Long Cyclic Codes over GF(4) and GF(8) Better Than BCH Codes in the High-Rate Region

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

***Abstract*—An explicit construction of an infinite family of cyclic codes is presented which, over $\mathrm{GF}(4)$ (resp., $\mathrm{GF}(8)$), have approximately $8/9$ (resp., $48/49$) the redundancy of BCH codes of the same minimum distance and length. As such, the new codes are the best codes currently known in a regime where the minimum distance is fixed and the code length goes to infinity.**

***Index Terms*—BCH code, code concatenation, cyclic code, decoding.**

I. Introduction

Let $A(q,n,d)$ denote the maximum size of a q-ary code of length n and minimum Hamming distance d. Following [8], we define the *redundancy coefficient* for any $d \in \mathbb{Z}^+$ by

$$\mathsf{c}(q,d) = \liminf_{n\to\infty} \frac{n - \log_q A(q,n,d)}{\log_q n} \ . \tag{1}$$

By the sphere-packing bound we have the lower bound

$$\mathsf{c}(q,d) \geq \left\lfloor \frac{d-1}{2} \right\rfloor . \tag{2}$$

On the other hand, when q is a power of a prime, primitive BCH codes[1] imply the upper bound

$$\mathsf{c}(q,d) \leq \mathsf{c}_{\mathrm{BCH}}(q,d) = \left\lceil \frac{q-1}{q}(d-2) \right\rceil , \tag{3}$$

where $\mathsf{c}_{\mathrm{BCH}}(q,d)$ is defined as in (1) except that $A(q,n,d)$ therein is replaced by the size of a primitive BCH code[2] of length n and designed minimum distance d over $\mathrm{GF}(q)$. The bound (3) coincides with (2) when either $q=2$ or $d=3$. The bound (3) was improved in [8] for $d \leq q+1$ to

$$\mathsf{c}(q,d) \leq d - 3 + \frac{1}{d-2} \ .$$

Better bounds are known for $d \leq 6$: e.g., it is known that $\mathsf{c}(4,5) = 2$ [4]; see also [2],[3],[8, §2]. For large d, however, the upper bound (3) seems to be the best currently known, to our knowledge[3]. Thus, denoting

$$\lambda(q) = \liminf_{d\to\infty} \frac{\mathsf{c}(q,d)}{d} \ ,$$

we have

$$\frac{1}{2} \leq \lambda(q) \leq \frac{q-1}{q} \ , \tag{4}$$

where the upper bound is due to primitive BCH codes. Note that $\lambda(q)$ determines the behavior of codes in the high-rate regime, since we first let n go to infinity (in (1)), and only then does d go to infinity.

The main contribution of this paper is an improvement on the upper bound in (4) for $q = 4, 8$. Given any finite field $F = \mathrm{GF}(q)$, where $q = r^h$ for some $h \geq 2$, and any $d \in \mathbb{Z}^+$, we present an explicit construction of an infinite sequence of codes of increasing lengths,

$$\mathbb{C}(d;r,h) = (\mathcal{C}(n_i,k_i,d;r,h))_{i=1}^{\infty} \ ,$$

with each $\mathcal{C}(n_i,k_i,d;r,h)$ being a *cyclic* $[n_i,k_i,\geq d]$ code over F, such that the limit

$$\mathsf{c}_{\mathrm{New}}(q,d) = \lim_{i\to\infty} \frac{n_i - k_i}{\log_q n_i}$$

satisfies

$$\mathsf{c}_{\mathrm{New}}(q,d) \leq \left\lceil \frac{r-1}{r} \left\lceil \frac{r-1}{r} \cdot \frac{q}{q-1}(d-1) \right\rceil \right\rceil \cdot h \ . \tag{5}$$

This, in turn, implies the upper bound

$$\begin{aligned} \lambda(q) &\leq \liminf_{d\to\infty} \frac{\mathsf{c}_{\mathrm{New}}(q,d)}{d} \\ &\leq \frac{(r-1)^2}{r^2} \cdot \frac{q}{q-1} \cdot h \ . \end{aligned}$$

In particular, $\lambda(4) \leq 2/3$ (compared to the upper bound $3/4$ obtained from (4)) and $\lambda(8) \leq 6/7$ (compared to $7/8$). In fact, the improvement turns out to be not just asymptotic (in d): the inequality $\mathsf{c}_{\mathrm{New}}(q,d) < \mathsf{c}_{\mathrm{BCH}}(q,d)$ holds for every $d \geq 11$ when $q=4$, and for every $d \geq 51$ when $q=8$.

The codes $\mathcal{C} = \mathcal{C}(n_i,k_i,d;r,h)$ are designed so that when they are used as outer codes in a concatenated scheme with certain irreducible cyclic inner codes $\mathcal{I}$ over $K = \mathrm{GF}(r)$, the resulting concatenated code, $\mathcal{C} * \mathcal{I}$, is a cyclic code over K, for which the BCH bound guarantees a prescribed lower bound D on the minimum distance. The parameter D is selected so

Ron M. Roth and Alexander Zeh are with the Computer Science Department, Technion, Haifa 3200003, Israel.

Emails: ronny@cs.technion.ac.il, alex@codingtheory.eu

This work was supported in part by Grants 1092/12 and 1396/16 from the Israel Science Foundation. A. Zeh was supported by the German Research Foundation (Deutsche Forschungsgemeinschaft, DFG) under grant Ze1016/1-1. This work was presented in part at the IEEE International Symposium on Information Theory, Barcelona, Spain, July 2016.

[1] Hereafter, by a primitive BCH code over $\mathrm{GF}(q)$ we mean a BCH code of length $q^m - 1$ defined by the roots $1, \gamma, \gamma^2, \ldots, \gamma^{d-2}$, where γ is a primitive element in $\mathrm{GF}(q^m)$.

[2] When $n \neq q^m - 1$, define the size to be, say, 1.

[3] As for improvements on the lower bound (2), it follows from a recent result in [5] that when the maximum size $A(q,n,d)$ in (1) is taken over linear codes over $\mathrm{GF}(q)$, then the respective redundancy coefficient, $\mathsf{c}_{\mathrm{Lin}}(q,d)$, is larger than 1 for every $q > 2$; in particular, if we replace $\mathsf{c}(q,d)$ by $\mathsf{c}_{\mathrm{Lin}}(q,d)$ in (2), then the inequality therein becomes strict when $d=4$ and $q>2$.

that the minimum distance of $\mathcal{C}$ is guaranteed to be at least the designed value d. This approach also yields an efficient decoding algorithm for correcting up to $(d-1)/2$ errors, as well as a list-decoding algorithm up to the Johnson radius: the decoding reduces to decoding the code $\mathcal{C}*\mathcal{I}$, using known decoding algorithms for BCH codes.

We recall that concatenation was used in [1] to construct binary cyclic codes which are "not so bad," especially in the low-rate range: there, the resulting concatenated code was the object of interest. In our case, however, it is the outer code that we design and analyze and, so, the product lower bound on the minimum distance of concatenated codes seemingly goes "the wrong way," in that D implies an upper bound rather than a lower bound on the minimum distance of $\mathcal{C}$. One of our solutions to this problem is selecting the inner code $\mathcal{I}$ to be an equidistant code.

II. Construction

A. Preliminaries

Let $q = r^h$ where r is a power of a prime and $h \geq 2$. Fix ℓ to be an integer such that $\gcd(\ell, r) = 1$ and the multiplicative order of r in $\mathbb{Z}_\ell^*$ equals h (e.g., $\ell = q-1$ or $\ell = (q-1)/(r-1)$).

Let n and d be given positive integers such that $\gcd(n, \ell) = \gcd(n, q) = 1$ and $d < n$. Let $\Phi = \mathrm{GF}(q^m)$ be the splitting field of $x^n - 1$; i.e., m is the smallest positive integer such that $n \,|\, q^m - 1$. Note that since $\gcd(\ell, n) = 1$ and $\ell \,|\, q-1$, we also have that $\ell n \,|\, q^m - 1$; namely, Φ is also the splitting field of $x^{\ell n} - 1$.

