Ensembles of codes over Abelian groups

Giacomo Como
Dipartimento di Matematica
Politecnico di Torino
C.so Duca degli Abruzzi 24
10129 Torino, Italy
Email: giacomo.como@polito.it

Fabio Fagnani
Dipartimento di Matematica
Politecnico di Torino
C.so Duca degli Abruzzi 24
10129 Torino, Italy
Email: fabio.fagnani@polito.it

***Abstract*— In this paper we study ensembles of Abelian group codes on symmetric channels. Our main example is the AWGN channel where the inputs are restricted to a GU constellation admitting $\mathbb{Z}_m$ as a generating group. For codes which are $\mathbb{Z}_m$-free modules, we prove a sort of Shannon theorem which exactly characterizes which are the rates for which reliable transmission is possible. In particular we prove that for the 2^r-PSK constellation, group codes over $\mathbb{Z}_{2^r}$ do achieve Shannon capacity. Finally, we study the performance of low density $\mathbb{Z}_m$-codes and we prove average convergence rate of their word error probability.**

Keywords: non-binary modulation, m-PSK, group codes, low density parity check codes.

I. Introduction

In this paper we study the performance of several classes of Abelian group codes over non-binary symmetric channels. The main example we have in mind is an n-dimensional AWGN channel with input constrained on a geometrically uniform constellation admitting $\mathbb{Z}_m$ as a generating group. In this setting, a natural class of codes to be considered are the subgroups of $\mathbb{Z}_m^N$: they replace the standard linear binary codes in the context of binary input symmetric channels and it is well known that they share many of their properties as for instance the uniform error property [2].

In this paper, we start a fundamental investigation of the performance of such codes with respect to the Shannon limit. We restrict ourselves to a special type of group codes, namely the free submodules of $\mathbb{Z}_m^N$: these codes will be called $\mathbb{Z}_m$-free codes. While it is evident that not all group codes inside $\mathbb{Z}_m^N$ are of this type, it had never been studied before how this algebraic assumption may limit the achievable performance.

We introduce a new concept of capacity ($\mathbb{Z}_m$-capacity) which turns out to be exactly what $\mathbb{Z}_m$-free codes can achieve on symmetric channels. This capacity essentially takes into consideration Shannon capacities of the various subchannels induced by restricting the inputs to subgroups of $\mathbb{Z}_m$. The proof that it can be achieved is carried on by establishing a sort of Shannon theorem in this context. This is done by averaging over all possible $\mathbb{Z}_m$-free codes and using the Gallager bound as in the linear binary case.

For the special case of the 2^r-PSK constellation we then prove that the $\mathbb{Z}_{2^r}$-capacity equals the classical capacity thus proving that on such constellations, $\mathbb{Z}_{2^r}$-free codes do reach capacity. We also present a couple of examples showing that this is not necessarily the case for other GU constellations.

Finally, we study low density parity check $\mathbb{Z}_m$–codes, establishing the exact averaged asymptotic performance of such codes when the block length goes to ∞. We prove results very similar to the linear case [3], [8], [9]: in particular we show that these codes can achieve the $\mathbb{Z}_m$–capacity if we allow the parameters describing the densities of the matrices to grow.

II. $\mathbb{Z}_m$-symmetric channels and $\mathbb{Z}_m$-codes

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, for every $s, r \in S$, *at least one* $g \in \Gamma(S)$ exists such that $gs = r$ (i.e. the action of $\Gamma(S)$ on S is transitive). A subgroup $G \leq \Gamma(S)$ (for two groups H and H' we write $H \leq H'$ to mean that H is a subgroup of H') is a *generating group* for S if 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). If G is a generating group of a constellation S, then for every $s \in S$ the map $\mu_s : G \to S$ defined by $\mu_s(g) = gs$ is a bijection: these maps are called *labelings*.

Now we introduce the class of channels we shall consider in this paper. For a discrete set A, we use the notation $\mathcal{P}(A)$ for the space of all probability laws over A; otherwise, when A is a continuous set, $\mathcal{P}(A)$ will denote the space of probability densities over A. A *memoryless channel* (MC) of input set $\mathcal{X}$ and discrete (continuous) output set $\mathcal{Y}$ is a family of transition probability laws (densities) $\{W(\cdot|x) \in \mathcal{P}(\mathcal{Y})\}_{x\in\mathcal{X}}$.

Let G be an arbitrary group.

