SIAM J. DISCRETE MATH.
Vol. 23, No. 1, pp. 19–53

AVERAGE SPECTRA AND MINIMUM DISTANCES OF LOW-DENSITY PARITY-CHECK CODES OVER ABELIAN GROUPS*

GIACOMO COMO† AND FABIO FAGNANI‡

Abstract. Ensembles of regular low-density parity-check codes over any finite Abelian group G are studied. The nonzero entries of the parity matrix are randomly chosen, independently and uniformly, from an arbitrary label group of automorphisms of G. Precise combinatorial results are established for the exponential growth rate of their average type-enumerating functions with respect to the code-length N. Minimum Bhattacharyya-distance properties are analyzed when such codes are employed over a memoryless G-symmetric transmission channel. In particular, minimum distances are shown to grow linearly in N with probability one, and lower bounds are provided for the typical asymptotic normalized minimum distance. Finally, some numerical results are presented, indicating that the choice of the label group strongly affects the value of the typical minimum distance.

Key words. low-density parity-check codes, group codes, minimum distance, type-spectrum, Ramanujan sums

AMS subject classifications. 94B12, 94B65, 11T24

DOI. 10.1137/070686615

1. Introduction.

Low-density parity-check (LDPC) codes have received a huge amount of attention in the last years. It is indeed the family of high-performance codes for which the deepest theoretical insight has been achieved. Their definition is quite simple: they are those binary-linear codes which can be described as kernels of matrices over the binary field $\mathbb{Z}_2$ with a "small" number of nonzero elements. Since the pioneering work [19], two streams of research are easily recognizable in the literature on LDPC codes. On the one hand, structural properties of such codes have been investigated: distance-spectra, minimum distances, and also capacity estimations under maximum-likelihood (ML) decoding [28, 29, 25, 37, 25, 26, 9, 15, 33]. On the other hand, they have been studied coupled with the well-known iterative decoding schemes [34, 35, 42, 31, 43, 24, 36, 14].

The need to use transmission channels with higher spectral efficiency naturally leads one to consider nonbinary codes and nonbinary LDPC codes. A typical example is provided by the m-PSK Gaussian channel. This is a channel accepting as possible input any element in the set $m\text{-PSK} := \{e^{\frac{2\pi}{m}li} \mid 1 \leq l \leq m\}$, while the received output is obtained by adding a homogeneous, zero-mean, two-dimensional Gaussian variable. When m is an integer power of 2—a case which is particularly relevant in practice—in principle binary codes can be used for transmission over this channel. Using any fixed bijection $\lambda : \mathbb{Z}_2^r \to 2^r\text{-PSK}$, binary-linear codes can be mapped into codes on the alphabet 2^r-PSK. The problem with this type of code is that, if $r > 2$, for any possible choice of λ they will not possess many of the symmetry properties that binary-linear codes enjoy on binary symmetric channels: Voronoi regions will not be congruent, Euclidean distance profiles will depend on the reference codeword, and

*Received by the editors March 28, 2007; accepted for publication (in revised form) June 6, 2008; published electronically October 24, 2008.
http://www.siam.org/journals/sidma/23-1/68661.html
†Dipartimento di Matematica, Politecnico di Torino, Corso Duca degli Abruzzi 24, 10129 Torino, Italy. Current address: Laboratory for Information and Decision Systems, Massachusetts Institute of Technology, 77 Mass. Ave., Cambridge, MA 02139 (giacomo@mit.edu).
‡Dipartimento di Matematica, Politecnico di Torino, Corso Duca degli Abruzzi 24, 10129 Torino, Italy (fabio.fagnani@polito.it).

the uniform error property will not hold. As a consequence the theoretical analysis becomes quite hard and design-criteria optimization exceedingly complicated; in [22, 4, 5] an average-coset approach has been adopted in order to overcome this problem. Actually, for such an input set, a much better candidate group structure is provided by the cyclic group $\mathbb{Z}_m$. Indeed, if we consider the natural map $\lambda : \mathbb{Z}_m \to m$-PSK (with $\lambda(l) = e^{\frac{2\pi i l}{m}}$), any subgroup $\mathcal{C} \subseteq \mathbb{Z}_m^N$ yields, through the embedding λ, a code over m-PSK possessing congruent Voronoi regions and invariant distance profiles [18, 27]. These codes (as well as the subgroups they come from) are called $\mathbb{Z}_m$-codes. All of this construction can be generalized to a broader family of transmission channels exhibiting symmetry with respect to the action of a finite group G, which will be called G-symmetric channels, and to a family of codes with group structure which will be called G-codes.

$\mathbb{Z}_m$-codes have been widely studied in the past (see, for instance, [3]). A remarkable fact is that, since $\mathbb{Z}_m$ is a commutative ring, they can be represented, as in the binary case, as images or kernels of matrices with coefficients in $\mathbb{Z}_m$. In this paper we are particularly interested in kernel representations: given a matrix Φ in $\mathbb{Z}_m^{L\times N}$,

$$\mathcal{C} := \{\boldsymbol{x} \in \mathbb{Z}_m^N \mid \Phi\boldsymbol{x} = 0\}$$

is obviously a $\mathbb{Z}_m$-code. Regular LDPC $\mathbb{Z}_m$-codes can easily be constructed by considering syndrome matrices with a fixed amount of nonzero elements both on each row and on each column and, as in the binary case, randomly selecting nonzero positions through a random-permutation approach. An interesting difference with respect to the binary case is the way to choose the nonzero elements of Φ. In this paper we will consider many different possibilities. Among them, we consider the so-called *unlabelled ensemble*, where nonzero elements are all equal to 1, and the *uniformly labelled ensemble*, where nonzero elements are instead, each one independently, chosen to be any possible invertible element in the ring $\mathbb{Z}_m$ with uniform probability. We will see that the latter ensemble will outperform the former. Of course our results could be extended to irregular LDPC ensembles, where the fraction of rows and columns with different amounts of nonzero entries (degree profile) is fixed, although this extension will not be considered here. Nonbinary LDPC codes have been considered for binary-input channels as well (see [32], for instance). In this case, they allow us to introduce a new design parameter, the choice of the nonzero entries in the parity matrix, to be optimized jointly with the degree profile.

