On the Gilbert-Varshamov distance of Abelian group codes

Giacomo Como
Dip. di Matem., Politecnico di Torino, Italy
visiting Yale University, New Haven, CT
Email: giacomo.como@polito.it

Fabio Fagnani
Dipartimento di Matematica
Politecnico di Torino, Italy
Email: fabio.fagnani@polito.it

***Abstract*— The problem of the minimum Bhattacharyya distance of group codes over symmetric channels is addressed. Ensembles of $\mathbb{Z}_m$-linear codes are introduced and their typical minimum distance characterized in terms of the Gilbert-Varshamov distances associated to the subgroups of $\mathbb{Z}_m$. For the AWGN channel with 8-PSK as input it is shown that the typical $\mathbb{Z}_8$-linear code achieves the Gilbert-Varshamov bound.**

I. Introduction

The Gilbert-Varshamov (GV) bound is one of the most famous lower bounds on the achievable minimum Hamming distance of binary codes. Given a rate R in $(0,1)$ and defined $\delta^{GV}(R)$ as the unique solution in $(0,1/2)$ of the equation $\mathrm{H}(x) = 1 - R$ ($\mathrm{H}(x)$ denotes the binary entropy), it states that there exist codes of length n and minimum distance at least $n\delta^{GV}(R)$, for every n. It was introduced in early '50s and since then has attracted a huge amount of attention from researchers. In particular the asymptotic tightness of the GV bound is one of the most famous unproved conjectures in coding theory, as pointed out by A.Vardy in his plenary talk at last ISIT [10]. This problem is closely related to the tightness of the expurgated error exponent at low rates. A well known fact is that the Gilbert-Varshamov bound is asymptotically achieved with probability one by the binary linear coding ensemble [6], while this is not the case for the random coding ensemble. In [1] the relationships of this problem with the typical distance spectra and typical error exponent of the random coding ensemble and of the linear coding ensemble, are explored for binary symmetric channels.

In this paper we will deal with an extension of these issues to the non binary case. There are many different notions of distance for non binary alphabets; the Hamming distance and the Lee distance for instance have been widely studied. However these distances have no direct application to the error exponents of channels usually considered. Here we will follow the approach of [2] considering the notion of Bhattacharyya distance of a memoryless channel and dealing with the corresponding Gilbert-Varshamov bound. We will focus on symmetric memoryless channels, an important special case of which is the AWGN channel with input restricted on a Geometrically Uniform (GU) constellation: in this case the Bhattacharyya distance corresponds to the squared Euclidean distance up to a scaling factor. Group codes for such a class of channels constitute a natural generalization of binary linear codes for binary symmetric channels [8], [5]. In [3], [4] Abelian group codes ensembles have been introduced and their error probability analyzed leading to an exact characterization of the capacity achievable by such codes.

In this paper also we will deal with Abelian codes ensembles. Our main contribution is an exact characterization of the minimum Bhattacharyya distance asymptotically achievable by ensembles of codes over the cyclic group $\mathbb{Z}_m$: it turns out that with probability one $\mathbb{Z}_m$-linear ensembles of codes asymptotically achieve a distance which is the minimum of the GV distances associated to the subchannels having as inputs all the possible nontrivial subgroups of $\mathbb{Z}_m$. This phenomenon closely resembles what has been shown in [3] and [4] for the capacity of Abelian group codes. In fact, both are related to the characterization of distance spectra for such codes. As a specific example we then consider the AWGN channel with the $8-PSK$ input constellation. We prove that in this case the above minimum of the GV distances is equal to the GV distance of the channel itself with respect to the squared Euclidean distance: in other terms typical $\mathbb{Z}_8$ group codes always achieve the GV distance on the AWGN channel with the $8-PSK$ input constellation.

In Section II the general notion of Bhattacharyya distance for symmetric channels is introduced and two examples are presented where it coincides respectively with the Hamming distance for BIOS channels and with the squared Euclidean distance for the AWGN channel with a GU constellation as input. In Section III we state the Gilbert-Varshamov bound on the Bhattacharyya distance. Section IV contains the main results consisting in an exact characterization the typical distance spectra and minimum distance of $\mathbb{Z}_m$-linear coding ensembles. In Section V we analyze the special case of the AWGN channel with $8-PSK$ input constellation.

II. Bhattacharyya distance for symmetric memoryless channels

In this section we introduce a general framework for the minimum distance. While perhaps looking rather abstract, we will see that this framework unifies many different definitions and allows to formulate a general problem.

Throughout this paper the base $\exp$ and $\log$ has to be considered the same arbitrary fixed positive number. For a finite set A, $\mathcal{P}(A)$ will denote the space of probability

measures over A. If a in A, δ_a in $\mathcal{P}(A)$ denotes the delta probability concentrated on a. The entropy function is

$$\mathrm{H} : \mathcal{P}(A) \to \mathbb{R}^+ , \qquad \mathrm{H}(\boldsymbol{\theta}) = -\sum_a \boldsymbol{\theta}(a) \log \boldsymbol{\theta}(a) .$$

For every n in $\mathbb{N}$, the A-type function is defined as

$$\boldsymbol{\upsilon}_A : A^n \to \mathcal{P}(A) , \quad [\boldsymbol{\upsilon}_A(\boldsymbol{x})](a) := \frac{1}{n} |\{1 \le i \le n : \, x_i = a\}| \, .$$

We define $\mathcal{P}_n(A) := \boldsymbol{\upsilon}_A(A^n)$ and $\mathcal{P}_{\mathbb{N}}(A) := \cup_{n \in \mathbb{N}} \mathcal{P}_n(A)$; the set $\mathcal{P}_{\mathbb{N}}(A)$ is countable and dense in $\mathcal{P}(A)$.

