Bounds on Mixed Codes with Finite Alphabets

Yonatan Yehezkeally*, **Haider Al Kim***†, **Sven Puchinger**‡, and **Antonia Wachter-Zeh***
*School of Computation, Information and Technology, Technical University of Munich, 80333 Munich, Germany
†Department of Electrical and Communication Engineering, University of Kufa, Iraq
‡Hensoldt Sensors GmbH, 89077 Ulm, Germany

***Abstract*—Mixed codes, which are error-correcting codes in the Cartesian product of different-sized spaces, model degrading storage systems well. While such codes have previously been studied for their algebraic properties (e.g., existence of perfect codes) or in the case of unbounded alphabet sizes, we focus on the case of finite alphabets, and generalize the Gilbert-Varshamov, sphere-packing, Elias-Bassalygo, and first linear programming bounds to that setting. In the latter case, our proof is also the first for the non-symmetric mono-alphabetic q-ary case using Navon and Samorodnitsky's Fourier-analytic approach.**

I. Introduction

In traditional coding theory, one generally studies codes where every coordinate is over the same alphabet (e.g., binary– or, more generally, q-ary–codes). A rich body of knowledge has been developed regarding constructions, and bounds on the parameters, of such error-correcting codes.

However, in some circumstances this assumption might not hold. Sidorenko et al. [20] suggested that this is the case in orthogonal-frequency-division-multiplexing (OFDM) transmission; it can also be viewed as a relaxation of the partially-stuck-cell setting [1], where both sender and receiver are aware (e.g., thorough periodic sampling) of which coordinates have smaller alphabets. The authors further believe that this generalization of classical error correction is of independent theoretical interest (see, e.g., their study in [5, Ch. 7]).

Codes for the setting of varying alphabet sizes are named *mixed*- (or *polyalphabetic*-) codes, and have been studied in the past. In comparison to [6], [9]–[11], [14], [19], the codes we consider are not necessarily perfect, and therefore can correct more than a single error. On the other hand, [20] generalized the Singleton bound to mixed codes, and presented constructions of MDS codes, based on this bound and known MDS "mother codes", by letting alphabet sizes grow with respect to the code block size. Similarly, [5, Cha. 7.3] constructed diameter-perfect mixed codes that meet a code-anticode bound proven therein, which also rely on unbounded alphabet sizes. A special class of mixed codes, termed error-block codes, were also studied in [7], [15], [21]. In contrast to these, we study the setting where alphabet sizes are bounded.

The rest of this manuscript is organized as follows. In Section II, we summarize the main contributions of this work. In Section III we present definitions and notations. Then, in Section IV we study the size of Hamming spheres in this space; in Section V we observe the list-decoding capabilities of mixed codes by generalizing the first Johnson bound, and in Section VI we develop lower- and upper bounds on the sizes of mixed codes. Finally, in Section VII we demonstrate that our bounds improve upon the known bound of [20, Th. 2], [5, Cor. 2.15] in some settings.

This project has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement No. 801434). Y. Yehezkeally was supported by a Carl Friedrich von Siemens postdoctoral research fellowship of the Alexander von Humboldt Foundation.

II. Main contribution

Our contributions in this work are as follows:

(i) While [20] presented a Gilbert-Varshamov lower bound and a sphere-packing upper bound based on a straightforward expression for sphere size, containing an exponential number of terms, we develop a recursive formula for the size of spheres which enables one to efficiently compute exact sizes in any given case, resulting in said bounds on code sizes.

(ii) We develop closed-form upper and lower bounds on the size of spheres, yielding asymptotic expressions for the size of balls which readily lend themselves to closed-form statements of the asymptotic Gilbert-Varshamov and sphere-packing bounds (more precisely, lower and upper bounds on these, respectively).

(iii) In comparison to a known bound ([20, Th. 2] and [5, Cor. 2.15], which curiously develop the same bound in this context), we develop the equivalence of the Elias-Bassalygo bound (in [2], and reported in [12]) and the first linear-programming (LP) bound [13], [16] for mixed codes, which we show are tighter, for codes with some minimum distances, when alphabet sizes are bounded. In particular, our treatment of the LP bound relies on Navon and Samorodnitsky's Fourier analysis approach [17]; to our knowledge its restriction to fixed alphabet size is the first time that a proof for the bound in the general q-ary case (e.g., not only symmetric codes) is suggested using these methods.

III. Preliminaries

The pertinent space is defined as follows. For $n \in \mathbb{N}$, take some $1 < q_1 \leqslant q_2 \leqslant \ldots \leqslant q_n$. For convenience we denote $[n] = \{1, 2, \ldots, n\}$. We let $\mathcal{Q} \triangleq \prod_{i=1}^{n} (\mathbb{Z}/q_i\mathbb{Z})$. This Cartesian product should be interpreted as a (finite) product of (finite) cyclic groups, with the resulting structure of a finite Abelian group.

We endow $\mathcal{Q}$ with the Hamming metric, defined $d(x,y) \triangleq \mathrm{wt}(x-y)$, where $\mathrm{wt}(x) \triangleq |\mathrm{supp}(x)|$. We denote the *sphere of radius* r *around* $x \in \mathcal{Q}$ in this metric by $S_r(x) \triangleq \{y \in \mathcal{Q} : d(x,y) = r\}$, and the *ball of radius* r *around* $x \in \mathcal{Q}$ by $B_r(x) \triangleq \{y \in \mathcal{Q} : d(x,y) \leqslant r\}$. We say a *code* $C \subseteq \mathcal{Q}$ has *minimum distance* d if for all $x, y \in C$, $x \neq y$ implies $d(x,y) \geqslant d$. Let $A(n,d), A_r(n,d), A_{\leqslant r}(n,d)$ denote the maximum size of code in $\mathcal{Q}, S_r(0), B_r(0)$ respectively, with minimal Hamming distance d.