LDPC codes over nonbinary alphabets were already introduced and studied in Gallager's seminal work [19]. Precisely, Gallager considered regular ensembles of LDPC $\mathbb{Z}_m$-codes with all nonzero entries equal to 1 (unlabelled ensembles in our terminology); he studied their Hamming distance-spectra and provided bounds for their error probabilities under ML and suboptimal iterative decoding over some highly symmetric channels. More recently, after the rediscovery of Gallager codes in the 1990s, LDPC codes over nonbinary fields, both for binary and nonbinary channels, have received a considerable amount of attention by researchers. In [13], the authors show empirical evidence that, appropriately choosing the values of the nonzero entries in the parity-check matrix, LDPC codes over the Galois field $\mathbb{F}_{2^r}$ perform better than the corresponding binary LDPC codes when used over binary-input output-symmetric channels. LDPC codes over $\mathbb{F}_{2^r}$ for binary-input output-symmetric channels have also been studied in [32] following a density-evolution approach. The works [4, 5, 17] contain quite a complete theoretical analysis of LDPC codes over finite fields for nonbinary channels considering both ML and belief-propagation decoding. Average

type-spectra of regular LDPC ensembles over $\mathbb{Z}_p$ in the special case when p is prime, and more in general over $\mathbb{F}_{p^r}$, have been studied in [17, 4]. In this case the structural theory of binary LDPC codes generalizes in an almost straightforward way. In particular it has been shown, using expurgation techniques and results from [39], that average type-spectra provide lower bounds to the typical error exponent of these ensembles and that this exponent can be made arbitrarily close to the random-coding one by allowing the density of the parity matrix to grow while keeping the rate constant. Finally the recent works [8, 30, 38] investigate the possibility of using hybrid nonbinary LDPC codes over multiple groups.

However, in the case of algebraic structures which are not fields (e.g., $\mathbb{Z}_m$ with nonprime m), the available theoretical results are very few. In [4], average type-spectra of unlabelled ensembles of LDPC $\mathbb{Z}_m$-codes have also been studied in the case when m is not prime, but there are no results on minimum Euclidean distances. In the papers [40, 1, 44] the case when m is not prime has been considered but mainly from an iterative-decoding perspective. Computer simulations have been reported in [40, 44] showing that, when mapped over the m-PSK constellation, LDPC $\mathbb{Z}_m$-codes guarantee better performance than their binary counterparts.

When m is not prime, the lack of field structure implies that the theory of $\mathbb{Z}_m$-codes itself (with no restriction on the density of their kernel representation) is not as simple as in the linear case. This issue has been addressed in [10, 11], where the capacity achievable by $\mathbb{Z}_m$-codes (and more in general by Abelian group codes) over symmetric channels—called $\mathbb{Z}_m$-capacity—has been characterized in terms of the capacities of the channels obtained by restricting the input to all nontrivial subgroups of $\mathbb{Z}_m$ (see (2.5) in section 2.3). For the m-PSK constellation (when m is an integer power of a prime) it has been proved that $\mathbb{Z}_m$-codes achieve capacity, while this is no longer the case for other possible geometrically uniform constellations. Type-spectra and minimum distances of ensembles of $\mathbb{Z}_m$-codes have been studied in [12], where it has been shown that the typical $\mathbb{Z}_8$-code asymptotically achieves the Gilbert–Varshamov bound of the 8-PSK AWGN channel. The study of the properties of group-code ensembles gives insight into the theory of LDPC codes over groups, since it allows one to distinguish between the possible loss in performance due to the group structure and the one due to the sparseness of the syndrome representation.

In this paper we will study in detail average type-spectra and minimum Bhattacharyya-distances of regular LDPC ensembles over any finite Abelian group G, in which the nonzero entries of the parity-check operator are randomly sampled, independently and uniformly, from an arbitrary group F of automorphisms of G (briefly F-labelled ensembles), generalizing all of the results in [19, 13, 17, 4]. This extension passes through the use of mathematical tools which do not show up in the binary case: group characters, arithmetic concepts (Möbius inversion formula, Ramanujan sums), combinatorial techniques (Cayley graphs), and convex-analytical techniques.

As a first result, we will find exact expressions in terms of combinatorial formulas for the average type-spectra of regular F-labelled ensembles of LDPC codes over G; see Theorem 3.5. For the unlabelled ensemble of LDPC codes over $\mathbb{Z}_m$, we will show that our results for average type-spectra coincide with those obtained in [19, 4], while for LDPC codes over finite fields the results of [13, 17, 4] will be recovered. Theorem 3.5 is instead completely original, to the best of our knowledge, for the uniformly labelled ensemble of LDPC codes over $\mathbb{Z}_m$, for which the average type-spectrum has an elegant expression in terms of Ramanujan sums. Coupling this analysis with an ad hoc analysis for the low-weight average type-enumerating functions, we will finally propose upper bounds to the probability distribution of the minimum Bhattacharyya distance

[6]. This will allow us to show that minimum distances grow linearly in N with probability one (see Theorems 5.1 and 5.2): in the coding terminology this means that such codes are asymptotically good with probability one. More precisely, we obtain almost sure lower bounds on the asymptotic normalized minimum distance of the LDPC ensembles. These bounds are defined as the solution of $(|G|-1)$-dimensional optimization problems. Proving the tightness of these bounds would require second-moment estimations for the type-enumerating functions and is a problem left for future research. However, concentration results available in the literature for the Hamming distance-spectra of regular ensembles of binary LDPC codes (see [33]) make us optimistic about the tightness of our bounds for regular ensembles of LDPC G-codes as well. Finally, we will present some numerical results for the average distance-spectra showing how strongly the choice of the label group F affects the value of the typical minimum distance. In particular, we will show that, for the 8-PSK AWGN channel, the distance properties of the uniformly labelled ensemble of LDPC $\mathbb{Z}_8$-codes are significantly better than those of the unlabelled ensemble. This is confirmed by Monte Carlo simulations of these codes which we have run, and it agrees with some of the simulation results reported in [4].