For two real valued functions $\boldsymbol{f}$ and $\boldsymbol{g}$ over A we consider their scalar product $\langle \boldsymbol{f}, \boldsymbol{g} \rangle = \sum_{a \in A} \boldsymbol{f}(a) \boldsymbol{g}(a)$; for a subset B of A, $\boldsymbol{f}|_B : B \to \mathbb{R}$ denotes the restriction of $\boldsymbol{f}$ to B.

For an arbitrary finite group G we shall denote by 1_G its unit element and generally use the multiplicative notation. When G is Abelian we shall switch to the additive notation with 0 denoting the unit element. We will also use the notation $\mathcal{P}^*(G) := \mathcal{P}(G) \setminus \{\delta_{1_G}\}$.

A memoryless channel (MC) of finite input set $\mathcal{X}$ and continuous output set $\mathcal{Y} = \mathbb{R}^\nu$ is described by a family of transition probability densities $\{W(\cdot|x)\}_{x \in \mathcal{X}}$. Our theory also works in a more general framework including channels with discrete outputs: this choice is only made for simplicity.

Consider two elements x, x' of $\mathcal{X}$. Since both $W(\cdot|x)$ $W(\cdot|x')$ are nonnegative measurable functions over $\mathcal{Y}$ the quantity $\int_{\mathcal{Y}} \sqrt{W(y|x)W(y|x')} \mathrm{d}y$ is well defined in $[0, +\infty]$. Both $\sqrt{W(\cdot|x)}$ and $\sqrt{W(\cdot|x')}$ are in $L^2(\mathcal{Y})$ so that Schwartz inequality gives

$$\begin{array}{rcl} 0 & \le & \int_{\mathcal{Y}} \sqrt{W(y|x)W(y|x')} \mathrm{d}y \\ & \le & \int_{\mathcal{Y}} W(y|x) \mathrm{d}\mu(y) \int_{\mathcal{Y}} W(y|x') \mathrm{d}y = 1 \, . \end{array}$$

The first inequality above is an equality iff the supports of $W(\cdot|x)$ and $W(\cdot|x')\big)$ intersects in a set of zero measure. Instead, the second inequality is equality iff $W(\cdot|x) = W(\cdot|x')$ almost surely, which means that actually x and x' have indistinguishable outputs. In this paper we will assume that for every $x \neq x'$

$$0 < \int_{\mathcal{Y}} \sqrt{W(y|x)W(y|x')} < 1 \, ;$$

While there is no loss of generality in the latter part of this assumption, the former excludes from our analysis the class of channels whose 0-error capacity is strictly positive.

To any memoryless channel we can associate a function $\boldsymbol{D} : \mathcal{X} \times \mathcal{X} \to \mathbb{R}^+$ defined by

$$\boldsymbol{D}(x, x') := -\log \int_{\mathcal{Y}} \sqrt{W(y|x)W(y|x')} \mathrm{d}\mu(y) \, .$$

This function is usually called the Bhattacharyya distance function of the channel and satisfies

$$\boldsymbol{D}(x, x') = \boldsymbol{D}(x', x) , \qquad \forall \, x, x' \in G , \tag{1}$$

$$\boldsymbol{d}(x, x') = 0 \qquad \Longleftrightarrow \qquad x = x' . \tag{2}$$

As in [4] we introduce the following definition of symmetry for memoryless channels.

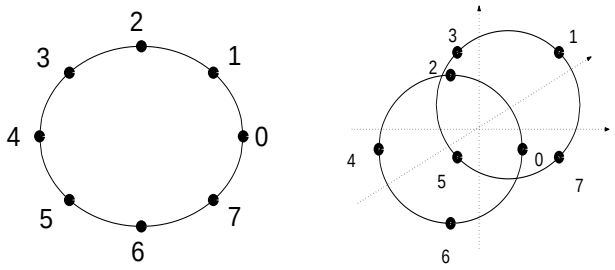

Fig. 1. Two GU constellations admitting generating group $\mathbb{Z}_8$

Definition 1 *A MC $\{W(\cdot|x)\}_{x \in \mathcal{X}}$ is G–symmetric if*

(i) *G acts simply and transitively on $\mathcal{X}$;*
(ii) *G acts isometrically on $\mathcal{Y}$;*
(iii) *$W(gy|gx) = W(y|x)$ for every $g \in G$, $x \in \mathcal{X}$, and $y \in \mathcal{Y}$.*

Notice that property (i) implies that for any fixed $x_0 \in \mathcal{X}$ we have a bijection $g \in G \mapsto g x_0 \in \mathcal{X}$. Through such a mapping G and $\mathcal{X}$ ca actually be identified and subset over G^N will naturally lead to codes of length N over $\mathcal{X}$. From now on we assume that the base point x_0 has been fixed and $\mathcal{X}$ will be identified with G. In particular, we will write $\boldsymbol{D}(g, h)$ for $\boldsymbol{D}(g x_0, h x_0)$.

