Bounds on the List-Decoding Radius of Reed-Solomon Codes

Gitit Ruckenstein* Ron M. Roth*

Abstract

Techniques are presented for computing upper and lower bounds on the number of errors that can be corrected by list decoders for general block codes and, specifically, for Reed-Solomon (RS) codes. The list decoder of Guruswami and Sudan implies such a lower bound (referred to here as the GS bound) for RS codes. It is shown that this lower bound, given by means of the code's length, the minimum Hamming distance, and the maximal allowed list size, applies in fact to all block codes. Ranges of code parameters are identified where the GS bound is tight for worst-case RS codes, in which case the list decoder of Guruswami and Sudan provably corrects the largest possible number of errors.

On the other hand, ranges of parameters are provided for which the GS lower bound can be strictly improved. In some cases the improvement applies to all block codes with a given minimum Hamming distance, while in others it applies only to RS codes.

Keywords: Block designs; Guruswami-Sudan algorithm; List decoding; MDS codes; Reed-Solomon codes; Sidon sets.
AMS subject classifications: 11T71, 05B05.

1 Introduction

An (n, M, d) (block) code $\mathcal{C}$ over an alphabet F of size q is an M-subset of F^n with minimum Hamming distance d between any two different codewords. In cases where F is a finite field and $\mathcal{C}$ is a linear subspace of F^n, namely $k = \log_q M = \dim \mathcal{C}$, we refer to $\mathcal{C}$ as an $[n, k, d]$ code. An (n, M, d) code is called maximum-distance separable (MDS) [11, Ch. 11]

*Computer Science Department, Technion, Haifa 32000, Israel. This work was supported by Grant No. 94/99 from the Israel Science Foundation. This work was presented in part at the 2001 International Symposium on Information Theory (ISIT'2001), Washington, D.C. e-mail: {gitit,ronny}@cs.technion.ac.il.

if $d = n+1-\log_q M$, thus satisfying the Singleton bound [3, Page 88] with equality; in particular, $k = \log_q M$ must be an integer.

An $[n, k, d]$ *(generalized) Reed-Solomon (in short, RS) code* over a finite field $F = \mathrm{GF}(q)$ is a linear MDS code that consists of all words (vectors) of the form $(f(\alpha_1)\ f(\alpha_2)\ \ldots\ f(\alpha_n))$, where $\alpha_1, \alpha_2, \ldots, \alpha_n$ are prescribed distinct elements of F, which are commonly referred to as the *code locators*, and $f(x)$ ranges over all polynomials of degree less than $k = n-d+1$ over F.

Denote by $\mathsf{d}_H(\boldsymbol{v}_1, \boldsymbol{v}_2)$ the Hamming distance between two words $\boldsymbol{v}_1, \boldsymbol{v}_2 \in F^n$. A *list-$\ell$ decoder with a decoding radius τ* for a code $\mathcal{C} \subseteq F^n$ is a mapping $\mathcal{D} : F^n \longrightarrow 2^{\mathcal{C}}$ such that (i) $|\mathcal{D}(\boldsymbol{v})| \leq \ell$ for every $\boldsymbol{v} \in F^n$, and (ii) $\boldsymbol{c} \in \mathcal{D}(\boldsymbol{v})$ if and only if $\boldsymbol{c} \in \mathcal{C}$ and $\mathsf{d}_H(\boldsymbol{c}, \boldsymbol{v}) \leq \tau$. In other words, given a received word $\boldsymbol{v} \in F^n$, the decoder $\mathcal{D}$ returns all the codewords in $\mathcal{C}$ that are at Hamming distance at most τ from $\boldsymbol{v}$, and the size of that list is guaranteed to be at most ℓ. The decoding radius τ therefore stands for the largest number of errors that are corrected by $\mathcal{D}$.

Denote by $\Delta_\ell(\mathcal{C})$ the largest decoding radius of any list-ℓ decoder for a code $\mathcal{C} \subseteq F^n$. The value $\Delta_\ell(\mathcal{C})$ is the largest integer value R such that all Hamming spheres of radius R in F^n contain at most ℓ codewords of $\mathcal{C}$.

Hereafter, by an *admissible quadruple* (ℓ, n, d, q) we mean that ℓ, n, d, and q are positive integers such that $1 \leq d \leq n$. By an *RS-admissible quadruple* (ℓ, n, d, q) we mean an admissible quadruple for which, in addition, $n \leq q$ and q is a power of a prime.

Given an admissible quadruple (ℓ, n, d, q), we define

$$\Delta_\ell(n, d; q) = \min_{\mathcal{C}} \Delta_\ell(\mathcal{C}) \ , \tag{1}$$

where the minimum is taken over all (n, M, d) block codes over an alphabet of size q. For an RS admissible quadruple (ℓ, n, d, q), we also define

$$\Delta_\ell^{\mathrm{RS}}(n, d; q) = \min_{\mathcal{C}} \Delta_\ell(\mathcal{C}) \ , \tag{2}$$

where the minimum is taken over all $[n, k, d]$ RS codes over $\mathrm{GF}(q)$. Studying these two quantities is the subject of this paper. Taking the minimum in (1) or (2) results in the value $\Delta_\ell(\mathcal{C})$ of the 'worst' code $\mathcal{C}$ in the respective family. In particular, we are interested here in the attainable performance of list-ℓ decoders of RS codes (i.e., in the largest number of errors that can be corrected by such decoders), independently of the particular choice of the code locators. From the practical side, this is justified by the structure of existing RS decoding algorithms, which are typically not tailored to specific selection of code locators. When $n = q$, the minimum in the definition of $\Delta_\ell^{\mathrm{RS}}(n, d; q)$ is taken over one set of code locators; in fact, this is also the case when $n = q-1$, where one can assume that all the code locators are nonzero (see [11, p. 305, Problem 7]).

Clearly, the quantities $\Delta_\ell(n,d;q^m)$ and $\Delta_\ell^{\rm RS}(n,d;q^m)$ are non-decreasing with ℓ and non-increasing with m, and for every admissible quadruple (ℓ,n,d,q),

$$\Delta_\ell(n,d;q) \le \Delta_\ell^{\rm RS}(n,d;q)\,.$$

It is well-known that

$$\Delta_1(n,d;q) = \Delta_1^{\rm RS}(n,d;q) = \lfloor (d-1)/2 \rfloor$$

(independently of q).

1.1 The Guruswami-Sudan bound

Guruswami and Sudan present in [7] a list-ℓ decoding algorithm for $[n,k,d]$ RS codes over GF(q) (see also the earlier work of Sudan [13]). The decoding radius of their decoder depends on the parameters (ℓ,n,d,q) as summarized in Theorem 1.1 below. We first introduce several notations that are required not only for the statement of their result, but also in our analysis throughout this paper.

Given $\ell \ge 1$, partition the real interval $[0,1)$ into the ℓ sub-intervals

$$[0,\rho_2), [\rho_2,\rho_3), \ldots, [\rho_\ell, 1)\,, \tag{3}$$

where

$$\rho_r = \rho_r(\ell) = \frac{r(r-1)}{\ell(\ell+1)}\,, \quad r = 1,2,\ldots,\ell+1\,. \tag{4}$$

Given integers n and d such that $1 \le d \le n$, define the relative minimum distance $\delta = d/n$. Let $r = r(\delta)$ be the unique index such that $1-\delta \in [\rho_r, \rho_{r+1})$. Also define

$$\tau_\ell(n,d) = \frac{1}{(\ell+1)r}\left(\binom{\ell+1}{2}d - \binom{\ell+1-r}{2}n\right)\,. \tag{5}$$

The mapping $\delta \mapsto \tau_\ell(n,n\delta)$ is piecewise-linear and continuous over $[0,1)$ for every fixed n. It can be easily verified that $\tau_\ell(n,d) < d$, for every value of ℓ, assuming $d \le n$. One can also verify that when $1-\delta \ge \rho_\ell$,

$$\tau_\ell(n,d) = d/2\,.$$

By its definition, $\tau_\ell(n,d)$ is an integer if and only if

$$(\ell+1)r \quad \text{divides} \quad \binom{\ell+1}{2}d - \binom{\ell+1-r}{2}n\,. \tag{6}$$

The following result follows from [7] and is proved in the Appendix.

Theorem 1.1 *For every RS-admissible quadruple (ℓ,n,d,q), the list-ℓ decoder in [7] for an $[n,k,d]$ RS code over* GF(q) *has a decoding radius $\lceil \tau_\ell(n,d) \rceil - 1$; so,*

$$\Delta_\ell^{\rm RS}(n,d;q) \ge \lceil \tau_\ell(n,d) \rceil - 1\,. \tag{7}$$

1.2 Main results

In this paper, we first generalize the result of [7] by showing that $\lceil \tau_\ell(n,d) \rceil - 1$, referred to as the *GS bound*, is a lower bound on the list-ℓ decoding radius of every (n, M, d) block code, as stated in Theorem 1.2.

Theorem 1.2 *Let (ℓ, n, d, q) be an admissible quadruple. Then*

$$\Delta_\ell(n, d; q) \geq \lceil \tau_\ell(n,d) \rceil - 1 \, . \tag{8}$$

Theorem 1.2, which is similar to a result by Johnson [11, Ch. 17, Thm. 2], is proved in Section 2.1 by using combinatorial arguments, while the result in Theorem 1.1 is based on algebraic analysis. When $d/n \leq 2/(\ell+1)\,(= 1 - \rho_\ell)$, (8) becomes

$$\Delta_\ell(n, d; q) \geq \lfloor (d-1)/2 \rfloor = \Delta_1(n, d; q) \, .$$

In a recent work [9], Justesen and Høholdt compute RS-admissible quadruples (ℓ, n, d, q) for which there exist (n, q^{n-d+1}, d) MDS and RS codes over $F = \mathrm{GF}(q)$ that attain the GS bound. A key ingredient in their technique is constructing what we call here a *failing list* of codewords. By a failing list of size $\ell+1$, we mean a set of $\ell+1$ words, $\{\boldsymbol{c}_0, \boldsymbol{c}_1, \ldots, \boldsymbol{c}_\ell\} \subseteq F^n$, such that the following two conditions hold:

- $\mathtt{d}_H(\boldsymbol{c}_s, \boldsymbol{c}_t) \geq d$ for every $0 \leq s < t \leq \ell$, and
- there is some $\boldsymbol{v} \in F^n$ such that $\mathtt{d}_H(\boldsymbol{c}_s, \boldsymbol{v}) \leq \lceil \tau_\ell(n,d) \rceil$ for every $0 \leq s \leq \ell$.

One can easily see that a failing list of size $\ell+1$ is contained in an (n, M, d) code $\mathcal{C}$ if and only if $\Delta_\ell(\mathcal{C})$ attains the GS bound. Several families of MDS codes and RS codes that contain such failing lists are presented in [9]; their constructions are based on block designs, and in each of these constructions, the relative minimum distance δ is such that $1-\delta = \rho_r(\ell)$.

In this work, we introduce a combinatorial configuration, akin to block designs, that defines a structure of failing lists which covers the *whole* range of rational δ values (and not just those for which $1-\delta = \rho_r(\ell)$). Furthermore, we prove that for triples (ℓ, n, d) that satisfy the divisibility condition (6), our structure completely characterizes the failing lists of size $\ell+1$ in any given (n, M, d) code over any alphabet F. This, in turn, provides sufficient and *necessary* conditions on the existence of such failing lists (see Proposition 2.3 in Section 2).

It turns out that our necessary conditions imply that there is a range of parameters where the GS bound is <u>not</u> tight for any code. For example, Proposition 1.3 below indicates the non-existence of failing lists in cases where the alphabet size is small.

Proposition 1.3 *Let (ℓ, n, d, q) be an admissible quadruple, let r be the unique integer such that $1 - d/n \in [\rho_r, \rho_{r+1})$, and assume that (6) holds. Then $\Delta_\ell(n, d; q) \geq \tau_\ell(n, d)$ if either of the following conditions hold:*

- $1 - d/n = \rho_r$ *and* $q < \ell{+}1{-}r$, *or*
- $1 - d/n > \rho_r$ *and* $q < \ell{+}2{-}r$.

Proposition 1.3 is proved in Section 2.4, where additional cases are indicated in which the GS bound is not tight. These cases are found by connecting the (non)-existence of failing lists to the (non)-existence of constant-weight codes and of block designs. (In contrast, Justesen and Høholdt identify triples (ℓ, n, d) for which the GS bound is tight for MDS codes over sufficiently large fields; see (the proof of) Theorem 4 in [9].)

The remaining results in our paper deal with RS codes. Here, we use the identity $k{-}1 = n{-}d$, and we slightly modify the common definition of *rate* of an $[n, k, d]$ MDS code and use it for the value $(k{-}1)/n = 1 - \delta$; as it turns out, this value fits more conveniently into our analysis. The intervals $[\rho_r, \rho_{r+1})$ are thus referred to as rate intervals.

First, we obtain sufficient and necessary conditions for the existence of failing lists in RS codes (see Lemma 3.1 in Section 3). Using our sufficient conditions, we identify families of RS codes (other than those obtained in [9]) that attain the GS bound. For triples (ℓ, n, k) that correspond to the first and last sub-intervals in (3) (specifically, $(k{-}1)/n \leq 2/(\ell(\ell{+}1))$ or $(k{-}1)/n \geq 1 - (2/(\ell{+}1))$), we find a variety of finite fields $\mathrm{GF}(q)$ over which there are $[n, k, d]$ RS codes that attain the GS bound. These results are summarized in Propositions 1.4 and 1.5 below and proved later on (with all subsequent results that are stated in this section) in Section 4.

Proposition 1.4 covers the high-rate range (i.e., small values of d/n) and identifies quadruples (ℓ, n, d, q) for which a list-ℓ decoder for the worst $[n, k, d]$ RS code, and hence for the worst (n, M, d) code, does no better than a list-1 ('classical') decoder.

Proposition 1.4 *Let the RS-admissible quadruple* (ℓ, n, d, q), *other than* $(3, 2, 1, 2)$, *satisfy*

$$d/n \;\leq\; \frac{2}{\ell{+}1} \;\left(= 1 - \rho_\ell\right) .$$

Assume in addition that when $d > 1$, *the integer* $\lceil (d{-}1)/2 \rceil$ *divides either* $q{-}1$ *or* q. *Then,*

$$\Delta_\ell^{\mathrm{RS}}(n, d; q) = \lceil \tau_\ell(n, d) \rceil - 1 = \lfloor (d{-}1)/2 \rfloor = \Delta_1^{\mathrm{RS}}(n, d; q) .$$

We show in Section 4.3 that there are infinitely many RS-admissible quadruples that satisfy the conditions of Proposition 1.4.

Proposition 1.5 covers the low-rate range (the leftmost sub-interval in (3), namely high values of d/n) and makes use of the following definition. A subset X of an Abelian group is called a *weak Sidon set* if every four distinct elements $\theta_1, \theta_2, \theta_3, \theta_4 \in X$ satisfy $\theta_1{+}\theta_2 \neq \theta_3{+}\theta_4$ (see [1], [4], [6], [12]). The notation $\mathbb{Z}_m$ will stand for the ring of integers modulo m.

