linear space of dimension $|J|$ over Φ. It follows from (7) that $\mathrm{rank}(\boldsymbol{G}(\beta)) \le \ell - |J|$, i.e., there must be at least $|J|$ indexes $i \in [\ell]$ for which $g_{i,i}(\beta) = 0$. It follows that $(x - \beta)^{|J|}$ divides $\det(\boldsymbol{G}(x)) = \prod_{i \in [\ell]} g_{i,i}(x)$, and, since $\boldsymbol{G}(x)$ is over $F[x]$, we have closure under conjugacy, namely, $(M_\pi(x))^{|J|} \mid \det(\boldsymbol{G}(x))$. □

Proof of Proposition 3. For each $\pi \in \mathcal{P}$, let J_π be a largest subset of $[0\,{:}\,h{-}1]$ such that, for some $\beta_\pi \in \pi$,

$$\beta_\pi^{q^j} \in \pi \quad \text{if and only if} \quad j \in J_\pi \ .$$

By Lemma 5,

$$\prod_{\pi \in \mathcal{P}} (M_\pi(x))^{|J_\pi|} \ \Bigm| \ \det(\boldsymbol{G}(x)) \ . \qquad (8)$$

Noting that $|J_\pi| = |\pi| \cdot h/m_\pi$, we get that $\deg \boldsymbol{G}(x) \ge \sum_{\pi \in \mathcal{P}} |J_\pi| \cdot m_\pi = |\Gamma| \cdot h$. □

Proof of Proposition 4. By Lemma 5, Eq. (8) holds when we take J_π to be the set $[0\,{:}\,\min(\ell, \rho_\pi){-}1]$, for every $\pi \in \mathcal{P}$. □

The sets J_π in the proof of Proposition 4 are very structured. One may wonder if the bound (4) continues to hold if each ρ_π therein is replaced by $|J_\pi|$, where J_π is an arbitrary subset of $[0\,{:}\,h{-}1]$ such that $\beta_\pi^{q^j} \in \pi$ for some $\beta_\pi \in \Phi$ and every $j \in J_\pi$. The answer is generally false, as demonstrated by a counterexample in Appendix B.

IV. Construction

Let F, Φ, Γ, and ℓ be as in Section I. We show a construction of an $\ell \times \ell$ matrix $\boldsymbol{G}(x)$ over $F[x]$ that satisfies properties (P1)–(P3). In certain cases, the degree of $\boldsymbol{G}(x)$ will reach the lower bound of Proposition 4, thereby solving Problem 1 for those cases.

For our construction, we fix $m \ge \ell$ to be a divisor of h (e.g., $m = h$) and γ_0 to be a proper element of $\mathrm{GF}(q^m)$ (i.e., γ_0 does not belong to any proper subfield of $\mathrm{GF}(q^m)$).

We use the notation $\mathcal{P}$, $M_\pi(x)$, and m_π, for $\pi \in \mathcal{P}$, as in Section III. We define the set $\mathcal{P}^* \subseteq \mathcal{P}$ by

$$\mathcal{P}^* = \mathcal{P}^*(m) = \Bigl\{\pi \in \mathcal{P} \ : \ |\pi| < \ell \ \text{ and } \ m \mid m_\pi\Bigr\} \ .$$

Our construction will be of the form

$$\boldsymbol{G}(x) = \Big(\prod_{\pi \in \mathcal{P} \setminus \mathcal{P}^*} M_\pi(x) \Big) \cdot \boldsymbol{G}^*(x) \; , \tag{9}$$

where $\boldsymbol{G}^*(x)$ is an $\ell \times \ell$ matrix that satisfies properties (P1)–(P3) with respect to the set $\Gamma^* = \cup_{\pi \in \mathcal{P}^*} \pi$ (compare with Remark 1).

For $1 \le s < i \le \ell$, define the sets

$$\mathcal{P}_{i,s} = \mathcal{P}_{i,s}(m) = \Big\{ \pi \in \mathcal{P}^* \;:\; s \le |\pi| < i \Big\} \; ,$$

and let $\Gamma_i^* = \cup_{\pi \in \mathcal{P}_{i,1}} \pi$; i.e., Γ_i^* consists of all elements in Γ that belong to partition elements $\pi \in \mathcal{P}^*$ of size less than i (thus, $\Gamma_1^* = \emptyset$).

As a first step in our construction of $\boldsymbol{G}^*(x)$, we construct for each $i \in [\ell]$ a bivariate polynomial $B_i(x,y) \in F[x,y]$ of y-degree less than i, with the property that

$$B_i\left(\beta, \gamma_0^{-1}\right) = 0 \; , \quad \text{for every } \beta \in \Gamma_i^* \; .$$

To this end, we assume some ordering on the elements of each $\pi \in \mathcal{P}^*$:

$$\pi = \left\{ \beta_{\pi,1}, \beta_{\pi,2}, \ldots, \beta_{\pi,|\pi|} \right\} \; .$$

Next, for $1 \le s < i \le \ell$, we define the following polynomials $p_{i,s}(x) \in F[x]$:

$$p_{i,s}(x) = \sum_{\pi \in \mathcal{P}_{i,s}} a_{i,\pi,s}(x) \cdot \prod_{\pi' \in \mathcal{P}_{i,s} \setminus \{\pi\}} M_{\pi'}(x) \; ,$$

where $a_{i,\pi,s}(x)$ is the unique polynomial in $F_{m_\pi}[x]$ such that

$$a_{i,\pi,s}(\beta_{\pi,s}) = \gamma_0 \cdot \Big(\prod_{\pi' \in \mathcal{P}_{i,s} \setminus \{\pi\}} M_{\pi'}(\beta_{\pi,s}) \Big)^{-1} \; .$$

Note that for every $\pi \in \mathcal{P}^*$ and $s \in [|\pi|]$, both γ_0 and $\beta_{\pi,s}$ are elements of $\mathrm{GF}(q^{m_\pi})$, with $\beta_{\pi,s}$ being a proper element of this field; hence, $a_{i,\pi,s}(x)$ is well defined.

The following lemma is immediate.

Lemma 6. *For $1 \le s < i \le \ell$ and $\pi \in \mathcal{P}_{i,s}$,*

$$p_{i,s}(\beta_{\pi,s}) = \gamma_0 \; .$$

The sought bivariate polynomial $B_i(x,y) \in F[x,y]$ is now defined for each $i \in [\ell]$ by

$$B_i(x,y) = \prod_{s=1}^{i-1} \left(1 - p_{i,s}(x) y \right) \; ,$$

where $B_1(x,y) \equiv 1$. We have the following lemma.

Lemma 7. *For $i \in [2 : \ell]$ and every $\beta \in \Gamma_i^*$,*

$$B_i\left(\beta, \gamma_0^{-1}\right) = 0 \; .$$

Proof. Given $\beta \in \Gamma_i^*$, let π be the unique subset in $\mathcal{P}_{i,1}$ that contains β; then $\beta = \beta_{\pi,s}$ for some $s \le |\pi| < i$, and for this s we have by Lemma 6 that $p_{i,s}(\beta) = \gamma_0$. It follows that

$$B_i\left(\beta, \gamma_0^{-1}\right) = \prod_{s=1}^{i-1} \left(1 - p_{i,s}(\beta) \gamma_0^{-1} \right) = 0 \; ,$$

as claimed. □

Our construction of the polynomial matrix $\boldsymbol{G}^*(x)$ in (9) is iterative. For each $i \in [\ell]$, we construct an $i \times i$ matrix $\boldsymbol{G}_i(x)$ over $F[x]$, as follows:

$$\boldsymbol{G}_i(x) = \left(\begin{array}{c|cccc} B_{i,0}(x) & B_{i,1}(x) & B_{i,2}(x) & \ldots & B_{i,i-1}(x) \\ \hline 0 & & & & \\ \vdots & \multicolumn{4}{c}{\Big(\prod_{\pi \in \mathcal{P}_{i,i-1}} M_\pi(x) \Big) \cdot \boldsymbol{G}_{i-1}(x)} \\ 0 & & & & \end{array} \right) , \tag{10}$$

where $\boldsymbol{G}_0(x)$ is the "empty" (0×0) matrix and

$$B_{i,0}(x), B_{i,1}(x), \ldots, B_{i,i-1}(x)$$

are the coefficients in $F[x]$ of $B_i(x,y)$, namely,

$$B_i(x,y) = \sum_{j=0}^{i-1} B_{i,j}(x) y^j \; .$$

We then let $\boldsymbol{G}^*(x) = \boldsymbol{G}_\ell(x)$. As we show in Proposition 8 below, the resulting matrix $\boldsymbol{G}(x)$ in (9) satisfies properties (P1)–(P3) with respect to the set Γ.