The remainder of this paper is organized as follows. Section 2 is devoted to a formal introduction of all of the fundamental concepts: G-symmetric channels and the associated Bhattacharyya distance, Abelian group codes and their capacity, and LDPC code ensembles over Abelian groups. In section 3 we study the average type-enumerating functions of these ensembles, and we determine their exact growth rate, namely the so-called average type-spectrum: the main result is Theorem 3.5. Section 4 is a technical one devoted to a detailed probabilistic analysis of low-weight codewords: the main result is Theorem 4.6. Using the results of sections 3 and 4 we are able to prove, in section 5, a probabilistic lower bound on the growth of minimum Euclidean distances for the LDPC ensembles when the block-length N goes to infinity; see Theorems 5.1 and 5.2. Finally, in section 6 we report some numerical simulations showing that the uniformly labelled ensemble of LDPC $\mathbb{Z}_8$-codes definitely outperforms the unlabelled one on the 8-PSK AWGN channel, and we draw some final conclusions. An appendix completes the paper, containing some of the most technical proofs and a technical lemma on semicontinuous functions.

2. The coding setting.

2.1. Notation. Throughout the paper $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{C}$ will denote the usual number sets. With $\mathbb{R}_+$ ($\mathbb{Z}_+$) we will indicate the set of nonnegative reals (integers). If z is in $\mathbb{C}$, then z^* is its conjugate. The functions log and exp are to be considered with respect to a fixed base $a > 1$. Conventionally, $\inf(\emptyset) = +\infty$, $\sup(\emptyset) = -\infty$. For any subset $B \subseteq A$, $\overline{B} := A \setminus B$ will denote the complement of B in A, while $\mathbb{1}_B : A \to \{0,1\}$ will denote the indicator function of B, defined by $\mathbb{1}_B(a) = 1$ if a belongs to B and $\mathbb{1}_B(a) = 0$ otherwise. For a finite set A, $L^2(A)$ will denote the vector space of all $\mathbb{C}$-valued functions on A, equipped with the Hermitian form $\langle \boldsymbol{f}, \boldsymbol{g} \rangle = \sum_{a \in A} \boldsymbol{f}(a)\boldsymbol{g}(a)^*$. For a function $\boldsymbol{f}$ in $L^2(A)$ we shall indicate by $\mathrm{supp}(\boldsymbol{f}) := \big\{a \in A \big| \, \boldsymbol{f}(a) \neq 0\big\}$ the support of $\boldsymbol{f}$. Given $\boldsymbol{f}, \boldsymbol{g} \in L^2(A)$, $\boldsymbol{f} \cdot \boldsymbol{g} \in L^2(A)$ will denote their pointwise product, while we define $\boldsymbol{f}^{\boldsymbol{g}} := \prod_{a \in \mathrm{supp}(\boldsymbol{f})} \boldsymbol{f}(a)^{\boldsymbol{g}(a)}$. We consider the simplex $\mathcal{P}(A)$ of probability measures on A, $\mathcal{P}(A) := \{\boldsymbol{\theta} : A \to \mathbb{R}_+ | \, \sum_a \boldsymbol{\theta}(a) = 1\}$. Given a subset $B \subseteq A$, we shall use the notation $\boldsymbol{\theta}(B) := \sum_{b \in B} \boldsymbol{\theta}(b)$. For a in A, δ_a in $\mathcal{P}(A)$ will be the probability measure concentrated on a. The entropy function $\mathrm{H} : \mathcal{P}(A) :\to \mathbb{R}$ and the Kullback–Leiber distance $D(\cdot||\cdot) : \mathcal{P}(A) \times \mathcal{P}(A) \to [0, +\infty]$

are defined, respectively, by

$$\mathrm{H}(\boldsymbol{\theta}) := -\sum_{a\in\mathrm{supp}(\boldsymbol{\theta})} \boldsymbol{\theta}(a)\log\boldsymbol{\theta}(a), \qquad D\left(\boldsymbol{\theta}||\boldsymbol{\theta}'\right) := \sum_{a\in\mathrm{supp}(\boldsymbol{\theta})} \boldsymbol{\theta}(a)\log\frac{\boldsymbol{\theta}(a)}{\boldsymbol{\theta}'(a)}.$$

Given $\boldsymbol{x}\in A^N$, its *A-type* (or empirical frequency) is the probability measure $\boldsymbol{\theta}_A(\boldsymbol{x})\in\mathcal{P}(A)$ given by $[\boldsymbol{\theta}_A(\boldsymbol{x})](a) = \frac{1}{N}|\{1\le i\le N : x_i = a\}|$. Define the set of types of all N-tuples by $\mathcal{P}_N(A) := \boldsymbol{\theta}_A(A^N)$, and let $\mathcal{P}_{\mathbb{N}}(A) := \bigcup_N \mathcal{P}_N(A)$ be the set of all A-types. The number of A-types $|\mathcal{P}_N(A)| = \binom{N+|A|-1}{|A|-1}$ is a quantity growing polynomially fast in N. Instead, the set of N-tuples of a given type $\boldsymbol{\theta}$, denoted by

$$A^N_{\boldsymbol{\theta}} := \left\{\boldsymbol{x}\in A^N \text{ such that (s.t.) } \boldsymbol{\theta}_A(\boldsymbol{x}) = \boldsymbol{\theta}\right\},$$

has cardinality growing exponentially fast with N. More precisely, for $\boldsymbol{\theta}\in\mathcal{P}_{\mathbb{N}}(A)$, consider the set $\mathcal{N}_{\boldsymbol{\theta}} := \{N : N\boldsymbol{\theta}(a)\in\mathbb{N}\ \forall a\in A\}$ which is infinite since $|A|\mathbb{N}\subseteq\mathcal{N}_{\boldsymbol{\theta}}$. Then, for every $N\in\mathcal{N}_{\boldsymbol{\theta}}$, we have $\left|A^N_{\boldsymbol{\theta}}\right| = \binom{N}{N\boldsymbol{\theta}} := N!/\prod_a (N\boldsymbol{\theta}(a))!$, and Stirling's formula implies that

$$\left|A^N_{\boldsymbol{\theta}}\right| \le \exp(N\,\mathrm{H}(\boldsymbol{\theta})), \qquad \lim_{N\in\mathcal{N}_{\boldsymbol{\theta}}} \frac{1}{N}\log\left|A^N_{\boldsymbol{\theta}}\right| = \mathrm{H}(\boldsymbol{\theta}). \tag{2.1}$$