Proposition 1.5 *For a prime p, let the RS-admissible quadruple $(\ell, n, d, q{=}p^h)$ satisfy*

$$\left(1-\rho_2 =\right)\ 1-\frac{2}{\ell(\ell{+}1)}\ \le\ d/n\ <\ 1\ .$$

Assume in addition that either

(a) $n{-}d \,|\, q{-}1$ and the additive group of $\mathbb{Z}_{(q-1)/(n-d)}$ contains a weak Sidon set of size $\ell{+}1$, or

(b) $n{-}d = p^b$ for some integer b and $\mathbb{Z}_p^{h-b}$ contains a weak Sidon set of size $\ell{+}1$.

Then,

$$\Delta_\ell^{\mathrm{RS}}(n,d;q) = \lceil \tau_\ell(n,d)\rceil - 1 = \lceil \ell n/(\ell{+}1) - \ell(n{-}d)/2\rceil - 1\ .$$

Based on known properties of Sidon sets, we show in Section 4.5 that each of the two cases, (a) and (b), in Proposition 1.5 covers infinitely many RS-admissible quadruples.

Observe that we have excluded the case $d = n$ (the repetition code) from Proposition 1.5. Here we have

$$\Delta_\ell^{\mathrm{RS}}(n,n;q) = \lceil \tau_\ell(n,n)\rceil - 1 = \lceil (\ell n/(\ell{+}1))\rceil - 1$$

only when $\ell < q$: there are $\ell{+}1$ codewords at Hamming distance $\le \lceil \ell n/(\ell{+}1)\rceil$ from a word $\boldsymbol{v}$ in which each of some $\ell{+}1$ elements of GF(q) occurs at least $\lfloor n/(\ell{+}1)\rfloor$ times. When $\ell \ge q$ we obviously have $\Delta_\ell^{\mathrm{RS}}(n,n;q) = n$.

Consider now the intermediate sub-intervals in (3), i.e., the mid-rate range

$$\frac{2}{\ell{+}1}\ <\ \frac{d}{n}\ <\ 1-\frac{2}{\ell(\ell{+}1)}\ ;$$

this range is nonempty for $\ell \ge 3$. The treatment of this range seems to be more elaborate than the extreme (rightmost and leftmost) sub-intervals. Hence, our results for the mid-rate range are quite partial; yet, they demonstrate that the techniques that are developed in this paper are applicable not only to the extreme sub-intervals. These results are presented in Section 4.4.

The propositions presented in this introduction section, together with those presented in Sections 4.1 and 4.4, imply, for example, that

$$\liminf_{q\to\infty} \Delta_3(n,k;q) = \lceil \tau_3(n,k)\rceil - 1$$

for all $1 \le k \le n \le 15$, except possibly for $(n,k) \in \{(4,2),(10,3),(14,6),(15,7)\}$. Verifying this statement is left to the reader.

On the other hand, as part of our treatment of the mid-rate range, we also find RS-admissible quadruples (ℓ, n, d, q) for which the GS lower bound is not tight. The next two propositions provide two examples of such quadruples.

Proposition 1.6 *Let $q \geq 11$ be a power of an odd prime. Then,*

$$\Delta_4^{\mathrm{RS}}(10, 7; q) \geq \tau_4(10, 7) = 4 \ .$$

In contrast, we show in Section 4.4 that $\Delta_4^{\mathrm{RS}}(10, 7; q) = \tau_4(10, 7) - 1 = 3$ when q is even. Moreover, it follows from Theorem 4 in [9] that $\Delta_4(10, 7; q) = \tau_4(10, 7) - 1 = 3$ for every large enough field size q.

Proposition 1.7 *For every $h \geq 4$,*

$$\Delta_{10}^{\mathrm{RS}}(11, 9; 2^h) \geq \tau_{10}(11, 9) = 6 \ .$$

This work is organized as follows: In Section 2, we develop the tools for synthesizing and analyzing failing lists in general codes. Theorem 1.2, Proposition 1.3, and some other combinatorial conditions on the tightness of the GS bound are proved using these tools. Specific tools for RS codes are then introduced in Section 3. Finally, Section 4 contains the proofs for Propositions 1.4–1.7.

2 Failing lists in general codes

Throughout this section, we fix the alphabet F of size q, the length n and minimum Hamming distance $d < n$ of an (n, M, d) code over F, and a list size ℓ. We let r be the unique integer such that $1 - d/n \in [\rho_r, \rho_{r+1})$, and we use the notation $\langle n \rangle$ for the set $\{1, 2, \ldots, n\}$.

2.1 Lower bound on $\Delta_\ell(n, d\,; q)$

Proof of Theorem 1.2: Assume to the contrary that there is an (n, M, d) code $\mathcal{C}$ for which $\Delta_\ell(\mathcal{C}) < \lceil \tau_\ell(n, d) \rceil - 1$. It follows that there is a set of $\ell+1$ codewords, $\mathcal{L} = \{\boldsymbol{c}_0, \boldsymbol{c}_1, \ldots, \boldsymbol{c}_\ell\} \subseteq \mathcal{C}$ and a word $\boldsymbol{v} \in F^n$ such that $\mathtt{d}_H(\boldsymbol{c}_s, \boldsymbol{v}) \leq \lceil \tau_\ell(n, d) \rceil$ for every $0 \leq s \leq \ell$.

For every $\mu \in \langle n \rangle$, denote by x_μ the number of words in $\mathcal{L}$ that agree with $\boldsymbol{v}$ on the μth position. On the one hand, it is clear that

$$\sum_{\mu=1}^{n} x_\mu > (\ell+1)(n - \tau_\ell(n, d)) \ . \tag{9}$$

On the other hand, the number of different (unordered) pairs $\{\boldsymbol{c}_s, \boldsymbol{c}_t\} \subseteq \mathcal{L}$ that agree on their μth coordinate is at least $\binom{x_\mu}{2}$. Since $\mathtt{d}_H(\boldsymbol{c}_s, \boldsymbol{c}_t) \geq d$ for every $0 \leq s < t \leq \ell$, it follows

that the total number of agreement coordinates, when ranging over all pairs $\{\boldsymbol{c}_s, \boldsymbol{c}_t\} \subseteq \mathcal{L}$, cannot exceed $\binom{\ell+1}{2}(n-d)$; therefore,

$$\sum_{\mu=1}^{n} \binom{x_\mu}{2} \leq \binom{\ell+1}{2}(n-d)\,. \tag{10}$$

Define

$$y = \frac{1}{r}\left(\binom{\ell+1}{2}(n-d) - \binom{r}{2}n\right)\,. \tag{11}$$

By the definition of the parameter r, we get that $0 \leq y < n$. It can be easily verified that the right-hand side of (9) equals $rn+y$. Denote $t = \lfloor y \rfloor + 1$. It follows from (9) that

$$\sum_{\mu=1}^{n} x_\mu \geq rn + t\,. \tag{12}$$

Regard $x_1, x_2, \ldots, x_n$ as integer variables that are constrained to satisfy (12). By [11, p. 526], the minimum of the sum $\sum_{\mu=1}^{n} \binom{x_\mu}{2}$ is

$$\tfrac{1}{2}(t(r+1)^2 + (n-t)r^2 - (rn+t)) \;=\; \binom{r}{2}n + rt \;>\; \binom{r}{2}n + ry \;=\; \binom{\ell+1}{2}(n-d)\,,$$

contradicting (10). ∎

The above proof is essentially a generalization of the proofs of Theorems 2 and 3 in [11, Ch. 17] to any finite alphabet: Theorem 2 therein is the Johnson bound on the size of a binary constant-weight code, and Theorem 3 follows from the Johnson bound by using arguments that take into account that the parameters we optimize over are integers. It turns out that a similar proof technique can be applied in our case, where non-binary codes are considered. (In [5, Theorem 4.2 (part 2)], the proof technique of the Johnson bound is refined for non-binary codes. It uses the observation that two codewords $\boldsymbol{c}_s$ and $\boldsymbol{c}_t$ in a non-binary code can both disagree with a given word $\boldsymbol{v}$ on a given position i while they also disagree with each other on position i. However, the proof in [5] does not take into account that some of the parameters involved are integer-valued. A further improvement on both Theorem 1.2 and [5, Theorem 4.2 (part 2)] has been recently reported in [14].)

2.2 (ℓ, r)-configurations

We define an (ℓ, r)-*configuration* as a set $\mathcal{L}$ of $\ell+1$ words in F^n such that for every position $\mu \in \langle n \rangle$ the following holds: there are exactly r or $r+1$ words in $\mathcal{L}$ that agree on that position by taking the same value, c_μ, and the remaining $\ell+1-r$ (respectively, $\ell-r$) words are all distinct on that position, neither does any of them take there the value c_μ.

We now repeat the definition with slight more detail. Let $S_1, S_2, \ldots, S_{\binom{\ell+1}{r}}$ be all the distinct subsets of $\{0, 1, \ldots, \ell\}$ of size r, and let $S'_1, S'_2, \ldots, S'_{\binom{\ell+1}{r+1}}$ be all the distinct subsets of

$\{0,1,\ldots,\ell\}$ of size $r{+}1$. A *partition vector* of $\langle n\rangle$ is an (ordered) list of $\binom{\ell+2}{r+1} = \binom{\ell+1}{r} + \binom{\ell+1}{r+1}$ disjoint subsets,

$$\left(I_1, I_2, \ldots, I_{\binom{\ell+1}{r}}, I'_1, I'_2, \ldots, I'_{\binom{\ell+1}{r+1}}\right) \ ,$$

whose union is $\langle n\rangle$. A partition vector $\mathcal{P}$ is said to be *proper* if $I'_j = \emptyset$ for all j. The existence of a proper (ℓ, r)-configuration over F implies $q \geq \ell{+}1{-}r$, where the existence of a non-proper configuration implies the weaker inequality $q \geq \ell{+}2{-}r$.

We will hereafter abbreviate notations and write $(I_i)_i \| (I'_j)_j$ for a partition vector; a proper partition vector will also be written as $(I_i)_i$. Given a partition vector $\mathcal{P} = (I_i)_i \| (I'_j)_j$, an (ℓ, r)-configuration with respect to $\mathcal{P}$ is a set of $\ell{+}1$ words $\mathcal{L} = \{\boldsymbol{c}_0, \boldsymbol{c}_1, \ldots, \boldsymbol{c}_\ell\} \subseteq F^n$ that satisfies the following two conditions:

- For every $i = 1, 2, \ldots, \binom{\ell+1}{r}$, the words in $\mathcal{L}_i = \{\boldsymbol{c}_s\}_{s \in S_i}$ are identical on the positions indexed by I_i, while none of the words in $\mathcal{L} \setminus \mathcal{L}_i$ agrees on any of those positions with any other word in $\mathcal{L}$.
- The same as the previous condition, with I'_j replacing I_i and $\mathcal{L}'_j = \{\boldsymbol{c}_s\}_{s \in S'_j}$ replacing $\mathcal{L}_i$ for $j = 1, 2, \ldots, \binom{\ell+1}{r+1}$.

The existence of an (ℓ, r)-configuration $\mathcal{L}$ with respect to a partition vector $\mathcal{P} = (I_i)_i \| (I'_j)_j$ implies the existence of an *incidence structure* $\boldsymbol{D}(\mathcal{L}) = (\mathcal{L}, \mathcal{B}, \mathcal{M})$ (see [2, Ch. 1]) with $\ell{+}1$ 'points,' corresponding to the codewords in $\mathcal{L}$, and a multi-set $\mathcal{B}$ of n (not necessarily distinct) 'blocks.' The $(\ell{+}1) \times n$ incidence matrix $\mathcal{M}$, which represents the incidence relation, is defined as follows:

$$\mathcal{M}_{s,\mu} = \begin{cases} 1 & \text{if } \mu \in I_i \text{ and } s \in S_i, \text{ for some } i \\ 1 & \text{if } \mu \in I'_j \text{ and } s \in S'_j, \text{ for some } j \\ 0 & \text{otherwise} \end{cases} , \qquad s \in \{0,1,\ldots,\ell\} \ , \quad \mu \in \langle n\rangle \ .$$

Using the terminology in [2], $\boldsymbol{D}(\mathcal{L})$ is an incidence structure with possibly repeated blocks and up to two block sizes, r and $r{+}1$; when the partition elements I_i and I_j are all of size ≤ 1, no repeated blocks appear, and when $\mathcal{P}$ is a proper partition vector, only the block size r is allowed.

Lemma 2.1 below provides sufficient conditions for an (ℓ, r)-configuration $\mathcal{L}$ to form a failing list.

Lemma 2.1 *Let $\mathcal{L} = \{\boldsymbol{c}_0, \boldsymbol{c}_1, \ldots, \boldsymbol{c}_\ell\}$ be an (ℓ, r)-configuration with respect to a partition vector $(I_i)_i \| (I'_j)_j$ of $\langle n\rangle$ that satisfies both*

$$\sum_{i\,:\,\{s,t\} \subseteq S_i} |I_i| \ + \sum_{j\,:\,\{s,t\} \subseteq S'_j} |I'_j| \ \leq \ n{-}d \ , \qquad 0 \leq s < t \leq \ell \ , \tag{13}$$

and

$$\sum_{i\,:\,s\in S_i} |I_i| \;+\; \sum_{j\,:\,s\in S'_j} |I'_j| \;\;\geq\;\; n - \lceil \tau_\ell(n,d) \rceil \;, \qquad 0 \leq s \leq \ell \;. \tag{14}$$

Then $\mathcal{L}$ is a failing list: each word in $\mathcal{L}$ is at Hamming distance at most $\lceil \tau_\ell(n,d) \rceil$ from the majority-vote word $\boldsymbol{v} \in F^n$ that agrees on any position in I_i (respectively, I'_j) with the words in $\mathcal{L}_i$ (respectively, $\mathcal{L}'_j$).

Proof: By (13), every two words in $\mathcal{L}$ agree on at most $n-d$ positions and, thus, $\mathtt{d}_H(\boldsymbol{c}_s, \boldsymbol{c}_t) \geq d$ for every $0 \leq s < t \leq \ell$. In addition, by (14), the Hamming distance of each word in $\mathcal{L}$ from the word $\boldsymbol{v}$ is not greater than $\lceil \tau_\ell(n,d) \rceil$. It follows that $\mathcal{L}$ is a failing list. ∎

The following corollary describes a case with certain symmetry where Lemma 2.1 can be applied. This special case is later used to indicate RS codes that contain failing lists.