Definition 1: A MC $\{W(\cdot|x) \in \mathcal{P}(\mathcal{Y})\}_{x\in S}$ is said to be *G–symmetric* if

- S is a GU constellation with generating group G;
- G acts on $\mathcal{Y}$;
- $W(y|x) = W(gy|gx)$ for every $g \in G$, $x \in S$, $y \in \mathcal{Y}$.

Note that, once fixed a labeling μ_s, we can identify the input set of a G–symmetric MC with the group G itself: in the sequel we will do that without explicitly saying.

A first important property of G–symmetric channels is that their Shannon capacity C and their random coding exponent

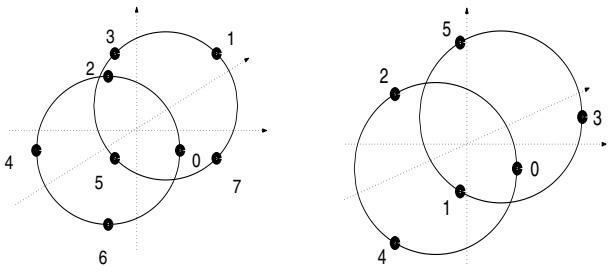

Fig. 1. $\mathbb{Z}_8$–labelled (8,h)–PSK and $\mathbb{Z}_6$–labelled 2–PAM×3–PSK

$E(R)$ (see [4] pagg.74,139 for formal definitions of these quantities) are both obtained with uniform distribution over the input set G.

Let S be an n–dimensional GU constellation equipped with a generating group G. Define the *S–AWGN channel* as the n–dimensional unquantized AWGN channel with input set S. Now let S' be another n–dimensional GU constellation such that $G \leq \Gamma(S')$. An *S'–quantization* is a map $Q : \mathbb{R}^n \to S'$ such that $||x - Q(x)|| = \min_{s \in S'} ||x - s||$. We define the *$(S, S')$–AWGN channel* as the DMC obtained by applying an S'–quantization Q to the output of the S–AWGN channel. Note that the special case $S = S'$ coincides with the hard decoding rule.

Proposition 2: The S–AWGN channel and the (S, S')–AWGN channel are both G–symmetric.

Example 1: Let m be a positive integer and L a positive real constant. Define the m–PSK constellation as

$$S{=}\{Le^{\frac{2\pi}{m}ki}, k = 1, \ldots, m\} \subset \mathbb{C} \cong \mathbb{R}^2 \ .$$

S admits $\mathbb{Z}_m$, i.e. the Abelian group of integers modulo m, as generating group. When m is even there is another generating group (see [2], [6]): the dihedral group $D_{m/2}$, which is noncommutative for $m \geq 6$. Now, let $m'{=}am$ be an arbitrary multiple of m and define the quantization map over Voronoi regions of the m'–PSK constellation:

$$Q : \mathbb{R}^2 \to \mathbb{Z}_{m'} \qquad Q(Ke^{\theta i}) = \left\lfloor \frac{m'\theta}{2\pi} \right\rfloor$$

The m–PSK–AWGN channel and the (m–PSK,m'–PSK)–AWGN channel are both $\mathbb{Z}_m$–symmetric and –whenever m is even– $D_{m/2}$–symmetric.

Example 2: Consider now the Cartesian product constellation m–PSK×2–PAM given by

$$S = \{(Le^{\frac{2\pi}{m}ki}, (-1)^l Lh),\ k = 0, 1, 2,\ l = 0, 1\} \subset \mathbb{C}{\times}\mathbb{R} \cong \mathbb{R}^3$$

where h and L are positive real constants, and shown in Fig.1 in the special case $m = 3$. It's easy to show that $\mathbb{Z}_m \times \mathbb{Z}_2$ is a generating group for S; note that, for odd m, $\mathbb{Z}_m \times \mathbb{Z}_2 \simeq \mathbb{Z}_{2m}$. Thus, for odd m, unquantized and quantized AWGN channels with input m–PSK×2–PAM are $\mathbb{Z}_{2m}$–symmetric.

Example 3: For even m we introduce the 3–dimensional (m,h)–PSK constellation

$$S = \{(Le^{\frac{2\pi}{m}(2k+l)i}, (-1)^l Lh),\ 1 \leq k \leq \tfrac{m}{2},\ l = 0, 1\} \subseteq \mathbb{C}{\times}\mathbb{R},$$

where h and L are positive real constants; an (8,h)–PSK constellation is shown in Fig.1. It can be shown that, such as the m–PSK, the (m,h)–PSK constellation has two different generating groups, $\mathbb{Z}_m$ and $D_{m/2}$; so, in the standard way, we obtain channels that are both $\mathbb{Z}_m$–symmetric and $D_{m/2}$–symmetric.