It is easy to verify that the Bhattacharyya distance function $\boldsymbol{D}$ of a G-symmetric memoryless channel satisfies

$$\boldsymbol{D}(g, h) = \boldsymbol{D}(h^{-1} g, 1_G) = \boldsymbol{d}(h^{-1} g) \, ,$$

where we define

$$\boldsymbol{d} : G \to \mathbb{R}^+ , \qquad \boldsymbol{d}(g) = \boldsymbol{D}(g, 1_G) , \qquad g \in G \, .$$

The arguments above motivate the following definition.

Definition 2 *A function $\boldsymbol{d} : G \to \mathbb{R}^+$ such that*

$$\boldsymbol{d}(g) = \boldsymbol{d}(g^{-1}) \qquad \boldsymbol{d}(g) = 0 \Leftrightarrow g = 1_G \, , \qquad g \in G \, ,$$

is called a G-Bhattacharyya weight function.

A Bhattacharyya weight function can be extended to direct products in a natural way. Given two elements $\boldsymbol{x}$ and $\boldsymbol{y}$ of the direct group product G^N, and a Bhattacharyya weight function $\boldsymbol{D}$, the $\boldsymbol{D}$-distance between $\boldsymbol{x}$ and $\boldsymbol{y}$ is defined by

$$\boldsymbol{D}(\boldsymbol{x}, \boldsymbol{y}) = \sum_{i=1}^N \boldsymbol{D}(x_i, y_i) = \sum_{i=1}^N \boldsymbol{d}(y_i^{-1} x_i) = n \langle \boldsymbol{\upsilon}_G(\boldsymbol{y}^{-1} \boldsymbol{x}), \boldsymbol{d} \rangle$$

Example 1 (Binary-input symmetric-output channels) Consider the case when $G = \mathbb{Z}_2$. $\mathbb{Z}_2$-symmetric channels are known in the literature as binary-input symmetric-output (BIOS) channels. In this case

$$n \langle \boldsymbol{d}, \boldsymbol{\upsilon}_{\mathbb{Z}_2}(\boldsymbol{x} - \boldsymbol{y}) \rangle = \boldsymbol{d}(1) \, |\{1 \le i \le N : \, x_i \neq y_i\}| \, ,$$

i.e. the $\boldsymbol{d}$-distance is proportional to the Hamming distance.

Example 2 (Geometrically Uniform AWGN channel) Given the n–dimensional Euclidean space $\mathbb{R}^n$, an n–dimensional constellation is a finite subset $S \subset \mathbb{R}^n$ that spans $\mathbb{R}^n$; we denote with $\Gamma(S)$ its symmetry group, i.e. the group of those isometries of $\mathbb{R}^n$ mapping S into S itself. A constellation S is said to be geometrically uniform (GU) if there exists a subgroup G of $\Gamma(S)$ such that for every $s, r \in S$ a unique $g \in G$ exists such that $gs = r$ (i.e. the action of G on S is simply transitive). Such a G is called a generating group for S: for every $s \in S$ the mapping $\mu_s : G \to S$ defined by $\mu_s : g \in G \mapsto gs \in S$ is a bijection called isometric labelling. Two examples of GU constellations both admitting $\mathbb{Z}_8$ as a generating group, are presented in Fig. 1. Both the constellations also admit the non Abelian dihedral group D_4 as a generating group.

It is easy to check that the AWGN channel with input restricted on GU constellation S admitting a generating group G is G-symmetric. Moreover, if we denote by σ^2 the variance, we have that

$$\begin{aligned}\boldsymbol{d}(g) &= -\log \int_{\mathbb{R}^n} \tfrac{1}{\sqrt{2\pi\sigma^2}^n} e^{-\left(||\boldsymbol{y}-\mu_s(g)||^2 + ||\boldsymbol{y}-\mu_s(1_G)||^2\right)/4\sigma^2} \mathrm{d}\boldsymbol{y} \\ &= ||\mu_s(g) - \mu_s(1_G)||^2 \log e/(2\pi\sigma^2)\,,\end{aligned}$$

i.e. the Bhattacharyya distance is proportional to the squared Euclidean distance.

III. Gilbert-Varshamov bound on the minimum Bhattacharyya distance

Suppose a finite group G and a G-Bhattacharyya function $\boldsymbol{d}$ are given. For N in $\mathbb{N}$, a block-code over G of length N is any subset $\mathcal{C}$ of G^N. It's rate is $R(\mathcal{C}) = \frac{1}{N}\log|\mathcal{C}|$; we define its complementary rate as

$$\overline{R}(\mathcal{C}) := 1 - \frac{R(\mathcal{C})}{\log|G|}\,.$$

For every $\boldsymbol{\theta}$ in $\mathcal{P}(G)$, $S_{\boldsymbol{\theta}}(\mathcal{C})$ will denote the number of codewords in $\mathcal{C}$ of type $\boldsymbol{\theta}$, while $N_{\boldsymbol{\theta}}(\mathcal{C})$ will denote the number of ordered pairs of codewords of $\mathcal{C}$ whose difference has type $\boldsymbol{\theta}$:

$$S_{\boldsymbol{\theta}}(\mathcal{C}) := \sum_{\boldsymbol{x}\in\mathcal{C}} \mathbb{1}_{\{\boldsymbol{\theta}\}}(\boldsymbol{v}_G(\boldsymbol{x}))\,,$$

$$N_{\boldsymbol{\theta}}(\mathcal{C}) := \sum_{(\boldsymbol{x},\boldsymbol{y})\in\mathcal{C}^2} \mathbb{1}_{\{\boldsymbol{\theta}\}}(\boldsymbol{v}_G(\boldsymbol{x}^{-1}\boldsymbol{y}))\,.$$