Corollary 2.2 *Suppose there are integers $\gamma > 0$ and $\gamma' \geq 0$ that satisfy*

$$\tbinom{\ell+1}{r}\gamma + \tbinom{\ell+1}{r+1}\gamma' = n \qquad \textit{and} \qquad \tbinom{\ell-1}{r-2}\gamma + \tbinom{\ell-1}{r-1}\gamma' = n-d \tag{15}$$

(here $\tau_\ell(n,d)$ is an integer and its value is given by $\binom{\ell}{r}\gamma + \binom{\ell}{r+1}\gamma'$). Let $\mathcal{L} = \{\boldsymbol{c}_0, \boldsymbol{c}_1, \ldots, \boldsymbol{c}_\ell\}$ be an (ℓ, r)-configuration with respect to a partition vector $(I_i)_i \| (I'_j)_j$ of $\langle n \rangle$ where $|I_i| = \gamma$ and $|I'_j| = \gamma'$. Let $\boldsymbol{v} \in F^n$ be the majority-vote word. Then $\mathcal{L}$ is a failing list in which $\mathtt{d}_H(\boldsymbol{c}_s, \boldsymbol{c}_t) = d$ for every $0 \leq s < t \leq \ell$ and $\mathtt{d}_H(\boldsymbol{c}_s, \boldsymbol{v}) = \tau_\ell(n,d)$ for every $0 \leq s \leq \ell$.

We point out that the failing lists described in [9], corresponding to cases where the relative minimum distance is $1 - \rho_r$, have a combinatorial structure which is a special case of the (ℓ, r)-configuration in Corollary 2.2, obtained when $\gamma' = 0$. As indicated in [9], the incidence structure $\boldsymbol{D}(\mathcal{L})$ in this case is a replication of the trivial (complete) BIBD with parameters $(\ell+1, r, (n-d)/\gamma)$. In such a BIBD, the $n = \binom{\ell+1}{r}$ blocks correspond to all the distinct r-subsets of the point set $\mathcal{L}$, each pair of points appears in exactly $(n-d)/\gamma = \binom{\ell}{r}$ blocks, and each single point appears in exactly $(n - \tau_\ell(n,d))/\gamma = \binom{\ell}{r-1}$ blocks.

Example 2.1 Figure 1 presents a $(3, 2)$-configuration of four words of length 10 over GF(11) and the respective majority-vote word $\boldsymbol{v}$. The words $\boldsymbol{c}_0, \boldsymbol{c}_1, \boldsymbol{c}_2, \boldsymbol{c}_3$ are codewords of a $[10, 4, 7]$ RS code whose code locators are $0, 5, 6, 4, 2, 1, 7, 3, 9, 8$. The configuration forms a failing list since every two codewords agree on $n-d = 3$ positions and $\boldsymbol{v}$ agrees with every codeword on $\tau_3(10, 7) = 4$ positions. Note that for every two distinct $s, t \in \{0, 1, 2, 3\}$ there is a unique position on which only $\boldsymbol{c}_s$ and $\boldsymbol{c}_t$ agree, and for every three distinct $s, t, u \in \{0, 1, 2, 3\}$ there is a unique position on which only $\boldsymbol{c}_s$, $\boldsymbol{c}_t$, and $\boldsymbol{c}_u$ agree. This list thus corresponds to the structure described in Corollary 2.2, where $\gamma = \gamma' = 1$. ∎

$$
\begin{array}{lcccccccccc}
\boldsymbol{c}_0 = & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\boldsymbol{c}_1 = & 0 & 0 & 2 & 3 & 0 & 4 & 4 & 5 & 10 & 1 \\
\boldsymbol{c}_2 = & 0 & 8 & 0 & 3 & 1 & 0 & 3 & 5 & 6 & 8 \\
\boldsymbol{c}_3 = & 6 & 0 & 0 & 3 & 8 & 5 & 0 & 1 & 10 & 8 \\
 & & & & & & & & & & \\
\boldsymbol{v} = & 0 & 0 & 0 & 3 & 0 & 0 & 0 & 5 & 10 & 8
\end{array}
$$

Figure 1: $(3,2)$-configuration over GF(11).

Example 2.2 Figure 2 presents a $(4,3)$-configuration of five codewords of a $[10,4,7]$ RS code over GF(16) (the field is represented as polynomials over GF(2) modulo x^4+x+1, and the four polynomial coefficients of each element are written in hexadecimal notation). The rate, $1-d/n = 3/10$, equals the boundary rate $\rho_3(4)$. This configuration follows the structure described in Corollary 2.2, where $\gamma = 1$ and $\gamma' = 0$, and it therefore forms a failing list. It can be easily verified that indeed every two codewords agree on $n-d = 3$ positions and $\boldsymbol{v}$ agrees with every codeword on $\tau_4(10,7) = 4$ positions. The list structure here corresponds to the (complete) BIBD$(5,3,3)$ (which has 10 blocks), and we show in the sequel (Lemma 4.4), that, in fact, *every* failing list of five codewords in a $(10,M,7)$ code over any alphabet F must have the form of a BIBD$(5,3,3)$. It follows that such a failing list cannot be realized over the binary alphabet, and by Propositions 4.3 and 1.6, it can be realized in RS codes over GF(q) if and only if q is a power of 2 not smaller than 16. ■

$$
\begin{array}{lcccccccccc}
\boldsymbol{c}_0 = & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\boldsymbol{c}_1 = & 0 & 0 & 0 & 9 & \mathrm{f} & 2 & \mathrm{a} & 4 & \mathrm{f} & \mathrm{b} \\
\boldsymbol{c}_2 = & 0 & 9 & 1 & 0 & 0 & \mathrm{b} & \mathrm{a} & 4 & 7 & \mathrm{c} \\
\boldsymbol{c}_3 = & \mathrm{a} & 0 & 5 & 0 & \mathrm{a} & 0 & \mathrm{a} & \mathrm{a} & \mathrm{f} & \mathrm{c} \\
\boldsymbol{c}_4 = & \mathrm{c} & 4 & 0 & \mathrm{f} & 0 & 0 & 1 & 4 & \mathrm{f} & \mathrm{c}
\end{array}
$$

Figure 2: $(4,3)$-configuration over GF(16).

Fix a list size ℓ and a rational number $\delta \in (0,1]$. We claim that one can always extend ℓ to some admissible quadruple (ℓ,n,d,q) with $d/n = \delta$, such that $\ell+1$ words that form a failing list are contained in F^n (where F is an alphabet of size q). Indeed, replacing d by $n\delta$ in (15) (where r is uniquely determined by δ and ℓ) transforms (15) into a set of two homogeneous equations in the three unknowns γ, γ', and n. A nontrivial integer solution must then exist. For any value of q greater than $\ell+2-r$, we can find $\ell+1$ words in F^n that form an (ℓ,r)-configuration with respect to some partition vector $\mathcal{P} = (I_i)_i \| (I'_j)_j$ of $\langle n \rangle$, where $|I_i| = \gamma$ for $1 \le i \le \binom{\ell+1}{r}$, and $|I'_j| = \gamma'$ for $1 \le j \le \binom{\ell+1}{r+1}$. By Corollary 2.2, this is a failing list.

2.3 Necessary conditions on the existence of failing lists

Proposition 2.3 below motivates our interest in failing lists that form (ℓ, r)-configurations. It states that when $\tau_\ell(n,d)$ is an integer, namely when (6) holds, every failing list of size $\ell{+}1$ is necessarily an (ℓ, r)-configuration. The sufficient condition for the existence of a failing list, as stated in Lemma 2.1, thus turns to be necessary in cases where (6) holds.

Proposition 2.3 *Let ℓ, r, n, and d be integers for which (6) holds, and let $\mathcal{L}$ be a failing list of size $\ell{+}1$ that is contained in an (n, M, d) code over F.*

N1 *The list $\mathcal{L}$ is an (ℓ, r)-configuration with respect to some partition vector $\mathcal{P} = (I_i)_i \| (I'_j)_j$ of $\langle n \rangle$ that satisfies conditions (13)–(14) with equality.*

N2 *$\mathcal{P}$ is proper (i.e., exactly r out of the $\ell{+}1$ words in $\mathcal{L}$ agree on every position) if and only if $1 - d/n = r(r{-}1)/(\ell(\ell{+}1)) = \rho_r$.*

N3 *If $1 - d/n = r(r{-}1)/(\ell(\ell{+}1))$, then $q \geq \ell{+}1{-}r$. Otherwise, $q \geq \ell{+}2{-}r$.*

Remark: Property N3 above is a re-statement of Proposition 1.3.

Proof: Let $\mathcal{L} = \{\boldsymbol{c}_0, \boldsymbol{c}_1, \ldots, \boldsymbol{c}_\ell\}$ be a failing list with the given parameters, and let $\boldsymbol{v}$ be the word in F^n for which $\mathsf{d}_H(\boldsymbol{c}_s, \boldsymbol{v}) \leq \tau = \tau_\ell(n,d)$ for every $s \in \{0, 1, \ldots, \ell\}$. As in the proof of Theorem 1.2, we denote by x_μ, $\mu \in \langle n \rangle$, the number of words in $\mathcal{L}$ that agree with $\boldsymbol{v}$ on the μth position. By arguments similar to those in the proof of Theorem 1.2, we get that

$$\sum_{\mu=1}^{n} x_\mu \geq (\ell{+}1)(n - \tau) \tag{16}$$

and

$$\sum_{\mu=1}^{n} \tbinom{x_\mu}{2} \leq \tbinom{\ell+1}{2}(n{-}d)\,. \tag{17}$$

Let y be as in (11). Under the assumption that (6) holds, y must be an integer. When $1 - d/n = \rho_r$, we get $y = 0$; otherwise, $0 < y < n$. Regard $x_1, x_2, \ldots, x_n$ as integer variables that are constrained to satisfy (16) with equality. By [11, p. 526], the minimum of the sum $\sum_{\mu=1}^{n} \binom{x_\mu}{2}$ is attained when (and only when) y of the variables take the value $r{+}1$ while the rest take the value r; such an assignment satisfies (17) with equality. Since the minimum could only increase if we constrained the sum $\sum_{\mu=1}^{n} x_\mu$ to be larger, we have thus characterized the only feasible solutions to (16)–(17).

We now define the partition vector $\mathcal{P}$ that is stated in the lemma. For every subset S_i (respectively, S'_j) of $\{0, 1, \ldots, \ell\}$ of size r (respectively, $r{+}1$), let I_i (respectively, I'_j) be the set

of positions on which the words in $\mathcal{L}_i = \{\boldsymbol{c}_s \,:\, s \in S_i\}$ (respectively, $\mathcal{L}_j = \{\boldsymbol{c}_s \,:\, s \in S'_j\}$)—and only these words—agree with $\boldsymbol{v}$.

Since the union of $\bigcup_i I_i$ and $\bigcup_j I'_j$ is necessarily $\langle n \rangle$, it follows that $\mathcal{P} = (I_i)_i \| (I'_j)_j$ is a partition vector. We have,

$$\sum_{i\,:\,\{s,t\}\subseteq S_i} |I_i| \;+\; \sum_{j\,:\,\{s,t\}\subseteq S'_j} |I'_j| \;\;\leq\;\; n - \mathsf{d}_H(\boldsymbol{c}_s, \boldsymbol{c}_t)\;, \qquad 0 \leq s < t \leq \ell\;, \tag{18}$$

and

$$\sum_{i\,:\,s\in S_i} |I_i| \;+\; \sum_{j\,:\,s\in S'_j} |I'_j| \;\;=\;\; n - \mathsf{d}_H(\boldsymbol{c}_s, \boldsymbol{v})\;, \qquad 0 \leq s \leq \ell\;. \tag{19}$$

Since $\mathcal{L}$ is a failing list, we can bound the right-hand side of (18) from above by $n-d$ and the right-hand size of (19) from below by $n-\tau$. This, in turn, implies that conditions (13)–(14) hold. Furthermore, since (16)–(17) hold with equality, we obtain,

$$\tfrac{1}{2} \sum_{0\leq s<t\leq \ell} \Big(\sum_{i\,:\,\{s,t\}\subseteq S_i} |I_i| \;+\; \sum_{j\,:\,\{s,t\}\subseteq S'_j} |I'_j| \Big) \;\;=\;\; \sum_{\mu=1}^{n} \tbinom{x_\mu}{2} = \tbinom{\ell+1}{2}(n-d)$$

and

$$\sum_{s=0}^{\ell} \Big(\sum_{i\,:\,s\in S_i} |I_i| \;+\; \sum_{j\,:\,s\in S'_j} |I'_j| \Big) \;\;=\;\; \sum_{\mu=1}^{n} x_\mu \;=\; (\ell{+}1)(n-\tau)\;.$$

It follows that conditions (13)–(14) hold with equality, and so does (18). The equality in (18) implies that when $x_\mu = r$ (respectively, $x_\mu = r{+}1$), there are exactly $\binom{r}{2}$ (respectively, $\binom{r+1}{2}$) different pairs of words in $\mathcal{L}$ that agree on their μth coordinate. In particular, a word in $\mathcal{L} \setminus \mathcal{L}_i$ (respectively, $\mathcal{L} \setminus \mathcal{L}'_j$) does not agree on any position in I_i (respectively, I'_j) with any other word in $\mathcal{L}$. We conclude that $\mathcal{L}$ is an (ℓ, r)-configuration with respect to the partition vector $\mathcal{P}$, and property N1 is thus proved. Recalling that $y{=}0$ when $1 - d/n = \rho_r$, property N2 is proved as well. Property N3 is implied by Properties N1–N2 and by the definition of an (ℓ, r)-configuration. ∎

2.4 Constant-weight codes, Block designs, and failing lists

One necessary condition on the existence of failing lists is given in Proposition 2.4 below by means of constant-weight codes. If F is an additive group, then an (n, d, w) constant-weight code over F is a subset of F^n such that the Hamming weight (i.e., the number of nonzero components) of every codeword is w and the minimum Hamming distance between different codewords is d (see also [11, page 524]).

Proposition 2.4 *Let (ℓ, n, d, q) be an admissible quadruple, let r be the unique integer such that $1 - d/n \in [\rho_r, \rho_{r+1})$, and assume that (6) holds. Suppose that a failing list is contained*

in some (n, M, d) code over an additive group F of size q. Then a (possibly different) failing list forms an $(n, d, \tau_\ell(n,d))$ constant-weight code $\bar{\mathcal{C}}$ over F, consisting of $\ell{+}1$ codewords. The Hamming distance between different codewords in $\bar{\mathcal{C}}$ is exactly d.

Proof: Let $\mathcal{L} = \{\boldsymbol{c}_s\}_{s=0}^{\ell}$ be the failing list, and let $\boldsymbol{v}$ be as in the proof of Proposition 2.3. By property N1 of that proposition, the set $\{\boldsymbol{c}_0{-}\boldsymbol{v}, \boldsymbol{c}_1{-}\boldsymbol{v}, \ldots, \boldsymbol{c}_\ell{-}\boldsymbol{v}\}$ forms the required constant-weight code over F. ∎

Let $\mathcal{L}$ be a failing list as in Proposition 2.3. We consider the incidence structure $\boldsymbol{D}(\mathcal{L}) = (\mathcal{L}, \mathcal{B}, \mathcal{M})$ as a generalization of a BIBD$(\ell{+}1, r, n{-}d)$, referred to as a *quasi*-BIBD and denoted QBIBD$(\ell{+}1, r, n{-}d; n)$. For an introduction on BIBDs, see [2], [8, Ch. 10], and [11, Section 2.5]. In a QBIBD, similarly to a BIBD, every pair of points appears in exactly $n{-}d$ blocks (the incidence structure is pairwise balanced), and each single point appears in exactly $n{-}\tau_\ell(n,d)$ blocks. However, in a QBIBD, y blocks are of size $r{+}1$, where y is defined by (11), and the remaining $n{-}y > 0$ blocks are of size r. In addition, repeated blocks are allowed in a QBIBD.