2.2. Symmetric channels. A memoryless channel (MC) is described by a finite input set $\mathcal{X}$, an output set consisting of a σ-finite measure space $\mathcal{Y} = (Y,\mathcal{B},\nu)$, and a family of transition probability densities $P(\cdot|x)$ on $\mathcal{Y}$ indexed by the possible inputs x in $\mathcal{X}$. Such a channel will be denoted by $(\mathcal{X},\mathcal{Y},P)$. In the applications there are essentially two possibilities: either Y is finite and ν is simply the counting measure (and in this case $P(\cdot|x)$ are simply probabilities on $\mathcal{Y}$), or $\mathcal{Y}$ is an n-dimensional Euclidean space and ν is the corresponding Lebesgue measure. Keeping this more abstract formalism will allow us to cover both cases at once.

We now recall the concept of a group action. Given a finite group G with identity 1_G and a (finite) set A, we say that G acts on A if, for every g in G, it is defined as a map from A to A denoted by $a\mapsto ga$, such that $1_G a = a$ for all a in A and $h(ga) = (hg)a$ for all h,g in G and a in A. The action of G over A is said to be (simply) transitive if for every $a,b\in A$ there exists one (and only one) element g of G such that $ga = b$. If the action is simply transitive, G and A are clearly in bijection: $g\mapsto ga_0$, where a_0 is some fixed reference element in A.

Given a σ-finite measure space $\mathcal{Y} = (Y,\mathcal{B},\nu)$, we say that the group G acts isometrically on $\mathcal{Y}$ if it is defined as an action of G on Y consisting of measurable bijections such that

$$\nu(gA) = \nu(A) \qquad \forall A\in\mathcal{B},\ \forall g\in G. \tag{2.2}$$

Notice that in the case, when Y is a finite set, (2.2) is trivially always verified so that in this case all actions are isometric. Instead, in the case when $Y = \mathbb{R}^n$, (2.2) is a real restriction and is verified if the maps $y\mapsto gy$ are isometries of $\mathbb{R}^n$.

DEFINITION 2.1. *An MC $(\mathcal{X},\mathcal{Y},P)$ is said to be* G-symmetric *if the following hold:*

(a) *there exists a simply transitive action of G on $\mathcal{X}$;*
(b) *there exists an isometric action of G on $\mathcal{Y}$;*
(c) *$P(y|x) = P(gy|gx)$ for every $g\in G$, every $x\in\mathcal{X}$, and ν-almost every $y\in\mathcal{Y}$.*

It follows from (a) that the input $\mathcal{X}$ of a G-symmetric MC and the group G are in bijection: we will often tend to identify them. In this paper we will exclusively consider the case when G is a finite Abelian group. We present a few fundamental examples.

Example 1 (binary-input output-symmetric channels). Consider the case when $G \simeq \mathbb{Z}_2$. $\mathbb{Z}_2$-symmetric channels are known in the coding literature as binary-input output-symmetric (BIOS) channels. Typical examples are the binary symmetric channel (BSC) and the binary erasure channel (BEC). By considering r consecutive uses of a BIOS channel $(\mathcal{X}, \mathcal{Y}, P)$, one obtains a $\mathbb{Z}_2^r$-symmetric MC with input set $\mathcal{X}^r$, output space $\mathcal{Y}^r$, and product transition probabilities $P(\boldsymbol{y}|\boldsymbol{x}) := \prod_{1\le k\le r} P(y_k|x_k)$.

Example 2 (m-ary symmetric channel). Consider a finite set $\mathcal{X}$ of cardinality $m \ge 2$ and some $\varepsilon \in [0,1]$. The *m-ary symmetric channel* is described by the triple $(\mathcal{X}, \mathcal{X}, P)$, where $P(y|x) = 1-\varepsilon$ if $y = x$ and $P(y|x) = \varepsilon/(m-1)$ otherwise. This channel returns the transmitted input symbol x as output with probability $1-\varepsilon$, while with probability ε a wrong symbol is received, uniformly distributed over the set $\mathcal{X} \setminus \{x\}$. The special case $m = 2$ corresponds to the BSC. The m-ary symmetric channel was considered by Gallager [19, sect. 5] to evaluate the performance of nonbinary LDPC codes. It exhibits the highest possible level of symmetry. Indeed, it is G-symmetric for every group G of order $|G| = m$. To see this, it is sufficient to observe that every group acts simply and transitively on itself. Notice that whenever $m = p^r$ for some prime p and positive integer r, the group G can be chosen to be $\mathbb{Z}_p^r$, which is compatible with the structure of the Galois field $\mathbb{F}_{p^r}$.

Example 3 (geometrically uniform AWGN channels). An n-dimensional constellation is a finite subset $S \subset \mathbb{R}^n$ spanning $\mathbb{R}^n$. We denote with $\mathrm{Iso}(S)$ 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 $\mathrm{Iso}(S)$ whose action on S is simply transitive. Such a G is called a generating group for S: for every $s \in S$ the mapping $\lambda_s : G \to S$ defined by $\lambda_s : g \in G \mapsto gs \in S$ is a bijection called isometric labeling.

Given a GU constellation $S \subset \mathbb{R}^n$ with generating group G, define the *S-AWGN channel* as the n-dimensional unquantized AWGN channel with input set S, output $\mathbb{R}^n$ with the usual Borel–Lebesgue measure structure, and transition probability densities given by $P(y|x) = N(y-x)$, where $N(x) = (2\pi\sigma^2)^{-n/2} e^{-||x||^2/2\sigma^2}$ is the density of an n-dimensional diagonal Gaussian random variable. Now let S' be another GU constellation such that $S \subseteq S'$ and G is isomorphic to a subgroup of $\mathrm{Iso}(S')$. Let us introduce the quantization map over the Voronoi regions of S' $q : \mathbb{R}^n \to S'$, $q(x) = \mathrm{argmin}_{s\in S'} ||x-s||$ (resolving nonuniqueness cases by assigning to $q(x)$ a value arbitrarily chosen from the set of minima). We define the *(S,S')-AWGN channel* as the MC obtained by applying q to the output of the S-AWGN channel. Note that the special case $S = S'$ coincides with the so-called hard decoding rule. It is easy to see that both the S-AWGN channel and the (S,S')-AWGN channel are G-symmetric.