Example 1. Suppose that $\ell = 2$ and that $\Gamma = \pi_1 \cup \pi_2$, where

$$\begin{aligned} \pi_1 &= \left\{ \beta_{\pi_1} \right\} \; , \\ \pi_2 &= \left\{ \beta_{\pi_2}, \beta_{\pi_2}^q, \beta_{\pi_2}^{q^2} \right\} \; , \end{aligned}$$

and where the minimal polynomial of β_{π_1} has degree $m_{\pi_1} \ge 2$. We take $m = m_{\pi_1}$ and $\gamma_0 = \beta_{\pi_1}$. For $i = 1$ we have $B_1(x,y) \equiv 1$ (regardless of Γ) and, respectively,

$$\boldsymbol{G}_1(x) = \left(\; 1 \; \right) \; .$$

Turning to $i = 2$, we have

$$B_2(x,y) = 1 - p_{2,1}(x) y = 1 - a_{2,\pi_1,1}(x) y = 1 - xy \; ,$$

since $a_{2,\pi_1,1}(x) = x$ is the unique polynomial in $F_m[x]$ that evaluates to $\gamma_0 = \beta_{\pi_1}$ at $x = \beta_{\pi_1}$. Hence,

$$\boldsymbol{G}^*(x) = \boldsymbol{G}_2(x) = \begin{pmatrix} 1 & -x \\ 0 & M_{\pi_1}(x) \end{pmatrix} \; .$$

Finally, $\boldsymbol{G}(x) = M_{\pi_2}(x) \cdot \boldsymbol{G}^*(x)$, and $(\beta_{\pi_1} \; 1)^T$ is a common eigenvector of $\boldsymbol{G}(x)$ with respect to the set Γ. The degree of $\boldsymbol{G}(x)$ is $m_{\pi_1} + 2m_{\pi_2}$, thereby attaining the lower bound of Proposition 4. □

Example 2. Suppose that $\ell = 3$ and that $\Gamma = \pi_1 \cup \pi_2 \cup \pi_3$, where π_1 and π_2 are as in Example 1 and

$$\pi_3 = \left\{ \beta_{\pi_3}, \beta_{\pi_3}^q \right\} \; ,$$

and, in addition, assume that $m_{\pi_1} \ge 3$ and that $m_{\pi_1} \mid m_{\pi_3}$ (e.g., $m_{\pi_1} = m_{\pi_3} = h \ge 3$). We select again $m = m_{\pi_1}$ and $\gamma_0 = \beta_{\pi_1}$. The matrices $\boldsymbol{G}_1(x)$ and $\boldsymbol{G}_2(x)$ will then be the same as in Example 1. As for $\boldsymbol{G}_3(x)$, we will have

$$\begin{aligned} B_3(x,y) &= \left(1 - p_{3,1}(x) y\right) \left(1 - p_{3,2}(x) y\right) \\ &= 1 - \left(p_{3,1}(x) + p_{3,2}(x)\right) y + p_{3,1}(x) p_{3,2}(x) y^2 \; , \end{aligned}$$

where

$$p_{3,1}(x) = a_{3,\pi_1,1}(x) M_{\pi_3}(x) + a_{3,\pi_3,1}(x) M_{\pi_1}(x) \; ,$$

with $a_{3,\pi_1,1}(x)$ being in $F_{m_{\pi_1}}[x]$ such that $a_{3,\pi_1,1}(\beta_{\pi_1}) = \beta_{\pi_1}/M_{\pi_3}(\beta_{\pi_1})$ and $a_{3,\pi_3,1}(x)$ being in $F_{m_{\pi_3}}[x]$ such that $a_{3,\pi_3,1}(\beta_{\pi_3}) = \beta_{\pi_1}/M_{\pi_1}(\beta_{\pi_3})$, and

$$p_{3,2}(x) = a_{3,\pi_3,2}(x)$$

is in $F_{m_{\pi_3}}[x]$ such that $a_{3,\pi_3,2}(\beta_{\pi_3}^q) = \beta_{\pi_1}$. Hence,

$$\begin{aligned} \boldsymbol{G}^*(x) &= \boldsymbol{G}_3(x) \\ &= \begin{pmatrix} 1 & -p_{3,1}(x) - p_{3,2}(x) & p_{3,1}(x)p_{3,2}(x) \\ 0 & M_{\pi_3}(x) & -xM_{\pi_3}(x) \\ 0 & 0 & M_{\pi_3}(x)M_{\pi_1}(x) \end{pmatrix} , \end{aligned}$$

and $\boldsymbol{G}(x) = M_{\pi_2}(x) \cdot \boldsymbol{G}^*(x)$. Note that

$$p_{3,1}(\beta_{\pi_1}) = p_{3,1}(\beta_{\pi_3}) = p_{3,2}(\beta_{\pi_3}^q) = \beta_{\pi_1} ,$$

which, in turn, implies that $B_3(\beta, \beta_{\pi_1}^{-1}) = 0$ for $\beta \in \Gamma_3^* = \pi_1 \cup \pi_3$ (see Lemma 7). It follows that $(\beta_{\pi_1}^2 \;\; \beta_{\pi_1} \;\; 1)^T$ is a common eigenvector of $\boldsymbol{G}(x)$ with respect to the set Γ. The degree of $\boldsymbol{G}(x)$, which equals $m_{\pi_1} + 2m_{\pi_3} + 3m_{\pi_2}$, attains the lower bound of Proposition 4. □

Proposition 8. *Given (F, Φ, Γ, ℓ), let $\boldsymbol{G}_\ell(x)$ be obtained from (10) by iterating over $i \in [\ell]$. Then the matrix*

$$\boldsymbol{G}(x) = \Bigl(\prod_{\pi \in \mathcal{P} \setminus \mathcal{P}^*} M_\pi(x) \Bigr) \cdot \boldsymbol{G}_\ell(x)$$

satisfies properties (P1)–(P3) with respect to Γ. A common eigenvector is given by

$$\boldsymbol{v} = \bigl(\gamma_0^{\ell-1} \; \gamma_0^{\ell-2} \; \ldots \; \gamma_0 \;\; 1 \bigr)^T , \tag{11}$$

for the selected element γ_0.

Proof. Properties (P1) and (P2) are straightforward. In order to establish (P3), it suffices to show that for every $\beta \in \Gamma^*$,

$$\boldsymbol{G}_\ell(\beta)\boldsymbol{v} = \boldsymbol{0} .$$

To this end, we show by induction on $i \in [\ell]$ that for every $\beta \in \Gamma_i^*$,

$$\boldsymbol{G}_i(\beta)\boldsymbol{v}_i = \boldsymbol{0} ,$$

where $\boldsymbol{v}_i = (\gamma_0^{i-1} \; \gamma_0^{i-2} \; \ldots \; \gamma_0 \;\; 1)^T$ (i.e., $\boldsymbol{v}_i$ is the i-suffix of $\boldsymbol{v}$).