Note that the number of blocks n appears as a parameter in the definition of a QBIBD since it is not uniquely determined by the other three parameters. However, the following connection between the parameters must hold:

$$\binom{r}{2} n \leq \binom{\ell+1}{2}(n{-}d) < \binom{r+1}{2} n \,. \tag{20}$$

When the left inequality in (20) holds with equality (i.e., the code relative minimum distance is $1 - \rho_r$), the n blocks are all of size r.

Some useful properties of a BIBD, such as Fisher's inequality (see, for example, [2, p. 81]), hold also for a QBIBD, as stated in the following lemma. The proof is essentially the same as in the case of a BIBD, and it is included for the sake of completeness.

Lemma 2.5 *In a* QBIBD$(\ell{+}1, r, n{-}d; n)$*, there are at least $\ell{+}1$ distinct blocks. In particular, $\ell{+}1 \leq n$.*

Proof: Let $\boldsymbol{D}(\mathcal{L}) = (\mathcal{L}, \mathcal{B}, \mathcal{M})$ be an incidence structure of a QBIBD$(\ell{+}1, r, n{-}d; n)$. The entries of the $(\ell{+}1) \times (\ell{+}1)$ matrix $\mathcal{M}\mathcal{M}^T$ are given by

$$(\mathcal{M}\mathcal{M}^T)_{s,t} = \begin{cases} n{-}\tau_\ell(n,d) & \text{if } s = t \\ n{-}d & \text{if } s \neq t \end{cases} ,$$

and, so,

$$\det \mathcal{M}\mathcal{M}^T = (d{-}\tau_\ell(n,d))^\ell \cdot (\ell(n{-}d){+}n - \tau_\ell(n,d)) \neq 0 \,.$$

It follows that $\mathcal{M}\mathcal{M}^T$ contains at least $\ell{+}1$ linearly independent—and hence distinct—columns. ∎

The following corollary is implied by Proposition 2.3 and Lemma 2.5.

Corollary 2.6 *Let ℓ, r, n, and d be integers for which (6) holds. Then a failing list of size $\ell+1$ is contained in an (n, M, d) code over some alphabet F only if there exists a* QBIBD$(\ell+1, r, n-d; n)$. *In particular, $\ell+1 \leq n$ whenever a failing list $\mathcal{L}$ exists.*

The next lemma deals with the special case $n = \ell+1$.

Lemma 2.7 *A* QBIBD$(n, r, n-d; n)$ *is a (symmetric)* BIBD$(n, r, n-d)$.

Proof: By Lemma 2.5, the n blocks are all distinct. Now, in a QBIBD$(n, r, n-d; n)$, each point appears in $n-\tau_\ell(n, d)$ blocks and, so, $\tau_\ell(n, d)$ is an integer. The divisibility condition (6), which necessarily holds here, becomes

$$2r \quad \text{divides} \quad r(r+1) + (n-1)(n-d)\,.$$

By (20), we also require

$$r(r-1) \leq (n-1)(n-d) < r(r+1)\,.$$

The above two constraints are satisfied only if $(n-1)(n-d) = r(r-1)$, implying that the n *distinct* blocks are all of the *same size* r. The QBIBD is thus a BIBD. ∎

Proposition 2.8 below deals with list sizes $\ell \geq n-1$. In particular, it states that when $\ell = n-1$, the GS bound can be attained only when there is a symmetric BIBD with parameters $(n, r, n-d)$. Such a design consists of n 'points' and n 'blocks' of size r, where each pair of distinct points appears in exactly $n-d$ blocks.

Proposition 2.8 *Let ℓ, r, n, d, q be as in Proposition 2.4.*

B1 *If $n = \ell+1$ then $\Delta_\ell(n, d; q) = \tau_\ell(n, d)-1$ only when there is a* BIBD$(n, r, n-d)$ *with $r(r-1) = (n-1)(n-d)$.*

B2 *If $n < \ell+1$ then $\Delta_\ell(n, d; q) \geq \tau_\ell(n, d)$.*

Proof: Combine Corollary 2.6 and Lemma 2.7. ∎

Necessary conditions on the parameters of a symmetric BIBD were given by Bruck, Chowla, and Ryser (see [2, page 100] or [8, page 133]). It follows from Proposition 2.8 that whenever these conditions are not satisfied by $(n, r, n-d)$, no (n, M, d) code attains the GS bound with equality. For example, since there is no BIBD$(22, 7, 2)$, we obtain for every alphabet size q,

$$\Delta_{21}(22, 20; q) \geq 15 = \tau_{21}(22, 20)\,.$$

Similarly,

$$\Delta_{42}(43, 42; q) \geq 36 = \tau_{42}(43, 42)\,.$$

3 Realizing failing lists in RS codes

Throughout this section we fix the finite field $F = \mathrm{GF}(q)$, the list size ℓ, and an $[n,k,d]$ RS code $\mathcal{C}$ over F with a set of code locators $\{\alpha_1, \alpha_2, \ldots, \alpha_n\} \subseteq F$. We let r be the unique integer such that $1-\delta = (k-1)/n \in [\rho_r, \rho_{r+1})$.

Suppose that $\mathcal{C}$ contains a set $\mathcal{L} = \{\boldsymbol{c}_0, \boldsymbol{c}_1, \ldots, \boldsymbol{c}_\ell\}$ which is an (ℓ, r)-configuration with respect to some partition vector $\mathcal{P}$ for which (13)–(14) are satisfied. Without loss of generality, assume that $\boldsymbol{c}_0$ is the zero codeword (otherwise, subtract $\boldsymbol{c}_0$ from each $\boldsymbol{c}_s$ to obtain another (ℓ, r)-configuration with respect to $\mathcal{P}$). For every two indexes s, t such that $0 \le s < t \le \ell$, the difference $\boldsymbol{c}_s - \boldsymbol{c}_t$ is a codeword that is obtained by evaluating a polynomial of degree $\le k-1$ at the code locators. We denote this polynomial by $a_{s,t} \cdot f_{s,t}(x)$, where $a_{s,t} \in F \setminus \{0\}$ and $f_{s,t}(x)$ is a monic polynomial of degree $\le k-1$.

For every subset $S_i \subseteq \{0, 1, \ldots, \ell\}$ of size r and every subset S'_j of size $r+1$, define

$$A_{S_i}(x) = \prod_{\mu \in I_i} (x - \alpha_\mu) \qquad \text{and} \qquad A_{S'_j}(x) = \prod_{\mu \in I'_j} (x - \alpha_\mu) \ . \tag{21}$$

By the definition of an (ℓ, r)-configuration with respect to a partition vector, it follows that the polynomials $f_{s,t}(x)$ are given by

$$f_{s,t}(x) = \prod_{i \,:\, \{s,t\} \subseteq S_i} A_{S_i}(x) \cdot \prod_{j \,:\, \{s,t\} \subseteq S'_j} A_{S'_j}(x) \tag{22}$$

(a product over an empty set is defined as 1). A necessary condition on the existence of the configuration $\mathcal{L}$ in $\mathcal{C}$ is:

$$a_{s,t} \cdot f_{s,t}(x) = a_{0,s} \cdot f_{0,s}(x) - a_{0,t} \cdot f_{0,t}(x) \ , \quad 0 < s < t \le \ell \ . \tag{23}$$

Conversely, suppose that $\mathcal{P} = (I_i)_i \| (I'_j)_j$ is a partition vector that satisfies (13)–(14), and let the polynomials $f_{s,t}(x)$ be defined by (22). If there are nonzero constants $a_{s,t} \in F$ that satisfy (23), then an (ℓ, r)-configuration with respect to $\mathcal{P}$ exists. Based on Lemma 2.1 and Proposition 2.3, the following lemma is obtained.

Lemma 3.1 *Let $(I_i)_i \| (I'_j)_j$ be a partition vector of $\langle n \rangle$ that satisfies (13)–(14) and let the polynomials $f_{s,t}(x)$, $0 \le s < t \le \ell$, be defined by (22).*

(a) If there are $\binom{\ell+1}{2}$ nonzero constants $a_{s,t} \in F$ such that (23) holds, then $\mathcal{C}$ contains a failing list that consists of the zero codeword and the following ℓ codewords

$$(f(\alpha_1)\ f(\alpha_2)\ \ldots\ f(\alpha_n)) \ , \quad f(x) \in \{a_{0,s} \cdot f_{0,s}(x)\}_{s=1}^{\ell} \ .$$

(b) In cases where (6) holds, the sufficient conditions in part (a) for the existence of a failing list of size $\ell+1$ are also necessary, and each polynomial $f_{s,t}(x)$ has degree $k-1$.

3.1 The difference condition and simple sets of polynomials

Three monic polynomials $f(x) = \sum_i f_i x^i$, $g(x) = \sum_i g_i x^i$, and $h(x) = \sum_i h_i x^i$ are said to satisfy the *difference condition* if there are $\tilde{f}, \tilde{g}, \tilde{h} \in F \setminus \{0\}$ for which

$$\tilde{h} \cdot h(x) = \tilde{f} \cdot f(x) - \tilde{g} \cdot g(x) \ . \tag{24}$$

Observe that every three polynomials in (23) must satisfy the difference conditions.

Lemma 3.2 *Three distinct monic polynomials of the same degree e, $f(x) = \sum_{i \le e} f_i x^i$, $g(x) = \sum_{i \le e} g_i x^i$, and $h(x) = \sum_{i \le e} h_i x^i$, satisfy the difference condition if and only if*

$$(f_i - h_i)(f_j - g_j) = (f_i - g_i)(f_j - h_j) \quad \textit{for every} \quad 0 \le i, j \le e \ . \tag{25}$$

Proof: The difference condition is satisfied if and only if there are $\tilde{f}, \tilde{g}, \tilde{h} \in F \setminus \{0\}$ for which

$$\tilde{h} \cdot h_i = \tilde{f} \cdot f_i - \tilde{g} \cdot g_i, \quad 0 \le i \le e \ , \tag{26}$$

and since $f(x)$, $g(x)$, and $h(x)$ are monic polynomials of the same degree e, we obtain, in particular, that

$$\tilde{h} = \tilde{f} - \tilde{g} \ . \tag{27}$$

A nontrivial solution for $\tilde{f}, \tilde{g}, \tilde{h}$ exists if and only if the following matrix is singular for every $0 \le i \le j \le e$:

$$\begin{pmatrix} 1 & -1 & -1 \\ f_i & -g_i & -h_i \\ f_j & -g_j & -h_j \end{pmatrix} \ .$$

This matrix, in turn, is singular if and only if (25) holds.

Now, the values of $\tilde{f}, \tilde{g}, \tilde{h}$ must be all nonzero in every nontrivial solution of (24), as required by the difference condition: by (27), it is impossible that exactly two of them are zero, and if only one is zero, then, by combining (26) and (27) we obtain that two out of three polynomials $f(x)$, $g(x)$, and $h(x)$ are identical; this, however, contradicts our assumption that these polynomials are distinct. ■

Our constructions that realize (22)–(23) will have the special structure defined next. A set of polynomials of degree e over F is *simple over a set $U \subseteq F$* if the following three conditions hold:

(S1) Each polynomial has e simple roots in U.

(S2) Every two distinct polynomials in the set are relatively prime.

(S3) The polynomials differ only in the ith coefficient, for some i. For example, they differ only in their constant term.

Corollary 3.3 *Every three polynomials in a simple set satisfy the difference condition.*

Proof: Let $f(x)$, $g(x)$, and $h(x)$ be three polynomials of degree e in a simple set. By property S3 of simple sets, $(f_i - h_i)(f_j - g_j) = (f_i - g_i)(f_j - h_j) = 0$, for every distinct i, j such that $0 \leq i, j \leq e$. Obviously, for $i = j$ we have $(f_i - h_i)(f_j - g_j) = (f_i - g_i)(f_j - h_j)$. By Lemma 3.2, the difference condition is satisfied. ■

3.2 Rates above $2/(\ell(\ell+1))$

Lemma 3.4 below provides a *sufficient* condition on the existence of failing lists of size $\ell+1$ in $\mathcal{C}$. The statement of the lemma makes use of the following notation. Let $\mathcal{P} = (I_i)_i \| (I'_j)_j$ be a partition vector of $\langle n \rangle$ and let $f_{s,t}(x)$, $0 \leq s < t \leq \ell$, be defined by (22). For every s, t, u such that $0 \leq s < t < u \leq \ell$, define

$$g_{s,t,u}(x) = \gcd(f_{s,t}(x), f_{s,u}(x), f_{t,u}(x)) \;=\; \prod_{i\,:\,\{s,t,u\}\subseteq S_i} A_{S_i}(x) \cdot \prod_{j\,:\,\{s,t,u\}\subseteq S'_j} A_{S'_j}(x)\;. \tag{28}$$

Lemma 3.4 *Let $\mathcal{P} = (I_i)_i \| (I'_j)_j$ be a partition vector of $\langle n \rangle$ for which (13)–(14) hold, and let $f_{s,t}(x)$ and $g_{s,t,u}(x)$ be the polynomials defined by (22) and (28), respectively. A failing list of size $\ell+1$ is contained in $\mathcal{C}$ if the following two conditions hold:*

- *For every $0 \leq s < t \leq \ell$, the polynomials $f_{0,s}(x)$, $f_{0,t}(x)$, and $f_{s,t}(x)$ satisfy the difference condition, and*
- *$g_{s,t,u}(x)$ does not divide $f_{0,s}(x)$ for every $0 < s < t < u \leq \ell$.*

Proof: We show that the sufficient conditions of Lemma 3.1(a) hold. If $f_{0,s}(x)$, $f_{0,t}(x)$, and $f_{s,t}(x)$ satisfy the difference condition, then, by definition, there must be nonzero $a_{0,s}, a_{0,t}, a_{s,t} \in F$ such that

$$a_{s,t} \cdot f_{s,t}(x) \;=\; a_{0,s} \cdot f_{0,s}(x) \;-\; a_{0,t} \cdot f_{0,t}(x)\;. \tag{29}$$

In case where $\ell = 2$, we are done.