The normalized minimum $\boldsymbol{d}$-distance of a code $\mathcal{C}$ is

$$\delta_{\boldsymbol{d}}(\mathcal{C}) := \inf\left\{\langle\boldsymbol{\theta},\boldsymbol{d}\rangle \,\middle|\, \boldsymbol{\theta}\in\mathcal{P}^*(G) : N_{\boldsymbol{\theta}}(\mathcal{C}) > 0\right\}\,.$$

A G-code of length N is a subgroup $\mathcal{C}$ of the direct group product G^N. For a G-code $N_{\boldsymbol{\theta}}(\mathcal{C}) = |\mathcal{C}|S^N_{\boldsymbol{\theta}}(\mathcal{C})$, so that

$$\delta_{\boldsymbol{d}}(\mathcal{C}) = \inf\left\{\langle\boldsymbol{\theta},\boldsymbol{d}\rangle \,\middle|\, \boldsymbol{\theta}\in\mathcal{P}^*(G) : S_{\boldsymbol{\theta}}(\mathcal{C}) > 0\right\}\,.$$

The Gilbert-Varshamov bound is a lower bound on the largest normalized minimum $\boldsymbol{d}$-distance achievable by codes over G with rate greater than or equal to some value R. The result can be summarized as follows. For every $\overline{R}$ in $[0,1]$ and δ in $[0,\overline{\boldsymbol{d}}]$, define

$$\delta^{GV}_{\boldsymbol{d}}(\overline{R}) := \inf\left\{\langle\boldsymbol{\theta},\boldsymbol{d}\rangle \,\middle|\, \boldsymbol{\theta}\in\mathcal{P}^*(G) :\, \mathrm{H}(\boldsymbol{\theta}) \geq \overline{R}\log|G|\right\}\,.$$

Theorem 3 *For every* $\overline{R}\in[0,1]$

$$\sup\left\{\delta_{\boldsymbol{d}}(\mathcal{C}) \,\middle|\, \mathcal{C} \text{ code over } G\,, \overline{R}(\mathcal{C}) \leq \overline{R}\right\} \geq \delta^{GV}_{\boldsymbol{d}}(\overline{R})$$

A proof of Theorem 3 can be found for instance in [2] and is essentially based on an estimation of the volume of discrete $\boldsymbol{d}$-balls in G^N [9].

Note that Theorem 3 guarantees the existence of a code over G with large enough minimum $\boldsymbol{d}$-distance, but this code needs not to be a G-code. Moreover it is possible to show that in this case the random coding ensemble (notice that, since the channel is G-symmetric, the optimal input distribution for both capacity and error exponent is the uniform one), with probability one does not achieve the GV bound [1].

When G is the binary field $\mathbb{Z}_2$ Theorem 3 reduces to the classical Gilbert-Varshamov bound for binary codes. As mentioned in the introduction, it is known that in this case the Gilbert-Varshamov bound is achievable by binary liner codes, and, more remarkably, it is achieved with probability one by the binary linear coding ensemble [1]. When G is any finite field $\mathbb{F}_q$, the same is also known to hold true for the random $\mathbb{F}_q$-linear ensemble.

The question we want to address is how this phenomenon generalizes to arbitrary finite groups G. In the sequel we will provide a complete answer for the class of cyclic groups. While our techniques can be generalized to arbitrary finite Abelian groups using Kronecker decomposition theorem, generalizations to nonAbelian groups seem to require completely different algebraic tools.

IV. Ensembles of cyclic group codes: distance spectra and minimum $\boldsymbol{d}$-distance

In this section we restrict ourself to the special class of finite groups, that of cyclic groups. For every positive integer m we denote by $\mathbb{Z}_m$ the group of integers modulo m. $\mathbb{Z}_m$ admits ring structure and $\mathbb{Z}_m^n$ is in fact a $\mathbb{Z}_m$-free module [7].

Let us consider a complementary design rate $\overline{R}$. For every N in $\mathbb{N}$ define $L := \lceil N\overline{R}\rceil$ and consider the set $\hom\left(\mathbb{Z}_m^N, \mathbb{Z}_m^L\right)$ of all homomorphisms from $\mathbb{Z}_m^N$ to $\mathbb{Z}_m^L$. To every ϕ in $\hom(\mathbb{Z}_m^N, \mathbb{Z}_m^L)$ a $\mathbb{Z}_m$-code is naturally associated, namely its kernel $\mathcal{C}_\phi := \ker(\phi)$. It is easy to check that the complementary rate of $\mathcal{C}_\phi$ is less than or equal to $\overline{R}$.

We now introduce a probabilistic structure on the set of all $\mathbb{Z}_m$-codes of complementary rate less than or equal to $\overline{R}$.