The induction base ($i = 1$) is obvious, since Γ_1^* is empty. Given $i > 1$, by applying the induction hypothesis to $i-1$ it follows that for every $\beta \in \Gamma_i^*$, the last $i-1$ entries of $\boldsymbol{G}_i(\beta)\boldsymbol{v}_i$ are all zero, since they form the vector $\bigl(\prod_{\pi \in \mathcal{P}_{i,i-1}} M_\pi(\beta)\bigr) \cdot \boldsymbol{G}_{i-1}(\beta)\boldsymbol{v}_{i-1}$. It remains to show that for these βs, the first entry of $\boldsymbol{G}_i(\beta)\boldsymbol{v}_i$ is zero as well. This entry, in turn, is given by

$$\sum_{j=0}^{i-1} B_{i,j}(\beta)\gamma_0^{i-1-s} = \gamma_0^{i-1} B_i\left(\beta, \gamma_0^{-1}\right) = 0 ,$$

where the second equality follows from Lemma 7. □

For the selected value of m (which determines the set $\mathcal{P}^* = \mathcal{P}^*(m)$), the degree of $\boldsymbol{G}(x)$ of our construction equals

$$\deg \boldsymbol{G}(x) = \Bigl(\ell \cdot \sum_{\pi \in \mathcal{P} \setminus \mathcal{P}^*} m_\pi \Bigr) + \sum_{\pi \in \mathcal{P}^*} |\pi| \cdot m_\pi . \tag{12}$$

In view of Proposition 4, we can identify sets Γ where this degree is the smallest possible. E.g., this will be the case if Γ satisfies the following two conditions.

(i) For some divisor $m \geq \ell$ of h, each element of $\Gamma \setminus F$ is a proper element of an extension field of $\mathrm{GF}(q^m)$.

(ii) Each subset $\pi \in \mathcal{P}(\Gamma)$ takes the form

$$\pi = \left\{ \beta_\pi, \; \beta_\pi^q, \; \beta_\pi^{q^2}, \ldots, \beta_\pi^{q^{|\pi|-1}} \right\} .$$

V. Back to quasi-cyclic codes

We now turn to the motivating application of this work, namely, designing quasi-cyclic codes. We start with the following proposition, which provides a sufficient condition that the construction of Section IV yields a generator polynomial matrix of a quasi-cyclic code.

Proposition 9. *Let $F = \mathrm{GF}(q)$ and $\Phi = \mathrm{GF}(q^h)$, and let $\ell \in [h]$ and $n \in \mathbb{Z}^+$ be given. Also, let $\Gamma \subseteq \Phi$ be such that $\beta^n = 1$ for every $\beta \in \Gamma$. Then the construction of $\boldsymbol{G}(x)$ for (F, Φ, Γ, ℓ), as given in Section IV, satisfies property (P4).*

Proof. By the construction it follows that for every $i \in [\ell]$, each entry along row i of $\boldsymbol{G}(x)$ is divisible (in $F[x]$) by the diagonal entry $g_{i,i}(x)$. Therefore, we can express $\boldsymbol{G}(x)$ in the form

$$\boldsymbol{G}(x) = \boldsymbol{D}(x)\widehat{\boldsymbol{G}}(x) , \tag{13}$$

where $\boldsymbol{D}(x)$ is an $\ell \times \ell$ diagonal matrix over $F[x]$ whose main diagonal is given by

$$(\boldsymbol{D}(x))_{i,i} = g_{i,i}(x) , \quad i \in [\ell] , \tag{14}$$

and $\widehat{\boldsymbol{G}}(x)$ is an $\ell \times \ell$ upper-triangular unimodular matrix over $F[x]$ (as $\det(\widehat{\boldsymbol{G}}(x)) = 1$; in fact, $\boldsymbol{D}(x)$ is the Smith normal form of $\boldsymbol{G}(x)$, since $g_{i,i}(x) \,|\, g_{i+1,i+1}(x)$ for all $i \in [\ell-1]$ [4, Ch. S1]). Hence, $\widehat{\boldsymbol{G}}(x)$ has an upper-triangular inverse, $(\widehat{\boldsymbol{G}}(x))^{-1}$, over $F[x]$.

By the construction in Section IV it also follows that every diagonal entry $g_{i,i}(x)$ is a product of distinct minimal polynomials of elements β of Γ. The assumption $\beta^n = 1$ therefore implies that $g_{i,i}(x)$ divides $x^n - 1$, for every $i \in [\ell]$.

Let $\boldsymbol{E}(x)$ be the $\ell \times \ell$ diagonal matrix over $F[x]$ whose main diagonal is given by

$$(\boldsymbol{E}(x))_{i,i} = (x^n - 1)/g_{i,i}(x) , \quad i \in [\ell] .$$

By (13)–(14) we then get that $\boldsymbol{G}(x)$ satisfies property (P4) with $\boldsymbol{H}(x) = (\widehat{\boldsymbol{G}}(x))^{-1}\boldsymbol{E}(x)$. □

Now, let $F = \mathrm{GF}(q)$, let $n \in \mathbb{Z}^+$ be such that $\gcd(n, q) = 1$, and let $\Phi = \mathrm{GF}(q^h)$ be the splitting field of $x^n - 1$. Given $\ell \in [h]$, $d \in \mathbb{Z}^+$, and $b \in \mathbb{Z}$, let the set $\Gamma_{\alpha,b,d}$ be defined by (2), where α is a primitive nth root of unity in Φ. Applying the construction of Section IV to $(F, \Phi, \Gamma_{\alpha,b,d}, \ell)$ with some divisor $m \geq \ell$ of h yields an $\ell \times \ell$ matrix $\boldsymbol{G}(x)$ over $F[x]$ which, by Proposition 9, generates a quasi-cyclic $[\ell \times n, k]$ code $\mathbb{C}$ over F, which we denote hereafter by

$$\mathbb{C}_F(\Gamma_{\alpha,b,d}, \ell, m)$$

(the parameter n is determined by α). This code has dimension $k = \ell n - \deg \boldsymbol{G}(x)$, where $\deg \boldsymbol{G}(x)$ is given by (12) (and we would select m so as to minimize $\deg \boldsymbol{G}(x)$). Moreover, by Proposition 1, the minimum distance (over F^ℓ) of $\mathbb{C}$ is at least d. And as demonstrated in Section IV, in certain cases of the set $\Gamma_{\alpha,b,d}$ (e.g., when conditions (i)–(ii) therein hold), the attained dimension is the largest possible assuming such a BCH-like design strategy. When this happens, $\mathbb{C}_F(\Gamma_{\alpha,b,d}, \ell, m)$ is equal to the subspace subcode $\mathbb{C}_{\mathrm{RS}}(\boldsymbol{v})$ of C_{RS} as defined in (3), with $\boldsymbol{v}$ taken as the common eigenvector of $\boldsymbol{G}(x)$ with respect to $\Gamma_{\alpha,b,d}$. Note that in any case, $\mathbb{C}_F(\Gamma_{\alpha,b,d}, \ell, m)$ is always a subcode of $\mathbb{C}_{\mathrm{RS}}(\boldsymbol{v})$.