Turning to larger values of ℓ, we need to show that the same coefficient $a_{0,s}$ multiplies $f_{0,s}(x)$ in (23), independently of t. Given $s \in \langle \ell-2 \rangle$, consider any indexes t and u such that

$s < t < u \leq \ell$. There must be nonzero $a_{0,s}, a_{0,t}, a_{s,t} \in F$ satisfying (29) and, by the same arguments, there must be nonzero $a_{0,u}, a_{t,u}, a_{s,u}, a'_{0,s} \in F$ such that

$$a_{t,u} \cdot f_{t,u}(x) = a_{0,t} \cdot f_{0,t}(x) - a_{0,u} \cdot f_{0,u}(x) \quad (30)$$

$$a_{s,u} \cdot f_{s,u}(x) = a'_{0,s} \cdot f_{0,s}(x) - a_{0,u} \cdot f_{0,u}(x) \; . \quad (31)$$

Subtracting (31) from the sum of (29) and (30) results in

$$a_{s,t} \cdot f_{s,t}(x) + a_{t,u} \cdot f_{t,u}(x) - a_{s,u} \cdot f_{s,u}(x) = (a_{0,s} - a'_{0,s}) \cdot f_{0,s}(x) \; . \quad (32)$$

Clearly, $g_{s,t,u}(x)$ divides the left-hand side of (32). However, according to the assumptions of the lemma, $g_{s,t,u}(x)$ does not divide $f_{0,s}(x)$. We therefore conclude that $a'_{0,s} = a_{0,s}$, i.e., the same coefficient $a_{0,s}$ does indeed multiply $f_{0,s}(x)$ in (23), independently of t. ■

Corollaries 3.5 and 3.6 below are derived from Lemma 3.4 and are used in Section 4 to indicate families of RS codes that contain failing lists of size $\ell+1$. Corollary 3.5 covers only the high-rate range $(k-1)/n \geq 1 - (2/(\ell+1))\,(= \rho_\ell)$, while Corollary 3.6 applies to $(k-1)/n > 2/(\ell(\ell+1))\,(= \rho_2)$.

Corollary 3.5 *Let the positive integer triple (ℓ, n, k) be such that $(k-1)/n \geq 1-(2/(\ell+1))$. A failing list is contained in $\mathcal{C}$ if there is some partition vector $\mathcal{P} = (I_1, I_2, \ldots, I_{\ell+1}, I'_1)$ of $\langle n \rangle$ such that the following holds:*

(a) (13)–(14) are satisfied, with equality in (13), and

(b) for every $0 \leq s < t \leq \ell$ in (22), the respective polynomials $f_{0,s}(x)$, $f_{0,t}(x)$, and $f_{s,t}(x)$, each of degree $k-1$, are <u>distinct</u> and satisfy the difference condition.

Proof: We show that whenever $r = \ell > 2$, for every $0 < s < t < u \leq \ell$ the polynomial $g_{s,t,u}(x)$ in (28) does not divide $f_{0,s}(x)$. The existence of a failing list will then follow from Lemma 3.4.

Without loss of generality we can assume that the sets S_i are defined so that $S_1 = \{1, 2, \ldots, \ell\}$. For every $0 < s < t < u$, the polynomial $g_{s,t,u}(x)$ does not divide $f_{0,s}(x)$ if and only if $\deg A_{S_1}(x) > 0$. Assume to the contrary that $\deg A_{S_1}(x) = 0$. Since $A_{S_1}(x) = f_{s,t}(x)/g_{0,s,t}(x)$, it then follows that $\deg g_{0,s,t}(x) = k-1$; therefore, $f_{0,s}(x) = g_{0,s,t}(x) = f_{0,t}(x)$, contradicting our assumption that $f_{0,s}(x)$ and $f_{0,t}(x)$ are distinct. ■

Corollary 3.6 *Let the positive integer triple (ℓ, n, k) be such that $(k-1)/n > 2/(\ell(\ell+1))$, and let $r > 1$, $\gamma > 0$, and $\gamma' \geq 0$ be integers for which (15) holds. Let $\mathcal{P} = (I_i)_i \| (I'_j)_j$ be a partition vector of $\langle n \rangle$ in which $|I_i| = \gamma$ and $|I'_j| = \gamma'$, and let $f_{s,t}(x)$ and $g_{s,t,u}(x)$ be the polynomials defined by (22) and (28), respectively. Suppose that for every $0 \leq s < t \leq \ell$, there is a polynomial divisor $\lambda_{s,t}(x)$ of $g_{0,s,t}(x)$ for which the set $\{f_{0,s}(x)/\lambda_{s,t}(x), f_{0,t}(x)/\lambda_{s,t}(x), f_{s,t}(x)/\lambda_{s,t}(x)\}$ is simple over the set of code locators of $\mathcal{C}$. Then $\mathcal{C}$ contains a failing list of size $\ell+1$.*

Proof: By Lemma 3.4, it suffices to show that $g_{s,t,u}(x)$ does not divide $f_{0,s}(x)$ for every $0 < s < t < u \leq \ell$. If $2 < r \leq \ell$, there is a nonempty partition element I_i in $\mathcal{P}$ that corresponds to a subset $S_i \subseteq \{0, 1, \ldots, \ell\}$ such that $\{s, t, u\} \subseteq S_i$ while $0 \notin S_i$. In this case, $A_{S_i}(x)$ divides $g_{s,t,u}(x)$ yet it does not divide $f_{0,s}(x)$; therefore, $g_{s,t,u}(x)$ does not divide $f_{0,s}(x)$, as required.

Assume now that $2 = r < \ell$. Since $(k-1)/n > 2/(\ell(\ell+1))$, there must exist a nonempty partition element I'_j in $\mathcal{P}$ that corresponds to a subset $S'_j = \{s, t, u\}$ of $\{0, 1, \ldots, \ell\}$. Since $|I'_j| = \gamma' > 0$, the polynomial $A_{S'_j}(x)$ divides $g_{s,t,u}(x)$ but not $f_{0,s}(x)$; thus, $g_{s,t,u}(x)$ does not divide $f_{0,s}(x)$, as required. ■

3.3 The low-rate range: $0 < (k-1)/n \leq 2/(\ell(\ell+1))$

Suppose that the rate of $\mathcal{C}$ satisfies $(k-1)/n < \rho_2 = 2/(\ell(\ell+1))$ and that $\mathcal{C}$ contains an $(\ell, 1)$-configuration $\mathcal{L}$. At most two out of the $\ell+1$ words in $\mathcal{L}$ agree on every position and, so, (22) becomes $f_{s,t}(x) = f_{s,t}(x)/g_{0,s,t}(x) = A_{S'_j}(x)$ for $S'_j = \{s, t\}$. Suppose now that $(k-1)/n = \rho_2$ and that $\mathcal{L}$ is an $(\ell, 2)$-configuration; here, $f_{s,t}(x) = f_{s,t}(x)/g_{0,s,t}(x) = A_{S_i}(x)$ for $S_i = \{s, t\}$. In both cases, the set $\{f_{s,t}(x)\}_{s,t}$ already satisfies conditions (S1) and (S2) for being simple over the set of code locators of $\mathcal{C}$. However, it turns out that when $\ell > 2$ in any of those two cases, taking the set $\{f_{s,t}(x)\}_{s,t}$ to be simple over the set of code locators does not guarantee the existence of multipliers $\{a_{s,t}\}_{s,t}$ for which (23) holds. An auxiliary condition on the coefficients of $\{f_{s,t}(x)\}_{s,t}$ is needed in this case, as stated in the following lemma.

Lemma 3.7 *Let the positive integer triple (ℓ, n, k) be such that $(k-1)/n \leq 2/(\ell(\ell+1))$. Suppose there exists a set $\{f^*_{0,1}(x), f^*_{0,2}(x), \ldots, f^*_{\ell-1,\ell}(x)\}$ of $\binom{\ell+1}{2}$ distinct polynomials of degree $k-1$ over F that is simple over a subset U of size $\binom{\ell+1}{2}(k-1)$ of the set of code locators of $\mathcal{C}$. Let e be the (unique) coefficient index in which the polynomials differ, and denote by $\psi_{s,t}$ the eth coefficient of $f^*_{s,t}(x)$. Assume that when $\ell > 2$, the coefficients $\psi_{s,t}$ satisfy the $\binom{\ell-1}{2}$ equations*

$$(\psi_{1,s}-\psi_{0,1})(\psi_{1,t}-\psi_{0,t})(\psi_{s,t}-\psi_{0,s}) = (\psi_{1,s}-\psi_{0,s})(\psi_{1,t}-\psi_{0,1})(\psi_{s,t}-\psi_{0,t}) \ , \quad 1 < s < t \leq \ell \ . \tag{33}$$

Then there exist nonzero $a_{0,1}, a_{0,2}, \ldots, a_{0,\ell} \in F$ such that the zero word and the following ℓ words,

$$(f(\alpha_1)\ f(\alpha_2)\ \ldots\ f(\alpha_n)) \ , \quad f(x) \in \{a_{0,s} \cdot f^*_{0,s}(x)\}_{s=1}^{\ell} \ ,$$

form a failing list in $\mathcal{C}$.

Proof: Our proof is based on Lemma 3.1(a). To this end, we first find a partition vector $\mathcal{P} = (I_i)_i \| (I'_j)_j$ of $\langle n \rangle$ that satisfies (13)–(14) and that allows us to express the polynomials

$f^*_{s,t}(x)$ in the form (22). When $(k-1)/n = \rho_2$ we select $\mathcal{P}$ to be proper and for every $S_i = \{s,t\}$ we let $I_i = \{\mu : f^*_{s,t}(\alpha_\mu) = 0\}$.

When $(k-1)/n < \rho_2$, we select $\mathcal{P} = (I_i)_i \| (I'_j)_j$ so that for $S'_j = \{s,t\}$ the partition element I'_j is given by $\{\mu : f^*_{s,t}(\alpha_\mu) = 0\}$. Each of the $\ell+1$ partition elements I_i, which correspond to singleton subsets S_i, contains at least $\lfloor (n-|U|)/(\ell+1) \rfloor$ of the remaining elements of $\langle n \rangle$. Since the various polynomials $f^*_{s,t}(x)$ are all distinct, $\mathcal{P}$ is indeed a partition vector. It is also clear that $\mathcal{P}$ satisfies (13) with equality. As for (14), for every $s = 0, 1, \ldots, \ell$,

$$\sum_{i:s\in S_i} |I_i| + \sum_{j:s\in S'_j} |I'_j| \geq \ell(k-1) + \left\lfloor \tfrac{n-|U|}{\ell+1} \right\rfloor = n - \left\lceil \tfrac{\ell n}{\ell+1} - \tfrac{\ell(k-1)}{2} \right\rceil = n - \lceil \tau_\ell(n,k) \rceil \ .$$

Given the partition vector $\mathcal{P}$, we have $f^*_{s,t}(x) = f_{s,t}(x)$, where $f_{s,t}(x)$ are given by (22). By Lemma 3.1(a), all we still need to show is that there are nonzero coefficients $a_{s,t}$, $0 \leq s < t \leq \ell$, for which (23) holds. We distinguish between three cases, according to the value of ℓ (omitting the obvious case $\ell = 1$).

Case 1: $\ell = 2$. The three polynomials $f_{0,1}(x)$, $f_{0,2}(x)$, and $f_{1,2}(x)$ satisfy condition (S3) of a simple set; therefore, by Lemma 3.2, they satisfy the difference condition.

Case 2: $\ell = 3$. Since $f_{0,1}(x), f_{0,2}(x), \ldots, f_{2,3}(x)$ satisfy condition (S3), the set of linear equations (23) has a nontrivial solution for the unknowns $a_{0,1}, a_{0,2}, \ldots, a_{2,3}$ if and only if there is a nontrivial solution for the following set of equations:

$$\begin{pmatrix} 1 & -1 & 0 & -1 & 0 & 0 \\ 1 & 0 & -1 & 0 & -1 & 0 \\ 0 & 1 & -1 & 0 & 0 & -1 \\ \psi_{0,1} & -\psi_{0,2} & 0 & -\psi_{1,2} & 0 & 0 \\ \psi_{0,1} & 0 & -\psi_{0,3} & 0 & -\psi_{1,3} & 0 \\ 0 & \psi_{0,2} & -\psi_{0,3} & 0 & 0 & -\psi_{2,3} \end{pmatrix} \begin{pmatrix} a_{0,1} \\ a_{0,2} \\ a_{0,3} \\ a_{1,2} \\ a_{1,3} \\ a_{2,3} \end{pmatrix} = \mathbf{0} \ . \tag{34}$$

However, the determinant of the matrix in (34) is zero if and only if

$$(\psi_{1,2} - \psi_{0,1})(\psi_{1,3} - \psi_{0,3})(\psi_{2,3} - \psi_{0,2}) = (\psi_{1,2} - \psi_{0,2})(\psi_{1,3} - \psi_{0,1})(\psi_{2,3} - \psi_{0,3}) \ ;$$

this is condition (33) for $\ell = 3$. Furthermore, if one of the elements $a_{0,1}, a_{0,2}, \ldots, a_{2,3}$ is zero, then either all these elements are zero, or else $\psi_{s',t'} = \psi_{s'',t''}$ for some $(s',t') \neq (s'',t'')$, where $0 \leq s' < t' \leq 3$ and $0 \leq s'' < t'' \leq 3$; yet, the latter contradicts our assumption that $f_{0,1}(x), f_{0,2}(x), \ldots, f_{2,3}(x)$ are all distinct. Therefore, in a nontrivial solution for $a_{0,1}, a_{0,2}, \ldots, a_{2,3}$, all these elements are nonzero.

Case 3: $\ell > 3$. Fix some s in the range $1 < s \leq \ell-2$, and consider another index t in the range $s < t \leq \ell-1$. Following the analysis of Case 2, there must exist nonzero $a_{0,1}, a_{0,s}, a_{0,t}, a_{1,s}, a_{1,t}, a_{s,t} \in F$ such that

$$\begin{aligned} a_{s,t} \cdot f_{s,t}(x) &= a_{0,s} \cdot f_{0,s}(x) - a_{0,t} \cdot f_{0,t}(x) \\ a_{1,s} \cdot f_{1,s}(x) &= a_{0,1} \cdot f_{0,1}(x) - a_{0,s} \cdot f_{0,s}(x) \\ a_{1,t} \cdot f_{1,t}(x) &= a_{0,1} \cdot f_{0,1}(x) - a_{0,t} \cdot f_{0,t}(x) \ . \end{aligned} \tag{35}$$

Let u be in the range $t < u \leq \ell$; there are five nonzero coefficients $a'_{0,s}, a'_{1,s}, a_{0,u}, a_{1,u}, a_{s,u}$ such that

$$\begin{aligned} a_{s,u} \cdot f_{s,u}(x) &= a'_{0,s} \cdot f_{0,s}(x) - a_{0,u} \cdot f_{0,u}(x) \\ a'_{1,s} \cdot f_{1,s}(x) &= a_{0,1} \cdot f_{0,1}(x) - a'_{0,s} \cdot f_{0,s}(x) \\ a_{1,u} \cdot f_{1,u}(x) &= a_{0,1} \cdot f_{0,1}(x) - a_{0,u} \cdot f_{0,u}(x) \ . \end{aligned} \tag{36}$$

Combining (35) and (36) results in

$$(a_{1,s} - a'_{1,s}) \cdot f_{1,s}(x) \ = \ (a'_{0,s} - a_{0,s}) \cdot f_{0,s}(x) \ ,$$

and since $f_{1,s}(x)$ and $f_{0,s}(x)$ are relatively prime, it follows that $a'_{0,s} = a_{0,s}$ and $a'_{1,s} = a_{1,s}$. Hence, the same nonzero constant $a_{0,s}$ multiplies $f_{0,s}(x)$ in (23), independently of t. ■

4 Proof of main results for RS codes

In this section (starting from sub-section 4.3), we prove Propositions 1.4–1.7. We use the tools developed in Section 3 and additional tools presented in following two sub-sections.