Definition 4 *For every* $\overline{R}\in[0,1]$ *the* $\mathbb{Z}_m$*-linear ensemble of complementary rate* $\overline{R}$ *is a sequence* $(\mathcal{C}_{\Phi_N})_{N\in\mathbb{N}}$ *of random variables, with* Φ_N *uniformly distributed over* $\hom\left(\mathbb{Z}_m^N, \mathbb{Z}_m^L\right)$. *Its distance spectra will be denoted by*

$$S^N_{\boldsymbol{\theta}} := S_{\boldsymbol{\theta}}\left(\mathcal{C}_{\Phi_N}\right)\,, \qquad \boldsymbol{\theta}\in\mathcal{P}(\mathbb{Z}_m)\,,$$

and its minimum Bhattacharyya distance by

$$\delta_{\boldsymbol{d}}^N := \delta_{\boldsymbol{d}}(\mathcal{C}_{\Phi_N})\,.$$

Consider a base $\mathcal{B}$ of $\mathbb{Z}_m^N$, i.e. a set of N $\mathbb{Z}_m$-linear independent elements of $\mathbb{Z}_m^N$. Since every ϕ in $\hom(\mathbb{Z}_m^N, \mathbb{Z}_m^L)$ can be uniquely characterized by the images of the elements of $\mathcal{B}$ [7], from Def.4 it follows that $\left\{\Phi_N \boldsymbol{b} \,\middle|\, \boldsymbol{b} \in \mathcal{B}\right\}$ is collection of independent random variables, identically distributed with uniform distribution over $\mathbb{Z}_m^L$.

We now introduce the function

$$l_m : \mathbb{Z}_m \to \mathbb{N}\,, \qquad l_m(\boldsymbol{\theta}) := \frac{m}{\gcd\left(\mathrm{supp}\left(\boldsymbol{\theta}\right)\right)}\,.$$

Let us fix $\boldsymbol{x}$ and $\boldsymbol{y}$ in $\mathbb{Z}_m^N$ such that $l_m(\boldsymbol{v}_{\mathbb{Z}_m}(\boldsymbol{x})) = l_m(\boldsymbol{v}_{\mathbb{Z}_m}(\boldsymbol{y})) = l$. This implies that $\boldsymbol{x}, \boldsymbol{y} \in \frac{m}{l}\mathbb{Z}_m^N$, and that $\frac{l}{m}\boldsymbol{x}$ is $\mathbb{Z}_m$-linear independent. It follows that there exists a basis of $\mathbb{Z}_m^N$ containing $\frac{l}{m}\boldsymbol{x}$. Thus the r.v. $\frac{l}{m}\Phi_N\boldsymbol{x}$ is uniformly distributed over $\mathbb{Z}_m^L$, and $\Phi_N\boldsymbol{x}$ is uniformly distributed over $\frac{m}{l}\mathbb{Z}_m^L$. The same is obviously true for the r.v.s $\frac{l}{m}\Phi_N\boldsymbol{y}$ and $\Phi_N\boldsymbol{y}$ respectively. Moreover, if $\frac{l}{m}\boldsymbol{y}$ and $\frac{l}{m}\boldsymbol{x}$ are linear independent, then there exists a basis of $\mathbb{Z}_m^N$ containing both: it follows that the r.v.s $\frac{l}{m}\Phi_N\boldsymbol{x}$ and $\frac{l}{m}\Phi_N\boldsymbol{y}$ are independent and so do $\Phi_N\boldsymbol{x}$ and $\Phi_N\boldsymbol{x}$.

Based on the reasonings above, standard combinatorial and probabilistic arguments allow to characterize the typical asymptotic distance spectra of the $\mathbb{Z}_m$-linear ensemble. First, both the expected value of the distance spectra of the $\mathbb{Z}_m$-linear ensemble and its variance can be evaluated as follows.

Theorem 5 *For every N in $\mathbb{N}$ and $\boldsymbol{\theta}$ in $\mathcal{P}_N\left(\mathbb{Z}_m\right)$ we have:*

$$\mathbb{E}\left[S_{\boldsymbol{\theta}}^N\right] = \binom{N}{N\boldsymbol{\theta}} l_m(\boldsymbol{\theta})^{-L}\,, \tag{3}$$

$$1 - m l_m(\boldsymbol{\theta})^{-L} \leq \frac{\mathrm{Var}\left[S_{\boldsymbol{\theta}}^N\right]}{\mathbb{E}\left[S_{\boldsymbol{\theta}}^N\right]} \leq m\left(1 - l_m(\boldsymbol{\theta})^{-L}\right)\,. \tag{4}$$

For every $\overline{R} \in [0,1]$ define

$$G_{\mathbb{Z}_m}^{\overline{R}}(\boldsymbol{\theta}) := \mathrm{H}(\boldsymbol{\theta}) - \overline{R}\log l_m(\boldsymbol{\theta})\,.$$

From (3) and (4) it follows that for every $\boldsymbol{\theta}$ in $\mathcal{P}_{\mathbb{N}}(\mathbb{Z}_m)$

$$\lim_{N\in\mathbb{N}} \frac{\log \mathbb{E}\left[S_{\boldsymbol{\theta}}^N\right]}{N} = \lim_{N\in\mathbb{N}} \frac{\log \mathrm{Var}\left[S_{\boldsymbol{\theta}}^N\right]}{N} = G_{\mathbb{Z}_m}^{\overline{R}}(\boldsymbol{\theta})\,.$$

The following result exactly characterizes the asymptotic distance spectra of the $\mathbb{Z}_m$-linear ensemble.