To simplify the notation in the sequel, we introduce the following function $\mathsf{f}_r : \mathbb{Z} \to \mathbb{Z}$:

$$\mathsf{f}_r(x) = \left\lceil \frac{r-1}{r} \cdot x \right\rceil \ .$$

We construct cyclic $[n, k, \geq d]$ codes $\mathcal{C} = \mathcal{C}(n, k, d; r, h)$ over $F = \mathrm{GF}(q)$ whose redundancy is bounded from above by

$$n - k \leq \mathsf{f}_r\left(\mathsf{f}_r\Big(\frac{q}{q-1}\,(d-1)\Big)\right) \cdot h \cdot m \ . \tag{6}$$

If we take $\ell = q-1$ and $n = (q^m-1)/\ell = (q^m-1)/(q-1)$, then $\gcd(n, \ell) = 1$ whenever $\gcd(m, q-1) = 1$ and, so, our construction will yield codes for infinitely many values of n, for any fixed r, h, and d; this, together with (6), implies (5). When $d \equiv 1 \pmod{(q-1)/(r-1)}$, we can simplify (6) to

$$\frac{n-k}{(d-1)m} \leq \frac{(r-1)^2}{r^2} \cdot \frac{q}{q-1} \cdot h \ . \tag{7}$$

We will show improvements on (6) in Proposition 4 and in Section III below.

Example 1. Let $r = h = 2$ (i.e., $q = 4$), $\ell = 3$, and $n = (4^m - 1)/3$, where $3 \nmid m$. Under these conditions we have $\gcd(n, \ell) = \gcd(n, q) = 1$. Substituting these values in (7) and assuming that $d \equiv 1 \pmod 3$, we obtain the following upper bound on the redundancy $n - k$:

$$\frac{2}{3}(d-1) \cdot m \leq \frac{2}{3}(d-1)\log_4(3n+1) \ . \tag{8}$$

In comparison, a primitive BCH code over $\mathrm{GF}(4)$ with the same designed minimum distance d and with a *shorter* length $n' = 4^{m-1} - 1 = 3(n-1)/4$ has a redundancy of

$$1 + \left\lceil \frac{3}{4}(d-2) \right\rceil \log_4(n'+1) = 1 + \left\lceil \frac{3}{4}(d-2) \right\rceil \log_4\Big(\frac{3n+1}{4}\Big) \ , \tag{9}$$

whenever $d - 2 \leq \sqrt{n'+1}$ [7, §9.3] (furthermore, when d is a power of 4, then d is the true minimum distance of the code [7, p. 260]). We conclude that in the high-rate range where $d \leq \sqrt{3n/4}$, the ratio between the redundancies (8) and (9) approaches $8/9$ as we let d grow. This will be the case also for general $d \in \mathbb{Z}^+$, using the more general bound (6). □

For reals y and z, denote by $[y, z\rangle$ the integer set $\{i \in \mathbb{Z} : y \leq i < z\}$. We use the shorthand notation $[z\rangle$ for $[0, z\rangle$.

Let

$$D = \left\lfloor \frac{r-1}{r} \cdot \frac{q}{q-1} \cdot \ell(d-1) \right\rfloor + 1 \ , \tag{10}$$

and fix integers $b \in [2-D, 1\rangle$ and $w \in [\ell\rangle$ such that $\gcd(w, \ell) = 1$. For each $j \in [h\rangle$, define the sets

$$\mathcal{S}_j = \big\{ s \in [b, b+D-1\rangle \ : \ s \equiv r^j w n \pmod{\ell} \big\} \tag{11}$$

and

$$\mathcal{R}_j = \big\{ i \in [n\rangle \ : \ r^j(wn + i\ell) \equiv s \pmod{(\ell n)}, \text{ for some } s \in \mathcal{S}_j \big\} \ . \tag{12}$$

Also, define the unions

$$\mathcal{S} = \bigcup_{j \in [h\rangle} \mathcal{S}_j \quad \text{and} \quad \mathcal{R} = \bigcup_{j \in [h\rangle} \mathcal{R}_j \ .$$

Note that the requirement $d < n$ implies that $D - 1 < \ell n$, and, so, if $s, s' \in \mathcal{S}$ satisfy $s \equiv s' \pmod{(\ell n)}$, then necessarily $s = s'$. In addition, since $\gcd(r^j, \ell n) = 1$ then, by the Chinese Remainder Theorem, for every $s \in \mathcal{S}$ there is a unique pair $(j, i) \in [h\rangle \times [n\rangle$ such that $r^j(wn + i\ell) \equiv s \pmod{(\ell n)}$. This, in turn, induces a bijection $s \mapsto i = i(s)$ from $\mathcal{S}_j$ to $\mathcal{R}_j$, for every $j \in [h\rangle$. The set $\{\mathcal{S}_j\}_{j \in [h\rangle}$ is a partition of $\mathcal{S}$: each subset $\mathcal{S}_j$ consists of (an arithmetic progression of) elements of $[b, b+D-2\rangle$ at length-ℓ intervals, with the first (smallest) element differing for distinct $j \in [h\rangle$.

The complement set $\overline{\mathcal{S}} = [b, b+D-1\rangle \setminus \mathcal{S}$ can be expressed in the form

$$\overline{\mathcal{S}} = \big\{ s \in [b, b+D-1\rangle \ : \ s \equiv e\, wn \pmod{\ell}, \text{ for some } e \in \mathcal{E} \big\} \ ,$$

where

$$\mathcal{E} = \big\{ e \in [\ell\rangle \ : \ e \not\equiv r^j \pmod{\ell}, \text{ for all } j \in [h\rangle \big\} \ . \tag{13}$$

B. Definition of the code

We define the code $\mathcal{C} = \mathcal{C}(n, k, d; r, h)$ by its set of roots (in Φ), which is given by the following union of conjugacy classes (w.r.t. F):

$$\Omega = \bigcup_{i \in \mathcal{R}} C_{\alpha^i} \ , \tag{14}$$

where α is a primitive nth root of unity in Φ and $C_{\alpha^i} = \{\alpha^{iq^t}\}_t$. Thus, the definition of $\mathcal{C}$ is a function of ℓ, α, b, and w (as well as of r, h, n, and d).

Remark 1. Since the set of roots of $\mathcal{C}$ is closed under conjugacy w.r.t. F, each set $\mathcal{R}_j$ can be replaced by

$$q^t \cdot \mathcal{R}_j = \left\{ i \in [n\rangle \ : \ i = q^t \cdot i', \text{ for some } i' \in \mathcal{R}_j \right\} \ ,$$

for any integer t. □

An equivalent formulation of the sets $\mathcal{R}_j$, which expresses their elements somewhat more explicitly, is included in Appendix A. We also note that the sets $\mathcal{R}_j$ typically intersect. We will take that into account when we compute an upper bound on the redundancy, $n-k$, of $\mathcal{C}$. Yet first we establish a lower bound on the minimum distance of $\mathcal{C}$.

C. Lower bound on the minimum distance

Our strategy for computing a lower bound on the minimum distance of $\mathcal{C}$ will be based on analyzing the minimum distance of a concatenated code obtained by using $\mathcal{C}$ as an outer code and a certain irreducible cyclic code $\mathcal{I}$ as an inner code. (In fact, the set of roots of $\mathcal{C}$ was selected so as to match this strategy in the first place.)

For this analysis, we recall known properties of concatenations of cyclic codes, specializing (for the sake of avoiding the introduction of further notation) to the case where the outer code is $\mathcal{C}$.