The *rate* of a code $C \subseteq \mathcal{Q}$ is defined by $R(C) \triangleq \frac{\log|C|}{\log|\mathcal{Q}|}$. For $0 \leqslant \delta \leqslant 1$ we shall be interested in the *maximum achievable rate*

$$R(\delta) \triangleq \frac{\log A(n, \lfloor \delta n \rfloor)}{\log|\mathcal{Q}|}. \tag{1}$$

We will also be interested in an asymptotic analysis of $R(\delta)$ as n grows to infinity; in these cases, we shall assume $\{q_i\}$ is sampled from a fixed set of alphabet sizes, where the incidence of each value is proportional to n.

Finally, we make the following notation for the arithmetic and geometric means of the alphabet sizes $\{q_i\}_{i=1}^n$:

$$\hat{q}_{\mathtt{a}} \triangleq \frac{1}{n}\sum_{i=1}^n q_i; \qquad \hat{q}_{\mathtt{g}} \triangleq \left(\prod_{i=1}^n q_i\right)^{1/n}, \tag{2}$$

as well as geometric and harmonic means of $\{q_i - 1\}_{i=1}^n$:

$$\hat{q}_{\mathtt{mg}} \triangleq \left(\prod_{i=1}^n (q_i - 1)\right)^{1/n} + 1; \qquad \hat{q}_{\mathtt{mh}} \triangleq \frac{n}{\sum_{i=1}^n \frac{1}{q_i - 1}} + 1. \tag{3}$$

(Note that in our notation $\hat{q}_{\mathtt{mg}} - 1, \hat{q}_{\mathtt{mh}} - 1$ are the geometric and harmonic means of $\{q_i - 1\}_{i=1}^n$, respectively; further, $\hat{q}_{\mathtt{a}} - 1$ is its arithmetic mean.)

Observe that $\hat{q}_{\mathtt{a}} \geqslant \hat{q}_{\mathtt{g}} \geqslant \hat{q}_{\mathtt{mg}} \geqslant \hat{q}_{\mathtt{mh}}$. Further, if n grows and $\{q_i\}_{i=1}^n$ is sampled as described above, $\hat{q}_{\mathtt{a}}, \hat{q}_{\mathtt{g}}, \hat{q}_{\mathtt{mg}}, \hat{q}_{\mathtt{mh}}$ are fixed with respect to n.

IV. Size of Spheres

In this section, we study the size of spheres $S_r(x)$ in Hamming distance on $\mathcal{Q}$. Since the Hamming distance is shift-invariant, we denote the size of the Hamming sphere $s_r \triangleq |S_r(0)|$, for $0 \leqslant r \leqslant n$. It was noted in [20, Eq. 5] that $s_r = \sum_{1 \leqslant i_1 < i_2 < \ldots < i_r \leqslant n} \prod_{j=1}^r (q_{i_j} - 1)$; however, this expression contains an exponential number of summands, and is challenging to work with. In this section, we instead develop a recursive expression for s_r, which can be evaluated in polynomial time, as well as develop bounds on it.

For convenience, we also denote for all $I \subseteq [n]$, $S_r(I) \triangleq \{x \in S_r(0) : \mathrm{supp}(x) \subseteq I\}$ and $s_r(I) \triangleq |S_r(I)|$ (so that $s_r = s_r([n])$). Then, observe the following:

Lemma 1 *1) For all* $0 \leqslant r \leqslant n$, $\sum_{i \in [n]} s_r([n] \setminus \{i\}) = (n-r)s_r$.

2) For all $0 \leqslant r < n$, $\sum_{i \in [n]} (q_i - 1)s_r([n] \setminus \{i\}) = (r+1)s_{r+1}$.

3) For all $0 \leqslant r < n-1$, $\sum_{i \in [n]} (q_i - 1)^2 s_r([n] \setminus \{i\}) = n(\hat{q}_{\mathtt{a}} - 1)s_{r+1} - (r+2)s_{r+2}$.

Proof:

1) Observe for $x \in S_r(0)$ that $x \in S_r([n] \setminus \{i\})$ if and only if $i \in \mathrm{supp}(x)$.
2) We note
$$(q_i - 1)s_r([n] \setminus \{i\}) = |\{x \in S_{r+1}(0) : i \in \mathrm{supp}(x)\}|.$$
3) Observe
$$\begin{aligned}
&\sum_{i \in [n]} (q_i - 1)^2 s_r([n] \setminus \{i\}) \\
&\quad = n(\hat{q}_{\mathtt{a}} - 1)s_{r+1} \\
&\qquad - \sum_{i \in [n]} (q_i - 1)(s_{r+1} - (q_i - 1)s_r([n] \setminus \{i\})) \\
&\quad = n(\hat{q}_{\mathtt{a}} - 1)s_{r+1} - \sum_{i \in [n]} (q_i - 1)s_{r+1}([n] \setminus \{i\}) \\
&\quad = n(\hat{q}_{\mathtt{a}} - 1)s_{r+1} - (r+2)s_{r+2}.
\end{aligned}$$
∎