The simplest example of a GU constellation is the so-called one-dimensional antipodal constellation $\{-1, 1\}$, admitting $\mathbb{Z}_2$ as a generating group. Another example is given by m orthogonal equal-energy signals: in this case the symmetry group coincides with the permutation group S_m, and any group of order m is a generating group. A two-dimensional example is the m-PSK constellation already introduced in section 1. Notice that the symmetry group of the m-PSK is isomorphic to D_m, the dihedral group with $2m$ elements. m-PSK always admits cyclic generating group $\mathbb{Z}_m$. When m is even, the m-PSK also admits a generating group isomorphic to $D_{m/2}$, which is non-Abelian for all $m \ge 6$. Notice that the only cases when m-PSK has a generating group admitting Galois field structure are when m is prime or $m = 4$.

In fact, when $m = 2^r$ with $r \geq 3$ or $m = p^r$ with $p \geq 3$ prime and $r \geq 2$, $\mathbb{Z}_p^r$ is not isomorphic to any subgroup of D_m and thus cannot be a generating group for m-PSK.

Consider an MC $(\mathcal{X}, \mathcal{Y}, P)$ and two input elements x, x' in $\mathcal{X}$. The Schwarz inequality gives

$$0 \leq \int_{\mathcal{Y}} \sqrt{P(y|x)P(y|x')}\mathrm{d}\nu(y) \leq \int_{\mathcal{Y}} P(y|x)\mathrm{d}\nu(y) \int_{\mathcal{Y}} P(y|x')\mathrm{d}\nu(y) = 1.$$

Moreover, the first of the previous inequalities holds as an equality iff $P(\,\cdot\,|x)P(\,\cdot\,|x') = 0$ ν-almost everywhere. Instead, the second inequality is equality iff $P(\cdot|x) = P(\cdot|x')$ ν-almost everywhere, which means that actually x and x' have indistinguishable outputs. Throughout this paper we will assume that $0 < \int_{\mathcal{Y}} \sqrt{P(y|x)P(y|x')}\mathrm{d}\nu(y) < 1$ for every $x \neq x'$. 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 MC we can associate a function

$$\boldsymbol{\Delta} : \mathcal{X} \times \mathcal{X} \to \mathbb{R}_+ , \qquad \boldsymbol{\Delta}(x, x') := -\log \int_{\mathcal{Y}} \sqrt{P(y|x)P(y|x')}\mathrm{d}\nu(y).$$

This function is usually called the *Bhattacharyya distance* (or simply $\boldsymbol{\Delta}$-distance) of the channel. $\boldsymbol{\Delta}$ is symmetric: $\boldsymbol{\Delta}(x, x') = \boldsymbol{\Delta}(x', x)$; moreover, $\boldsymbol{\Delta}(x, x') = 0$ iff $x = x'$. The Bhattacharyya distance can be extended to direct products in a natural way. Given $\boldsymbol{x}, \boldsymbol{x}'$ in $\mathcal{X}^N$, we put $\boldsymbol{\Delta}(\boldsymbol{x}, \boldsymbol{x}') = \sum_{i=1}^N \boldsymbol{\Delta}(x_i, x_i')$. The *minimum* $\boldsymbol{\Delta}$*-distance* of a code $\mathcal{C} \subseteq \mathcal{X}^N$ is defined as

$$\mathrm{d}_{\min}(\mathcal{C}) := \min\{\boldsymbol{\Delta}(\boldsymbol{x}, \boldsymbol{x}') \;\big|\; \boldsymbol{x}, \boldsymbol{x}' \in \mathcal{C},\ \boldsymbol{x} \neq \boldsymbol{x}'\}.$$

If the MC $(\mathcal{X}, \mathcal{Y}, P)$ is G-symmetric, it is easy to verify that $\boldsymbol{\Delta}(gx, gx') = \boldsymbol{\Delta}(x, x')$ for all x, x' in $\mathcal{X}$ and g in G. Identifying $\mathcal{X}$ with G as usual, we can introduce the so-called *Bhattacharyya weight*:

$$\boldsymbol{\delta} : G \to \mathbb{R}_+, \qquad \boldsymbol{\delta}(x) := \boldsymbol{\Delta}(x, 1_G), \qquad x \in G.$$

In this way we have $\boldsymbol{\Delta}(x, x') = \boldsymbol{\delta}(x^{-1}x')$.

In the case of a BIOS channel, we have that

$$\boldsymbol{\Delta}(\boldsymbol{x}, \boldsymbol{x}') = \sum_{1 \leq i \leq N} \boldsymbol{\delta}(x_i - x_i') = \boldsymbol{\delta}(1)\,|\{1 \leq i \leq N :\, x_i \neq x_i'\}| \qquad \forall\, \boldsymbol{x}, \boldsymbol{x}' \in \mathcal{X}^N;$$

i.e., the $\boldsymbol{\Delta}$-distance is proportional to the Hamming distance (the number of different entries of two strings).

For the m-ary symmetric channel of Example 2 we obtain

$$\boldsymbol{\Delta}(\boldsymbol{x}, \boldsymbol{x}') = -\log\left(\varepsilon\tfrac{m-2}{m-1} + \sqrt{\tfrac{(1-\varepsilon)\varepsilon}{m-1}}\right)|\{1 \leq i \leq N \,:\, x_i \neq x_i'\}| \qquad \forall\, \boldsymbol{x}, \boldsymbol{x}' \in \mathcal{X}^N,$$

so that, once again, the $\boldsymbol{\Delta}$-distance is proportional to the Hamming distance.