Corollary 6 *For the uniform $\mathbb{Z}_m$-linear ensemble of rate R we have that, with probability 1,*

- $\lim_{N\in\mathbb{N}} S_{\boldsymbol{\theta}}^N = 0\,,\ \forall\,\boldsymbol{\theta} \in \mathcal{P}_{\mathbb{N}}(\mathbb{Z}_m) : G_{\mathbb{Z}_m}^{\overline{R}}(\boldsymbol{\theta}) < 0\,;$
- $\lim_{N\in\mathbb{N}} \frac{1}{N}\log S_{\boldsymbol{\theta}}^N = G_{\mathbb{Z}_m}^{\overline{R}}(\boldsymbol{\theta})\,,\ \forall\,\boldsymbol{\theta} \in \mathcal{P}_{\mathbb{N}}(\mathbb{Z}_m) : G_{\mathbb{Z}_m}^{\overline{R}}(\boldsymbol{\theta}) > 0\,.$

Proof (sketch) In order to show the first point it is sufficient to use a first order method and (3) and Borel Cantelli lemma. For the second part a first order method based on (3) is sufficient to show that

$$\limsup_{N\in\mathbb{N}} \frac{1}{N}\log S_{\boldsymbol{\theta}}^N \leq G_{\mathbb{Z}_m}^{\overline{R}}(\boldsymbol{\theta})\,,$$

while a second moment method based on (4) allows to show that

$$\liminf_{N\in\mathbb{N}} \frac{1}{N}\log S_{\boldsymbol{\theta}}^N \geq G_{\mathbb{Z}_m}^{\overline{R}}(\boldsymbol{\theta})\,.$$

■

We are now ready to evaluate the typical asymptotic minimum $\boldsymbol{d}$-distance of the $\mathbb{Z}_m$-linear ensemble of complementary rate $\overline{R}$. We can rewrite

$$\delta_{\boldsymbol{d}}^N := \inf\left\{\langle\boldsymbol{\theta},\boldsymbol{d}\rangle \,\middle|\, \boldsymbol{\theta} \in \mathcal{P}_N^*(G) :\ S_{\boldsymbol{\theta}}^N > 0\right\}\,.$$

In order to state our main result we need some more notation. For a subset A of $\mathbb{Z}_m$ we define

$$\Delta_A := \{\boldsymbol{\theta} \in \mathcal{P}^*(G) :\ \mathrm{supp}(\boldsymbol{\theta}) \subseteq A\}\,,$$

$$\delta_{\boldsymbol{d}}^{GV}(A, \overline{R}) := \inf\left\{\langle\boldsymbol{\theta},\boldsymbol{d}\rangle \,\middle|\, \boldsymbol{\theta} \in \Delta_A\,, \mathrm{H}(\boldsymbol{\theta}) \geq \overline{R}\log|A|\right\}\,.$$

Theorem 7 *For any $\mathbb{Z}_m$-Bhattacharyya function $\boldsymbol{d}$, the uniform $\mathbb{Z}_m$-linear ensemble of complementary rate $\overline{R}$ has normalized minimum $\boldsymbol{d}$-distance satisfying*

$$\mathbb{P}\left(\lim_{N\in\mathbb{N}} \delta_{\boldsymbol{d}}^N = \delta_{\boldsymbol{d}}^{\mathbb{Z}_m}(\overline{R})\right) = 1\,,$$

where

$$\delta_{\boldsymbol{d}}^{\mathbb{Z}_m}(\overline{R}) := \min\left\{\delta_{\boldsymbol{d}}^{GV}(\tfrac{m}{l}\mathbb{Z}_m, \overline{R}) \,\middle|\, l \in \mathbb{D}_m,\, l > 1\right\}\,. \tag{5}$$

Proof (sketch) A first observation is that the closure of the set $\{l_m(\boldsymbol{\theta}) = l\}$ in $\mathcal{P}(\mathbb{Z}_m)$ is $\Delta_{\frac{m}{l}\mathbb{Z}_m}$. Then continuity arguments allow to show that

$$\delta_{\boldsymbol{d}}^{\mathbb{Z}_m}(\overline{R}) = \inf\left\{\langle\boldsymbol{\theta},\boldsymbol{d}\rangle \,\middle|\, \boldsymbol{\theta} \in \mathcal{P}^*(\mathbb{Z}_m) :\ G_{\mathbb{Z}_m}^{\overline{R}}(\boldsymbol{\theta}) \geq 0\right\}\,.$$

Define the events

$$A_N := \bigcup_{\boldsymbol{\theta}\in\mathcal{P}_{\mathbb{N}}(\mathbb{Z}_m) : G_{\mathbb{Z}_m}^{\overline{R}}(\boldsymbol{\theta}) < 0} \{S_{\boldsymbol{\theta}}^N > 0\}\,,\ N \in \mathbb{N}\,.$$

From the first point of Corollary 6, since the set $\mathcal{P}_{\mathbb{N}}(\mathbb{Z}_m)$ is countable, we have that $\mathbb{P}\left(A_N \text{ i.o. }\right) = 0$. It follows that

$$\begin{aligned}\mathbb{P}\left(\liminf_N \delta_{\boldsymbol{d}}^N \geq \delta_{\boldsymbol{d}}^{\mathbb{Z}_m}(\overline{R})\right) &\geq 1 - \mathbb{P}\left(\left\{\delta_{\boldsymbol{d}}^N \leq \delta_{\boldsymbol{d}}^{\mathbb{Z}_m}(\overline{R})\right\} \text{i.o.}\right)\\ &\geq 1 - \mathbb{P}\left(A_N \,\text{i.o. }\right) = 1\,.\end{aligned}$$