In this paper we will focus on $\mathbb{Z}_m$–symmetric channels; note that the additive group $\mathbb{Z}_m$ also has ring structure. Since the input of a $\mathbb{Z}_m$–symmetric channel can be identified with $\mathbb{Z}_m$, block encoders for such channels are (eventually non injective) maps $f : M \to \mathbb{Z}_m^N$, where N is the *block length* and A a finite set; the *rate* of f is defined as the logarithm of its domain cardinality divided by the block length: $R := \frac{\log |M|}{N}$ (throughout this paper the base of $\log$ and $\exp$ will be the same, arbitrary fixed, positive number).

We restrict our investigation to the class of *$\mathbb{Z}_m$–encoders*, where we define a $\mathbb{Z}_m$–encoder of length N and rate R as a $\mathbb{Z}_m$–module homomorphism $\phi_m : M \to \mathbb{Z}_m^N$, such that $\frac{log M}{N} = R$. An important subclass of $\mathbb{Z}_m$–encoders is that of *$\mathbb{Z}_m$–free encoders*: a $\mathbb{Z}_m$–free encoder is a $\mathbb{Z}_m$–encoder whose domain is a finite free module over $\mathbb{Z}_m$. We recall that, for a given ring A, a finitely generated A-free module is an Abelian group M isomorphic to A^K for some $K \in \mathbb{N}$: we emphasize the fact that, if A is not a field, then not every A–module is free (definitions and properties of modules can be found in any algebra textbook, see for example [5]).

One important reason for considering $\mathbb{Z}_m$–encoders is that for them the *uniform error property* (UEP) under ML decoding holds true when they are employed on a $\mathbb{Z}_m$-symmetric channel. This means that the *word error probability* using a $\mathbb{Z}_m$–encoder $\phi_m \in \mathrm{Hom}(M, \mathbb{Z}_m^N)$, conditioned to the transmission of any information word $u \in M$, which we denote by $P_w(e|\phi_m, u)$, does not depend on u. In particular we have that $P_w(e|\phi_m, u) = P_w(e|\phi_m, 0)$. This also implies that the average word error probability can be computed as

$$P_w(e|\phi_m) := \frac{1}{|M|} \sum_{u \in M} P_w(e|\phi_m, u) = P_w(e|\phi_m, 0) \ .$$

III. $\mathbb{Z}_m$–CAPACITY AND THE CONVERSE TO THE CHANNEL CODING THEOREM FOR $\mathbb{Z}_m$–FREE ENCODERS

Now we want to enlighten some algebraic obstructions affecting $\mathbb{Z}_m$–free encoders: this is done by introducing a new concept of capacity for $\mathbb{Z}_m$–symmetric channels and showing that no reliable transmission is possible with $\mathbb{Z}_m$–free encoders at rates above this capacity.

Suppose a $\mathbb{Z}_m$–symmetric channel is given and let

$$\phi_m : \mathbb{Z}_m^K \to \mathbb{Z}_m^N$$

be a free $\mathbb{Z}_m$–encoder of rate $R_m = \frac{K}{N} \log m$. Let $l{>}1$ be a divisor of m (we denote this with $l|m$). Consider the encoder $\phi_l : \frac{m}{l}\mathbb{Z}_m^K \to \mathbb{Z}_m^N$ obtained from ϕ_m by restricting its domain from $\mathbb{Z}_m^K$ to $\frac{m}{l}\mathbb{Z}_m^K$. The rate of ϕ_l is given by

$$R_l := \frac{K}{N} \log l = R_m \frac{\log l}{\log m} \ .$$

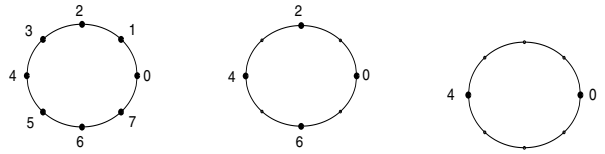

Fig. 2. 8-th, 4-th and 2-nd subchannels of the $\mathbb{Z}_8$–symmetric 8–PSK AWGN

Note that the image of ϕ_l is contained in the subgroup $\frac{m}{l}\mathbb{Z}_m^N$. So, let us consider the channel obtained by restricting the input set from $\mathbb{Z}_m$ to $\frac{m}{l}\mathbb{Z}_m$ (see fig.2 for the case of 8–PSK): we shall call it the *l–th subchannel* and denote by C_l its classical Shannon capacity and by $E_l(R)$ its random coding exponent.