Let β be a primitive ℓth root of unity in $\Phi = \mathrm{GF}(q^m)$ and let $\mathcal{I}$ be the irreducible cyclic $[\ell, h]$ code over $K = \mathrm{GF}(r)$ whose check polynomial equals the minimal polynomial, $M_\beta(x)$, of β w.r.t. K; by the conditions on ℓ we indeed have that $\deg M_\beta(x) = h$. Define the mapping $\varphi : F \to K^\ell$ for every $\delta \in F$ by

$$\varphi(\delta) = \left(\mathrm{Tr}(\delta) \ \ \mathrm{Tr}(\delta\beta^{-1}) \ \ \mathrm{Tr}(\delta\beta^{-2}) \ \ldots \ \mathrm{Tr}(\delta\beta^{-(\ell-1)}) \right) , \tag{15}$$

where $\mathrm{Tr}(x) = \mathrm{Tr}_{F/K}(x)$ stands for the trace polynomial $x + x^r + x^{r^2} + \ldots + x^{r^{h-1}}$. It is known that the set of images of φ is $\mathcal{I}$ and that the mapping $\varphi : F \to \mathcal{I}$ is in fact an isomorphism; see[4] [7, §18.5].

We extend the mapping φ to words $\boldsymbol{x} = (x_j)_{j \in [n\rangle}$ in F^n by

$$\varphi(\boldsymbol{x}) = (\varphi(x_0) \mid \varphi(x_1) \mid \ \ldots \ \mid \varphi(x_{n-1})) \ (\in K^{\ell n}) \ , \tag{16}$$

and define $\mathcal{C} * \mathcal{I}$ to be the following concatenated code over K:

$$\mathcal{C} * \mathcal{I} = \{ \varphi(\boldsymbol{c}) \ : \ \boldsymbol{c} \in \mathcal{C} \} \ .$$

Recalling that $\gcd(\ell, n) = 1$, we have the following result.

Lemma 1 ([7, §18.5, Theorem 5])**.** *Up to a fixed permutation of coordinates, the code $\mathcal{C} * \mathcal{I}$ is cyclic (of length ℓn and dimension hk).*

Moreover, we have a full characterization of the set of roots of $\mathcal{C} * \mathcal{I}$ in the splitting field, Φ, of $x^{\ell n} - 1$.

[4]The results that we quote hereafter from [7, §18.5] are proved there for the case $r = 2$, yet they generalize in a straightforward manner to any r. See also [1].

Lemma 2 ([7, §18.5, Theorem 6])**.** *Let Ω be the set of roots of $\mathcal{C}$ (as in (14)). Then the set of roots of $\mathcal{C} * \mathcal{I}$ is given by the union of*

$$\bigcup_{j \in [h\rangle} \left\{ (\beta\omega)^{r^j} \ : \ \omega \in \Omega \right\} \tag{17}$$

and

$$\bigcup_{e \in \mathcal{E}} \left\{ \beta^e \alpha^i \ : \ i \in [n\rangle \right\} \tag{18}$$

(where $\mathcal{E}$ is defined in (13)).

Theorem 3. *The minimum distance of $\mathcal{C}$ is at least d.*

Proof. Let γ be a primitive (ℓn)th root of unity in Φ such that $\alpha = \gamma^\ell$, and let $\beta = \gamma^{wn}$ (which is a primitive ℓth root of unity in Φ). Consider the concatenated code $\mathcal{C} * \mathcal{I}$, where $\mathcal{I}$ is the irreducible cyclic $[\ell, h]$ code over K whose check polynomial is $M_\beta(x)$. By Lemma 2 we get that the set of roots of $\mathcal{C} * \mathcal{I}$ (in Φ) includes both

$$\begin{aligned} \bigcup_{j \in [h\rangle} \left\{ (\beta\alpha^i)^{r^j} \ : \ i \in \mathcal{R} \right\} &\supseteq \bigcup_{j \in [h\rangle} \left\{ \beta^{r^j} \alpha^{r^j i} \ : \ i \in \mathcal{R}_j \right\} \\ &= \bigcup_{j \in [h\rangle} \left\{ \gamma^{r^j (wn + i\ell)} \ : \ i \in \mathcal{R}_j \right\} = \bigcup_{j \in [h\rangle} \{ \gamma^s \ : \ s \in \mathcal{S}_j \} \\ &= \{ \gamma^s \ : \ s \in \mathcal{S} \} \end{aligned}$$

and

$$\begin{aligned} \bigcup_{e \in \mathcal{E}} \left\{ \beta^e \alpha^i \ : \ i \in [n\rangle \right\} &= \bigcup_{e \in \mathcal{E}} \left\{ \gamma^{e\, wn + i\ell} \ : \ i \in [n\rangle \right\} \\ &\supseteq \left\{ \gamma^s \ : \ s \in \overline{\mathcal{S}} \right\} \ . \end{aligned}$$

It follows that the elements in $\{\gamma^s \ : \ s \in [b, b+D-1\rangle\}$ are all roots of $\mathcal{C} * \mathcal{I}$, thereby implying by the BCH bound that the minimum distance of $\mathcal{C} * \mathcal{I}$ is at least D.

It remains to show that this implies that the minimum distance of $\mathcal{C}$ is at least d. Assume to the contrary, and let $\boldsymbol{c}$ be a nonzero codeword in $\mathcal{C}$ of Hamming weight (over F) $\mathsf{w}_F(\boldsymbol{c}) \leq d-1$. Consider the $q-1$ codewords $\varphi(\mu \cdot \boldsymbol{c})$ of $\mathcal{C} * \mathcal{I}$, where μ ranges over the elements of F^*. Their average weight (over K) equals

$$\frac{r^{h-1}(r-1)}{r^h - 1} \cdot \ell \cdot \mathsf{w}_F(\boldsymbol{c}) < \left\lfloor \frac{r-1}{r} \cdot \frac{q}{q-1} \cdot \ell(d-1) \right\rfloor + 1 = D \ , \tag{19}$$

where the multiplier of $\mathsf{w}_F(\boldsymbol{c})$ in the left-hand side of (19) is the average weight (over K) of the nonzero codewords of $\mathcal{I}$ (being a linear $[\ell, h]$ code over K with no all-zero coordinate). The inequality in (19) implies the sought contradiction. □

Remark 2. The averaging argument in the last proof becomes vacuous in case $\mathcal{I}$ is taken as an equidistant code: here, the left-hand side of (19) equals the weight of the concatenated codeword that is produced from $\boldsymbol{c}$. □

In the proof of the lower bound D on the minimum distance of $\mathcal{C} * \mathcal{I}$, both subsets—(17) and (18)—of the set of roots of $\mathcal{C} * \mathcal{I}$ contribute to the set, $\{\gamma^s \ : \ s \in [b, b+D-1\rangle\}$, of $D-1$ consecutive powers of γ. Specifically, partitioning $[b, b+D-1\rangle$ into ℓ disjoint arithmetic progressions, each consisting of integers at length-ℓ intervals, the contribution of (17) corresponds to h of these arithmetic progressions

(namely, $\mathcal{S}_0, \mathcal{S}_1, \ldots, \mathcal{S}_{h-1}$, forming together the set $\mathcal{S}$), while the contribution of (18) corresponds to the remaining $\ell - h$ progressions (forming together the set $\overline{\mathcal{S}}$). Yet only the subset (17) actually depends on the set of roots of $\mathcal{C}$; the contribution of the subset (18) comes "free," without adding to the redundancy of $\mathcal{C}$. This may explain the savings in redundancy that is sometimes achieved by the construction $\mathcal{C}$.

We next provide a more detailed analysis of the redundancy of $\mathcal{C}$.