Theorem 2 *It holds that* $s_0 = 1$, *and for* $0 < r \leqslant n$,

$$s_r = \frac{1}{r}\sum_{k=0}^{r-1} (-1)^k s_{r-1-k} \sum_{i \in [n]} (q_i - 1)^{k+1}.$$

Proof: That $s_0 = 1$ is immediate. Then, for $0 < r \leqslant n$ and $1 \leqslant i \leqslant n$, we note

$$\begin{aligned}
s_r([n] \setminus \{i\}) &= s_r([n]) - (q_i - 1)s_{r-1}([n] \setminus \{i\}) \\
&= s_r([n]) - (q_i - 1)\big(s_{r-1}([n]) \\
&\qquad - (q_i - 1)s_{r-2}([n] \setminus \{i\})\big) \\
&= \ldots = \sum_{k=0}^{r} (-1)^k (q_i - 1)^k s_{r-k}.
\end{aligned}$$

Hence from part 2 of Lemma 1,

$$\begin{aligned}
s_r &= \frac{1}{r}\sum_{i \in [n]} (q_i - 1)s_{r-1}([n] \setminus \{i\}) \\
&= \frac{1}{r}\sum_{i \in [n]}\sum_{k=0}^{r-1} (-1)^k (q_i - 1)^{k+1} s_{r-1-k} \\
&= \frac{1}{r}\sum_{k=0}^{r-1} (-1)^k s_{r-1-k} \sum_{i \in [n]} (q_i - 1)^{k+1}.
\end{aligned}$$
∎

Observe that Theorem 2 suggests a polynomial-run-time algorithm for computing s_r and $|B_r(x)| = \sum_{k=0}^r s_k$.

Theorem 3 *For* $0 \leqslant r < n$, *the ratio* $\frac{(r+1)s_{r+1}}{(n-r)s_r}$ *is decreasing in* r*; in particular,*

$$\frac{(\hat{q}_{\mathtt{mh}} - 1)(n-r)}{r+1} \leqslant \frac{s_{r+1}}{s_r} \leqslant \frac{(\hat{q}_{\mathtt{a}} - 1)(n-r)}{r+1}.$$

Proof: Firstly, observe that $\frac{s_1}{s_0} = n(\hat{q}_{\mathtt{a}} - 1)$ and $\frac{s_n}{s_{n-1}} = \frac{\hat{q}_{\mathtt{mh}} - 1}{n}$, achieving the upper and lower bounds, respectively. Hence the latter part of the claim follows from the former.

Next, substitute in the sequel $a_i \triangleq q_i - 1$ and $b_i \triangleq s_r([n] \setminus \{i\})$, and observe that a_i (b_i) is monotone non-decreasing (non-increasing, respectively). Assume to the contrary that $\frac{(r+2)s_{r+2}}{(n-r-1)s_{r+1}} > \frac{(r+1)s_{r+1}}{(n-r)s_r}$ for some $0 \leqslant r \leqslant n-2$; it follows that

$$(n-r)(r+1)(r+2)s_{r+2}s_r > (n-r-1)(r+1)^2 s_{r+1}^2,$$

and from parts 1 to 3 of Lemma 1 this is equivalent to

$$\left(\sum_{i\in[n]} b_i\right)\left(\left(\sum_{i\in[n]} a_i\right)\left(\sum_{i\in[n]} a_i b_i\right) - (r+1)\sum_{i\in[n]} a_i^2 b_i\right) > (n-r-1)\left(\sum_{i\in[n]} a_i b_i\right)^2.$$

Rearranging, we have

$$\left(\sum_{i,j\in[n]} a_i b_i b_j \Big(\Big(\sum\nolimits_{k\in[n]} a_k\Big) - n a_j\Big)\right) > (r+1)\left(\sum_{i,j\in[n]} a_i b_i b_j (a_i - a_j)\right).$$

Observe that the right-hand side is non-negative, since

$$\begin{aligned}\sum_{i,j\in[n]} & a_i b_i b_j (a_i - a_j) \\ &= \frac{1}{2}\sum_{i,j\in[n]} \left(a_i b_i b_j (a_i - a_j) + a_j b_j b_i (a_j - a_i)\right) \\ &= \frac{1}{2}\sum_{i,j\in[n]} b_i b_j (a_i - a_j)^2 \geqslant 0.\end{aligned}$$

Hence, in particular,

$$\sum_{i,j\in[n]} a_i b_i b_j \Big(\Big(\sum\nolimits_{k\in[n]} a_k\Big) - n a_j\Big) > \sum_{i,j\in[n]} a_i b_i b_j (a_i - a_j),$$

which we rearrange to

$$\begin{aligned} 0 &< \sum_{i,j\in[n]} a_i b_i b_j \Big(\Big(\sum\nolimits_{k\in[n]} a_k\Big) - (n-1)a_j - a_i\Big) \\ &= \sum_{i,j\in[n]} \sum_{k\in[n]\setminus\{i\}} a_i b_i b_j (a_k - a_j) \\ &= \sum_{i,j,k\in[n]} a_i b_i b_j (a_k - a_j) - \sum_{i,j\in[n]} a_i b_i b_j (a_i - a_j) \\ &= \frac{1}{2}\sum_{i,j,k\in[n]} a_i b_i (b_j - b_k)(a_k - a_j) \\ &\quad - \frac{1}{2}\sum_{i,j\in[n]} b_i b_j (a_j - a_i)^2 \leqslant 0, \end{aligned}$$

in contradiction, where the last step follows from $(b_j - b_k)(a_k - a_j) \leqslant 0$ for all j, k. ■

We can now prove the following bounds on the size of spheres:

Theorem 4 *It holds that* $\binom{n}{r}\big(\hat{q}_{\mathtt{mg}} - 1\big)^r \leqslant s_r \leqslant \binom{n}{r}(\hat{q}_{\mathtt{a}} - 1)^r$.