4.1 Properties of $\Delta_\ell^{\rm RS}(n, d\,; q)$

Proposition 4.1 below describes some simple relations satisfied by $\Delta_\ell^{\rm RS}(n, d; q)$.

Proposition 4.1 *Let (ℓ, n, d, q) be an RS-admissible quadruple. Then,*

(a) $\Delta_\ell^{\rm RS}(n{-}1, d{-}1; q) \leq \Delta_\ell^{\rm RS}(n, d; q) \leq \Delta_\ell^{\rm RS}(n{-}1, d{-}1; q) + 1 \quad$ *for* $\quad d > 1$.

(b) $\Delta_\ell^{\rm RS}(n, d; q) \leq \Delta_\ell^{\rm RS}(n{-}1, d; q) \quad$ *for* $\quad d < n$.

Proof: *Part (a):* Let $\mathcal{C}$ be an $[n, k, d]$ RS code over GF(q) where $k < n$ $(d > 1)$ and let $\mathcal{C}'$ be obtained by deleting the last coordinate from each codeword of $\mathcal{C}$. A list-ℓ decoder for $\mathcal{C}$ can be obtained by truncating the last coordinate from the received word and applying a list-ℓ decoder for $\mathcal{C}'$ to the resulting word. Hence, $\Delta_\ell(\mathcal{C}) \geq \Delta_\ell(\mathcal{C}')$, and, so, $\Delta_\ell(n, d; q) \geq \Delta_\ell(n{-}1, d{-}1; q)$. On the other hand, a list-ℓ decoder for $\mathcal{C}'$ can be obtained by appending an arbitrary nth coordinate to the received word, followed by an application of a list-ℓ decoder for $\mathcal{C}$. Therefore, $\Delta_\ell(\mathcal{C}') \geq \Delta_\ell(\mathcal{C}) - 1$ and, since $\mathcal{C}'$ can be any $[n{-}1, k, d{-}1]$ RS code, $\Delta_\ell(n{-}1, d{-}1; q) \geq \Delta_\ell(n, d; q) - 1$.

Part (b): Every $[n{-}1, k{-}1, d]$ RS code $\mathcal{C}$ over GF(q) with $n \leq q$ can be extended to an $[n, k, d]$ (generalized) RS code $\overline{\mathcal{C}}$ over GF(q) by adding one column to the parity-check matrix of $\mathcal{C}$; (see [11, Section 10.8]). Therefore, a list-ℓ decoder for $\mathcal{C}$ can be obtained by appending a zero coordinate to the received word and then applying a list-ℓ decoder for $\overline{\mathcal{C}}$. Hence, $\Delta_\ell(\mathcal{C}) \geq \Delta_\ell(\overline{\mathcal{C}})$ and, so, $\Delta_\ell(n{-}1, d; q) \geq \Delta_\ell(n, d; q)$. ■

4.2 Types of simple sets of polynomials

In some of our proofs, we will use two types of sets of polynomials that are simple over certain sets U, as follows.

Type 1: Assume that $e \mid q-1$ and let α be a primitive element in $F = \mathrm{GF}(q)$. The set

$$\left\{x^e - \alpha^{ei} \ : \ 0 \le i < (q-1)/e\right\}$$

is simple over $F \setminus \{0\}$.

Type 2: Assume that $q = p^h$ and $e = p^b < q$. If we regard $F = \mathrm{GF}(q)$ as a linear space over $\mathrm{GF}(p)$, then the p^b elements of every b-dimensional subspace F' of F are the roots of some nonzero linearized polynomial $\eta(x) = \sum_{i=0}^{b} \eta_i x^{p^i}$ over F (see [10, Ch. 4] or [11, Ch. 4]). The polynomial $\eta(x)$ defines a linear mapping $\eta : F \to F$ over $\mathrm{GF}(p)$. The range R_η of the mapping $x \mapsto \eta(x)$ over F is a subspace of F of dimension $h-b$ in which every two distinct elements have disjoint sets of p^b pre-images under η. The set

$$\left\{\eta(x) - \beta \ : \ \beta \in R_\eta\right\}$$

is thus simple over F.

4.3 The high-rate range: Proposition 1.4

Proof of Proposition 1.4: We consider here codes at rates $(k-1)/n \ge 1-(2/(\ell+1)) = \rho_\ell$. Starting with the case $k = n$, we have $\ell < 2n \le 1 + (q-1)n$ for all RS-admissible quadruples $(\ell, n, d, q) \ne (3, 2, 1, 2)$; so, in this case, $\Delta_\ell(n, 1; q) = 0$.

We assume from now on in the proof that $d = n-k+1$ is an even number (in such cases (6) holds); the case of odd d follows from Proposition 4.1(a). We show that there is an $[n, k, d]$ RS code $\mathcal{C}$ over $F = \mathrm{GF}(q)$ that contains a failing list of size $\ell+1$.

Let S_1' be the set $\{0, 1, \ldots, \ell\}$ and $S_1, S_2, \ldots, S_{\ell+1}$ be the subsets of S_1' of size ℓ. Using any of the constructions of simple sets in Section 4.2, we let $\{A_{S_i}(x)\}_{i=1}^{\ell+1}$ be a simple set over F, where $\deg A_{S_i}(x) = d/2$ for every i. We denote by U_i the set of $d/2$ roots of $A_{S_i}(x)$ in F and by U the union $\bigcup_{i=1}^{\ell+1} U_i$. Also, define U_1' to be a subset of $F \setminus U$ of size $n - (\ell+1)d/2$ and let

$$A_{S_1'}(x) = \prod_{\alpha \in U_1'} (x - \alpha) \ .$$

Define $\mathcal{P}$ to be a partition vector $(I_1, I_2, \ldots, I_{\ell+1}, I_1')$ of $\langle n \rangle$ with $|I_i| = d/2$ and $|I_1'| = n - (\ell+1)d/2$, and let $\mathcal{C}$ be defined by the code locators $\alpha_1, \alpha_2 \ldots, \alpha_n$, where $U_i = \{\alpha_\mu\}_{\mu \in I_i}$ and $U_1' = \{\alpha_\mu\}_{\mu \in I_1'}$.

By construction, $\mathcal{P}$ satisfies both (13) and (14) with equality. Finally, let the polynomials $f_{s,t}(x)$ be defined by (22). For every $s < t$, the set $\left\{ \frac{f_{0,s}(x)}{g_{0,s,t}(x)}, \frac{f_{0,t}(x)}{g_{0,s,t}(x)}, \frac{f_{s,t}(x)}{g_{0,s,t}(x)} \right\}$ contains three different polynomials from $\{A_{S_i}(x)\}_{i=1}^{\ell+1}$ and is therefore a simple set over U. Hence, the polynomials $f_{0,s}(x)$, $f_{0,t}(x)$, and $f_{s,t}(x)$ satisfy the difference condition. Corollaries 3.5 and 3.6 now imply that $\mathcal{C}$ contains a failing list of size $\ell+1$. ∎

We next show that there are infinitely many quadruples satisfying the conditions of this proposition. The quadruples (ℓ, n, d, q) where $2 \le d \le 5$ and $\ell \le \frac{2n}{d} - 1$ satisfy the conditions for every field size $q \ge n$. Another example consists of the quadruples (ℓ, n, d, q) where $q = n = 2^m$, $d = 2^p$, for $1 < p < m$, and $\ell \le 2^{m-p+1} - 1$. In this case, $d/n = 2^{p-m} \le 2/(\ell+1)$ and $\lceil (d-1)/2 \rceil = 2^{p-1}$ divides $q = 2^m$.

4.4 The mid-rate range

Propositions 4.2 and 4.3 below identify cases where the GS bound is tight for code rate around 0.3 and list sizes 3 or 4.

4.4.1 List-3 decoders for RS codes at rates ≈ 0.3

Proposition 4.2 *Let $(3, 10m+\nu+\kappa, 7m+\nu+1, q)$ be an RS-admissible quadruple, where $q = p^h$ for a prime p; the integer pair (ν, κ) belongs to the set $\{(\nu,\kappa) : -1 \le \nu \le 1,\ 1 \le \kappa \le 5-3\nu\}$; and m is a positive integer such either (a) $m \,|\, q-1$ and $q \ge 11m$, or (b) $m \,|\, q$ and $p \notin \{3, 5, 7\}$. Then,*

$$\Delta_3^{\mathrm{RS}}(10m+\nu+\kappa, 7m+\nu+1; q) = \lceil \tau_3(10m+\nu+\kappa, 7m+\nu+1) \rceil - 1 = 4m + \nu \ .$$

Proof: It suffices to prove the proposition for $(\nu, \kappa) = (-1, 1)$, in which case $\tau_3(10m, 7m) = 4m$; the results for the remaining values of (ν, κ) follow from Proposition 4.1: for $\kappa = 1$, the result follows from Part (a) of Proposition 4.1, and then, for every fixed ν, it follows from Part (b). We construct an $[n{=}10m, k{=}3m{+}1, d{=}7m]$ RS code $\mathcal{C}$ over F that contains a failing list of size $\ell{+}1 = 4$; note that here $r = 2$ and that $\gamma = \gamma' = m$ satisfy (15).

Part (a): We assume that the field size q is such that $q{-}1 = m \cdot b$ where $b \ge 11$, and we let α be an element of order b in the multiplicative group of $F = \mathrm{GF}(q)$. We define six polynomials $A_{\{s,t\}}(x)$, $0 \le s < t \le 3$, and four polynomials $A_{\{s,t,u\}}(x)$, $0 \le s < t < u \le 3$ as follows:

$$\begin{array}{lll}
A_{\{0,1\}}(x) = x^m - \alpha^2 \ , & A_{\{0,2\}}(x) = x^m - \alpha \ , & A_{\{0,3\}}(x) = x^m - \alpha^7 \ , \\
A_{\{1,2\}}(x) = x^m - \alpha^3 \ , & A_{\{1,3\}}(x) = x^m - \alpha^9 \ , & A_{\{2,3\}}(x) = x^m - \alpha^8 \ , \\
A_{\{0,1,2\}}(x) = x^m - \alpha^{11} \ , & A_{\{0,1,3\}}(x) = x^m - \alpha^5 \ , & A_{\{0,2,3\}}(x) = x^m - \alpha^6 \ , \\
A_{\{1,2,3\}}(x) = x^m - \alpha^4 \ . & &
\end{array}$$

Note that any two of these ten polynomial are relatively prime, and each has m simple roots in F.

For every $S_i = \{s,t\}$ (respectively, $S'_j = \{s,t,u\}$), let U_i (respectively, U'_j) denote the set of roots of $A_{S_i}(x)$ (respectively, $A_{S'_j}(x)$) in F. Define accordingly a partition vector $\mathcal{P} = (I_i)_{i=1}^6 \| (I'_j)_{i=1}^4$ such that $U_i = \{\alpha_\mu\}_{\mu \in I_i}$ and $U'_j = \{\alpha_\mu\}_{\mu \in I'_j}$. Denote by U the union of $\bigcup_{i=1}^6 U_i$ and $\bigcup_{j=1}^4 U'_j$, and define $\mathcal{C}$ to be the $[10m, 3m+1, 7m]$ RS code over F whose set of code locators is U.

Next, we define the polynomials $f_{s,t}(x)$ by (22) and obtain

$$\begin{array}{ll} f_{0,1}(x) = (x^m-\alpha^2)(x^m-\alpha^5)(x^m-\alpha^{11}) \ , & f_{0,2}(x) = (x^m-\alpha)(x^m-\alpha^6)(x^m-\alpha^{11}) \\ f_{0,3}(x) = (x^m-\alpha^5)(x^m-\alpha^6)(x^m-\alpha^7) \ , & f_{1,2}(x) = (x^m-\alpha^3)(x^m-\alpha^4)(x^m-\alpha^{11}) \ , \\ f_{1,3}(x) = (x^m-\alpha^4)(x^m-\alpha^5)(x^m-\alpha^9) \ , & f_{2,3}(x) = (x^m-\alpha^4)(x^m-\alpha^6)(x^m-\alpha^8) \ . \end{array}$$

Similarly, we define the polynomials $g_{0,s,t}(x)$ by (28), and the sets

$$\left\{ \frac{f_{0,s}(x)}{g_{0,s,t}(x)}, \frac{f_{0,t}(x)}{g_{0,s,t}(x)}, \frac{f_{s,t}(x)}{g_{0,s,t}(x)} \right\} \ , \quad 0 < s < t \leq 3 \ , \tag{37}$$

are given by

$$\begin{array}{rcl} \left\{ \frac{f_{0,1}(x)}{g_{0,1,2}(x)}, \frac{f_{0,2}(x)}{g_{0,1,2}(x)}, \frac{f_{1,2}(x)}{g_{0,1,2}(x)} \right\} & = & \left\{ (x^m-\alpha^2)(x^m-\alpha^5), (x^m-\alpha)(x^m-\alpha^6), (x^m-\alpha^3)(x^m-\alpha^4) \right\} \\ \left\{ \frac{f_{0,1}(x)}{g_{0,1,3}(x)}, \frac{f_{0,3}(x)}{g_{0,1,3}(x)}, \frac{f_{1,3}(x)}{g_{0,1,3}(x)} \right\} & = & \left\{ (x^m-\alpha^2)(x^m-\alpha^{11}), (x^m-\alpha^6)(x^m-\alpha^7), (x^m-\alpha^4)(x^m-\alpha^9) \right\} \\ \left\{ \frac{f_{0,2}(x)}{g_{0,2,3}(x)}, \frac{f_{0,3}(x)}{g_{0,2,3}(x)}, \frac{f_{2,3}(x)}{g_{0,2,3}(x)} \right\} & = & \left\{ (x^m-\alpha)(x^m-\alpha^{11}), (x^m-\alpha^5)(x^m-\alpha^7), (x^m-\alpha^4)(x^m-\alpha^8) \right\} \ . \end{array}$$

Each of these three sets of polynomials is simple over U, since the three polynomials in each set differ only in their coefficient of x^m. Applying Corollary 3.6 to the partition vector $(I_i)_{i=1}^6 \| (I'_j)_{i=1}^4$, it follows that $\mathcal{C}$ contains a failing list of size 4.