D. Upper bound on the redundancy

Our analysis of the redundancy of $\mathcal{C}$ will use our condition on the selection of b, which guarantees that $0 \in [b, b+D-1\rangle$; thus, the set $[b, b+D-1\rangle$ is closed under division by r, in the sense that if $s \in [b, b+D-1\rangle$ is divisible by r, then $s/r \in [b, b+D-1\rangle$. Let i be an element in $\mathcal{R}_j$, for some $j \in [h\rangle$. Then, from (12),

$$r^j(wn + i\ell) \equiv s \pmod{(\ell n)} ,$$

for some $s \in \mathcal{S}_j$. Suppose in addition that $r \,|\, s$. Then,

$$r^{j-1}(wn + i\ell) \equiv (s/r) \pmod{(\ell n)} .$$

Hence, if $j > 0$, then $i \in \mathcal{R}_{j-1}$. Otherwise (if $j = 0$), then there exists $i' \in \mathcal{R}_{h-1}$ such that $qi' \equiv i \pmod{n}$ and

$$r^{h-1}(wn + i'\ell) \equiv (s/r) \pmod{(\ell n)}$$

(note that $r^{h-1}wn \equiv r^{-1}wn \pmod{(\ell n)}$ and that $\alpha^{i'} \in C_{\alpha^i}$; see Remark 1). It follows that the code $\mathcal{C}$ can be equivalently defined with the sets $\mathcal{R}_j$ replaced by

$$\mathcal{R}_j^* = \big\{ i \in [n\rangle \ : \ r^j(wn + i\ell) \equiv s \pmod{(\ell n)}, \text{ for some } s \in \mathcal{S}_j^* \big\} , \quad (20)$$

where

$$\mathcal{S}_j^* = \big\{ s \in \mathcal{S}_j \ : \ r \nmid s \big\} . \quad (21)$$

Namely, the set of roots of $\mathcal{C}$ is $\bigcup_{i \in \mathcal{R}^*} C_{\alpha^i}$, where

$$\mathcal{R}^* = \bigcup_{j \in [h\rangle} \mathcal{R}_j^* .$$

Hence, since $|C_{\alpha^i}| \le m$, the redundancy of $\mathcal{C}$ satisfies

$$\begin{aligned} n - k &= \Big| \bigcup_{i \in \mathcal{R}^*} C_{\alpha^i} \Big| \le |\mathcal{R}^*| \cdot m \\ &\le \Big(\sum_{j \in [h\rangle} |\mathcal{R}_j^*| \Big) \cdot m = \Big(\sum_{j \in [h\rangle} |\mathcal{S}_j^*| \Big) \cdot m . \end{aligned}$$

That is,

$$n - k \le |\mathcal{S}^*| \cdot m , \quad (22)$$

where

$$\mathcal{S}^* = \bigcup_{j \in [h\rangle} \mathcal{S}_j^* = \big\{ s \in \mathcal{S} \ : \ r \nmid s \big\} .$$

Selecting $b = 0$, we get

$$|\mathcal{S}_j| = |\mathcal{R}_j| \le \left\lceil \frac{D-2}{\ell} \right\rceil$$

and, so,

$$|\mathcal{S}^*| = \sum_{j \in [h\rangle} |\mathcal{S}_j^*| \le \sum_{j \in [h\rangle} \mathsf{f}_r\left(|\mathcal{S}_j|\right) \le \mathsf{f}_r\Big(\left\lceil \frac{D-2}{\ell} \right\rceil \Big) \cdot h . \quad (23)$$

Finally, plugging (10) into (23) we obtain (6) from (22).

Example 2. We construct $\mathcal{C}$ for $r = h = 2$, $n = 341$, $d = 11$, $\ell = r^h - 1 = 3$, $b = -10$, and $w = 1$. By (10) we get $D = 21$ and, writing $\mathcal{J} = [b, b+D-1\rangle = [-10, 10\rangle$, from the definition of $\mathcal{S}_j$ in (11) we obtain:

$$\begin{aligned} \mathcal{S}_0 &= \big\{ s \in \mathcal{J} \ : \ s \equiv 2 \pmod 3 \big\} = \{-7, -4, -1, 2, 5, 8\} \\ \mathcal{S}_1 &= \big\{ s \in \mathcal{J} \ : \ s \equiv 1 \pmod 3 \big\} = \{-8, -5, -2, 1, 4, 7\} . \end{aligned}$$

Pruning all the even numbers, we get the following sets $\mathcal{S}_j^*$, with the corresponding sets $\mathcal{R}_j^*$ (see (20)–(21)):

$$\begin{aligned} \mathcal{S}_0^* &= \big\{-7, -1, 5\big\} , \quad & \mathcal{S}_1^* &= \big\{-5, 1, 7\big\} , \\ \mathcal{R}_0^* &= \big\{225, 227, 229\big\} , \quad & \mathcal{R}_1^* &= \big\{56, 57, 58\big\} , \end{aligned}$$

and the set $\mathcal{S}^*$ is given by the union

$$\mathcal{S}^* = \mathcal{S}_0^* \cup \mathcal{S}_1^* = \big\{-7, -5, -1, 1, 5, 7\big\} .$$

The root set of $\mathcal{C}$ consists of the union of the conjugacy classes C_{α^i}, where α is a primitive 341st root of unity in $\Phi = \mathrm{GF}(4^5)$ and i ranges over the set

$$\mathcal{R}^* = \mathcal{R}_0^* \cup \mathcal{R}_1^* = \big\{56, 57, 58, 225, 227, 229\big\} .$$

The six elements in $\mathcal{R}^*$ belong to distinct conjugacy classes, each of size 5. Hence, $n - k = 30$. □

The following proposition presents improved upper bounds on the size of $\mathcal{S}^*$, for the case where ℓ is a prime. (See Appendix B for a proof.)

Proposition 4. *When ℓ is a prime, there is a choice for $w \in [1, \ell\rangle$ such that*

$$\begin{aligned} |\mathcal{S}^*| \ \le \ & \frac{h}{\ell - 1} \Bigg(\mathsf{f}_r\left(-b\right) - \mathsf{f}_r\Big(\Big\lfloor \frac{-b}{\ell} \Big\rfloor \Big) \\ & + \mathsf{f}_r\left(b+D-2\right) - \mathsf{f}_r\Big(\Big\lfloor \frac{b+D-2}{\ell} \Big\rfloor \Big) \Bigg) . \quad (24) \end{aligned}$$

In particular,

$$|\mathcal{S}^*| \le \frac{r-1}{r\ell} \cdot D \cdot h . \quad (25)$$

Furthermore, when $-b \equiv D-2 \equiv -1 \pmod \ell$ and $\lfloor -b/\ell \rfloor \equiv \lfloor (D-2)/\ell \rfloor \equiv -1 \pmod r$, then, for that w,

$$|\mathcal{S}^*| \le \frac{r-1}{r} \cdot \frac{D-1}{\ell} \cdot h . \quad (26)$$

For the case where $d \equiv 1 \pmod{(q-1)/(r-1)}$, the bound (26) coincides with (7).

Remark 3. Two values w and w' yield the same set $\mathcal{S}^*$ if they belong to the same cyclotomic coset modulo ℓ w.r.t. $K = \mathrm{GF}(r)$, namely, if $w' \equiv r^j w \pmod \ell$, for some $j \in [h\rangle$. □

III. Fine tuning for GF(4) and GF(8)

We present two constructions over $\mathrm{GF}(4)$ (with $r = h = 2$).

Construction A. We take $n = (4^m - 1)/3$, where $3 \nmid m$. Under these conditions we have $\gcd(n, 3) = 1$, allowing us to take $\ell = 3$. The value of D is determined by (10) to be

$$D = 2d - 1$$

and, from (22) we get

$$n-k \le |\mathcal{S}^*| \cdot m \le |\mathcal{S}^*| \log_4(3n+1) \ ,$$

where, by (25),

$$|\mathcal{S}^*| \le \left\lfloor \frac{2d-1}{3} \right\rfloor = \frac{2d-3+v}{3} \ , \tag{27}$$

with v being the remainder of d modulo 3. (Comparing to Example 1, we obtained there the same upper bound on $n-k$ for $d \equiv 1 \pmod 3$, yet (6) yields a weaker bound when $d \not\equiv 1 \pmod 3$.)

In Appendix C, we show that when $d \equiv 2 \pmod 3$, the bound (27) can be improved to

$$|\mathcal{S}^*| \le \frac{2d-4}{3} \ , \tag{28}$$

if we use (24) and select $b \equiv 2$ or $3 \pmod 6$.