Proof: For the right inequality, observe from Theorem 3 that

$$s_r = \prod_{k=0}^{r-1} \frac{s_{k+1}}{s_k} \leqslant \prod_{k=0}^{r-1} \frac{(\hat{q}_{\mathtt{a}} - 1)(n-k)}{k+1} = \binom{n}{r}(\hat{q}_{\mathtt{a}} - 1)^r.$$

On the other hand, from the arithmetic and geometric mean inequality we directly observe

$$\begin{aligned} s_r &= \sum_{\substack{R\subseteq[n]\\|R|=r}} \prod_{i\in R}(q_i - 1) \geqslant \binom{n}{r}\left(\prod_{\substack{R\subseteq[n]\\|R|=r}} \prod_{i\in R}(q_i - 1)\right)^{1/\binom{n}{r}} \\ &= \binom{n}{r}\left(\prod_{i=1}^{n}(q_i - 1)^{\binom{n-1}{r-1}}\right)^{1/\binom{n}{r}} = \binom{n}{r}\big(\hat{q}_{\mathtt{mg}} - 1\big)^r. \end{aligned}$$ ■

Conjecture 5 *Observe that* $s_1 = n(\hat{q}_{\mathtt{a}} - 1)$ *and* $s_n = \big(\hat{q}_{\mathtt{mg}} - 1\big)^n$*, achieving the upper and lower bounds of Theorem 4, respectively. We conjecture that* $\big(s_r/\binom{n}{r}\big)^{1/r}$ *is also decreasing, for* $1 \leqslant r \leqslant n$.

Corollary 6 *For* $0 \leqslant r \leqslant \Big(1 - \frac{1}{\hat{q}_{\mathtt{a}}}\Big)n$ *it holds that*

$$\tfrac{1}{n+1}\hat{q}_{\mathtt{mg}}^{\,nH_{\hat{q}_{\mathtt{mg}}}(r/n)} \leqslant |B_r(0)| \leqslant \hat{q}_{\mathtt{a}}^{\,nH_{\hat{q}_{\mathtt{a}}}(r/n)}.$$

where $H_q(x) = x\log_q(q-1) - x\log_q(x) - (1-x)\log_q(1-x)$ *is the* q*-ary entropy function.*

Proof: We rely on the well-known bounds on the size of the q-ary Hamming ball (see, e.g., [18, Lemmas 4.7-8]), and the bounds of Theorem 4. ■

V. Johnson radius and list-decodability

Definition 7 *For* $q > 1$ *and* $\delta < 1 - \frac{1}{q}$ *we denote the* Johnson radius

$$J_q(\delta) \triangleq \left(1 - \frac{1}{q}\right)\left(1 - \sqrt{1 - \frac{\delta}{1 - \frac{1}{q}}}\right).$$

Observe that $\frac{\delta}{2} \leqslant J_q(\delta) \leqslant \delta < 1 - \frac{1}{q}$. Essentially, for $r < J_q(d/n)\cdot n$ it holds that $qr^2 > (q-1)(2r-d)n$.

We next follow the approach of [2, Lem.], and attributed to Johnson in [8, Th. 7.3.1], to bound $A_r(n,d), A_{\leqslant r}(n,d)$:

Lemma 8 *If* $\hat{q}_{\mathtt{a}} r^2 > (\hat{q}_{\mathtt{a}} - 1)(2r-d)n$ *then*

$$A_r(n,d) \leqslant A_{\leqslant r}(n,d) \leqslant \frac{(\hat{q}_{\mathtt{a}} - 1)nd}{\hat{q}_{\mathtt{a}} r^2 - (\hat{q}_{\mathtt{a}} - 1)(2r-d)n}.$$

Proof: That $A_r(n,d) \leqslant A_{\leqslant r}(n,d)$ follows from the definitions. Denote then $A \triangleq A_{\leqslant r}(n,d)$, and build a matrix with A rows, each an element of a maximum-size code in $B_r(0)$. Hence

(a) Every row has at most r nonzero coordinates. (Here, the meaning of 0 depends on the column, but this fact has no effect on our argument, and will be ignored).

(b) The coordinate-wise difference of any two distinct rows has at least d nonzero coordinates.