The l–subchannel is $\frac{m}{l}\mathbb{Z}_m$–symmetric, so that C_l and $E_l(R)$ are both obtained with uniform distribution over the input set $\frac{m}{l}\mathbb{Z}_m$. The converse to the channel coding theorem (see [4] Th. 4.3.4), implies that necessary condition for $P_w(e|\phi_l)$ to be made arbitrarily small is that $R_l \leq C_l$, i.e.

$$R_m \leq \frac{\log m}{\log l} C_l \ .$$

On the other hand, it is clear that, for every $l \mid m$, we have $P_w(e|\phi_m) \geq P_w(e|\phi_l)$; thus, if $P_w(e|\phi_l)$ is bounded away from 0 independently of the block length N, so is $P_w(e|\phi_m)$. This reasoning leads to the following conclusion, providing an intrinsic limitation for free $\mathbb{Z}_m$–encoders over $\mathbb{Z}_m$–symmetric channels. First an important definition:

Definition 3: The *$\mathbb{Z}_m$–capacity* of a $\mathbb{Z}_m$–symmetric channel is

$$\hat{C}_m := \min_{\substack{l|m \\ l>1}} \frac{\log m}{\log l} C_l$$

where, for every $l \,|\, m$, C_l is the Shannon capacity of the l–th subchannel.

Theorem 4: Consider a $\mathbb{Z}_m$–symmetric channel and let $\hat{C}_m$ be its $\mathbb{Z}_m$–capacity. Then, for every $R > \hat{C}_m$ there exists $K_R > 0$ depending on R but not on N, such that, for every free $\mathbb{Z}_m$–encoder ϕ_m of rate R, with any decoding rule, the corresponding word error probability satisfies

$$P_w(e|\phi_m) \geq K_R \ .$$

Note that, while for an arbitrary $\mathbb{Z}_m$–symmetric channel we have $\hat{C}_m \leq C_m$, when m is a prime number (for instance in the binary case) $\hat{C}_m = C_m$.

IV. Ensembles of $\mathbb{Z}_m$–free codes

In this section we present a result which completes Theorem 4 by stating that at every rate $R < \hat{C}_m$ reliable transmission is possible using $\mathbb{Z}_m$–free encoders. This is done using a probabilistic method: we define a sequence of random $\mathbb{Z}_m$–free encoders and show that the sequence of their averaged word error probabilities converges to 0 exponentially in the block length.

Given $N \in \mathbb{N}$ and $R \in [0, \log m]$ define

$$K := \left\lceil \tfrac{R}{\log m} N \right\rceil \ .$$

The ensemble $\mathcal{E}_{\mathbb{Z}_m}(N,R)$ consists of the set all encoders $\phi_m \in \mathrm{Hom}(\mathbb{Z}_m^K, \mathbb{Z}_m^N)$ equipped with the uniform probability. Let $\overline{P(e)}^{(N,R)}$ denote the word error probability averaged over this ensemble.

We have the following fundamental result.

Theorem 5: The following estimation holds true:

$$\overline{P_w(e)}^{(N,R)} \leq \sum_{\substack{l|m \\ l>1}} \exp(-N E_l(R_l)) \tag{1}$$

where, for every $l \mid m$, $l > 1$, $E_l(R)$ is the random coding exponent of the l–th subchannel and $R_l := \frac{K}{N} \log l$ is its rate. *Sketch of the proof:* We first notice that because of the uniform error property all estimations of the word error probability can be done assuming that the information word $u = \mathbf{0}$ has been transmitted. We then consider the following partition of the set of encoder's input:

$$\mathbb{Z}_m^K = \textstyle\bigcup_{l|m} H_{K,l} \ ,$$

$$H_{K,l} := \{\mathbf{u} \in \mathbb{Z}_m^K : \gcd(u_1, \ldots, u_K, m) = \tfrac{m}{l}\} \subseteq \tfrac{m}{l}\mathbb{Z}_m^K \ .$$