In order to show that

$$\mathbb{P}\left(\limsup_N \delta_{\boldsymbol{d}}^N \leq \delta_{\boldsymbol{d}}^{\mathbb{Z}_m}(\overline{R})\right) = 1\,,$$

one uses the second point of Corollary 6 and the density of $\mathcal{P}_{\mathbb{N}}(\mathbb{Z}_m) \cap \Delta_{\frac{m}{l}\mathbb{Z}_m}$ in $\Delta_{\frac{m}{l}\mathbb{Z}_m}$. ■

Theorem 7 characterizes the typical normalized $\boldsymbol{d}$-distance achieved by ensembles of $\mathbb{Z}_m$-free codes in the simple form

(5). It turns out that $\delta_{\boldsymbol{d}}^{\mathbb{Z}_m}(\overline{R})$ is the minimum of Gilbert-Varshamov $\boldsymbol{d}$-distances associated to all the nontrivial subgroups of $\mathbb{Z}_m$ so that clearly

$$\delta_{\boldsymbol{d}}^{\mathbb{Z}_m}(\overline{R}) \leq \delta_{\boldsymbol{d}}^{GV}(\overline{R})\,.$$

When m is a prime number the only non trivial subgroup is $\mathbb{Z}_m$ itself, so that always in this case we have $\delta_{\boldsymbol{d}}^{\mathbb{Z}_m}(\overline{R}) = \delta_{\boldsymbol{d}}^{GV}(\overline{R})$ and Theorem 7 directly implies that the Gilbert-Varshamov bound is achieved with probability one by the $\mathbb{Z}_m$-linear random coding ensemble.

When m is not prime, the presence of proper subgroups of $\mathbb{Z}_m$ may prevent this to hold true. In fact it is possible to construct examples when $\delta_{\boldsymbol{d}}^{\mathbb{Z}_m}(\overline{R}) < \delta_{\boldsymbol{d}}^{GV}(\overline{R})$, for instance using the AWGN channel with input restricted to the 3-dimensional GU constellation depicted in the righthand side of Fig. 1. In next section instead, we will analyze a simple case when $\delta_{\boldsymbol{d}}^{\mathbb{Z}_m}(\overline{R}) = \delta_{\boldsymbol{d}}^{GV}(\overline{R})$.

V. The 8-PSK AWGN case

In this section we restrict ourselves to the 8-PSK AWGN channel and prove that in this special case the $\mathbb{Z}_8$-linear ensemble minimum $\boldsymbol{d}$-distance achieves the Gilbert-Varshamov bound asymptotically with probability one.

Theorem 8 *For every $\overline{R}$ in $(0,1)$*

$$\delta_{\boldsymbol{d}}^{\mathbb{Z}_8}(\overline{R}) = \delta_{\boldsymbol{d}}^{GV}(\overline{R})\,.$$

Proof We will show that

$$\delta_{\boldsymbol{d}}^{GV}(\overline{R}, 4\mathbb{Z}_8) = \delta_{\boldsymbol{d}}^{GV}(\overline{R}, 2\mathbb{Z}_8) \geq \delta_{\boldsymbol{d}}^{GV}(\overline{R}, \mathbb{Z}_8)\,. \qquad (6)$$

Since by definition

$$\delta_{\boldsymbol{d}}^{\mathbb{Z}_8}(\overline{R}) = \min\left\{\delta_{\boldsymbol{d}}^{GV}(\overline{R}, 4\mathbb{Z}_8), \delta_{\boldsymbol{d}}^{GV}(\overline{R}, 2\mathbb{Z}_8), \delta_{\boldsymbol{d}}^{GV}(\overline{R}, \mathbb{Z}_8)\right\}\,,$$

(6) clearly implies the claim.

Simple geometrical considerations based on Pythagoras theorems allow to show that

$$\begin{array}{c} \boldsymbol{d}(4) = 2\boldsymbol{d}(2) = 2\boldsymbol{d}(6)\,, \\ \boldsymbol{d}(1) = \boldsymbol{d}(7)\,, \qquad \boldsymbol{d}(3) = \boldsymbol{d}(5)\,, \\ \boldsymbol{d}(1) = \boldsymbol{d}(4) - \boldsymbol{d}(3) < \frac{1}{4}\,. \end{array} \qquad (7)$$

Using Lagrange multipliers it is possible to write

$$\delta_{\boldsymbol{d}}^{GV}(\overline{R}, 4\mathbb{Z}_8) = \langle \frac{e^{-\lambda \boldsymbol{d}|_{4\mathbb{Z}_8}}}{Z_2(\lambda)}, \boldsymbol{d}\rangle = \frac{\boldsymbol{d}(4)e^{-\lambda \boldsymbol{d}(4)}}{Z_2(\lambda)}\,,$$

where λ solves $\mathrm{H}\left(\frac{e^{-\lambda \boldsymbol{d}|_{4\mathbb{Z}_8}}}{Z_2(\lambda)}\right) = \overline{R}\log 2$, while