For $1 \leqslant i \leqslant n$ and any $j \in \mathbb{Z}/q_i\mathbb{Z}$, we let $k_{i,j}$ denote the number of incidences of j in the i's column of our matrix. Then we observe

$$\sum_{i=1}^{n} \sum_{0\neq j\in\mathbb{Z}/q_i\mathbb{Z}} k_{i,j} \leqslant Ar; \qquad \sum_{i=1}^{n} \sum_{j\in\mathbb{Z}/q_i\mathbb{Z}} k_{i,j} = An.$$

We note that the total number of nonzero elements in the $A(A-1)$ differences of any two distinct rows (when order is considered) is $\sum_{i=1}^{n}\sum_{j\in\mathbb{Z}/q_i\mathbb{Z}} k_{i,j}(A-k_{i,j})$. This number is at least $A(A-1)d$, by assumption. Then, denoting $\rho \triangleq \frac{1}{A}\sum_{i=1}^{n}\sum_{0\neq j\in\mathbb{Z}/q_i\mathbb{Z}} k_{i,j} \leqslant r$,

$$\begin{aligned}
A(A-1)d &\leqslant \sum_{i=1}^{n} \sum_{j\in\mathbb{Z}/q_i\mathbb{Z}} k_{i,j}(A-k_{i,j}) \\
&= A\sum_{i=1}^{n} \sum_{j\in\mathbb{Z}/q_i\mathbb{Z}} k_{i,j} - \sum_{i=1}^{n} \sum_{0\neq j\in\mathbb{Z}/q_i\mathbb{Z}} k_{i,j}^2 - \sum_{i=1}^{n} k_{i,0}^2 \\
&\leqslant A^2 n - \frac{A^2\rho^2}{\sum_{i=1}^{n}(q_i-1)} - \frac{A^2(n-\rho)^2}{n},
\end{aligned}$$

where the last inequality uses Titu's lemma. By rearrangement of addends and multiplication by $\frac{(\hat{q}_{\mathsf{a}}-1)n}{A}$:

$$\begin{aligned}
&(\hat{q}_{\mathsf{a}}-1)nd \geqslant A\big[\hat{q}_{\mathsf{a}}\rho^2 - (\hat{q}_{\mathsf{a}}-1)(2\rho-d)n\big] \\
&\quad = A\left[(\hat{q}_{\mathsf{a}}-1)nd - \frac{(\hat{q}_{\mathsf{a}}-1)^2}{\hat{q}_{\mathsf{a}}}\left(n^2 - \left(n - \frac{\rho}{1-1/\hat{q}_{\mathsf{a}}}\right)^2\right)\right] \\
&\quad \geqslant A\left[(\hat{q}_{\mathsf{a}}-1)nd - \frac{(\hat{q}_{\mathsf{a}}-1)^2}{\hat{q}_{\mathsf{a}}}\left(n^2 - \left(n - \frac{r}{1-1/\hat{q}_{\mathsf{a}}}\right)^2\right)\right] \\
&\quad = A\big[\hat{q}_{\mathsf{a}}r^2 - (\hat{q}_{\mathsf{a}}-1)(2r-d)n\big].
\end{aligned}$$

The claim follows directly. ■

Corollary 9 *Take a code $C \subseteq \mathcal{Q}$ with minimum distance d, $0 < d < \left(1 - \frac{1}{\hat{q}_{\mathsf{a}}}\right)n$. For any $\rho \in \mathbb{N}$, $\rho < J_{\hat{q}_{\mathsf{a}}}(d/n)\cdot n$, and any $x \in \mathcal{Q}$, it holds that $|C \cap B_\rho(x)| \leqslant (\hat{q}_{\mathsf{a}}-1)dn$.*

Proof: From the shift-invariance of the Hamming distance, $C\cap B_\rho(x) = (C-x)\cap B_\rho(0)$, implying $|C\cap B_\rho(x)| \leqslant A_{\leqslant\rho}(n,d)$. Then, by assumption we have $\hat{q}_{\mathsf{a}}\rho^2 > (\hat{q}_{\mathsf{a}}-1)(2\rho-d)n$, and since all quantities are integers, $\hat{q}_{\mathsf{a}}\rho^2 \geqslant 1 + (\hat{q}_{\mathsf{a}}-1)(2\rho-d)n$. Finally, observe from Lemma 8 that $A_{\leqslant\rho}(n,d) \leqslant \frac{(\hat{q}_{\mathsf{a}}-1)nd}{\hat{q}_{\mathsf{a}}\rho^2-(\hat{q}_{\mathsf{a}}-1)(2\rho-d)n} \leqslant (\hat{q}_{\mathsf{a}}-1)nd$, as required. ■

The last corollary establishes a number of errors beyond $\left\lfloor\frac{d-1}{2}\right\rfloor$ in which codes with minimum distance d allow list-decoding with list size quadratic in n, although unique decoding is no longer assured. Indeed, we note from $J_{\hat{q}_{\mathsf{a}}}(\delta) > \frac{\delta}{2}$ that for sufficiently large n, $\rho \triangleq \lceil J_{\hat{q}_{\mathsf{a}}}(d/n)\cdot n\rceil - 1 > \left\lfloor\frac{d-1}{2}\right\rfloor$.

VI. Bounds

In this section, we explore generalizations of known bounds on mono-alphabetic q-ary codes. We first present the known 'Singleton-like' bound [20, Th. 2], which is also developed as a 'code-anticode' bound [5, Cor. 2.15] with the diameter-$(d-1)$ anticode $\left(\prod_{i=1}^{n-d+1}\{0\}\right) \times \left(\prod_{i=n-d+2}^{n}(\mathbb{Z}/q_i\mathbb{Z})\right)$:

Theorem 10 *If $C \subseteq \mathcal{Q}$ has minimum distance d, then*

$$|C| \leqslant \prod_{i=1}^{n-d+1} q_i.$$

Next, we start with a corollary of the bounds of the last section; these are asymptotic version of the Gilbert-Varshamov and sphere-packing bounds.