Remark 3. As can be seen from (12), the inclusion of an eigenvalue β in $\Gamma_{\alpha,b,d}$ generally results in an increase of $\deg \boldsymbol{G}(x)$ (and therefore in a decrease of k) by the degree of the minimal polynomial of β; this holds even when $\Gamma_{\alpha,b,d}$ contains other conjugates of β, unless their number is at least ℓ. Moreover, the effect on $\deg \boldsymbol{G}(x)$ of eigenvalues that belong to small (proper) subfields of Φ can be larger than just adding the degree of their minimal polynomial; e.g., an inclusion of an element of F in $\Gamma_{\alpha,b,d}$ results in an increase of $\deg \boldsymbol{G}(x)$ by ℓ (and not just by 1). So the common strategy used when designing BCH codes, of constructing a designed root set $\Gamma_{\alpha,b,d}$ which intersects as few and as small conjugacy classes as possible, becomes less effective as ℓ becomes larger than 1. □

Example 3. When $n = q^h - 1$, $d \le \sqrt{n} - 1$, and $b \in \{0, 1\}$, the set $\Gamma_{\alpha,b,d}$ satisfies conditions (i)–(ii) in Section IV for any divisor $m \ge \ell$ of h (see [16, p. 232, Problem 7.1]). In this case we get from (12) that the redundancy of $\mathbb{C}_F(\Gamma_{\alpha,b,d}, \ell, m)$ (as a linear code over F) equals

$$\ell n - k = \deg \boldsymbol{G}(x) = \begin{cases} \left\lceil \frac{q^\ell - 1}{q^\ell}(d{-}1) \right\rceil h & \text{if } b = 1 \\ \ell + \left\lceil \frac{q^\ell - 1}{q^\ell}(d{-}2) \right\rceil h & \text{if } b = 0 \end{cases}, \tag{15}$$

and that is since the inclusion of an element β in $\Gamma_{\alpha,b,d}$ does not increase the redundancy if β equals the q^ℓth power of some other element in $\Gamma_{\alpha,b,d}$ (for $b = 0$, the additive term ℓ is due to the element $1 \in \Gamma_{\alpha,b,d}$). Observe that if, in addition, $\ell \,|\, h$, then (15) is known to be the redundancy (measured in symbols of F) of an $[n, k]$ primitive BCH code over $\mathrm{GF}(q^\ell)$. In fact, when $\ell \,|\, h$, we will get precisely such a BCH code if we apply the construction of Section IV to $\Gamma_{\alpha,b,d}$ and select $m = \ell$ therein. Indeed, when doing so, the common eigenvector $\boldsymbol{v}$, which is given by (11), is over $\mathrm{GF}(q^\ell)$, and for every codeword $\boldsymbol{c}(x) \in \mathbb{C}_F(\Gamma_{\alpha,b,d}, \ell, \ell)$, the polynomial $\boldsymbol{c}(x) \cdot \boldsymbol{v}$ is over $\mathrm{GF}(q^\ell)$ and vanishes at the elements of $\Gamma_{\alpha,b,d}$; in other words, it is a codeword of a BCH code $\mathbb{C}_{\mathrm{BCH}}$ over $\mathrm{GF}(q^\ell)$ of length $n = (q^\ell)^{h/\ell} - 1$. The dimension of $\mathbb{C}_{\mathrm{BCH}}$ (over F) is the same as that of $\mathbb{C}_F(\Gamma_{\alpha,b,d}, \ell, \ell)$ and, therefore, the two codes are in fact equivalent. (The condition $\ell \,|\, h$ is assumed also in the construction of the BCH-like quasi-cyclic codes in [2, §3] and these codes, too, are equivalent to $\mathbb{C}_{\mathrm{BCH}}$.)

Thus, quasi-cyclic codes provide us the flexibility of attaining dimensions as in (15) also when h is not divisible by ℓ. □

We end this section by comparing the redundancy in Example 3 with those obtained by two schemes: shortening BCH codes over $\mathrm{GF}(q^\ell)$ (Example 4) and ℓ-level interleaving of BCH codes over $F = \mathrm{GF}(q)$ (Example 5).

Example 4. For $n = q^h - 1$, $d \le \sqrt{n} - 1$, and $b \in \{0, 1\}$, let $h' = \ell \cdot \lceil h/\ell \rceil$; note that $h' > h$ when ℓ does not divide h (when $\ell \,|\, h$, the rest of this example coincides with the respective case in Example 3). We can construct a (shortened quasi-cyclic) linear $[\ell \times n, k']$ code $\mathbb{C}'$ over F by shortening a primitive BCH code[5] of length $q^{h'} - 1$ over $\mathrm{GF}(q^\ell)$ defined by the consecutive root sequence $\Gamma_{\alpha',b,d}$ as in (2), where α' is a primitive element in $\mathrm{GF}(q^{h'})$. The minimum distance (over F^ℓ) of $\mathbb{C}'$ is at least d, and its redundancy, $\ell n - k'$ (being measured in symbols of F), is given by (15), except that h therein is replaced by h'. □

Example 5. For $n = q^h - 1$, $d \le \sqrt{n} - 1$, and $b \in \{0, 1\}$, let $\mathcal{C}_{\mathrm{BCH}}$ be a primitive BCH code of length n over $F = \mathrm{GF}(q)$ defined by the consecutive root sequence $\Gamma_{\alpha,b,d}$ (as in (2), where α is a primitive element in $\mathrm{GF}(q^h)$). The ℓ-level interleaving of $\mathcal{C}_{\mathrm{BCH}}$ produces a quasi-cyclic $[\ell \times n, \ell k'']$ code over F, which we denote by $\mathcal{C}_{\mathrm{BCH}}^{\odot \ell}$. The minimum distance (over F^ℓ) of $\mathcal{C}_{\mathrm{BCH}}^{\odot \ell}$ is at least d, and its redundancy (when measured in symbols of F) equals

$$\ell(n - k'') = \begin{cases} \ell \left\lceil \frac{q-1}{q}(d{-}1) \right\rceil h & \text{if } b = 1 \\ \ell + \ell \left\lceil \frac{q-1}{q}(d{-}2) \right\rceil h & \text{if } b = 0 \end{cases} \tag{16}$$

(see [16, p. 260, Problem 8.12]). It is easy to see that (16) is generally larger—and is never smaller—than (15). □

Table I compares the redundancies of (shortened) quasi-cyclic $[\ell \times n, k]$ binary codes obtained by the constructions in Examples 3–5, for several choices of ℓ, n $(= 2^h{-}1)$, and designed minimum distance d; in all cases we have taken $b = 0$ (the last two columns in the table will be referred to in Section VI).[6]

VI. Decoding

In this section, we present a list decoding algorithm for the code $\mathbb{C}_F(\Gamma_{\alpha,b,d}, \ell, m)$ defined in Section V. Our error model will be that of ℓ-phased burst errors: an error means that a column of the transmitted $\ell \times n$ array (over F) gets corrupted in at least one of its entries, and the number of errors is the number of columns that are altered.

Recalling that $\mathbb{C}_F(\Gamma_{\alpha,b,d}, \ell, m)$ is (a subcode of) the code $\mathbb{C}_{\mathrm{RS}}(\boldsymbol{v})$ defined in (3), our discussion here will be more general in that we present a list decoding algorithm for subspace subcodes of generalized Reed–Solomon (GRS) codes. Our algorithm is based on a similar idea that led to the list decoding of alternant codes (as subfield subcodes of GRS codes), based on the Koetter–Vardy (in short, KV) algorithm [10].

[5] Recall that for fixed d and sufficiently large lengths, primitive BCH codes have (asymptotically) the smallest redundancy among all known constructions of linear code families, except when the field size is 4 or 8 (see [18] and [21]).

[6] The parameters (ℓ, n, d) in the table are in the range where the construction in Example 4 still has a smaller redundancy than the construction in [18]. According to the tables in [6] (which intersect with Table I on four parameter choices) the construction in Example 3 for $(\ell{=}2, n{=}127, d{=}6)$ improves by one bit over the smallest redundancy currently known for linear codes of length 127 and minimum distance 6 over $\mathrm{GF}(2^2)$.