An instance of this construction, for $n = 341$ and $d = 11$, was shown earlier in Example 2. Since there is only one cyclotomic coset modulo 3 w.r.t. $\mathrm{GF}(2)$, the construction does not depend on the choice of w: changing w from 1 to 2 will merely switch the roles of $\mathcal{S}_0^*$ and $\mathcal{S}_1^*$ (see Remark 3). □

Construction B. We take $n = (2^m+1)/3$, where $m \equiv 1$ or $5 \pmod 6$ (namely, m is neither even nor a multiple of 3). Under these conditions, n is an integer such that $\gcd(n,3) = 1$ and, so, we take $\ell = 3$. The value of D is, again, taken by (10) to be $D = 2d-1$, and we select $b = -d+1$. Thus, the set of roots of $\mathcal{C} * \mathcal{I}$ contains the set $\{\gamma^s \ : \ s \in [-d+1, d-1\rangle\}$, where γ is a (2^m+1)st root of unity in $\mathrm{GF}(2^{2m})$. Yet γ^s and γ^{-s} are conjugate w.r.t. $\mathrm{GF}(2)$; therefore, when designing $\mathcal{C}$, we can replace the interval $[b, b+D-1\rangle$ in (11) by $[0, d\rangle$. Consequently, substituting $b \leftarrow 0$ and $D \leftarrow d+1$ in (25) yields:

$$n-k \le |\mathcal{S}^*| \cdot m \le 2|\mathcal{S}^*| \log_4(3n-1) \ ,$$

where

$$2|\mathcal{S}^*| \le 2\left\lfloor \frac{d+1}{3} \right\rfloor = \begin{cases} (2d-2v)/3 & \text{if } v = 0,1 \\ (2d-2v+3)/3 & \text{if } v = 2 \end{cases} \ , \tag{29}$$

with v being the remainder of d modulo 3.

In Appendix C, we show that when $d \equiv 5 \pmod 6$, the bound (29) can be improved to

$$2|\mathcal{S}^*| \le \frac{2d-4}{3} \ . \tag{30}$$

□

Remark 4. In their 1978 paper [4], Dumer and Zinoviev presented two constructions of cyclic codes of minimum distance $d = 5$ over $\mathrm{GF}(4)$, which are optimal w.r.t. the linear-code version of the sphere-packing bound. These constructions are, in fact, special cases of Constructions A and B. □

Remark 5. In the above constructions, $D = 2d-1$ is odd, so either b or $b+D-1$ must be even. This means that we would end up with the same constructions if the sets $\mathcal{S}_j$ were defined in (11) with $[b, b+D-1\rangle$ replaced by $[b', b'+D'-1\rangle$, where $D' = D+1 = 2d$ and either $b' = b$ (if b is even) or $b' = b-1$ (otherwise). □

In Table I, we list for several values of d the upper bound on $\mathsf{c}(4,d)$ given by (3) and the respective bounds, $\mathsf{c}_{\mathrm{A}}(4,d)$ and $\mathsf{c}_{\mathrm{B}}(4,d)$, obtained by Constructions A and B (Eqs. (27)–(30); numbers in italics correspond to the improved bounds (28) and (30)). Clearly, all these bounds are integers, and it can be readily verified analytically that $\mathsf{c}_{\mathrm{A}}(4,d)$ is strictly smaller than $\mathsf{c}_{\mathrm{BCH}}(4,d)$ for every $d \ge 11$. While $\mathsf{c}_{\mathrm{B}}(4,d)$ is larger than $\mathsf{c}_{\mathrm{BCH}}(4,d)$ for some values of d (and is never smaller than $\mathsf{c}_{\mathrm{A}}(4,d)$ for any d), it becomes strictly smaller than $\mathsf{c}_{\mathrm{BCH}}(4,d)$ for every $d \ge 27$.

TABLE I
UPPER BOUNDS ON $\mathsf{c}(4,d)$ OBTAINED FROM BCH CODES AND FROM CONSTRUCTIONS A AND B.

d	$\mathsf{c}_{\mathrm{BCH}}(4,d)$	$\mathsf{c}_{\mathrm{A}}(4,d)$	$\mathsf{c}_{\mathrm{B}}(4,d)$
3	1	1	2
4	2	2	2
5	3	*2*	*2*
6	3	3	4
7	4	4	4
8	5	*4*	6
9	6	5	6
10	6	6	6
11	7	*6*	*6*
12	8	7	8
13	9	8	8
14	9	*8*	10
15	10	9	10
16	11	10	10
17	12	*10*	*10*
18	12	11	12
19	13	12	12
20	14	*12*	14
21	15	13	14
22	15	14	14
23	16	*14*	*14*
24	17	15	16
25	18	16	16
26	18	*16*	18
27	19	17	18

We turn now to a construction over $\mathrm{GF}(8)$ (with $r = 2$ and $h = 3$).

Construction C. We take $n = (8^m-1)/7$, where $7 \nmid m$, in which case $\gcd(n,7) = 1$, so we can take $\ell = 7$. The value of D is determined by (10) to be

$$D = 4d-3$$

and, by (22) and (25) we get

$$n-k \le |\mathcal{S}^*| \cdot m \le |\mathcal{S}^*| \log_8(7n+1) \ ,$$

where

$$|\mathcal{S}^*| \le \left\lfloor \frac{6d-5}{7} \right\rfloor = \begin{cases} (6d-7+v)/7 & \text{if } v = 0,1,2 \\ (6d-14+v)/7 & \text{otherwise} \end{cases} \ , \tag{31}$$

with v being the remainder of d modulo 7.

We show in Appendix C that when $d \equiv 2 \pmod 7$, the bound (31) can be improved to

$$|\mathcal{S}^*| \le \frac{6d-12}{7} \ . \tag{32}$$

□

Remark 6. If we select $b = -5$, Construction C would be unaffected if the sets $\mathcal{S}_j$ were defined in (11) with the interval $[b, b+D-1\rangle$ replaced by $[b', b'+D'-1\rangle$, where $b' = -8$ and $D' = D + 3 = 4d$. This is because the three added values, -8, -7, and -6, would not be in $\mathcal{S}^*$. □

Example 3. We apply Construction C with $n = (8^4-1)/7 = 585$, $d = 9$, $\ell = 7$, $b = -8$, and $w = 6$. By (10) we get $D = 33$ and, letting $\mathcal{J} = [b, b+D-1\rangle = [-8, 24\rangle$, we obtain from (11):

$$\begin{aligned}\mathcal{S}_0 &= \big\{s \in \mathcal{J} \,:\, s \equiv 3 \pmod 7\big\} = \{-4, 3, 10, 17\}\\ \mathcal{S}_1 &= \big\{s \in \mathcal{J} \,:\, s \equiv 6 \pmod 7\big\} = \{-1, 6, 13, 20\}\\ \mathcal{S}_2 &= \big\{s \in \mathcal{J} \,:\, s \equiv 5 \pmod 7\big\} = \{-2, 5, 12, 19\}\,.\end{aligned}$$

Pruning all the even numbers yields the following sets $\mathcal{S}_j^*$ and the respective sets $\mathcal{R}_j^*$:

$$\begin{aligned}&\mathcal{S}_0^* = \big\{3, 17\big\}\,,\quad \mathcal{S}_1^* = \big\{-1, 13\big\}\,,\quad \mathcal{S}_2^* = \big\{5, 19\big\}\,,\\ &\mathcal{R}_0^* = \big\{84, 86\big\}\,,\ \mathcal{R}_1^* = \big\{376, 377\big\}\,,\ \mathcal{R}_2^* = \big\{230, 523\big\}\,,\end{aligned}$$

and the set $\mathcal{S}^*$ is given by

$$\mathcal{S}^* = \mathcal{S}_0^* \cup \mathcal{S}_1^* \cup \mathcal{S}_2^* = \big\{-1, 3, 5, 13, 17, 19\big\}\,.$$

The root set of $\mathcal{C}$ consists of the union of the conjugacy classes C_{α^i}, where α is a primitive 585th root of unity in $\Phi = \mathrm{GF}(8^4)$ and i ranges over the set

$$\mathcal{R}^* = \mathcal{R}_0^* \cup \mathcal{R}_1^* \cup \mathcal{R}_2^* = \big\{84, 86, 230, 376, 377, 523\big\}\,.$$

The elements in $\mathcal{R}^*$ belong to distinct conjugacy classes, each of size 4. Hence, $n - k = 24$. □

It can be verified analytically that the upper bound on $\mathsf{c}(8, d)$ given by (31)–(32) is never larger than the upper bound given by (3), and is strictly smaller than the latter for every $d \geq 51$.