Corollary 11 *For $0 \leqslant \delta \leqslant 1 - \frac{1}{\hat{q}_{\mathsf{a}}}$ it holds that*

$$\begin{aligned}
1 - \tfrac{\log(\hat{q}_{\mathsf{a}})}{\log(\hat{q}_{\mathsf{g}})} H_{\hat{q}_{\mathsf{a}}}(\delta) + o(1) &\leqslant R(\delta) \\
&\leqslant 1 - \tfrac{\log(\hat{q}_{\mathsf{mg}})}{\log(\hat{q}_{\mathsf{g}})} H_{\hat{q}_{\mathsf{mg}}}(\tfrac{\delta}{2}) + o(1)
\end{aligned}$$

Proof: We utilize well-known proofs for these bounds (e.g., [18, Ch. 4.5]), based on Corollary 6. ■

A. Elias-Bassalygo bound

In this section we pursue a parallel to the Elias-Bassalygo bound for mixed codes. We start with a proof of the *Elias-Bassalygo inequality* (see, e.g., a corollary in [2, Eq. 5]), also referred to in [5, Eq. 2.2] as the *local inequality lemma*.

Lemma 12 *For all $r \leqslant n$, it holds that $A(n,d) \leqslant \frac{|\mathcal{Q}|}{s_r}A_r(n,d)$.*

Proof: Take some maximum size code $C \subseteq \mathcal{Q}$ with minimum distance d. We observe that for each $c \in C$, there exist exactly s_r distinct $x \in \mathcal{Q}$ such that $x + c \in S_r(0)$. It follows that $\sum_{x\in\mathcal{Q}}|(x+C)\cap S_r(0)| = s_r|C| = s_r A(n,d)$. By the pigeonhole principle there must exist $x \in \mathcal{Q}$ such that $|(x+C)\cap S_r(0)| \geqslant \frac{s_r A(n,d)}{|\mathcal{Q}|}$. Note that $(x+C)\cap S_r(0)$ is a code in $S_r(0)$ with minimum distance d (the Hamming distance is shift invariant), hence $A_r(n,d) \geqslant \frac{s_r A(n,d)}{|\mathcal{Q}|}$, as required. ■

Corollary 13 *For $d < \left(1-\frac{1}{\hat{q}_{\mathsf{a}}}\right)n$ and $r < J_{\hat{q}_{\mathsf{a}}}(d/n)\cdot n$ it holds that*

$$A(n,d) \leqslant \frac{|\mathcal{Q}|}{s_r}\cdot\frac{(\hat{q}_{\mathsf{a}}-1)nd}{\hat{q}_{\mathsf{a}}r^2 - (\hat{q}_{\mathsf{a}}-1)(2r-d)n}.$$

Proof: The claim follows from Lemmas 8 and 12. ■

Corollary 14 *For $\delta < \left(1-\frac{1}{\hat{q}_{\mathsf{a}}}\right)$ it holds that*

$$R(\delta) \leqslant 1 - \frac{\log(\hat{q}_{\mathsf{mg}})}{\log(\hat{q}_{\mathsf{g}})} H_{\hat{q}_{\mathsf{mg}}}(J_{\hat{q}_{\mathsf{a}}}(\delta)) + o(1).$$

Proof: We denote $d_n \triangleq \lfloor\delta n\rfloor$ and let $r_n \triangleq \left\lfloor\left(1-\frac{1}{\hat{q}_{\mathsf{a}}}\right)\left[1-\sqrt{1-\frac{(d_n-1)/n}{1-\frac{1}{\hat{q}_{\mathsf{a}}}}}\right]n\right\rfloor$; then by Corollary 13 $A(n,d_n) \leqslant \frac{|\mathcal{Q}|}{s_{r_n}}\cdot d_n$.

Next, by Theorem 4

$$\begin{aligned}\log A(n,d_n) &\leqslant \log|\mathcal{Q}| - \log\binom{n}{r_n} - r_n\log(\hat{q}_{\mathtt{mg}}-1) + \log(d_n)\\ &= \log|\mathcal{Q}| - (\log(2)nH_2(r_n/n) - O(\log n))\\ &\quad - r_n\log(\hat{q}_{\mathtt{mg}}-1) + \log(d_n)\\ &= \log|\mathcal{Q}| - \log(\hat{q}_{\mathtt{mg}})nH_{\hat{q}_{\mathtt{mg}}}(r_n/n) + O(\log n),\end{aligned}$$

which concludes the proof. ■

Before concluding, we observe from $J_{\hat{q}_{\mathtt{a}}}(\delta) > \frac{\delta}{2}$ that Corollary 14 is tighter than the sphere-packing upper bound of Corollary 11.

B. First linear-programming bound

We adapt techniques utilized in [3] for a Fourier analytic approach to the development of the first linear-programming bound on q-ary codes (first developed in the binary case by McEliece et al. [16] and later generalized by Levenshtein [13]), to the case of mixed codes. These methods draw on a similar treatment of the binary case in [17]. We stress that [3] proved the bound in the mono-alphabetic q-ary case for a class of *symmetric* codes (containing all linear codes, and, in the binary case, all codes); our analysis shows that this requirement can be dropped (since q-ary codes are a private case of our setting, our results directly apply to that case as well). We also choose to more rigorously treat the Fourier duality.