TABLE I
REDUNDANCY OF (SHORTENED) QUASI-CYCLIC $[\ell \times n, k]$ CODES OVER $\mathrm{GF}(2)$.

h	ℓ	n	d	Redundancy			τ	L
				Example 3	Example 4	Example 5		
5	2	31	6	17	20	22	3	10
7	2	127	6	23	26	30	3	42
9	2	511	22	137	152	182	11	46
5	3	31	6	23	27	33	3	10
7	3	127	6	31	39	45	3	42
10	3	1,023	30	253	303	423	15	68
5	4	31	6	24	36	44	3	10
7	4	127	6	32	36	60	3	42
9	4	511	22	175	232	364	11	46

Let $F = \mathrm{GF}(q)$ and $\Phi = \mathrm{GF}(q^h)$, and let $\mathsf{C}_{\mathrm{GRS}} \subseteq \Phi_n[x]$ be the following $[n, n{-}d{+}1, d]$ GRS code over Φ:

$$\mathsf{C}_{\mathrm{GRS}} = \left\{ \sum_{j=0}^{n-1} \eta_j f(\alpha_j) x^j \;:\; f(x) \in \Phi_{n-d+1}[x] \right\} ,$$

where $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$ are (the code locators which are) distinct elements in Φ, and $\eta_0, \eta_1, \ldots, \eta_{n-1}$ are nonzero (column multipliers) in Φ. Given $\ell \in [h]$ and a column vector $\boldsymbol{v} \in \Phi^\ell$ whose entries are linearly independent over F, define the code $\mathbb{C}$ by

$$\mathbb{C} = \mathbb{C}_{\mathrm{GRS}}(\boldsymbol{v}) = \left\{ \boldsymbol{c}(x) \in (F_n[x])^\ell \;:\; \boldsymbol{c}(x) \cdot \boldsymbol{v} \in \mathsf{C}_{\mathrm{GRS}} \right\} .$$

Note that $\mathsf{C}_{\mathrm{GRS}}$ is not necessarily a cyclic code over Φ and, therefore, $\mathbb{C}$ is not assumed to be quasi-cyclic in this section; nevertheless, we follow the notational convention of previous sections in regarding $\ell \times n$ arrays over F as elements of $(F_n[x])^\ell$.

Let $\Sigma = \mathsf{span}_F(\boldsymbol{v}) \subseteq \Phi$ be the ℓ-dimensional subspace of Φ over F that is spanned by the entries of $\boldsymbol{v}$. With any $\boldsymbol{a}(x) \in (F_n[x])^\ell$, we associate the following polynomial

$$\boldsymbol{A}(x) = A_0 + A_1 x + \ldots + A_{n-1} x^{n-1} = \boldsymbol{a}(x) \cdot \boldsymbol{v}$$

in the set $\Sigma_n[x]$ of polynomials of degree less than n over Σ. Accordingly, we can represent $\mathbb{C}$ through the following subspace subcode of $\mathsf{C}_{\mathrm{GRS}}$:

$$\tilde{\mathbb{C}} = \mathsf{C}_{\mathrm{GRS}} \cap \Sigma_n[x] \,. \tag{17}$$

Let $\boldsymbol{c}(x) \in \mathbb{C}$ be the transmitted $\ell \times n$ codeword and let $\boldsymbol{y}(x) = \boldsymbol{c}(x) + \boldsymbol{e}(x)$ be the received $\ell \times n$ array over F, where $\boldsymbol{e}(x)$ is an $\ell \times n$ error array over F containing a number of nonzero columns which does not exceed a prescribed decoding radius τ. Writing

$$\boldsymbol{C}(x) = C_0 + C_1 x + \ldots + C_{n-1} x^{n-1} = \boldsymbol{c}(x) \cdot \boldsymbol{v}$$

and

$$\boldsymbol{Y}(x) = Y_0 + Y_1 x + \ldots + Y_{n-1} x^{n-1} = \boldsymbol{y}(x) \cdot \boldsymbol{v}$$

(both in $\Sigma_n[x]$), the distance between $\boldsymbol{C}(x)$ and $\boldsymbol{Y}(x)$, denoted $\mathsf{d}(\boldsymbol{C}(x), \boldsymbol{Y}(x))$, stands for the number of errors that have occurred, namely, the number of indexes j for which $Y_j \neq C_j$.

Clearly, any list decoder for $\mathsf{C}_{\mathrm{GRS}}$ can be applied to decode any subset—and therefore any subspace subcode—of $\mathsf{C}_{\mathrm{GRS}}$. This applies in particular to decoding with a list size of 1, which corresponds to bounded-distance decoding (with decoding radius $\tau = \lfloor (d{-}1)/2 \rfloor$) and can be performed by any of the known decoding algorithms for GRS codes. For larger list sizes, however, the smaller alphabet of Σ (compared to Φ) allows us in many cases to guarantee a larger τ than the guaranteed decoding radius for $\mathsf{C}_{\mathrm{GRS}}$.

Figure 1 presents our interpolation-based list decoding algorithm for the code $\tilde{\mathbb{C}}$. Among its input parameters, the algorithm is provided with the target list size L and two nonnegative integers $\bar{r} < r \leq L$ which play a role in the interpolation step of the algorithm (Step 1). The decoding radius τ can be any positive integer that satisfies the inequality

$$\frac{\tau}{n} < \Theta_{q^\ell}\left(\frac{d}{n}, L, r, \bar{r} \right) , \tag{18}$$

where

$$\Theta_\sigma(\delta, L, r, \bar{r}) = \frac{\binom{L+1}{2}\delta - \binom{L+1-r}{2} - \binom{\bar{r}+1}{2}(\sigma{-}1)}{(L{+}1)(r{-}\bar{r})} \tag{19}$$

(with σ standing for the alphabet size of $\tilde{\mathbb{C}}$ and δ for the relative minimum distance of the underlying code $\mathsf{C}_{\mathrm{GRS}}$; typically, r and $\bar{r}$ are taken so that (19) is maximized—see discussion after Lemma 10). The (w_x, w_z)-weighted-degree of a bivariate polynomial $Q(x, z) \in \Phi[x, z]$ is denoted in Figure 1 by $\deg_{w_x, w_z} Q$, and the notation $\mathsf{mult}\{Q, (x_0, z_0)\}$ stands for the multiplicity of a bivariate polynomial $Q(x, z) \in \Phi[x, z]$ at the point $(x_0, z_0) \in \Phi^2$.

The algorithm is a rather straightforward extension of the KV algorithm when applied to the decoding of alternant codes, and, respectively, the analysis of the latter carries over to our algorithm, with the size, q, of the base field now replaced by the size, q^ℓ, of the set Σ. We will give here an outline of the analysis, following the exposition in [16, §9.6].

Conditions (20) and (21) determine the number of significant coefficients of the polynomial $Q(x, z)$ that is sought in Step 1. Given an index $j \in [0 : n{-}1]$, when $A = Y_j$ (respectively, $A \in \Sigma \setminus \{Y_j\}$), the condition in (22) translates into $\binom{r+1}{2}$ (respectively, $\binom{\bar{r}+1}{2}$) homogeneous linear equations in the coefficients of $Q(x, z)$. The inequality (18) guarantees that the number of (unknown) coefficients of $Q(x, y)$ exceeds the number of equations and, therefore, we can always find a nonzero $Q(x, y)$ in Step 1 (see [16, Lemmas 9.5 and 9.7]).

Input:

List size L, multiplicities $r, \bar{r}$.
Decoding radius τ satisfying (18).
Received word $\boldsymbol{Y}(x) = \sum_{j=0}^{n-1} Y_j x^j \in \Sigma_n[x]$.

1) *Interpolation:* Find $Q(x,z) \in \Phi[x,z] \setminus \{0\}$ such that

$$\begin{aligned} \deg_{0,1} Q &\leq L \ , && (20) \\ \deg_{1,n-d} Q &< r(n-\tau) + \bar{r}\tau \ , && (21) \end{aligned}$$

and for every $j \in [0:n{-}1]$ and $A \in \Sigma$:

$$\mathsf{mult}\{Q, (\alpha_j, A/\eta_j)\} \geq \begin{cases} r & \text{if } A = Y_j \\ \bar{r} & \text{otherwise.} \end{cases} \qquad (22)$$

2) *Root-finding:* Calculate the set

$$\mathcal{F} = \Big\{ f(x) \in \Phi_{n-d+1}[x] \ : \ (z - f(x)) \,|\, Q(x,z) \Big\} \ .$$

3) Calculate the set

$$\mathcal{S} = \Big\{ \boldsymbol{C}(x) = \sum_{j=0}^{n-1} \eta_j f(\alpha_j) x^j \ : \\ f(x) \in \mathcal{F} \ \text{ and } \ \mathsf{d}\left(\boldsymbol{C}(x), \boldsymbol{Y}(x)\right) \leq \tau \Big\} \ .$$

Output: List $\mathcal{S}$ of (no more than L) codewords of $\tilde{\mathbb{C}}$.