IV. Decoding

We describe a decoding method for the code $\mathcal{C}$ (over $F = \mathrm{GF}(q)$, where $q = r^h$) as defined in Section II-B, assuming that ℓ is such that there exists an irreducible cyclic $[\ell, h]$ code $\mathcal{I}$ over $K = \mathrm{GF}(r)$ which is equidistant (and, so, its minimum distance is $\Delta = ((q(r-1)/r)/(q-1)) \cdot \ell)$. E.g., for $\ell = q-1$, that code is the simplex code over K. Note that in all the constructions of Section III we had $\ell = q - 1$.

Let φ be the mapping defined in (15)–(16), and let the received word be $\boldsymbol{y} = \boldsymbol{c} + \boldsymbol{e}$, where $\boldsymbol{c} \in \mathcal{C}$ and $\boldsymbol{e}$ is the error word. Then

$$\varphi(\boldsymbol{y}) = \varphi(\boldsymbol{c}) + \varphi(\boldsymbol{e})\,,$$

where $\varphi(\boldsymbol{c}) \in \mathcal{C} * \mathcal{I}$ and $\mathsf{w}_K(\varphi(\boldsymbol{e})) = \Delta \cdot \mathsf{w}_F(\boldsymbol{e})$. Namely, the mapping $\varphi(\cdot)$ inflates the number of errors in $\boldsymbol{e}$ by a factor of Δ. From (10) we have $D - 1 = \Delta(d-1)$ and, so, we can obtain a bounded-distance decoder $\mathcal{D} : F^n \to \mathcal{C}$ (that corrects up to $(d-1)/2$ errors) from any bounded-distance decoder $\tilde{\mathcal{D}} : K^{\ell n} \to \mathcal{C} * \mathcal{I}$ (that corrects up to $(D-1)/2 = \Delta(d-1)/2$ errors) by

$$\mathcal{D}(\boldsymbol{y}) = \varphi^{-1}\left(\tilde{\mathcal{D}}(\varphi(\boldsymbol{y}))\right)\,. \tag{33}$$

And since $\mathcal{C} * \mathcal{I}$ is a subcode of a BCH code with designed minimum distance D, the decoder $\mathcal{D}$ can be efficiently implemented. In fact, we can obtain a fairly efficient decoder for $\mathcal{C}$ (with a slow-down by a factor of $q-1$) also when $\mathcal{I}$ is not equidistant: we compute $\boldsymbol{c}_\mu = \mu^{-1} \cdot \varphi^{-1}(\tilde{\mathcal{D}}(\varphi(\mu \cdot \boldsymbol{y})))$ for $\mu \in F^*$ until we reach a μ for which $\mathsf{w}_F(\boldsymbol{y} - \boldsymbol{c}_\mu) \leq (d-1)/2$.

The scheme (33) generalizes to the case where $\mathcal{D}$ and $\tilde{\mathcal{D}}$ are list decoders for the respective codes (and where the definition of $\varphi(\cdot)$ is extended to sets in the obvious manner). Specifically, $\mathcal{D}$ is a list-L decoder for $\mathcal{C}$ with decoding radius τ, whenever $\tilde{\mathcal{D}}$ is a list-L decoder for $\mathcal{C} * \mathcal{I}$ with decoding radius (at least) $\Delta \cdot \tau$. There are known efficient list decoding algorithms for $\mathcal{C} * \mathcal{I}$ that reach the Johnson decoding radius [6], i.e., the decoding radius can be any positive integer $\tilde{\tau}$ that satisfies

$$\frac{L+1}{L}\left(2\tilde{\tau} - \frac{r}{r-1} \cdot \frac{\tilde{\tau}^2}{\ell n}\right) < D\,.$$

Substituting $\tilde{\tau} = \Delta \cdot \tau$ in the latter equation and recalling the definition of Δ, we obtain

$$\frac{L+1}{L}\left(2\tau - \frac{q}{q-1} \cdot \frac{\tau^2}{n}\right) < \frac{D}{\Delta}\,.$$

Hence, if $D = \Delta \cdot d$, then the scheme (33) defines, in effect, a list decoder for $\mathcal{C}$ that attains the Johnson radius (when stated for the alphabet size q of $\mathcal{C}$). Now, while in (10) we set D to the (smaller) value $\Delta(d-1)+1$, for all the constructions over $\mathrm{GF}(4)$ and $\mathrm{GF}(8)$ that were presented in Section III, we could replace (10) by the equality $D = \Delta \cdot d$, without affecting the constructions[5] (see Remarks 5 and 6).

Appendix A
Equivalent characterization of the set of roots

We present here an equivalent formulation of the sets $\mathcal{R}_j$, as defined in (12), which expresses their elements somewhat more explicitly. For each $j \in [h\rangle$, let $u_j \in \mathbb{Z}$ and $v_j \in [\ell\rangle$ be (uniquely) defined by

$$r^j w n - b = u_j \ell + v_j\,.$$

We then have:

$$\begin{aligned}\mathcal{R}_j &= \big\{i \in [n\rangle \,:\, r^j i\ell \equiv (\sigma - u_j\ell - v_j) \pmod{(\ell n)},\\ &\qquad \text{for some } \sigma \in [D-1\rangle\big\}\\ &= \big\{i \in [n\rangle \,:\, r^j i\ell \equiv (\tau - u_j)\ell \pmod{(\ell n)},\\ &\qquad \text{for some } \tau \in [(D-1-v_j)/\ell\rangle\big\}\,,\end{aligned}$$

namely,

$$\begin{aligned}\mathcal{R}_j &= \big\{i \in [n\rangle \,:\, i \equiv (r^j)^{-1}\vartheta \pmod n,\\ &\qquad \text{for some } \vartheta \in [-u_j, (D-1-v_j)/\ell - u_j\rangle\big\}\,,\end{aligned}$$

where $(r^j)^{-1}$ stands for the inverse of r^j in $\mathbb{Z}_n^*$. By Remark 1, the inverse $(r^j)^{-1}$ can be replaced by r^{h-j}.

Appendix B
Proof of Proposition 4

For $j \in [h\rangle$ and $x \in \mathbb{N}$, let $\mathcal{T}_j(x, w)$ be obtained by substituting $b \leftarrow 0$ and $D \leftarrow x + 2$ in (11), namely,

$$\mathcal{T}_j(x, w) = \big\{s \in [x+1\rangle \,:\, s \equiv r^j w n \pmod \ell\big\}\,.$$

[5]Clearly, the *true* minimum distance of $\mathcal{C} * \mathcal{I}$ is at least $\Delta \cdot d$. Yet, to claim efficiency of the decoding algorithm, we need to consider the *designed* minimum distance of $\mathcal{C} * \mathcal{I}$.

Also, let

$$\mathcal{T}(x,w) = \bigcup_{j\in[h\rangle} \mathcal{T}_j(x,w)$$

and

$$\mathcal{T}^*(x,w) = \left\{ s \in \mathcal{T}(x,w) \ : \ r \not| s \right\} .$$

Lemma 5. *When ℓ is a prime, for every $x \in \mathbb{N}$ there is an element $w^* = w^*(x)$ in $[1,\ell\rangle$ such that*

$$|\mathcal{T}^*(x,w^*)| \leq \frac{h}{\ell-1}\left(\mathsf{f}_r(x) - \mathsf{f}_r\Big(\Big\lfloor \frac{x}{\ell} \Big\rfloor\Big)\right) .$$

Proof. We start by computing the expected value of the size of $\mathcal{T}_j(x,w)$, when w is regarded as a random variable uniformly distributed over $[1,\ell\rangle$.