The Hamming metric on $\mathcal{Q}$ is fully represented by the graph on vertex set $\mathcal{Q}$, where $x, y \in \mathcal{Q}$ are connected by an (undirected) edge if and only if $d(x,y) = 1$. That is, for any $x, y \in \mathcal{Q}$ it holds that $d(x,y)$ is also the *graph distance* of x, y (i.e., the length of the shortest path in the graph between x, y). Motivated by this fact, throughout this section we let $\mathcal{A}$ be the *adjacency matrix* of this graph. By abuse of notation, we let $\mathcal{A}$ operate on functions $f\colon \mathcal{Q} \to \mathbb{C}$ by considering f to be an $|\mathcal{Q}|$-tuple over $\mathbb{C}$ (indexed identically to $\mathcal{A}$).

The purpose of this section is to develop an upper bound on $R(\delta)$, parallel to the first linear-programming bound. The methods we use rely on Fourier analysis in finite Abelian groups; due to space limitation, we delegate to an arXiv.org version of this manuscript [22] a review of basic notions, mostly based on [4], as well as proofs for two main propositions necessary for this section, Theorem 16 and Corollary 17.

Definition 15 *For a subset $B \subseteq \mathcal{Q}$, we define the* maximum eigenvalue of B *by*

$$\lambda_B \triangleq \max\left\{ \frac{\langle \mathcal{A}f\ ,\ f\rangle}{\langle f\ ,\ f\rangle} : f\colon \mathcal{Q}\to\mathbb{R},\ \mathrm{supp}(f)\subseteq B \right\}.$$

It is the maximum eigenvalue of the minor of $\mathcal{A}$ corresponding to B; i.e., the adjacency matrix of the subgraph of the Hamming graph spanned by the elements of B. Since the entries of $\mathcal{A}$ are non-negative, by Perron's theorem, λ_B is non-negative, greater than or equal to the absolute value of any other eigenvalue, and there exists a non-negative eigenfunction $f_B\colon \mathcal{Q}\to\mathbb{R}$, $f_B \geqslant 0$, of λ_B (that is, $\mathcal{A}f_B = \lambda_B f_B$).

Theorem 16 *Let $C \subseteq \mathcal{Q}$ be a code with minimum distance d. Take a symmetric $B \subseteq \mathcal{Q}$ such that $\lambda_B \geqslant (n+1)(\hat{q}_{\mathtt{a}}-1) - \sum_{i=1}^{d} q_i$. Then*

$$|C| \leqslant n|B|.$$

Corollary 17 *Take $2\sqrt{n} < r \leqslant n$. Then $\lambda_{B_r(0)} \geqslant 2\sqrt{(\hat{q}_{\mathtt{a}}-1)r(n-r)} + (\hat{q}_{\mathtt{a}}-2)r + o(n)$.*

Based on these results, we can now show the following.

Theorem 18 *Denote*

$$\rho = \frac{n}{\hat{q}_{\mathtt{a}}}\left((\hat{q}_{\mathtt{a}}-1) - (\hat{q}_{\mathtt{a}}-2)\check{\delta} - 2\sqrt{(\hat{q}_{\mathtt{a}}-1)\check{\delta}\big(1-\check{\delta}\big)} \right),$$

where $\check{\delta} \triangleq \frac{1}{\hat{q}_{\mathtt{a}}n}\sum_{i=1}^{d} q_i$. If $C \subseteq \mathcal{Q}$ has minimum distance d, then

$$\log|C| \leqslant n\log(\hat{q}_{\mathtt{a}})H_{\hat{q}_{\mathtt{a}}}(\rho/n) + o(n).$$

Proof: We find the solution in r to the equation $2\sqrt{(\hat{q}_{\mathtt{a}}-1)r(n-r)} + (\hat{q}_{\mathtt{a}}-2)r = (\hat{q}_{\mathtt{a}}-1)n - \sum_{i=1}^{d} q_i = (\hat{q}_{\mathtt{a}}-1)n - \hat{q}_{\mathtt{a}}n\check{\delta}$. Indeed, this equation holds if and only if

$$\begin{aligned}4(\hat{q}_{\mathtt{a}}-1)r(n-r) &= (\hat{q}_{\mathtt{a}}-2)^2 r^2\\ &\quad - 2(\hat{q}_{\mathtt{a}}-2)\big((\hat{q}_{\mathtt{a}}-1)n - \hat{q}_{\mathtt{a}}n\check{\delta}\big)r\\ &\quad + \big((\hat{q}_{\mathtt{a}}-1)n - \hat{q}_{\mathtt{a}}n\check{\delta}\big)^2\\ \iff\ 0 &= \hat{q}_{\mathtt{a}}^2 r^2\\ &\quad - 2n\hat{q}_{\mathtt{a}}\big((\hat{q}_{\mathtt{a}}-1) - (\hat{q}_{\mathtt{a}}-2)\check{\delta}\big)r\\ &\quad + n^2\big((\hat{q}_{\mathtt{a}}-1) - \hat{q}_{\mathtt{a}}\check{\delta}\big)^2.\end{aligned}$$

This implies the two solutions

$$r_\pm = \frac{n}{\hat{q}_{\mathtt{a}}}\left((\hat{q}_{\mathtt{a}}-1) - (\hat{q}_{\mathtt{a}}-2)\check{\delta} \pm 2\sqrt{(\hat{q}_{\mathtt{a}}-1)\check{\delta}\big(1-\check{\delta}\big)} \right)$$

(trivially, $\rho = r_- < r_+$). It follows from Theorem 16 and Corollary 17 that $|C| \leqslant n|B_r(0)|$ for $r = \rho + o(n)$, and from Corollary 6 we obtain the claim. ■

VII. Conclusion

In conclusion, we refer the reader to the arXiv.org version of this manuscript [22] for plots of the lower bound of Corollary 11 with the upper bounds of Corollary 14 and Theorem 18, in comparison to the known upper bound of Theorem 10, in some special cases. These demonstrate that our proven bounds compete with the known one for some choices of alphabet sizes and normalized minimum distance. In principle, our bounds are more competitive for smaller alphabet sizes (which can be expected, given that the Singleton bound is already competitive in the mono-alphabetic 64-ary case), and for distributions of alphabet sizes closer to the mono-alphabetic case.