Fig. 1. List decoder for the code $\tilde{\mathbb{C}}$ defined by (17).

There are known algorithms for implementing Steps 1 and 2 efficiently [1], [8], [9], [12], [15], [17].

The next lemma parallels Lemma 9.8 in [16] and establishes the correctness of the decoding algorithm.

Lemma 10. *Given $\boldsymbol{Y}(x) \in \Sigma_n[x]$, suppose that $Q(x,z) \in \Phi[x,y] \setminus \{0\}$ satisfies conditions (20)–(22). Let $f(x) \in \Phi_{n-d+1}(x)$ be such that the respective codeword $\boldsymbol{C}(x) = \sum_{j=0}^{n-1} \eta_j f(\alpha_j) x^j$ of $\mathsf{C}_{\mathrm{GRS}}$ satisfies $\mathsf{d}\left(\boldsymbol{C}(x), \boldsymbol{Y}(x)\right) \leq \tau$. Then, $Q(x, f(x)) \equiv 0$, namely, $z - f(x)$ divides $Q(x,z)$.*

Proof. Denote $\mathcal{I} = \{j \,:\, f(\alpha_j) = Y_j/\eta_j\}$ and $\overline{\mathcal{I}} = [0:n{-}1] \setminus \mathcal{I}$, and suppose that $|\overline{\mathcal{I}}| \leq \tau$. It follows from (22) that $Q(x, f(x))$ is divisible by

$$\prod_{j \in \mathcal{I}} (x - \alpha_i)^r \prod_{j \in \overline{\mathcal{I}}} (x - \alpha_i)^{\bar{r}} \ ,$$

which, in turn, has degree

$$\begin{aligned} |\mathcal{I}| r + |\overline{\mathcal{I}}| \bar{r} &= nr + |\overline{\mathcal{I}}|(\bar{r} - r) \\ &\geq nr + \tau(\bar{r} - r) = r(n-\tau) + \bar{r}\tau \ . \end{aligned}$$

Hence, by (21) it follows that $Q(x, f(x)) \equiv 0$. □

Thus, if the number of ℓ-phased errors does not exceed τ, then the returned list $\mathcal{S}$ must contain the correct codeword. Moreover, since $\deg_{0,1} Q(x,z) \leq L$, the list $\mathcal{S}$ contains at most L codewords.

Observe that (19) is non-increasing in the alphabet size σ, which means that we may gain in the decoding radius compared to the underlying code $\mathsf{C}_{\mathrm{GRS}}$, for which we would need to substitute $\ell = h$ in (18). The maximization of (19) over $(r, \bar{r})$ yields the expression for the (finite list size) Johnson bound [16, §9.8 and Problem 9.10], which, for $L \to \infty$, approaches (from below) the expression

$$\theta_\sigma\left(\delta\right) = \frac{\sigma - 1}{\sigma} \left(1 - \sqrt{1 - \frac{\sigma}{\sigma - 1} \cdot \delta} \right) \ . \qquad (23)$$

Remark 4. When $\bar{r} > 0$, the number of interpolation points in Step 1 in Figure 1 is $q^\ell n$; so, in that respect, our algorithm has the same drawback as the KV algorithm when the latter is used for decoding alternant codes over $\mathrm{GF}(q^\ell)$ (such as the codes in Example 4). On the other hand, when $\bar{r} = 0$, the number of interpolation points is only n; this is also the case where the KV algorithm reduces to the Guruswami–Sudan algorithm [16, §9.5]. □

Remark 5. Suppose that $\mathcal{C}$ is *any* code of length n and minimum distance d over *any* alphabet Σ of size q^ℓ, and let τ and L be positive integers that satisfy (18) for some $(r, \bar{r})$. Then there exists a list decoder for $\mathcal{C}$ which returns lists of size at most L that always contain the correct codeword, provided that the number of errors (when measured in symbols of Σ) does not exceed τ (see [16, §9.8]). However, in general, such a decoder is not guaranteed to be efficient. The KV algorithm (for list decoding alternant codes over $\mathrm{GF}(q^\ell)$) and the algorithm in Figure 1 (for list decoding $\tilde{\mathbb{C}}$ over $\Sigma = \mathsf{span}_F(\boldsymbol{v})$) are efficient when ℓ is fixed or when $\bar{r} = 0$. □

It follows from Remark 5 that the inequality (18) is sufficient for having a list decoder for any of the codes presented in Examples 3–5. To the best of our knowledge, maximizing (19) over $(r, \bar{r})$ yields, in general, the best trade-off between τ and L currently known for these examples. And as noted in Remark 5, when d in (18) is taken as the designed minimum distance, then the list decoder for Examples 3 and 4 is also guaranteed to be efficient (assuming fixed ℓ or $\bar{r} = 0$). Moreover, by a result of Gopalan *et al.* [5], in many cases it is also efficient for the code $\mathcal{C}^{\odot \ell}$ in Example 5. Specifically, given τ and L_0 that satisfy

$$\frac{\tau}{n} < \Theta_q\left(\frac{d}{n}, L_0, r, \bar{r}\right) \qquad (24)$$

(which is the inequality (18) with $\ell = 1$), Algorithm 2 in [5] is shown therein to be a decoder for $\mathcal{C}^{\odot \ell}$ with decoding radius τ and list size bounded from above by

$$\binom{\iota + \kappa}{\kappa} L_0^\kappa \ , \qquad (25)$$

where

$$\iota = \left\lceil \frac{\tau}{d - \tau} \right\rceil \quad \text{and} \quad \kappa = \left\lceil \log_2 \left(\frac{d}{d - \tau} \right) \right\rceil \ .$$

The inequality (24) is weaker than (18) in that L_0 may be smaller than the smallest L that satisfies (18) for a given τ. Yet (25) is generally larger than that L, which means that the list produced by Algorithm 2 in [5] can be pruned to at most L codewords.

We conclude that while Examples 3–5 have the same guarantee for list decoding performance, in Example 3 we pay the smallest redundancy for it.

The last two columns in Table I contain pairs (τ, L) that are attainable by (18), for the special case $\tau = d/2$; in this case, the smallest L equals $\lfloor 2d/n \rfloor$ (see Appendix C).[7] Note that in this case, $\iota = \kappa = 1$ and $L_0 = L$ in (25) and, so, Eq. (25) evaluates to $2L$.

It is yet to be found whether there is a counterpart of Wu's algorithm (as in [3] and [20]) that can replace Figure 1. One can speculate that for the same pair (τ, L), the multiplicity r would be replaced in such an algorithm by $L{-}r$, thereby making such an algorithm favorable in the high-rate range.

Acknowledgment

The authors would like to thank the reviewers for their comments and suggestions.

Appendix A
Relationship to the model in [19]

We point out here the connection between our setting in Section II and the setting in [19]. Given a quasi-cyclic $[\ell{\times}n, k]$ code $\mathbb{C}$ over $F = \mathrm{GF}(q)$, the goal in [19] is to find a lower bound on the minimum distance of $\mathbb{C}$ when $\mathbb{C}$ is seen as a code of length ℓn over F, rather than as a code of length n over F^ℓ. Instead of just requiring property (P3), the analysis in [19, §III.B] considers more generally the linear subspace ("eigencode") $C \subseteq F^\ell$ which consists of all vectors in F^ℓ that are orthogonal to the following eigenspace over $\Phi = \mathrm{GF}(q^h)$:

$$\mathcal{V} = \left\{ \boldsymbol{v} \in \Phi^\ell \;:\; \boldsymbol{G}(\beta)\boldsymbol{v} = \boldsymbol{0} \;\text{ for every }\; \beta \in \Gamma \right\}$$

(namely, $C = \{ \boldsymbol{e} \in F^\ell \;:\; \boldsymbol{e}\cdot\boldsymbol{v} = 0 \text{ for every } \boldsymbol{v} \in \mathcal{V} \}$). When C contains nonzero vectors, the code $\mathbb{C}$ might potentially contain $\ell \times n$ arrays in which only one column is nonzero (and that column is then a vector of C). Therefore, to fit our setting (where we are interested in the minimum distance measured in symbols of F^ℓ), we need C to be the trivial code $\{\boldsymbol{0}\}$. The next lemma shows that this condition is, in fact, equivalent to property (P3), provided that $\ell \in [h]$.