Write $x = \ell\cdot a + z$, where $a \in \mathbb{Z}$ and $z \in [\ell\rangle$. For every given $j \in [h\rangle$,

$$\mathsf{E}_w\left\{|\mathcal{T}_j(x,w)|\right\} = \frac{z}{\ell-1}\cdot(a+1) + \frac{\ell-1-z}{\ell-1}\cdot a = a + \frac{z}{\ell-1} .$$

Therefore,

$$\mathsf{E}_w\left\{|\mathcal{T}(x,w)|\right\} = \sum_{j\in[h\rangle} \mathsf{E}_w\left\{|\mathcal{T}_j(x,w)|\right\} = h\cdot\left(a + \frac{z}{\ell-1}\right) . \tag{34}$$

Next, consider the set

$$\mathcal{L}(x) = \left\{ s \in [x+1\rangle \ : \ r \,|\, s \text{ and } \ell \not| s \right\} ,$$

which is of size

$$|\mathcal{L}(x)| = \Big\lfloor \frac{x}{r} \Big\rfloor - \Big\lfloor \frac{1}{r}\Big\lfloor \frac{x}{\ell}\Big\rfloor \Big\rfloor = \Big\lfloor \frac{\ell\cdot a + z}{r} \Big\rfloor - \Big\lfloor \frac{a}{r} \Big\rfloor . \tag{35}$$

For every given $j \in [h\rangle$ and $s \in \mathcal{L}(x)$ we have

$$\mathsf{Prob}_w\left\{ s \in \mathcal{T}_j(x,w)\right\} = \frac{1}{\ell-1}$$

and, so,

$$\begin{aligned} &\mathsf{E}_w\left\{|\mathcal{T}(x,w)\cap\mathcal{L}(x)|\right\} \\ &\quad = \sum_{j\in[h\rangle}\sum_{s\in\mathcal{L}(x)} \mathsf{Prob}_w\left\{ s \in \mathcal{T}_j(x,w)\right\} \\ &\quad = \frac{h}{\ell-1}\cdot|\mathcal{L}(x)| . \end{aligned} \tag{36}$$

Combining (34)–(36) we obtain

$$\begin{aligned} &\mathsf{E}_w\left\{|\mathcal{T}^*(x,w)|\right\} \\ &\quad = \mathsf{E}_w\left\{|\mathcal{T}(x,w)\setminus\mathcal{L}(x)|\right\} \\ &\quad = \mathsf{E}_w\left\{|\mathcal{T}(x,w)|\right\} - \mathsf{E}_w\left\{|\mathcal{T}(x,w)\cap\mathcal{L}(x)|\right\} \\ &\quad = h\cdot\left(a+\frac{z}{\ell-1}\right) \\ &\qquad - \frac{h}{\ell-1}\left(\Big\lfloor\frac{\ell\cdot a+z}{r}\Big\rfloor - \Big\lfloor\frac{a}{r}\Big\rfloor\right) . \end{aligned}$$

Therefore, there is a choice $w^* \in [1,\ell\rangle$ such that the respective set $\mathcal{T}^*(x,w^*)$ satisfies

$$\begin{aligned} &|\mathcal{T}^*(x,w^*)| \\ &\quad \leq h\cdot\left(a+\frac{z}{\ell-1}\right) - \frac{h}{\ell-1}\left(\Big\lfloor\frac{\ell\cdot a+z}{r}\Big\rfloor - \Big\lfloor\frac{a}{r}\Big\rfloor\right) \\ &\quad = \frac{h}{\ell-1}\left(\ell\cdot a + z - \Big\lfloor\frac{\ell\cdot a+z}{r}\Big\rfloor - a + \Big\lfloor\frac{a}{r}\Big\rfloor\right) \\ &\quad = \frac{h}{\ell-1}\left(x - \Big\lfloor\frac{x}{r}\Big\rfloor + \Big\lfloor\frac{x}{\ell}\Big\rfloor - \Big\lfloor\frac{1}{r}\Big\lfloor\frac{x}{\ell}\Big\rfloor\Big\rfloor\right) \\ &\quad = \frac{h}{\ell-1}\left(\mathsf{f}_r(x) - \mathsf{f}_r\Big(\Big\lfloor\frac{x}{\ell}\Big\rfloor\Big)\right) , \end{aligned} \tag{37}$$

as claimed. □

Lemma 6. *When ℓ is a prime, for every $x \in \mathbb{N}$ there is an element $w^* = w^*(x)$ in $[1,\ell\rangle$ such that*

$$|\mathcal{T}^*(x,w^*)| \leq \frac{r-1}{r\ell}\cdot(x+2)\cdot h . \tag{38}$$

Furthermore, when $x \equiv -1 \pmod{\ell}$ and $\lfloor x/\ell \rfloor \equiv -1 \pmod{r}$, then

$$|\mathcal{T}^*(x,w^*)| \leq \frac{r-1}{r\ell}\cdot(x+1)\cdot h . \tag{39}$$

Proof. By (37), in order to prove (38), it suffices to show that

$$\begin{aligned} a + \frac{z}{\ell-1} - \frac{1}{\ell-1}\left(\Big\lfloor\frac{\ell\cdot a+z}{r}\Big\rfloor - \Big\lfloor\frac{a}{r}\Big\rfloor\right) \\ \leq \frac{(r-1)(\ell\cdot a+z+2)}{r\ell} . \end{aligned}$$

Equivalently,

$$\begin{aligned} &\frac{(\ell-1)\cdot a}{r} + \Big\lfloor\frac{a}{r}\Big\rfloor \\ &\quad \leq \Big\lfloor\frac{\ell\cdot a+z}{r}\Big\rfloor + 2 - \frac{(r+\ell-1)(z+2)}{r\ell} . \end{aligned} \tag{40}$$

To establish (40), we assume first that $z \leq \ell-2$. Since

$$\Big\lfloor\frac{\ell\cdot a+z}{r}\Big\rfloor \geq \frac{\ell\cdot a+z}{r} - \frac{r-1}{r} ,$$

we get that (40) is implied by

$$\begin{aligned} &\frac{(\ell-1)\cdot a}{r} + \frac{a}{r} \\ &\quad \leq \frac{\ell\cdot a+z}{r} - \frac{r-1}{r} + 2 - \frac{(r+\ell-1)(z+2)}{r\ell} . \end{aligned} \tag{41}$$

The terms in (41) that depend on a cancel out, which allows to easily verify that (41) holds whenever $z \leq \ell-2$.

We assume now that $z = \ell-1$, in which case (40) reduces to

$$\begin{aligned} &\frac{(\ell-1)\cdot a}{r} + \Big\lfloor\frac{a}{r}\Big\rfloor \\ &\quad \leq \Big\lfloor\frac{\ell\cdot a+\ell-1}{r}\Big\rfloor + 2 - \frac{(r+\ell-1)(\ell+1)}{r\ell} . \end{aligned}$$

Next, we substitute $a = ur + v$, where $u \in \mathbb{Z}$ and $v \in [r\rangle$. The terms that depend on u cancel out and we are left with

$$\frac{(\ell-1)\cdot v}{r} + \Big\lfloor\frac{v}{r}\Big\rfloor \leq \Big\lfloor\frac{\ell\cdot v+\ell-1}{r}\Big\rfloor + 2 - \frac{(r+\ell-1)(\ell+1)}{r\ell} .$$

Obviously, $\lfloor v/r \rfloor = 0$. Multiplying by r and then adding $v+\ell-1$ to both sides yield

$$\ell\cdot v+\ell-1 \le r\cdot\Big\lfloor\frac{\ell\cdot v+\ell-1}{r}\Big\rfloor + 2r-\frac{(r+\ell-1)(\ell+1)}{\ell}+v+\ell-1\;,$$

which simplifies to

$$\Big(\ell\cdot(v+1)-1\Big)-r\cdot\Big\lfloor\frac{\ell\cdot(v+1)-1}{r}\Big\rfloor\le\frac{\ell-1}{\ell}\cdot(r-1)+v\;. \tag{42}$$