Finally, for the S-AWGN channel of Example 3, by considering any isometric labeling $\lambda_s : G \to S$, we obtain

$$\begin{aligned} \boldsymbol{\Delta}(\boldsymbol{x}, \boldsymbol{x}') &= \sum_{k=1}^N -\log \int_{\mathbb{R}^n} \frac{e^{-\left(||\boldsymbol{y} - \lambda_s(x_k)||^2 + ||\boldsymbol{y} - \lambda_s(x_k')||^2\right)/4\sigma^2}}{(2\pi\sigma^2)^{n/2}}\mathrm{d}\boldsymbol{y} \\ &= \frac{\log e}{8\sigma^2} \sum_{k=1}^N ||\lambda_s(x_k) - \lambda_s(x_k')||^2 ; \end{aligned}$$

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

2.3. Group codes and type-enumerating functions. When transmitting over an MC which is symmetric according to Definition 2.1, a natural class of codes to be considered is that of group codes. A *G-code* of length N is any subgroup of the direct group product G^N. Group codes are generalizations of binary-linear codes (the latter correspond to the case $G \simeq \mathbb{Z}_2$). In fact, G-codes enjoy many of the properties of binary-linear codes. For instance, when a G-code $\mathcal{C}$ is employed on a G-symmetric MC, ML decision regions (Voronoi regions in the Gaussian case) are congruent, and then the error probability does not depend on the transmitted codeword: this is called the uniform error property [18].

For every G-code $\mathcal{C}$ of length N we now introduce some combinatorial quantities characterizing its performance. The *type-enumerating function* of a G-code $\mathcal{C}$ is defined as

$$W_{\mathcal{C}} : \mathcal{P}(G) \to \mathbb{Z}_+, \qquad W_{\mathcal{C}}(\boldsymbol{\theta}) := \sum_{\boldsymbol{x} \in G^N_{\boldsymbol{\theta}}} \mathbb{1}_{\mathcal{C}}(\boldsymbol{x}) \qquad \forall\, \boldsymbol{\theta} \in \mathcal{P}(G),$$

where $G^N_{\boldsymbol{\theta}}$ is the set of N-tuples of type $\boldsymbol{\theta}$. Notice that since $\mathcal{C}$ is a subgroup of G^N, 1_{G^N} is always a codeword so that $W_{\mathcal{C}}(\delta_{1_G}) = 1$.

Assume we have fixed a G-symmetric MC $(\mathcal{X}, \mathcal{Y}, P)$, and let $\boldsymbol{\delta}$ be its associated Bhattacharyya weight. The minimum $\boldsymbol{\Delta}$-distance of a G-code $\mathcal{C}$ of length N is a function of its type-enumerating function:

(2.3)
$$\mathrm{d}_{\min}(\mathcal{C}) = \min\{\boldsymbol{\delta}(\boldsymbol{x}) \mid \boldsymbol{x} \in \mathcal{C} \setminus \{\mathbf{0}\}\} = N \inf\left\{\langle \boldsymbol{\delta}, \boldsymbol{\theta}\rangle \middle| \, \boldsymbol{\theta} \in \mathcal{P}(G) \setminus \{\delta_0\} : W_{\mathcal{C}}(\boldsymbol{\theta}) > 0\right\}.$$

Type-enumerating functions and minimum Bhattacharyya distances play an important role in the estimation of the ML decoding error probability of G-codes over G-symmetric MCs. For instance, the so-called union-Bhattacharyya bound, for the error probability of a G-code $\mathcal{C}$ of length N, can be written in the form

$$p_e(\mathcal{C}) \leq \sum_{\boldsymbol{\theta} \in \mathcal{P}(G)} W_{\mathcal{C}}(\boldsymbol{\theta}) \exp\left(-N\langle \boldsymbol{\delta}, \boldsymbol{\theta}\rangle\right). \tag{2.4}$$

Bounds tighter than (2.4) can be obtained for the error probability of G-codes over G-symmetric channels based on variations of the Gallager bound [20, 39].

Observe that both (2.3) and (2.4) do not generally hold when a G-code is employed on an MC which is not G-symmetric. While this is not an issue for the highly symmetric channels considered in Example 2, it does matter for the symmetric channels introduced in Example 3. As a concrete example, one may think of the 8-PSK Gaussian channel: in this case, while both (2.3) and (2.4) are true for $\mathbb{Z}_8$-codes, for a $\mathbb{Z}_2^3$-code $\mathcal{C}$, and a fortiori for a $\mathbb{F}_8$-linear code, neither (2.3) nor (2.4) holds. In fact, the type-enumerating function of a $\mathbb{Z}_2^3$-code is not sufficient for characterizing its performance on the 8-PSK Gaussian channel. In order to overcome this problem, an average coset ensemble approach needs to be used [22, 4, 5].

It is a well-known result in information theory [20] that binary-linear codes allow one to achieve the capacity of any BIOS channels. More in general, linear codes over the Galois field $\mathbb{F}_{p^r}$ are known to achieve the capacity of any $\mathbb{Z}_p^r$-symmetric channel [16]. A similar result was conjectured in [27] for G-codes on G-symmetric MCs. In [11], the capacity C_G achievable by G-codes on G-symmetric MCs has been characterized for any finite Abelian group G. When G is cyclic of order

$m = p_1^{r_1^m} p_2^{r_2^m} \dots p_s^{r_s^m}$, for distinct primes $p_1, \dots, p_s$, it has been shown that

$$C_{\mathbb{Z}_m} = \max_{\boldsymbol{\alpha} \in \mathcal{P}(\{1,\dots,s\})} \min_{l | m, l>1} \frac{C_{p^s}}{\sum_{1 \le j \le s} \boldsymbol{\alpha}(j) \frac{r_j^l}{r_j^m}} \le C, \tag{2.5}$$

where C_l denotes the Shannon capacity of the $\mathbb{Z}_l$-symmetric channel obtained by restricting the input of the original channel to the subgroup $\frac{m}{l}\mathbb{Z}_m$. It has been shown in [11] that for a wide class of G-symmetric channels, including the p^r-PSK Gaussian channel (for prime p) both with quantized and unquantized output, G-capacity C_G and Shannon capacity C do coincide, while this is no longer the case for other G-symmetric channels.