Lemma 11. *For $\ell \in [h]$, let $\mathcal{V}$ be a linear subspace of Φ^ℓ with the property that no nonzero vector in F^ℓ is orthogonal to $\mathcal{V}$. Then there exists a vector $\boldsymbol{v} \in \mathcal{V}$ whose entries are linearly independent over F.*

Proof. Let V be an $\ell \times r$ matrix over Φ whose columns form a basis of $\mathcal{V}$, and let $\mathcal{E}$ be the set of all nonzero vectors in F^ℓ with a leading nonzero entry equaling 1. We show that there exists a column vector $\boldsymbol{w} \in \Phi^r$ such that $\boldsymbol{e}V\boldsymbol{w} \neq 0$ for every $\boldsymbol{e} \in \mathcal{E}$; the vector $V\boldsymbol{w}$ can then be taken as $\boldsymbol{v}$. For every $\boldsymbol{e} \in \mathcal{E}$, define the "bad set"

$$\mathcal{V}(\boldsymbol{e}) = \{ \boldsymbol{w} \in \Phi^r \;:\; \boldsymbol{e}V\boldsymbol{w} = 0 \} \;.$$

Clearly, $\mathcal{V}(\boldsymbol{e})$ is a linear subspace of Φ^r; furthermore, by the assumption in the lemma, $\mathcal{V}(\boldsymbol{e}) \neq \Phi^r$. Therefore, $|\mathcal{V}(\boldsymbol{e})| \leq |\Phi|^{r-1}$ and, so, ranging over all $\boldsymbol{e} \in \mathcal{E}$, the total number of vectors in the bad sets is bounded from above by

$$|\cup_{\boldsymbol{e}\in\mathcal{E}} \mathcal{V}(\boldsymbol{e})| \leq \sum_{\boldsymbol{e}\in\mathcal{E}} |\mathcal{V}(\boldsymbol{e})| \leq \frac{q^\ell - 1}{q-1} \cdot |\Phi|^{r-1} < \frac{1}{q-1} \cdot |\Phi|^r \;,$$

where the last inequality follows from $\ell \leq h$. Hence, there exists a vector $\boldsymbol{v} = V\boldsymbol{w}$ that belongs to none of the bad sets. □

Remark 6. The condition $\ell \in [h]$ in Lemma 11 can always be met simply by (possibly) replacing Φ with an extension field of Φ of extension degree $\lceil \ell/h \rceil$. □

Appendix B
Counterexample

We show here by a counterexample that, in general, the bound (4) no longer holds if each ρ_π therein is replaced by $|J_\pi|$, where J_π is an arbitrary subset of $[0 \,{:}\, h{-}1]$ such that $\beta_\pi^{q^j} \in \pi$ for some $\beta_\pi \in \Phi$ and every $j \in J_\pi$.

Example 6. Suppose that h is a multiple of an integer $t > 1$ such that $h/t \geq \ell \geq 2$. Let ξ be a primitive element in Φ, let ω be an element in $\mathrm{GF}(q^t) \setminus F$, and let $a(x)$ be the unique polynomial in $F_h[x]$ such that $a(\xi) = \omega$ (since ξ is primitive, such a polynomial exists). Take $J = \{0, t, 2t, \ldots, (\ell{-}1)t\}$ and

$$\Gamma = \{ \xi^{q^j} \;:\; j \in J \}$$

(and, so, $\mathcal{P} = \{\Gamma\}$ and $J_\Gamma = J$), and consider the $\ell \times \ell$ matrix

$$\boldsymbol{G}(x) = \left(\begin{array}{c|cccc} 1 & a(x) & a(x) & \ldots & a(x) \\ \cline{2-5} 0 & & & & \\ \vdots & \multicolumn{4}{c}{M_\Gamma(x) \cdot \boldsymbol{I}_{\ell-1}} \\ 0 & & & & \end{array} \right) , \tag{26}$$

where $M_\Gamma(x)$ is the minimal polynomial of ξ with respect to F. Let γ be the element $-\omega \cdot \sum_{i=0}^{\ell-2} \xi^i$ in Φ, and consider the following $\ell{-}1$ vectors

$$\boldsymbol{v}_j = \left(\gamma^{q^j} \; \xi^{(\ell-2)q^j} \; \xi^{(\ell-3)q^j} \; \ldots \; \xi^{q^j} \; 1 \right)^T, \; j \in J \setminus \{(\ell{-}1)t\}.$$

It can be readily verified that $\boldsymbol{G}(\beta)\boldsymbol{v}_j = \boldsymbol{0}$ for every $\beta \in \Gamma$ and $j \in J \setminus \{(\ell{-}1)t\}$. Since $\ell \leq h/t$, we get by the choice of ξ that the powers $1, \xi, \xi^2, \ldots, \xi^{\ell-2}$ are linearly independent over $\mathrm{GF}(q^t)$ and, *a fortiori*, are also so over F. In addition, γ is defined through a (unique) linear combination over $\mathrm{GF}(q^t)$ of these powers, and this linear combination contains elements that are not in F; hence, all the entries in $\boldsymbol{v}_0$—and therefore all the entries in each $\boldsymbol{v}_j$—are linearly independent over F. We conclude that each $\boldsymbol{v}_j$ is a common eigenvector with respect to the set Γ, as in property (P3) (moreover, by [13, pp. 109–110] it follows that $\boldsymbol{v}_0, \boldsymbol{v}_1, \ldots, \boldsymbol{v}_{\ell-2}$ are linearly independent over Φ, thus spanning the right kernel of $\boldsymbol{G}(\beta)$ for every $\beta \in \Gamma$). The degree of $\boldsymbol{G}(x)$ in (26) is $(\ell{-}1) \cdot \deg M_\Gamma(x) = (\ell{-}1)m_\Gamma = (\ell{-}1)h$, while the lower bound in (4), when ρ_Γ is replaced by $|J_\Gamma| = |J| = \ell$, evaluates to ℓh. □

Appendix C
Decoding radius $d/2$

We start with the next lemma, which characterizes a range of parameters for which (18) (or (24)) can hold only when $\tau \leq (d{+}1)/2$.

[7] When $\tau = d/2$, there are in fact simpler alternatives to the KV algorithm or to Figure 1; see, for example [20, §2].

Lemma 12. *For $n > (1/8) \cdot (\sigma/(\sigma{-}1)) \cdot (d+2)^2$,*

$$n \cdot \theta_\sigma\left(\frac{d}{n}\right) < \frac{d}{2} + 1\ , \tag{27}$$

where $\theta_\sigma(\delta)$ is defined in (23).

Proof. Starting from

$$n > \frac{1}{8} \cdot \frac{\sigma}{\sigma{-}1} \cdot (d+2)^2\ ,$$

it is fairly easy to see that the latter inequality is obtained by simplifying the inequality

$$n^2 - \frac{\sigma\, n\, d}{\sigma - 1} > \left(n - \frac{\sigma}{\sigma{-}1}\left(\frac{d}{2}+1\right)\right)^2\ .$$

Taking the square root of both sides and rearranging terms yield

$$\frac{\sigma{-}1}{\sigma}\left(n - \sqrt{n^2 - \frac{\sigma\, n\, d}{\sigma - 1}}\right) < \frac{d}{2} + 1$$

which, in turn, is equivalent to (27). □

Since the right-hand side of (18) is bounded from above by $\theta_{q^\ell}(d/n)$ (and approaches it from below when maximizing over $(r, \bar{r})$ and taking L to infinity), we get that the inequality (18) holds only when $\tau \le \lfloor (d{+}1)/2 \rfloor$.