Part (b): We assume that the field size q is p^h for a prime $p \geq 11$ and that $m = p^b$ for $b < h$; the case $p = 2$ is omitted, as it is covered by Proposition 4.3 (to be proved right below). Let $\eta(x)$ be a linearized polynomial of degree m over $F = \mathrm{GF}(q)$ that has m simple roots in $\mathrm{GF}(q)$. Let β be a nonzero element in the range of the mapping $\eta : F \to F$; by linearity, the (distinct) elements $0, \beta, 2\beta, \ldots, 10\beta$ are also in that range. As in part (a), we define six polynomials $A_{\{s,t\}}(x)$, $0 \leq s < t \leq 3$, and four polynomials $A_{\{s,t,u\}}(x)$, $0 \leq s < t < u \leq 3$, each having m simple roots in F and every two are relatively prime:

$$\begin{array}{lll} A_{\{0,1\}}(x) = \eta(x) - 2\beta \ , & A_{\{0,2\}}(x) = \eta(x) - \beta \ , & A_{\{0,3\}}(x) = \eta(x) - 7\beta \ , \\ A_{\{1,2\}}(x) = \eta(x) - 3\beta \ , & A_{\{1,3\}}(x) = \eta(x) - 9\beta \ , & A_{\{2,3\}}(x) = \eta(x) - 8\beta \ , \\ A_{\{0,1,2\}}(x) = \eta(x) - 11\beta \ , & A_{\{0,1,3\}}(x) = \eta(x) - 5\beta \ , & A_{\{0,2,3\}}(x) = \eta(x) - 6\beta \ , \\ A_{\{1,2,3\}}(x) = \eta(x) - 4\beta \ . & & \end{array}$$

The proof now continues as in part (a); in particular, the sets (37) that result in this case are simple, as the three polynomials in each set differ only in their constant term. ∎

The failing list in Figure 1 is obtained from the construction in the proof of part (b) by taking $F = \mathrm{GF}(11)$, $m = 1$, $\eta(x) = x$, and $\beta = 1$.

4.4.2 List-4 decoders for RS codes at rates ≈ 0.3

Proposition 4.3 *Let* $(4, 10m+\nu+\kappa, 7m+\nu+1, q)$ *be an RS-admissible quadruple, where* (ν, κ) *is an integer pair in the set* $\{(2,1)\} \cup \{(\nu,\kappa) : -1 \le \nu \le 1,\ 1 \le \kappa \le 9-6\nu\}$ *and* q *and* m *are powers of 2. Then,*

$$\Delta_4^{\rm RS}(10m+\nu+\kappa, 7m+\nu+1; q) = \lceil \tau_4(10m+\nu+\kappa, 7m+\nu+1) \rceil - 1 = 4m + \nu \ .$$

Proof: We prove the proposition for $(\nu,\kappa) = (-1,1)$, in which case $\tau_4(10m, 7m) = 4m$; the results for the other values for (ν,κ) extend directly from Proposition 4.1. We construct an $[n{=}10m, k{=}3m{+}1, d{=}7m]$ RS code $\mathcal{C}$ over $F = \mathrm{GF}(2^h)$ that contains a failing list of size $\ell{+}1 = 5$; here $r = 3$, and the values $\gamma = m$ and $\gamma' = 0$ satisfy (15).

Let $\eta(x)$ be a linearized polynomial of degree $m = 2^b \le 2^{h-4}$ over F that has m simple roots in F. The range, R_η, of the mapping $x \mapsto \eta(x)$ over F is a linear space of dimension $h{-}b \ge 4$ over $\mathrm{GF}(2)$; therefore, one can find four elements $\beta_0, \beta_1, \beta_2, \beta_3 \in R_\eta$ that are linearly independent over $\mathrm{GF}(2)$. We represent each of the 16 elements $\sum_{i=0}^{3} \epsilon_i \beta_i$, $\epsilon_i \in \mathrm{GF}(2)$, as a 4-tuple $(\epsilon_0\, \epsilon_1\, \epsilon_2\, \epsilon_3)$.

Define the ten polynomials $A_{\{s,t,u\}}(x)$, $0 \le s < t < u \le \ell$, as follows:

$$\begin{array}{ll}
A_{\{0,1,2\}}(x) = \eta(x) - (1\,0\,0\,0)\ , & A_{\{0,1,3\}}(x) = \eta(x) - (0\,1\,0\,0)\ , \\
A_{\{0,1,4\}}(x) = \eta(x) - (0\,0\,1\,0)\ , & A_{\{0,2,3\}}(x) = \eta(x) - (0\,0\,0\,1)\ , \\
A_{\{0,2,4\}}(x) = \eta(x) - (0\,1\,1\,1)\ , & A_{\{0,3,4\}}(x) = \eta(x) - (1\,0\,1\,1)\ , \\
A_{\{1,2,3\}}(x) = \eta(x) - (1\,0\,0\,1)\ , & A_{\{1,2,4\}}(x) = \eta(x) - (1\,1\,1\,1)\ , \\
A_{\{1,3,4\}}(x) = \eta(x) - (0\,0\,1\,1)\ , & A_{\{2,3,4\}}(x) = \eta(x) - (0\,1\,1\,0)\ .
\end{array}$$

For every subset S_i of $\{0,1,2,3,4\}$ of size 3, let U_i denote the set of the $\gamma = m = 2^b$ roots of $A_{S_i}(x)$ in F, and denote by U the union $\bigcup_{i=1}^{10} I_i$. Define the partition vector $\mathcal{P} = (I_i)_{i=1}^{10}$ so that $U_i = \{\alpha_\mu\}_{\mu \in I_i}$. The code $\mathcal{C}$ is now defined as a $[10m, 3m{+}1, 7m]$ RS code over F whose set of code locators is U.

Let the polynomials $f_{s,t}(x)$ and $g_{s,t,u}(x)$ be defined by (22) and (28) respectively. It can be verified that each of the six sets

$$\left\{ \tfrac{f_{0,s}(x)}{g_{0,s,t}(x)}, \tfrac{f_{0,t}(x)}{g_{0,s,t}(x)}, \tfrac{f_{s,t}(x)}{g_{0,s,t}(x)} \right\}\ , \quad 0 < s < t \le 4\ , \tag{38}$$

is simple over F. In particular, the polynomials—each of degree $2m$—in every set differ only in their constant terms. For example,

$$\begin{array}{rcl}
\frac{f_{0,1}(x)}{g_{0,1,2}(x)} & = & A_{\{0,1,3\}}(x) \cdot A_{\{0,1,4\}}(x) \ = \ x^{2m} + (0\,1\,1\,0)\cdot x^m + (0\,1\,0\,0)\cdot(0\,0\,1\,0) \\
\frac{f_{0,2}(x)}{g_{0,1,2}(x)} & = & A_{\{0,2,3\}}(x) \cdot A_{\{0,2,4\}}(x) \ = \ x^{2m} + (0\,1\,1\,0)\cdot x^m + (0\,0\,0\,1)\cdot(0\,1\,1\,1) \\
\frac{f_{1,2}(x)}{g_{0,1,2}(x)} & = & A_{\{1,2,3\}}(x) \cdot A_{\{1,2,4\}}(x) \ = \ x^{2m} + (0\,1\,1\,0)\cdot x^m + (1\,0\,0\,1)\cdot(1\,1\,1\,1)
\end{array}$$

(multiplications are in F). Applying Corollary 3.6 to the proper partition vector $(I_i)_{i=1}^{10}$, it follows that $\mathcal{C}$ contains a failing list of size 5. ∎

The failing list in Figure 2 is obtained from the construction in the last proof by taking $F = \mathrm{GF}(2^4)$, $m = 1$, $\eta(x) = x$, and $\beta_i = \alpha^i$, where α is a root of $x^4 + x + 1$.

We turn next to proving Proposition 1.6, namely, to showing that the GS bound is not tight for RS-admissible quadruples $(\ell, n, d, q) = (4, 10, 7, q)$ where q is odd. The next lemma characterizes the structure of a failing list of size 5 in a any $(10, M, 7)$ code over any field.

Lemma 4.4 *Let $q = p^h$ where p is a prime. Every failing list of size 5 in a $(10, M, 7)$ code over $\mathrm{GF}(q)$ is a $(4, 3)$-configuration with respect to a proper partition vector $\mathcal{P} = (I_i)_{i=1}^{10}$, where $|I_i| = 1$ for all i. Every failing list of size 5 thus corresponds to a $\mathrm{BIBD}(5, 3, 3)$.*

Proof: The parameters $\ell = 4$, $r = 3$, $n = \binom{\ell+1}{r} = 10$, and $d = 7$ satisfy (6). Therefore, by Proposition 2.3, every failing list of size 5 forms an $(4, 3)$-configuration with respect to a partition vector $\mathcal{P} = (I_i)_{i=1}^{10} \| (I'_j)_{j=1}^{5}$ for which (13)–(14) hold with equality. Furthermore, since $\rho_r(\ell) = \rho_3(4) = 3/10 = 1 - d/n$, the partition vector $\mathcal{P}$ is proper: exactly $r = 3$ codewords agree on every position. We next show that each set I_i has size 1.

Assume to the contrary; since $\sum_{i=1}^{10} |I_i| = 10$, at least one of the partition elements, say I_1, is empty. Without loss of generality, let $S_1 = \{0, 1, 2\}$ and let the sets I_2 through I_7 correspond, respectively, to $S_2 = \{0, 1, 3\}$, $S_3 = \{0, 1, 4\}$, $S_4 = \{0, 2, 3\}$, $S_5 = \{0, 2, 4\}$, $S_6 = \{1, 2, 3\}$, and $S_7 = \{1, 2, 4\}$. We have,

$$\sum_{i=2}^{7} |I_i| \;=\; \sum_{0 \le s < t \le 2} \Big(\sum_{i\,:\,\{s,t\} \subseteq S_i} |I_i| \Big) \;=\; 9 \;,$$

where the second equality follows from the equality in (13). Hence, either $|I_2| + |I_4| + |I_6| \ge 5$ or $|I_3| + |I_5| + |I_7| \ge 5$. Assuming the former inequality (the arguments for the latter are similar) we obtain—again from (13),

$$\sum_{s \in \{0,1,2\}} \Big(\sum_{i\,:\,\{s,3\} \subseteq S_i} |I_i| \Big) \;\ge\; 2(|I_2| + |I_4| + |I_6|) \;\ge\; 10 \;.$$

Therefore, there must be $s \in \{0, 1, 2\}$ such that

$$\sum_{i\,:\,\{s,3\} \subseteq S_i} |I_i| \ge 4 \;,$$

thereby contradicting (13). ∎

Proof of Proposition 1.6: Assume to the contrary that there is a $[10, 4, 7]$ RS code $\mathcal{C}$ over GF(q), q odd, that contains a failing list $\mathcal{L}$ of size 5. By Lemma 4.4, this failing list is a $(4, 3)$-configuration with respect to a proper partition vector $\mathcal{P} = (I_i)_{i=1}^{10}$, where $|I_i| = 1$ for all i. Let $\alpha_1, \alpha_2, \ldots, \alpha_{10}$ be the code locators of $\mathcal{C}$. The polynomials $A_{S_i}(x)$, which are defined by (21), can be written, without loss of generality, as

$$\begin{array}{lll} A_{\{0,1,2\}}(x) = x - \alpha_1 \ , & A_{\{0,1,3\}}(x) = x - \alpha_2 \ , & A_{\{0,1,4\}}(x) = x - \alpha_3 \ , \\ A_{\{0,2,3\}}(x) = x - \alpha_4 \ , & A_{\{0,2,4\}}(x) = x - \alpha_5 \ , & A_{\{0,3,4\}}(x) = x - \alpha_6 \ , \\ A_{\{1,2,3\}}(x) = x - \alpha_7 \ , & A_{\{1,2,4\}}(x) = x - \alpha_8 \ , & A_{\{1,3,4\}}(x) = x - \alpha_9 \ , \\ A_{\{2,3,4\}}(x) = x - \alpha_{10} \ . & & \end{array}$$

The polynomials $f_{s,t}(x)$, $0 \le s < t \le 4$, are defined accordingly by (22).

By Lemma 3.1(b), the ten polynomials $f_{s,t}(x)$ must satisfy (23). In particular, for every $0 \le s < t \le 4$, the three polynomials $f_{0,s}(x)/g_{0,s,t}$, $f_{0,t}(x)/g_{0,s,t}(x)$, and $f_{s,t}(x)/g_{0,s,t}(x)$, which take the form $(x - \alpha_{i_1})(x - \alpha_{i_2})$, must satisfy the difference condition. By Lemma 3.2, this happens if and only if the code locators satisfy the following six equations:

$$\begin{aligned} (\alpha_1\alpha_3 - \alpha_7\alpha_9)(\alpha_1 + \alpha_3 - \alpha_4 - \alpha_6) &= (\alpha_1\alpha_3 - \alpha_4\alpha_6)(\alpha_1 + \alpha_3 - \alpha_7 - \alpha_9) && (39) \\ (\alpha_1\alpha_2 - \alpha_8\alpha_9)(\alpha_1 + \alpha_2 - \alpha_5 - \alpha_6) &= (\alpha_1\alpha_2 - \alpha_5\alpha_6)(\alpha_1 + \alpha_2 - \alpha_8 - \alpha_9) && (40) \\ (\alpha_2\alpha_3 - \alpha_7\alpha_8)(\alpha_2 + \alpha_3 - \alpha_4 - \alpha_5) &= (\alpha_2\alpha_3 - \alpha_4\alpha_5)(\alpha_2 + \alpha_3 - \alpha_7 - \alpha_8) && (41) \\ (\alpha_2\alpha_6 - \alpha_7\alpha_{10})(\alpha_2 + \alpha_6 - \alpha_1 - \alpha_5) &= (\alpha_2\alpha_6 - \alpha_1\alpha_5)(\alpha_2 + \alpha_6 - \alpha_7 - \alpha_{10}) && (42) \\ (\alpha_3\alpha_6 - \alpha_8\alpha_{10})(\alpha_3 + \alpha_6 - \alpha_1 - \alpha_4) &= (\alpha_3\alpha_6 - \alpha_1\alpha_4)(\alpha_3 + \alpha_6 - \alpha_8 - \alpha_{10}) && (43) \\ (\alpha_2\alpha_4 - \alpha_9\alpha_{10})(\alpha_2 + \alpha_4 - \alpha_3 - \alpha_5) &= (\alpha_2\alpha_4 - \alpha_3\alpha_5)(\alpha_2 + \alpha_4 - \alpha_9 - \alpha_{10}) \end{aligned}$$

Defining

$$\epsilon_7 = (\alpha_3 - \alpha_4)/(\alpha_7 - \alpha_4) \ , \quad \epsilon_8 = (\alpha_2 - \alpha_5)/(\alpha_8 - \alpha_5) \ , \quad \text{and} \quad \epsilon_9 = (\alpha_1 - \alpha_6)/(\alpha_9 - \alpha_6) \ , \tag{44}$$

equations (39)–(41) can be re-written as

$$\begin{pmatrix} \alpha_2 - \alpha_4 & \alpha_3 - \alpha_5 & 0 \\ \alpha_1 - \alpha_4 & 0 & \alpha_3 - \alpha_6 \\ 0 & \alpha_1 - \alpha_5 & \alpha_2 - \alpha_6 \end{pmatrix} \begin{pmatrix} \epsilon_7 \\ \epsilon_8 \\ \epsilon_9 \end{pmatrix} = \begin{pmatrix} \alpha_2 - \alpha_4 + \alpha_3 - \alpha_5 \\ \alpha_1 - \alpha_4 + \alpha_3 - \alpha_6 \\ \alpha_1 - \alpha_5 + \alpha_2 - \alpha_6 \end{pmatrix} . \tag{45}$$

Now, if the matrix in (45) were nonsingular, then the unique solution of (45) would be $\epsilon_7 = \epsilon_8 = \epsilon_9 = 1$, thereby requiring from (44) that certain code locators be identical, namely, $\alpha_7 = \alpha_3$, $\alpha_8 = \alpha_2$, and $\alpha_9 = \alpha_1$. Since this is impossible, the matrix in (45) must be singular, and this occurs if and only if

$$-(\alpha_1 - \alpha_5)(\alpha_2 - \alpha_4)(\alpha_3 - \alpha_6) = (\alpha_1 - \alpha_4)(\alpha_2 - \alpha_6)(\alpha_3 - \alpha_5) \ . \tag{46}$$

Re-iterating the analysis, with equations (39)–(41) now replaced by (41)–(43), we obtain

$$-(\alpha_6 - \alpha_5)(\alpha_2 - \alpha_4)(\alpha_3 - \alpha_1) = (\alpha_6 - \alpha_4)(\alpha_2 - \alpha_1)(\alpha_3 - \alpha_5) \ . \tag{47}$$

Subtracting (46) from (47) and simplifying the result yields

$$2(\alpha_1 - \alpha_6)(\alpha_2 - \alpha_4)(\alpha_3 - \alpha_5) \;=\; 0 \;.$$

However, this is a contradiction whenever q is odd. We thus conclude that $\mathcal{C}$ cannot contain the failing list $\mathcal{L}$. ∎

4.4.3 List-10 decoders for $[11, 3, 9]$ RS codes

Proof of Proposition 1.7: Assume to the contrary that there is an $[11, 3, 9]$ RS code over GF(2^h) that contains a failing list $\mathcal{L}$ of size 11. By Proposition 2.3 and by property B1 in Proposition 2.8, the failing list corresponds to a symmetric BIBD$(11, 5, 2)$ (which has 11 blocks), namely it forms a $(10, 5)$-configuration with respect to a proper partition vector $\mathcal{P} = (I_i)_i$ such that eleven partition elements I_i have size 1 whereas all the other partition elements in $\mathcal{P}$ are empty.