$$\begin{aligned} \delta_{\boldsymbol{d}}^{GV}(\overline{R}, 2\mathbb{Z}_8) &= \langle \tfrac{\exp(-\lambda' \boldsymbol{d}|_{2\mathbb{Z}_8})}{Z_4(\lambda)}, \boldsymbol{d}|_{2\mathbb{Z}_8}\rangle \\ &= \tfrac{\boldsymbol{d}(4)\exp(-\lambda' \boldsymbol{d}(2)) + \boldsymbol{d}(4)\exp(-\lambda' \boldsymbol{d}(4))}{Z_4(\lambda)} \\ &= \tfrac{\boldsymbol{d}(4)\exp(-\lambda' \boldsymbol{d}(4))}{Z_2(\lambda')}\,, \end{aligned}$$

where λ' solves $\mathrm{H}\left(\frac{e^{-\lambda \boldsymbol{d}|_{2\mathbb{Z}_8}}}{Z_4(\lambda)}\right) = \overline{R}\log 4$. From (7) it follows that $\mathrm{H}\left(\frac{e^{-\lambda \boldsymbol{d}|_{2\mathbb{Z}_8}}}{Z_4(\lambda)}\right) = 2\,\mathrm{H}\left(\frac{e^{-\lambda \boldsymbol{d}|_{4\mathbb{Z}_8}}}{Z_2(\lambda)}\right)$, so that $\lambda = \lambda'$ and thus the equality in (6) holds true. In order to show the inequality in (6), we introduce the $\mathbb{Z}_8$-type $\boldsymbol{\theta}$ defined by

$$\begin{array}{c} \boldsymbol{\theta}(0) := (1-\alpha)^3\,, \qquad \boldsymbol{\theta}(1) := \boldsymbol{\theta}(2) := \boldsymbol{\theta}(7) := \alpha(1-\alpha)^2\,, \\ \boldsymbol{\theta}(4) := \alpha^3\,, \qquad \boldsymbol{\theta}(6) := \boldsymbol{\theta}(5) := \boldsymbol{\theta}(3) := \alpha^2(1-\alpha)\,, \end{array}$$

where $\alpha := \frac{\exp(-\lambda \boldsymbol{d}(4))}{Z_2(\lambda)}$. It can be verified that

$$\mathrm{H}(\boldsymbol{\theta}) = 3\,\mathrm{H}\left(\frac{\exp(-\lambda \boldsymbol{d}|_{4\mathbb{Z}_8})}{Z_2(\lambda)}\right) = \overline{R}\,.$$

A straightforward calculation gives us

$$\langle \boldsymbol{\theta}, \boldsymbol{d}\rangle = \left(1 - \left(2\boldsymbol{d}(1) - \frac{1}{2}\boldsymbol{d}(4)\right)\left(2\alpha^2 - 3\alpha + 1\right)\right)\alpha \geq \alpha\,,$$

last inequality following from (7). ■

Corollary 9 *With probability 1 minimum $\boldsymbol{d}$ distance of the $\mathbb{Z}_8$-linear ensemble achieves the Gilbert-Varshamov bound of the 8-PSK AWGN channel.*

VI. Conclusions

In this paper we have analyzed the asymptotic behavior of the minimal Bhattacharyya distance of Abelian group codes over symmetric channels. In particular we have proven that typical $\mathbb{Z}_8$-codes achieve the GV bound over the AWGN channel with input on the $8-PSK$ constellation. We believe a lot more needs to be understood about this problem. As a first goal, we are currently trying to extend our final result to all $p^r - PSK$ constellations (where p is a prime number). Secondly, we would like to study the typical behavior of the minimal Bhattacharyya distance of linear (or affine) binary codes over non-binary symmetric channels. For the specific case of PSK constellations we conjecture that linear binary codes will exhibit smaller typical distances than Abelian group codes. We believe that this type of analysis is a first fundamental step to understand the behavior of more structured ensembles of codes, for instance LDPC or turbo group codes over non-binary symmetric channels.

References

[1] A. Barg and G. D. Forney, Jr., "Random codes: Minimum distances and error exponents", *IEEE Trans. Inform. Theory*, vol. 48 , no. 9, 2568-2573, 2002.

[2] R. Blahut, "Composition Bounds for Channel Block Codes", *IEEE Trans. Inform. Theory*, vol. 23 , no. 6, 656-674, 1977.

[3] G. Como and F. Fagnani, "Ensembles of codes over Abelian groups", *Proc. of ISIT 2005*, 1788-1792, 2005.

[4] G. Como and F. Fagnani, "The capacity of Abelian group codes over symmetric channels", submitted to *IEEE Trans. Inform. Theory*, 2005, av. at http://calvino.polito.it/ricerca/2005/pdf/33_2005/art_33_2005.pdf.

[5] G. D. Forney, Jr., "Geometrically Uniform Codes", *IEEE Trans. Inform. Theory*, vol. 37, pp. 1241-1260, 1991.

[6] R. G. Gallager, *Low Density Parity Check Codes*, MIT Press, Cambridge MA, 1963.

[7] T. W. Hungerford, *Algebra*, Springer Verlag, New York, 1974.

[8] H.-A. Loeliger, "Signal Sets Matched To Groups", *IEEE Trans. Inform. Theory*, vol. 37, no. 6, pp. 1675-1679, 1991.

[9] H.-A. Loeliger, "An Upper Bound on the Volume of Discrete Spheres", *IEEE Trans. Inform. Theory*, vol. 40, no. 6, pp. 2071-2073, 1994.

[10] A.Vardy, "What's New and Exciting in Algebraic and Combinatorial Coding Theory?", Plenary Lecture at ISIT 2006, http://media.itsoc.org/isit2006/vardy/