2.4. LDPC codes over Abelian groups. For any finite Abelian group G, we now describe the ensembles of LDPC G-codes which will be considered in this paper. For every given degree pair (c, d) in $\mathbb{N}^2$, we consider the set of admissible block-lengths $\mathcal{N}_{(c,d)} := \{N \in \mathbb{N} \text{ s.t. } d \mid Nc\}$, and for every N in $\mathcal{N}_{(c,d)}$ we define $L = Nc/d$. Consider the c-repetition operator

$$\mathrm{Rep}_c^N : G^N \to G^{Nc}, \qquad (\mathrm{Rep}_c^N \boldsymbol{x})_i = x_{\lceil i/c \rceil}, \tag{2.6}$$

where $\lceil x \rceil$ denotes the lowest integer not below x, and the d-check summation operator

$$\mathrm{Sum}_d^N : G^{Nc} \to G^L, \qquad (\mathrm{Sum}_d^N \boldsymbol{x})_i = \sum_{k=i(d-1)+1}^{id} x_k. \tag{2.7}$$

Consider the group of permutations on Nc elements, S_{Nc}, and let Π'_N be a random variable uniformly distributed over S_{Nc}. Moreover, consider a subgroup F of $\mathrm{Aut}(G)$, the automorphism group of G, and let $(\Lambda_j)_{1 \le j \le Nc}$ be a family of independent random variables identically distributed uniformly on F, independent of Π'_N. Define the random diagonal automorphism $\Pi''_N \in \mathrm{Aut}(G^{Nc})$ by $(\Pi''_N \boldsymbol{x})_j := \Lambda_j x_j$ for $1 \le j \le Nc$. Finally, for every $N \in \mathcal{N}_{(c,d)}$ define the random syndrome homomorphism

$$\Phi_N : G^N \to G^L, \qquad \Phi_N := \mathrm{Sum}_d^N \, \Pi'_N \Pi''_N \, \mathrm{Rep}_c^N \tag{2.8}$$

and the associated random G-code $\mathcal{C}_N := \ker \Phi_N$. This is called the (c, d)-*regular* F-*labelled ensemble*. F will be called the *label group*. The two extreme cases $F = \{1\}$ and $F = \mathrm{Aut}(G)$ will be referred to, respectively, as the *unlabelled* and the *uniformly labelled* (c, d)-regular ensembles.

The reason for considering only automorphisms as possible labels, avoiding the use of noninvertible labels, is clarified by the following proposition. For any group H, we denote the set of endomorphisms of H by $\mathrm{End}(H)$.

PROPOSITION 2.2. *Assume that, for all $N \in \mathcal{N}_{(c,d)}$, $\Phi_N : G^N \to G^L$ is defined as in* (2.8) *with Π'_N uniformly distributed over S_{Nc} and $\Pi''_N \in \mathrm{End}(G^{Nc})$ is defined by $(\Pi''_N \boldsymbol{x})_j := \Lambda_j x_j$ for $1 \le j \le Nc$, where (Λ_j) are independently and identically distributed according to some probability distribution $\boldsymbol{\mu} \in \mathcal{P}(\mathrm{End}(G))$ such that $\mathrm{supp}(\boldsymbol{\mu}) \not\subseteq \mathrm{Aut}(G)$. Then, for all $k \in G \setminus \{0\}$ such that $\Lambda k = 0$ for some $\Lambda \in \mathrm{supp}(\boldsymbol{\mu})$*

$$\mathbb{P}(\mathrm{d}_{\min}(\ker \Phi_N) \le \boldsymbol{\delta}(k)) \ge 1 - (1 - \boldsymbol{\mu}(\Lambda)^c)^N \overset{N \to \infty}{\longrightarrow} 1.$$

Proof. Consider $\Lambda \in \mathrm{supp}(\boldsymbol{\mu}) \setminus \mathrm{Aut}(G)$, and $k \in \ker \Lambda \setminus \{0\}$. For $1 \le s \le N$, let $e_s^k \in G^N$ be the N-tuple with all-zero entries but the sth one, which is equal to k. If

$\Lambda_j = \Lambda$ for all $(s-1)c+1 \le j \le sc$, then $\Pi''_N \operatorname{Rep}_c^N e_s^k = \mathbf{0}$, so that $\Phi_N e_s^k = \mathbf{0}$, and $\mathrm{d}_{\min}(\ker \Phi_N) \le \boldsymbol{\delta}(k)$. Since the events

$$E_s^N := \bigcap_{(s-1)c+1 \le j \le sc} \{\Lambda_j = \Lambda\}$$

are independent for $1 \le s \le N$ and all have probability $1 - \boldsymbol{\mu}(\Lambda)^c$, it follows that

$$\mathbb{P}(\mathrm{d}_{\min}(\ker \Phi_N) \le \boldsymbol{\delta}(k)) \ge \mathbb{P}\left(\bigcup_{1 \le s \le N} E_s^N \right) = 1 - \left(1 - \mathbb{P}\left(E_s^N\right)\right)^N = \left(1 - \boldsymbol{\mu}(\Lambda)^c\right)^N . \quad \square$$

We wish to underline the fact that the proof of Proposition 2.2 strongly relied on the independence assumption we made for the labels Λ_j. Indeed, by introducing proper dependence structures for the random labels which allow us to avoid certain configurations, it is possible to consider ensembles of LDPC G-codes with noninvertible labels as well. This possibility will not be considered in the present paper but will be explored in a future work.

As LDPC G-codes are special G-codes admitting sparse kernel representation, they suffer from all of the limitations in performance of G-codes. In particular, the capacity they can achieve on a G-symmetric channel is upper bounded by the G-capacity of that channel. This explains why the authors of [4] had to restrict themselves to prime values of m while studying LDPC $\mathbb{Z}_m$-codes, albeit the average type-spectra they obtained for the unlabelled ensemble did not need such an assumption. In fact, they noticed that for nonprime m "expurgation is impossible" and LDPC $\mathbb{Z}_m$-codes result "bounded away from the random-coding spectrum." The same restriction to prime values of m (or more in general to groups G admitting Galois field structure) was required both in [4] and [17] in order to study the uniformly labelled ensemble.