The left-hand side of (42) is the remainder of $\ell\cdot(v+1)-1$ when divided by r and, as such, it is at most $r-1$. Suppose first that this remainder equals $r-1$. This means that

$$\ell\cdot(v+1)-1\equiv r-1\pmod r\;,$$

namely, r divides $\ell\cdot(v+1)$. Yet this is possible if and only if $v=r-1$, in which case (42) clearly holds. In fact, substituting $z=\ell-1$ and $a=ur+r-1$ in (37) yields $(u+1)(r-1)\cdot h$, which, in turn, equals $((r-1)(x+1)/(r\ell))\cdot h$, thereby proving (39). Assuming now that the remainder on the left-hand side of (42) is at most $r-2$, we get that (42) holds if either

$$r-2\le\frac{\ell-1}{\ell}\cdot(r-1)+v \tag{43}$$

or

$$\ell\cdot(v+1)-1\le\frac{\ell-1}{\ell}\cdot(r-1)+v\;. \tag{44}$$

And, indeed, (43) is satisfied when $v+1\ge(r-1)/\ell$, and (43) is satisfied when $v+1\le(r-1)/\ell$. □

Proof of Proposition 4. We have

$$|\mathcal{S}^*|=|\mathcal{S}^*\cap\mathbb{Z}^-|+|\mathcal{S}^*\cap\mathbb{Z}^+|=|\mathcal{T}^*(-b)|+|\mathcal{T}^*(b+D-2)|\;.$$

The sought bounds then follow from Lemmas 5 and 6. □

Appendix C
Further improvements for GF(4) and GF(8)

We start by providing an improved upper bound on the redundancy of Construction A in Section III, for the case where $d\equiv 2\pmod 3$. Specifically, we show that in this case, the upper bound (27) can be improved to (28), if we use (24) and select $b\equiv 2$ or $3\pmod 6$.

Write $d=3u+2$ and $b=z-6y$, where $u,y\in\mathbb{Z}^+$ and $z\in\{2,3\}$. Here $b+D-2=6u-6y+z+1$, and, so, by (24):

$$\begin{aligned}|\mathcal{S}^*| &\le \mathsf{f}_2\,(6y-z)-\mathsf{f}_2\Big(\Big\lfloor\frac{6y-z}{3}\Big\rfloor\Big)\\ &\qquad+\mathsf{f}_2\,(6u-6y+z+1)-\mathsf{f}_2\Big(\Big\lfloor\frac{6u-6y+z+1}{3}\Big\rfloor\Big)\\ &= (3y-1)-y+(3u-3y+2)-(u-y+1)\\ &= 2u=\frac{2d-4}{3}\;.\end{aligned}$$

The elements of $\mathcal{S}^*$ in this case are the integers in the interval $[z-6y,6u-6y+z+2\rangle$ that are neither even nor multiples of 3. This means that the first (smallest) element in $\mathcal{S}^*$ is $5-6y$ and the last element is $6u-6y+1$.

Turning to Construction B in Section III, we next show that for $d\equiv 5\pmod 6$, the upper bound (29) can be improved to (30). Writing $d=6u+5$ and substituting $b\leftarrow 0$ and $D\leftarrow d+1=6u+6$ in (24), we get:

$$\begin{aligned}|\mathcal{S}^*| &\le \mathsf{f}_2\,(6u+4)-\mathsf{f}_2\Big(\Big\lfloor\frac{6u+4}{3}\Big\rfloor\Big)\\ &= (3u+2)-(u+1)\\ &= 2u+1=\frac{d-2}{3}\;.\end{aligned}$$

Finally we turn to Construction C and show that when $d\equiv 2\pmod 7$, the bound (31) can be improved to (32), by selecting b so that its remainder modulo 14 is in $[4,8\rangle$.

Write $d=7u+2$ and $b=z-14y$, where $u,y\in\mathbb{Z}^+$ and $z\in[4,8\rangle$. Here $b+D-2=28u-14y+z+3$, and, so, by (24):

$$\begin{aligned}|\mathcal{S}^*| &\le \frac{3}{6}\Big(\mathsf{f}_2\,(14y-z)-\mathsf{f}_2\Big(\Big\lfloor\frac{14y-z}{7}\Big\rfloor\Big)\\ &\qquad+\mathsf{f}_2\,(28u-14y+z+3)-\mathsf{f}_2\Big(\Big\lfloor\frac{28u-14y+z+3}{7}\Big\rfloor\Big)\Big)\\ &= \frac{1}{2}\Big((7y-\lfloor z/2\rfloor)-y\\ &\qquad+(14u-7y+\lceil(z+3)/2\rceil)-(2u-y+1)\Big)\\ &= 6u+\frac{1}{2}=\frac{6d-12}{7}+\frac{1}{2}\;,\end{aligned}$$

i.e., there exists a choice $w\in[1,7\rangle$ such that

$$|\mathcal{S}^*|\le\frac{6d-12}{7}\;. \tag{45}$$

There are two cyclotomic cosets modulo 7 w.r.t. GF(2), namely, $\{1,2,4\}$ and $\{3,5,6\}$, and it remains to determine which one we need to select w from so as to achieve (45) (see Remark 3). In other words, we need to find w which minimizes

$$\Big|\big\{\text{odd } s\in[b,b+D-1\rangle\;:\;s\equiv 2^j wn\pmod 7,\ \text{for some } j\in[3\rangle\big\}\Big|\;.$$

Recalling that $D-1=4d-4=28u+4\equiv 4\pmod{14}$, this is equivalent to minimizing

$$\Big|\big\{\text{odd } s\in[z-14,z+4\rangle\;:\;s\equiv 2^j wn\pmod 7,\ \text{for some } j\in[3\rangle\big\}\Big|\;.$$

A simple check reveals that when $z\in\{4,5\}$, we should select w so that the remainder of wn modulo 7 is in $\{1,2,4\}$, and when $z\in\{6,7\}$, that remainder should be in $\{3,5,6\}$. As a matter of fact, such a check shows that (45) can be achieved for the larger range $z\in[2,9\rangle$ (the averaging argument in the proof of Lemma 5 renders (24) too crude to imply that). Moreover, for $z\in\{2,6\}$, the construction would remain the same even when the interval $[b,b+D-1\rangle$ in (11) were replaced by $[b,b+D'-1\rangle$, where $D'=D+3=4d$.

References

[1] E.R. Berlekamp, J. Justesen, "Some long cyclic linear binary codes are not so bad," *IEEE Trans. Inf. Theory*, 20 (1974), 351–356.

[2] I.I. Dumer, "Nonbinary codes with distances 4, 5, and 6 of cardinality greater than the BCH codes," *Probl. Peredachi Inf.*, 24 (1988), no. 3, 42–54.

[3] I.I. Dumer, "Nonbinary double-error-correcting codes designed by means of algebraic varieties," *IEEE Trans. Inf. Theory*, 41 (1995), 1657–1666.

[4] I.I. Dumer, V.A. Zinoviev, "Some new maximal codes over GF(4)," *Probl. Peredachi Inf.*, 14 (1978), no. 3, 24–34.
[5] J.S. Ellenberg, D. Gijswijt, "On large subsets of $\mathbb{F}_q^n$ with no three-term arithmetic progression," preprint.
[6] R. Koetter, A. Vardy, "Algebraic soft-decision decoding of Reed–Solomon codes," *IEEE Trans. Inf. Theory*, 49 (2003), 2809–2825.
[7] F.J. MacWilliams, N.J.A. Sloane, *The Theory of Error-Correcting Codes,* North-Holland, Amsterdam, 1977.
[8] 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.

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. Currently, A. Zeh is a post-doctoral researcher at Technion–Israel Institute of Technology. His research interests include coding and information theory, signal processing, telecommunications and the implementation of fast algorithms on FPGAs.