The reason for choosing such a partition is that it can be shown that for every $\mathbf{u} \in H_{K,l}$, if Φ is a random variable uniformly distributed over $\mathrm{Hom}(\mathbb{Z}_m^K, \mathbb{Z}_m^N)$, then $\Phi\mathbf{u}$ is uniformly distributed over $\frac{m}{l}\mathbb{Z}_m^N$. For every $l \mid m$, $l > 1$ we define the random encoder Φ_l by restricting Φ's domain to the set $\{\mathbf{0}\} \cup H_{K,l}$. A union bound yields

$$P_w(e|\Phi_m, \mathbf{0}) \leq \sum_{\substack{l|m \\ l>1}} P_w(e|\Phi_l, \mathbf{0}) \ .$$

We then apply the Gallager bound (see [4], Th. 5.6.1) separately to each term $P_w(e|\Phi_l, \mathbf{0})$, and finally average over the ensemble. The result follows from the fact that each random coding exponent $E_l(R)$ is obtained with uniform distribution over the input set $\frac{m}{l}\mathbb{Z}_m$.

Standard probabilistic arguments yield the following:

Corollary 6: Consider a $\mathbb{Z}_m$–symmetric channel whose $\mathbb{Z}_m$–capacity is $\hat{C}_m$. Then, for every $R < \hat{C}_m$and for every $\varepsilon > 0$, there exists a free $\mathbb{Z}_m$–encoder ϕ_m, of rate greater than or equal to R, whose ML decoding word error probability satisfies

$$P_w(e|\phi_m) < \varepsilon \ . \tag{2}$$

Proof: Since $R < \hat{C}_m$, if follows that, for every $l \mid m$, $l > 1$, $R_l = \frac{\log l}{\log m} R < C_l$ and so $E_l(R_l) > 0$. Thus Theorem 5 implies that $\overline{P_w(e)}^{(N,R)}$ is exponentially decreasing to zero as $N \to +\infty$. So $N_0 \in \mathbb{N}$ exists such that $\overline{P_w(e)}^{(N,R)} < \varepsilon$ for every $N \geq N_0$; but at least one encoder $\phi_m \in \mathrm{Hom}(\mathbb{Z}_m^K, \mathbb{Z}_m^N)$ is such that $P_w(e|\phi_m) \leq \overline{P_w(e)}^{(N,R)}$, so (2) follows.

V. $\mathbb{Z}_{2^r}$-codes over 2^r-PSK achieve capacity!

Theorem 4 and Corollary 6 clearly show that the $\mathbb{Z}_m$–capacity is the fundamental limit for the rate of a reliable transmission with free $\mathbb{Z}_m$–encoders over a $\mathbb{Z}_m$–symmetric channel.

For prime p, $\mathbb{Z}_p$ has the structure of the Galois field GF(p), and –as we have already observed– the $\mathbb{Z}_p$–capacity coincides with the classical capacity; in this case Corollary 6 states that linear codes over $\mathbb{Z}_p$ achieve Shannon capacity of every $\mathbb{Z}_p$–symmetric channel, a well known result (see [6] Th. 6).

For non prime m it remains to answer the question whether $\hat{C}_m = C_m$ or $\hat{C}_m < C_m$: in the former case there would be no algebraic obstructions to free $\mathbb{Z}_m$–encoders, in the latter the restriction to free $\mathbb{Z}_m$–encoders would cause a loss of capacity.

In this section we investigate capacity inequalities of (S, S')–AWGN channels for the three GU constellations introduced in Examples 1, 2, 3; these special cases are both of interest in applications and representative of three typical situations that may occur.

Example 4: First, fix a positive integer r and consider the (2^r–PSK)–AWGN channel. Denote with $C_{r,q}$ its capacity.

Theorem 7: For $1 \leq r \leq q-1$ the following inequality holds true:

$$rC_{r+1} \leq (r+1)C_r \ . \tag{3}$$

The proof, which will be given elsewhere, is essentially based on convexity properties of the entropy function and on the structure of the order of Euclidean distances of a generic point in $\mathbb{R}^2$ from the point of 2^r–PSK.

From Theorem 7 it immediately follows that, for every $1 \leq s \leq r$, we have $C_r \leq \frac{r}{s} C_s$ and so

$$\hat{C}_{2^r} = C_{2^r} \ . \tag{4}$$

Thus, Corollary 6 implies that *free $\mathbb{Z}_{2^r}$–encoders achieve capacity of any (2^r–PSK)–AWGN channel*. This result is not trivial since it does not hold true for every GU constellation with cyclic generating group $\mathbb{Z}_m$, as next two examples show.