As this BIBD is essentially unique (see [2, page 73]), we can assume, without loss of generality, that the nonempty partition elements in $\mathcal{P}$ are $I_i = \{i\}$, $1 \le i \le 11$, where $S_1, S_2, \ldots, S_{11}$ are given by

$$\begin{array}{llll} S_1 = \{1,3,4,5,9\}\,, & S_2 = \{2,4,5,6,10\}\,, & S_3 = \{0,3,5,6,7\}\,, & S_4 = \{1,4,6,7,8\}\,, \\ S_5 = \{2,5,7,8,9\}\,, & S_6 = \{3,6,8,9,10\}\,, & S_7 = \{0,4,7,9,10\}\,, & S_8 = \{0,1,5,8,10\}\,, \\ S_9 = \{0,1,2,6,9\}\,, & S_{10} = \{1,2,3,7,10\}\,, & S_{11} = \{0,2,3,4,8\}\,. & \end{array}$$

Define $A_{S_i}(x)$ and $f_{s,t}(x)$ accordingly by (21) and (22). In particular, we obtain

$$\begin{array}{lll} f_{0,2}(x) = (x-\alpha_9)(x-\alpha_{11})\,, & f_{0,7}(x) = (x-\alpha_3)(x-\alpha_7)\,, & f_{0,5}(x) = (x-\alpha_3)(x-\alpha_8)\,, \\ f_{0,10}(x) = (x-\alpha_7)(x-\alpha_8)\,, & f_{2,7}(x) = (x-\alpha_5)(x-\alpha_{10})\,, & f_{2,5}(x) = (x-\alpha_2)(x-\alpha_5)\,, \\ f_{2,10}(x) = (x-\alpha_2)(x-\alpha_{10})\,. & & \end{array}$$

By Lemma 3.1(b), each of the following sets of three polynomials must satisfy the difference condition: $\{f_{0,2}(x), f_{0,7}(x), f_{2,7}(x)\}$, $\{f_{0,2}(x), f_{0,5}(x), f_{2,5}(x)\}$, and $\{f_{0,2}(x), f_{0,10}(x), f_{2,10}(x)\}$. By Lemma 3.2 we then obtain the following equations on the code locators:

$$\begin{aligned} (\alpha_9 + \alpha_{11} - \alpha_3 - \alpha_7)(\alpha_9\alpha_{11} - \alpha_5\alpha_{10}) &= (\alpha_9 + \alpha_{11} - \alpha_5 - \alpha_{10})(\alpha_9\alpha_{11} - \alpha_3\alpha_7) && (48) \\ (\alpha_9 + \alpha_{11} - \alpha_3 - \alpha_8)(\alpha_9\alpha_{11} - \alpha_2\alpha_5) &= (\alpha_9 + \alpha_{11} - \alpha_2 - \alpha_5)(\alpha_9\alpha_{11} - \alpha_3\alpha_8) && (49) \\ (\alpha_9 + \alpha_{11} - \alpha_7 - \alpha_8)(\alpha_9\alpha_{11} - \alpha_2\alpha_{10}) &= (\alpha_9 + \alpha_{11} - \alpha_2 - \alpha_{10})(\alpha_9\alpha_{11} - \alpha_7\alpha_8)\,. && (50) \end{aligned}$$

Defining

$$\epsilon_3 = \frac{(\alpha_{11}-\alpha_3)(\alpha_9-\alpha_3)}{\alpha_5-\alpha_3}\,, \quad \epsilon_7 = \frac{(\alpha_{11}-\alpha_7)(\alpha_9-\alpha_7)}{\alpha_{10}-\alpha_7}\,, \quad \text{and} \quad \epsilon_8 = \frac{(\alpha_{11}-\alpha_8)(\alpha_9-\alpha_8)}{\alpha_2-\alpha_8}\,,$$

we can re-write (48)–(50) as

$$\begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} \epsilon_3 \\ \epsilon_7 \\ \epsilon_8 \end{pmatrix} = \begin{pmatrix} \alpha_{11}-\alpha_3+\alpha_9-\alpha_7 \\ \alpha_{11}-\alpha_3+\alpha_9-\alpha_8 \\ \alpha_{11}-\alpha_8+\alpha_9-\alpha_7 \end{pmatrix} .$$

Summing up these equations and recalling that the field size is even, the left-hand side is identically zero while the right-hand side equals the nonzero value $\alpha_9 + \alpha_{11}$; hence a contradiction. ∎

4.5 The low-rate range: Proposition 1.5

Proof of Proposition 1.5: The proof is based on Lemma 3.7. One can verify that a sufficient condition for (33) to hold is that $\{\psi_{s,t}\}_{s,t}$ take either the form $\psi_{s,t} = \psi_s \psi_t$ or the form $\psi_{s,t} = \psi_s + \psi_t$, for some $\ell+1$ values $\psi_0, \psi_1, \ldots, \psi_\ell$. The values ψ_s must form a weak Sidon set (in the respective group) so as to have distinct values of $\psi_{s,t}$. We now consider the two types of polynomials presented in Section 4.2, taking e to be $k-1$.

Using polynomials of Type 1 as the $\binom{\ell+1}{2}$ polynomials $\{f^*_{s,t}(x)\}_{0\le s<t\le \ell}$ in Lemma 3.7, we require that $(k-1)|(q-1)$ and select the respective constant terms $\psi_{0,1}, \psi_{0,2}, \ldots, \psi_{\ell-1,\ell}$ so that they satisfy $\psi_{s,t} = \psi_s \psi_t$. The set $\{\psi_0, \psi_1, \ldots, \psi_\ell\}$ should be a weak Sidon set of size $\ell+1$ in the multiplicative group of GF(q). If α is a primitive element in GF(q) and $\psi_s = \alpha^{\xi_s}$, then an equivalent requirement is that $\{\xi_0, \xi_1, \ldots, \xi_\ell\}$ be a weak Sidon set contained in the additive group of $\mathbb{Z}_{(q-1)/(k-1)}$.

When using polynomials of Type 2 over GF(p^h) as $\{f^*_{s,t}(x)\}_{0\le s<t\le \ell}$, we require that $k-1 = p^b$, where $b < h$, and we select the constant terms so that they satisfy $\psi_{s,t} = \psi_s + \psi_t$. The set $\{\psi_0, \psi_1, \ldots, \psi_\ell\}$ should be a weak Sidon set of size $\ell+1$ in the range, R_η, of a linearized polynomial $\eta(x)$ of degree p^b over F with p^b simple roots in GF(p^h). This range is an $(h-b)$-dimensional linear space over GF(p) and is therefore isomorphic to $\mathbb{Z}_p^{h-b}$. ∎

It is known that the additive group of $\mathbb{Z}_{(q-1)/(k-1)}$ contains a weak Sidon set of size $\ell+1$ whenever

$$\ell^2 \cdot (1 + o(1)) < (q-1)/(k-1) , \tag{51}$$

where $o(1)$ stands for an expression that goes to zero as $\ell \to \infty$ [6, Theorem 1]. In particular, for quadruples (ℓ, n, d, q) where $q = p^{2m}$, $n = q-1$, and $k = n - d + 1 = p^m$, we get that $(k-1)|(q-1)$. The size of $\mathbb{Z}_{(q-1)/(k-1)}$ is p^m+1. By [6, Theorem 1], $\mathbb{Z}_{(q-1)/(k-1)}$ contains some weak Sidon set of size $\ell+1$ where ℓ satisfies (51). It follows that $\ell^2 < n/(k-1)$, and thus $d/n \ge 1 - 2/(\ell(\ell+1))$, as required. We conclude that there are infinitely many quadruples that satisfy the requirements of Proposition 1.5 (part (a)).

For the group $\mathbb{Z}_p^{h-b}$ in part (b) of Proposition 1.5, the known bounds imply a weak Sidon set of size ℓ whenever

$$\ell^{2+o(1)} < q/(n-d) = p^{h-b} \tag{52}$$

(see [1, Section 5]). If $n = q$, such a list size ℓ also satisfies the requirement $d/n \geq 1 - 2/(\ell(\ell+1))$. We can therefore find infinitely many quadruples $(\ell, n = p^h, d = p^h - p^b, q = p^h)$ satisfying the conditions of the proposition (part (b)).

Appendix

Proof of Theorem 1.1: As shown in [7], the Guruswami-Sudan algorithm is a list-ℓ decoder with a decoding radius τ, if there is a positive integer m such that the following two conditions hold:

$$\begin{aligned} r(n-\tau) &\geq m + \ell(k-1) && (53) \\ \binom{r+1}{2} n &< (\ell+1)m + \binom{\ell+1}{2}(k-1) \ . && (54) \end{aligned}$$

(In terms of [7], $m+\ell(k-1)$ is the weighted degree of the bivariate polynomial $Q(x,y)$ which is computed by the algorithm.)

It can be easily verified that every integer τ that satisfies (53)–(54) for some positive integer m must be smaller than $\tau_\ell(n,d)$; therefore, $\tau \leq \lceil \tau_\ell(n,d) \rceil - 1$. Next we show the converse result: we prove that $\tau = \lceil \tau_\ell(n,d) \rceil - 1$ satisfies (53)–(54) for some positive integer m. Define

$$m' = \tfrac{1}{\ell+1} \left(\binom{r+1}{2} n - \binom{\ell+1}{2}(k-1) \right) \ .$$

Since $(k-1)/n < \rho_{r+1}$, the value of m' is positive. We can now incorporate m' into the expression for $\tau_\ell(n,d)$ in (5) to obtain

$$\tau_\ell(n,d) = \tfrac{1}{(\ell+1)r} \left(\binom{\ell+1}{2}(n-(k-1)) - \binom{\ell+1-r}{2} n \right) = \tfrac{1}{r} \left(rn - m' - \ell(k-1) \right) \ . \qquad (55)$$

If $\tau_\ell(n,d)$ is an integer, then m' must be an integer too; in this case, $m = m' + 1$ and $\tau = \tau_\ell(n,d) - 1$ satisfy (53)–(54).

On the other hand, if $\tau_\ell(n,d)$ is not an integer, then

$$r\tau = r(\lceil \tau_\ell(n,d) \rceil - 1) < rn - m' - \ell(k-1) \ ,$$

and, therefore,

$$r\tau \leq rn - \lceil m' \rceil - \ell(k-1) \ .$$

Hence, $m = \lceil m' \rceil$ and $\tau = \lceil \tau_\ell(n,d) \rceil - 1$ satisfy (53). Furthermore, this value of m is positive and satisfies (54) as well.

Fix the triple (ℓ, n, d), and consider the function

$$t_{\ell,n,d}(r) = \tfrac{1}{(\ell+1)r} \left(\binom{\ell+1}{2} d - \binom{\ell+1-r}{2} n \right) \ .$$

It can be easily verified that $t_{\ell,n,d}(r+1) \geq t_{\ell,n,d}(r)$ only for $1 - d/n \geq (r(r+1))/(\ell(\ell+1)) = \rho_{r+1}$. Hence, the value of r which maximizes the decoding radius of the Guruswami-Sudan algorithm is the one for which $1 - d/n = (k-1)/n \in [\rho_r, \rho_{r+1})$, as claimed in Theorem 1.1. ■

References

[1] L. Babai, V. T. Sós , *Sidon sets in groups and induced subgraphs of Cayley graphs, Europ. J. Combinatorics,* 6 (1985), 101–114.

[2] Th. Beth, D. Jungnickel, H. Lenz, *Design Theory,* Cambridge University Press, Cambridge, 1986.

[3] I.F. Blake, R.C. Mullin, *The Mathematical Theory of Coding,* Academic Press, New York, 1975.

[4] A.E. Brouwer, J.B. Shearer, N.J.A. Sloane, W.D. Smith, *A new table of constant weight codes, IEEE Trans. Inform. Theory,* 36 (1990), 1334–1380.

[5] O. Goldreich, R. Rubinfeld, M. Sudan, *Learning polynomials with queries: the highly noisy case, SIAM J. Disc. Math.,* 13 (2000), 535–570.

[6] R.L. Graham, N.J.A. Sloane, *On additive bases and harmonious graphs, SIAM J. Alg. Disc. Math.,* 1 (1980), 382–404.

[7] V. Guruswami, M. Sudan, *Improved decoding of Reed-Solomon and algebraic-geometric codes, IEEE Trans. Inform. Theory,* 45 (1999), 1757–1767.

[8] M. Hall, *Combinatorial Theory,* A Wiley-Interscience Publication, New York, 1986.

[9] J. Justesen, T. Høholdt, *Bounds on list decoding of MDS codes, IEEE Trans. Inform. Theory,* 47 (2001), 1604–1609.

[10] R. Lidl, H. Niederreiter, *Finite Fields,* Addison-Wesley, Reading, Massachusetts, 1983.

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

[12] R. M. Roth, G. Seroussi, *Location-correcting codes, IEEE Trans. Inform. Theory,* 42 (1996), 554–565.

[13] M. Sudan, *Decoding of Reed-Solomon codes beyond the error-correction bound, J. Compl.,* 13 (1997), 180–193.

[14] I. Tal, R.M. Roth, *On list decoding of alternant codes in the Hamming and Lee Metrics, Proc. IEEE Int'l Symp. Inform. Theory (ISIT'2003),* Yokohama, Japan (June 2003).