Next, we consider the special case $\tau = d/2$.

Lemma 13. *If d is even and $\tau = d/2$, then the smallest L for which (18) holds is*

$$L = \left\lfloor \frac{2n}{d} \right\rfloor\ , \tag{28}$$

and this minimum is attained for $(r, \bar{r}) = (L{-}1, 0)$; when $\sigma = q^\ell = 2$, it is also attained for $(r, \bar{r}) = (L, 1)$.

Note that the expression (28) is the largest size of any constant-weight code of length n and minimum distance d over an Abelian group, where the constant weight is $d/2$.

Proof of Lemma 13. For $\tau = d/2 = n\delta/2$ and $\sigma = q^\ell$ we can rewrite (18) as

$$(L{+}1)(L{-}r{+}\bar{r}) \cdot \frac{\delta}{2} > \binom{L{+}1{-}r}{2} + \binom{\bar{r}{+}1}{2}(\sigma{-}1)\ .$$

Denoting $s = L - r$, and noting that the last inequality cannot hold if $s = \bar{r} = 0$, we obtain

$$(L{+}1) \cdot \frac{\delta}{2} > \frac{1}{s + \bar{r}}\left(\binom{s+1}{2} + \binom{\bar{r}{+}1}{2}(\sigma{-}1)\right)\ . \tag{29}$$

Clearly, $s \le \binom{s+1}{2}$, with equality holding only when $s = 0, 1$. Similarly, $\bar{r} \le \binom{\bar{r}+1}{2}(\sigma{-}1)$, with equality holding only when either $\bar{r} = 0$ or $(\bar{r}, \sigma) = (1, 2)$. It follows that the minimum value taken by the right-hand side of (29) is 1, and that minimum is attained when $(s, \bar{r}) = (1, 0)$ or when $(s, \bar{r}, \sigma) = (0, 1, 2)$. At the minimum, Eq. (29) becomes $(L{+}1) \cdot (\delta/2) > 1$, which, in turn, is satisfied if and only if $L \ge \lfloor 2/\delta \rfloor$. □

References

[1] M. Alekhnovich, "Linear Diophantine equations over polynomials and soft decoding of Reed–Solomon codes," *IEEE Trans. Inf. Theory,* 51 (2005), 2257–2265.

[2] M. Barbier, C. Chabot, G. Quintin, "On quasi-cyclic codes as a generalization of cyclic codes," *Finite Fields Appl.*, 18 (2012), 904–919.

[3] P. Beelen, T. Høholdt, J. S. R. Nielsen, Y. Wu, "On rational interpolation-based list-decoding and list-decoding binary Goppa codes," *IEEE Trans. Inf. Theory*, 59 (2013), 3269–3281.

[4] I. Gohberg, P. Lancaster, L. Rodman, *Matrix Polynomials*, SIAM, Philadelphia, 2009.

[5] P. Gopalan, V. Guruswami, P. Raghavendra, "List decoding tensor products and interleaved codes," *SIAM J. Comput.,* 40 (2011), 1432–1462.

[6] M. Grassl, "Bounds on the minimum distance of linear codes and quantum codes," available online at `http://www.codetables.de` (accessed on Sep. 27, 2018).

[7] M. Hattori, R. J. McEliece, G. Solomon, "Subspace subcodes of Reed–Solomon codes," *IEEE Trans. Inf. Theory,* 44 (1998), 1861–1880.

[8] R. Koetter, *On algebraic decoding of algebraic-geometric and cyclic codes*, Ph.D. dissertation, University of Linköping, Linköping, Sweden, 1996.

[9] R. Koetter, J. Ma, A. Vardy, "The re-encoding transformation in algebraic list-decoding of Reed–Solomon codes," *IEEE Trans. Inf. Theory,* 47 (2011), 633–647.

[10] R. Koetter, A. Vardy, "Algebraic soft-decision decoding of Reed–Solomon codes," *IEEE Trans. Inf. Theory,* 49 (2003), 2809–2825.

[11] K. Lally, P. Fitzpatrick, "Algebraic structure of quasicyclic codes," *Disc. Appl. Math.*, 111 (2001), 157–175.

[12] K. Lee, M. O'Sullivan, "List decoding of Reed–Solomon codes from a Gröbner basis perspective," *J. Symb. Comput.*, 43 (2008), 645–658.

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

[14] H. Matsui, "On generator and parity-check polynomial matrices of generalized quasi-cyclic codes," *Finite Fields Th. App.* 34 (2015), 280–304.

[15] H. O'Keeffe, P. Fitzpatrick, "Gröbner basis solution of constrained interpolation problems," *Linear Algebra Appl.,* 351–352 (2002), 533–551.

[16] R. M. Roth, *Introduction to Coding Theory,* Cambridge University Press, Cambridge, UK, 2006.

[17] R. M. Roth, G. Ruckenstein, *Efficient decoding of Reed–Solomon codes beyond half the minimum distance, IEEE Trans. Inf. Theory,* 46 (2000), 246–257.

[18] R. M. Roth, A. Zeh, "Long cyclic codes over $\mathrm{GF}(4)$ and $\mathrm{GF}(8)$ better than BCH codes in the high-rate region," *IEEE Trans. Inf. Theory,* 63 (2017), 150–158.

[19] P. Semenov, P. Trifonov, "Spectral methods for quasi-cyclic code analysis," *IEEE Commun. Lett.,* 16 (2012), 1840–1843.

[20] Y. Wu, "New list decoding algorithms for Reed–Solomon and BCH codes," *IEEE Trans. Inf. Theory,* 54 (2008), 3611–3630.

[21] S. Yekhanin, I. I. Dumer, "Long nonbinary codes exceeding the Gilbert–Varshamov bound for any fixed distance," *IEEE Trans. Inf. Theory*, 50 (2004), 2357–2362.

[22] A. Zeh, S. Ling, "Decoding of quasi-cyclic codes up to a new lower bound on the minimum distance," *Proc. IEEE Int'l Symp. Inf. Theory,* Honolulu, Hawaii (June 2014), 2584–2588.

Ron M. Roth (M'88–SM'97–F'03) received the B.Sc. degree in computer engineering, the M.Sc. in electrical engineering, and the D.Sc. in computer science from Technion—Israel Institute of Technology, Haifa, Israel, in 1980, 1984, and 1988, respectively. Since 1988 he has been with the Computer Science Department at Technion, where he now holds the General Yaakov Dori Chair in Engineering. During the academic years 1989–91 he was a Visiting Scientist at IBM Research Division, Almaden Research Center, San Jose, California, and during 1996–97, 2004–05, and 2011–2012 he was on sabbatical leave at Hewlett–Packard Laboratories, Palo Alto, California. He is the author of the book *Introduction to Coding Theory*, published by Cambridge University Press in 2006. Dr. Roth was an associate editor for coding theory in IEEE Transactions on Information Theory from 1998 till 2001, and he is now serving as an associate editor in *SIAM Journal on Discrete Mathematics*. His research interests include coding theory, information theory, and their application to the theory of complexity.

Alexander Zeh (S'08–M'13) received his Dipl.-Ing. (BA) degree (B.A. equivalent) in 2004 from the University of Applied Science in Stuttgart and his Dipl.- Ing. in electrical engineering from the University of Stuttgart. He participated in the double-diploma program with Télécom ParisTech (former ENST) from 2006 to 2008 and received also a French diploma. In 2013, he received a Ph.D. degree from the University of Ulm, Germany, in electrical engineering and from the Computer Science Department (LIX), École Polytechnique ParisTech, Paris, France. During 2013–2016, Dr. Zeh was a post-doctoral researcher at Technion–Israel Institute of Technology. Since 2016, he has been a specialist for automotive cybersecurity at Infineon Technologies AG. His research interests include coding and information theory, signal processing, telecommunications and the implementation of fast algorithms on FPGAs.