Example 5: Consider now the 3–PSK×2–PAM constellation introduced in Example 2. It is easy to show that the capacity of the $\mathbb{Z}_6$–symmetric (3–PSK×2–PAM)–AWGN channel satisfies

$$C_6 = C_2 + C_3 \tag{5}$$

where C_2 and C_3 coincide with the capacities of the (2–PAM)–AWGN and the (3–PSK)–AWGN channel, respectively. Then, a direct calculation shows that necessary and sufficient condition for $\hat{C}_6 = C_6$ to hold is

$$\log 3 \ C_2 = \log 2 \ C_3 \ . \tag{6}$$

Equation (6) is not satisfied by almost all values of h and N_0 (indeed it can be shown that equation (6) has exactly one solution in h for every fixed value of $\frac{L}{N_0} \in (0, +\infty)$).

Thus, typically we have

$$\hat{C}_6 < C_6 \ ,$$

and from Theorem 4 it follows that *free $\mathbb{Z}_6$–codes do not achieve capacity* of this channel.

Instead, let us relax our request for free $\mathbb{Z}_6$–encoders and simply look for $\mathbb{Z}_6$–encoders, i.e. homomorphisms

$$\phi_6 : \mathbb{Z}_2^{K_2} \times \mathbb{Z}_3^{K_3} \to \mathbb{Z}_6^N, \ \phi_6(\mathbf{u}_2, \mathbf{u}_3) = 3\phi_2\mathbf{u}_2 + 2\phi_3\mathbf{u}_3 \ , \tag{7}$$

where $\phi_2 \in \mathrm{Hom}(\mathbb{Z}_2^{K_2}, \mathbb{Z}_2^N)$ and $\phi_3 \in \mathrm{Hom}(\mathbb{Z}_3^{K_3}, \mathbb{Z}_3^N)$. The rate of the encoder ϕ_6 defined by (7) is $R_6 = R_2 + R_3$ where $R_2 = \frac{K_2}{N} \log 2$ and $R_3 = \frac{K_3}{N} \log 3$ are the rates of encoders ϕ_2 and ϕ_3 respectively.

Suppose now a design rate $R_6 < C_6$ is assigned; define

$$R_2 = \frac{C_2}{C_6} R \ , \quad R_3 = \frac{C_3}{C_6} R \ .$$

From (5) we have $R_2 < C_2$ and $R_3 < C_3$ and so, by Corollary 6, for every $\varepsilon > 0$ a free $\mathbb{Z}_2$–encoder ϕ_2 and free $\mathbb{Z}_3$–encoder exist whose word error probabilities under ML decoding satisfy respectively $P_w(e|\phi_2) < \frac{\varepsilon}{2}$ and $P_w(e|\phi_3) < \frac{\varepsilon}{2}$. The word error probability under ML decoding of the $\mathbb{Z}_6$–encoder ϕ_6 defined by (7) satisfies then

$$P_w(e|\phi_6) = P_w(e|\phi_2) + P_w(e|\phi_3) - P_w(e|\phi_2)P_w(e|\phi_3) < \varepsilon \ .$$

Thus *(non free) $\mathbb{Z}_6$–encoders achieve the capacity* of the (3–PSK×2–PAM)–AWGN channel.

Similar considerations can be extended to every constellation S which is the Cartesian product of two GU constellation of generating group $\mathbb{Z}_{m_1}$ and $\mathbb{Z}_{m_2}$ respectively. If m_1 and m_2 are relatively prime, then $\mathbb{Z}_{m_1 m_2} \simeq \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2}$ is a generating group for S; if $\hat{C}_{m_1} = C_{m_1}$ and $\hat{C}_{m_2} = C_{m_2}$, then, even if $\hat{C}_{m_1 m_2} < C_{m_1 m_2}$ so that $\mathbb{Z}_{m_1 m_2}$–free encoders do not achieve the capacity of the (S, S)–AWGN channel, you can achieve capacity with non–free $\mathbb{Z}_{m_1 m_2}$–encoders.

Example 6: Finally consider the (2^r,h)–PSK constellation introduced in Example 3. For $h \to 0$, (2^r,h)–PSK collapses into 2^r–PSK. So, by continuity, for sufficiently small values of h, (4) remains true for the ((2^r,h)–PSK)–AWGN channel and we can assert that *free $\mathbb{Z}_{2^r}$–codes achieve capacity*.

Conversely, it can be shown that

$$\lim_{h \to +\infty} rC_{2^{r-1}} - (r-1)C_{2^r} < 0 \ .$$

So, for high values of h, we have $\hat{C}_{2^r} < C_{2^r}$ and thus *$\mathbb{Z}_{2^r}$–free codes do not achieve capacity*.