A natural question is whether efficiently en-/decodable codes can be constructed to approach these bounds; we delegate an answer for this question to a future work.

References

[1] H. Al Kim, S. Puchinger, and A. Wachter-Zeh, "Error correction for partially stuck memory cells," in *2019 XVI International Symposium "Problems of Redundancy in Information and Control Systems" (REDUNDANCY)*, 2019, pp. 87–92.

[2] L. A. Bassalygo, "New upper bounds for error correcting codes," *Problems Inform. Transmission*, vol. 1, no. 4, pp. 32–35, 1965.

[3] S. Bhattacharya and A. Banerjee, "A Fourier analytic proof of the q-ary LP bound (undergradute project)," Nov. 2018, [Online; accessed 07-July-2021]. Available: https://sagnikb.github.io/assets/pdfs/Adversarial_Channels.pdf

[4] K. Conrad, "Characters of finite abelian groups (lecture notes)," 2010, [Online; accessed 07-July-2021]. Available: https://kconrad.math.uconn.edu/blurbs/grouptheory/charthy.pdf

[5] T. Etzion, *Perfect Codes and Related Structures*. WORLD SCIENTIFIC, 2022.

[6] T. Etzion and G. Greenberg, "Constructions for perfect mixed codes and other covering codes," *IEEE Trans. on Inform. Theory*, vol. 39, no. 1, pp. 209–214, Jan. 1993.

[7] K. Feng, L. Xu, and F. J. Hickernell, "Linear error-block codes," *Finite Fields and Their Applications*, vol. 12, no. 4, pp. 638–652, 2006, special Issue Celebrating Prof. Zhe-Xian Wan's 80th Birthday.

[8] V. Guruswami, A. Rudra, and M. Sudan, "Essential coding theory (book draft)," Mar. 2019, [Online; accessed 07-July-2021]. Available: https://cse.buffalo.edu/faculty/atri/courses/coding-theory/book/

[9] O. Heden, "A new construction of group and nongroup perfect codes," *Information and Control*, vol. 34, no. 4, pp. 314–323, 1977.

[10] M. Herzog and J. Schönheim, "Linear and nonlinear single-error-correcting perfect mixed codes," *Information and Control*, vol. 18, no. 4, pp. 364–368, May 1971.

[11] ——, "Group partition, factorization and the vector covering problem," *Canadian Mathematical Bulletin*, vol. 15, no. 2, p. 207–214, Jun. 1972.

[12] S. M. Johnson, "Improved asymptotic bounds for error-correcting codes," *IEEE Trans. on Inform. Theory*, vol. 9, no. 3, pp. 198–205, Jul. 1963.

[13] V. I. Levenshtein, "Universal bounds for codes and designs," in *Handbook of coding theory*, V. Pless and W. C. Huffman, Eds. Amsterdam: Elsevier, 1998, pp. 499–648.

[14] B. Lindström, "Group partitions and mixed perfect codes," *Canadian Mathematical Bulletin*, vol. 18, no. 1, pp. 57–60, 1975.

[15] S. Ling and F. Özbudak, "Constructions and bounds on linear error-block codes," *Designs, Codes and Cryptography*, vol. 45, no. 3, pp. 297–316, Dec. 2007.

[16] R. J. McEliece, E. R. Rodemich, H. Rumsey, and L. R. Welch, "New upper bounds on the rate of a code via the delsarte-macwilliams inequalities," *IEEE Trans. on Inform. Theory*, vol. 23, no. 2, pp. 157–166, Mar. 1977.

[17] M. Navon and A. Samorodnitsky, "Linear programming bounds for codes via a covering argument," *Discrete & Computational Geometry*, vol. 41, no. 2, pp. 199–207, 2009.

[18] R. M. Roth, *Introduction to Coding Theory*. Cambridge Univ. Press, 2006.

[19] J. Schönheim, "Mixed codes," in *Calgary Int. Conf. of Combinatorial Structures and their Applications*. New York: Gordon and Breach, 1970, p. 385.

[20] V. Sidorenko, G. Schmidt, E. M. Gabidulin, M. Bossert, and V. Afanassiev, "On polyalphabetic block codes," in *Proceedings of the 2005 IEEE Information Theory Workshop on Coding and Complexity (ITW'2005), Awaji Island, Japan*, Oct. 2005, pp. 207–210.

[21] P. Udomkavanich and S. Jitman, "Bounds and modifications on linear error-block codes," *International Mathematical Forum*, vol. 5, no. 1-4, pp. 35–50, 2010.

[22] Y. Yehezkeally, H. Al Kim, S. Puchinger, and A. Wachter-Zeh, "Bounds on mixed codes with finite alphabets," *arXiv preprint arXiv:2212.09314*, Sep. 2021. [Online]. Available: https://arxiv.org/abs/2212.09314