Moreover, since (2^r,h)–PSK is not the Cartesian product of two orthogonal constellations, we cannot repeat the considerations made for the 3–PSK×2–PAM modulation to find non–free $\mathbb{Z}_{2^r}$–encoders of arbitrarily small word error probability.

Actually it can be shown that, for high values of h, also non–free $\mathbb{Z}_{2^r}$–encoders do not achieve capacity of the ((2^r,h)–PSK)–AWGN channel.

Instead, we think the dihedral group $D_{2^{r-1}}$ should be used as generating group for $(2^r, h)$–PSK constellation, and one should look for $D_{2^{r-1}}$–codes, i.e. subgroups of $D_{2^{r-1}}^N$.

VI. Low density $\mathbb{Z}_m$-codes

In this section we study the performance of $\mathbb{Z}_m$–LDPC codes over $\mathbb{Z}_m$–symmetric channels with ML decoding. The idea is to compare low density ensembles performances with those of $\mathbb{Z}_m$–free encoder ensembles $\mathcal{E}_{\mathbb{Z}_m}(R, N)$ established in Theorems 4 and 5.

Following [7] and [1], we define low density ensembles by their Tanner graph. Let c, d, N be three integers such that

$L := \frac{c}{d} N \in \mathbb{N}$, and fix an arbitrary $\pi \in S_{Nc}$, where we are using the standard notation S_n to denote the group of permutations of the set $\{1, \ldots, n\}$. Define the (c,d)–regular bipartite graph $\mathcal{G}_\pi = (\mathcal{N} \cup \mathcal{M}, E_\pi)$, where $\mathcal{N} = \{v_1, \ldots, v_N\}$ is the variable node set, $\mathcal{M} = \{h_1, \ldots, h_L\}$ is the check node set, and $E_\pi = \Big((v_{\lceil \frac{i}{c} \rceil}, h_{\lceil \frac{\pi(i)}{d} \rceil}),\ 1 \le i \le Nc \Big) \in (\mathcal{N} \times \mathcal{M})^{Ld}$ is the edge multiset. Note that we allow the presence of parallel edges, i.e. edges connecting the same couple of nodes, so that actually $\mathcal{G}_\pi$ is a multigraph. From $\mathcal{G}_\pi$ we define the homomorphism $\phi_\pi : \mathbb{Z}_m^N \to \mathbb{Z}_m^L$ by

$$(\phi_\pi \mathbf{x})_j = \sum_{(v_n, h_j) \in E_\pi} x_n \ , \qquad j = 1, \ldots, L \ ,$$

and finally the code $\mathcal{C}_\pi = \ker \phi_\pi$.

Now let Π be a random variable uniformly distributed over S_{Nc}. Π naturally induces a probabilistic structure over the set of $\mathbb{Z}_m$–codes of length N through the above construction. This probability space is the *ensemble of (c,d)–regular LDPC codes of length N*, and we denote it by $\mathcal{E}_{LDPC}(N,c,d)$. Note that all codes in the ensemble have rate greater than or equal to $\frac{N-L}{N} \log m = (1 - \frac{c}{d}) \log m$. Fix an arbitrary $\mathbb{Z}_m$–symmetric channel of $\mathbb{Z}_m$–capacity $\hat{C}_m$, and let $\overline{P_w(e)}^{(N,c,d)}$ be the ML decoding word error probability averaged over the ensemble $\mathcal{E}_{LDPC}(N,c,d)$.

Given two real sequences $(a_N)_{N \in \mathbb{N}}$ and $(b_N)_{N \in \mathbb{N}}$, we use the notation $a_N \asymp b_N$ to mean that two positive constants A and B, independent of N, exist such that $A a_n \le b_n \le B a_n$ definitively in N. We have the following result:

Theorem 8: Let R be an assigned design rate such that

$$0 < R < \hat{C}_m \qquad .$$

Then there exists a couple of integers (c,d) such that

$$c \ge 3 \ , \qquad \frac{R}{\log m} \le 1 - \frac{c}{d} \ , \tag{8}$$

$$\overline{P(e)}^{(N,c,d)} \asymp \begin{cases} N^{2-c} & \text{if } \gcd(c,m) = 1 \\ N^{1 - \frac{a-1}{a} c} & \text{if } \gcd(c,m) > 1 \end{cases} \ , \tag{9}$$

where $a := \mathrm{lpcf}(c,m)$ is the lowest prime common factor between c and m.

A proof of Theorem 8 will be given elsewhere. The upper bounds have been proved using arguments similar to those of [9] and [1] and essentially based on the random coding techniques for non random codes introduced in [10]. The main difference with respect to the proofs of [1] is that we carefully took into account the presence of subchannels. The technique to establish the lower bounds is rather standard and essentially consists in estimating the probability of having $d_{\min}(\mathcal{C})$ equal to 1 or 2, where the minimum distance $d_{\min}(\mathcal{C})$ of a code $\mathcal{C} \le \mathbb{Z}_m^N$ is as usual defined as the number of nonzero elements minimized over all but the all–zero codewords of $\mathcal{C}$.

Theorem 8 generalizes the results for the binary LDPC ensembles (see [8] Th. 4; analogously a generalization of Th. 3 can be prooved). As in the binary case, being free to choose the parameters c and d, for every assigned design rate $R < \hat{C}_m$ it is possible to find a (c,d)–regular LDPC $\mathbb{Z}_m$–code of rate greater than or equal to R and arbitrary low error probability.

Moreover, as in the binary case, $\overline{P_w(e)}^{(N,c,d)}$ is polynomially rather than exponentially decreasing in the block–length N. This is due to the presence in the ensembles $\mathcal{E}_{LDPC}(c,d,N)$ of codes with very low minimum distance. Actually the ML decoding word error probability of a typical $\mathbb{Z}_m$–code in $\mathcal{E}_{LDPC}(c,d,N)$ is exponentially decreasing to 0 in N; it is possible to show that by expurgating the ensemble of an asymptotically vanishing fraction of codes of poor performances, a technique already used by Gallager in his Ph.D. thesis ([3]).

VII. Conclusions

In this paper we analyzed the performances of block codes over $\mathbb{Z}_m$ with $\mathbb{Z}_m$–module structure. We proved that reliable communication is possible over the quantized or unquantized AWGN channel using $\mathbb{Z}_m$–free codes at every rate less than a fundamental limit which we called the $\mathbb{Z}_m$–capacity. We showed that for the 2^r–PSK constellation the $\mathbb{Z}_{2^r}$–capacity coincides with the classical Shannon capacity, while this is not the case for other GU constellations of practical interest. Finally we studied the performances of ML–decoded LDPC $\mathbb{Z}_m$–codes, and found that, as in the binary case, they can achieve $\mathbb{Z}_m$–capacity, if we allow their density parameters to grow suitably. Many questions remain open, and we are currently working on:

1) finding the $\mathbb{Z}_m$–capacity of other GU constellations and extending our analysis to non-free codes and to codes over noncommutative groups;
2) considering different non binary LDPC code ensembles, and especially irregular ones, since in the binary case it has been proved ([7]) they have better performances when used with iterative decoding;
3) studying BP–decoded LDPC codes performances in order to find out new design criteria for such codes.

References

[1] A. Bennatan, D. Burshetein , "On The Application of LDPC Codes to Arbitrary Discrete Memoryless Channels", *IEEE Trans. Inf. Theory*, vol. 50, pp.417-438, Mar. 2004.

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

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

[4] R. G. Gallager, *Information Theory and Reliable Communication*, Wiley, New York, 1968.

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

[6] H.-A. Loeliger, "Signal Sets Matched To Groups", *IEEE Trans. Inform. Theory*, vol. 37, n. 6, pp. 1675-1679, Nov. 1991.

[7] M.G. Luby, M. Mitzenmacher, M.A. Shokrollahi, D.A. Spielman, "Improved Low–Density Parity–Check Codes Using Irregular Graphs and Belief–Propagation", *IEEE Trans. Inform. Theory*, vol. 47, n. 2, pp. 585-598, Feb. 2001.

[8] D.J.C. MacKay, "Good Error Correcting Codes Based On Very Sparse Matrices", *IEEE Trans. Inf. Theory*, vol. 45, pp.399-431, Mar. 1999.

[9] G. Miller, D. Burshetein , "Bounds on the Maximum Likelihood Decoding Error Probability of Low–Density Parity–Check Codes", *IEEE Trans. Inf. Theory*, vol. 47, pp.2696-2710, Nov. 2001.

[10] N. Shulman, M. Feder, "Random Coding Techniques for Nonrandom Codes", *IEEE Trans. Inform. Theory*, vol. 45, NO.6, pp. 2001-2004, 1999.