In this paper regular ensembles of F-labelled LDPC G-codes will be studied for any finite Abelian group G. In particular we will find estimations for their average type-enumerating functions $\overline{W_{\mathcal{C}_N}(\boldsymbol{\theta})}$ and explicit combinatorial formulas for their average type-spectra defined as the limit of $N^{-1} \log \overline{W_{\mathcal{C}_N}(\boldsymbol{\theta})}$. Coupling this analysis with an ad hoc analysis of the type-enumerator functions for small weight codewords, we will finally propose upper bounds to the repartition function of the minimum normalized distance $\frac{1}{N} \mathrm{d}_{\min}(\mathcal{C}_N)$. This will allow us to show that, if $c > 2$, minimum distances grow linearly in N with high probability. We will also show that the typical minimum distance (more precisely the lower bound on it—conjectured to be tight—provided by the average type-spectra) of the uniformly labelled LDPC ensemble is significantly larger than the typical minimum distance of the corresponding unlabelled ensemble.

In [10] it was claimed that, for any m, the (c, d)-regular ensemble allows one to achieve a nonzero capacity over any $\mathbb{Z}_m$-symmetric channel, and that this capacity can be made arbitrarily close to the $\mathbb{Z}_m$-capacity of the channel, if the parameters (c, d) are allowed to grow. In fact, the same is true for the uniformly labelled ensembles as well; see section 6.2. This implies that LDPC $\mathbb{Z}_m$-codes allow one to achieve the Shannon capacity of a $\mathbb{Z}_m$-symmetric channel whenever $\mathbb{Z}_m$-codes do. While explicit proofs of these facts will not be given here due to the lack of space, they can be obtained from the combinatorial results of sections 3 and 4 using standard upper-bounding techniques for the average error probability of group codes [20, 39]. Similar reasonings can be made for minimum distances and error exponents of LDPC codes. In particular, minimum Bhattacharyya distances of $\mathbb{Z}_m$-codes have been studied in [12].

3. Average type-spectra of LDPC G-codes. In this section we first present some considerations on semidirect-product group actions. Then in section 3.2 we introduce LDPC codes in a slightly more general setting, and we show how regular F-labelled ensembles of LDPC G-codes introduced in section 2.4 can be cast in this framework. In section 3.3 we prove the main result, Theorem 3.5, characterizing the average type-spectra of regular F-labelled ensembles. Finally, in section 3.4 we show how previous results in the literature can be recovered as particular cases of Theorem 3.5, and we provide an explicit formula for the average type-spectrum of the uniformly labelled ensemble over the cyclic group, which is instead an original result.

3.1. Group actions. We recall here some basic facts about semidirect group actions; the reader is referred to the standard textbook [23] for further details. Assume that a group F acts on a set A. A subset $B \subseteq A$ is said to be F-invariant if $fb \in B$ for every $b \in B$ and $f \in F$. Clearly, if B is F-invariant, F acts on B as well. For every a in A, the relative orbit $Fa := \{b \in A \text{ s.t. } b = fa \text{ for some } f \in F\}$ is F-invariant and its action on it is transitive. The set of orbits is denoted by A/F and called the quotient of A by the action of F. There is a canonical surjection $\pi_F : A \to A/F$ which associates an element a with the orbit it belongs to. Given $a \in A$, we define its stabilizer as $\mathrm{Stab}_F(a) := \{f \in F \text{ s.t. } fa = a\}$. The well-known class formula gives $|F| = |Fa| \cdot |\mathrm{Stab}_F(a)|$.

If A and B are sets and the group F acts on A, a map $\phi : A \to B$ is said to be F-invariant if $\phi(fa) = \phi(a)$ for every $a \in A$ and $f \in F$. As an example, the canonical surjection $\pi_F : A \to A/F$ is an F-invariant map. Suppose we have an F-invariant map $\phi : A \to B$; then it is immediate to see that we can define a map $\tilde{\phi} : A/F \to B$ such that $\phi = \tilde{\phi} \circ \pi_F$. Notice that if it happens that ϕ is onto and moreover $\phi(a) = \phi(a')$ iff $Fa = Fa'$, then the map $\tilde{\phi}$ is a bijection, and thus A/F and B are in one-to-one correspondence. We will often use this fact in order to characterize quotient spaces.

We now introduce an example which will play a fundamental role in our future derivations. Given any set A, the permutation group S_N acts naturally on A^N: given $\boldsymbol{a} \in A^N$ and σ in S_N, we define $\sigma\boldsymbol{a} \in A^N$ by $(\sigma\boldsymbol{a})_j = \boldsymbol{a}_{\sigma^{-1}(j)}$. Orbits can easily be described using types. Given $\boldsymbol{a}, \boldsymbol{b} \in A^N$, it is immediate to see that

$$\exists\, \sigma \in S_N \ : \ \sigma\boldsymbol{a} = \boldsymbol{b} \ \Leftrightarrow \ \boldsymbol{\theta}_A(\boldsymbol{a}) = \boldsymbol{\theta}_A(\boldsymbol{b}).$$

This says that the subsets $A^N_{\boldsymbol{\theta}}$ of type-$\boldsymbol{\theta}$ N-tuples are exactly the orbits for the action of the permutation group S_N on A^N, and we have a natural bijection $A^N/S_N \simeq \mathcal{P}_N(A)$ (obtained through the mapping $\boldsymbol{a} \mapsto \boldsymbol{\theta}_A(\boldsymbol{a})$).

Now suppose we are given an action of a group F on the set A. This extends to a componentwise action of F^N on A^N with the orbit set $A^N/F^N \simeq (A/F)^N$. We would like to combine this action with the action of the permutation group on A^N, and the way to do this is as follows: we consider the semidirect product

$$S_N \ltimes F^N, \qquad (\sigma_1, \boldsymbol{g}_1)(\sigma_2, \boldsymbol{g}_2) = (\sigma_1\sigma_2, (\sigma_2^{-1}\boldsymbol{g}_1)\boldsymbol{g}_2)$$

and the action on A^N given by $(\sigma, \boldsymbol{g})\boldsymbol{a} = \sigma(\boldsymbol{g}\boldsymbol{a})$.

We now want to characterize the set of orbits of this semidirect action. Notice that the map $\pi_F : A \to A/F$ induces a natural map $\pi_F^\sharp : \mathcal{P}(A) \to \mathcal{P}(A/F)$, where $[\pi_F^\sharp\boldsymbol{\theta}](Fa) = \sum_{b \in Fa} \boldsymbol{\theta}(b)$. It is easy to see that the following diagram commutes:

$$\begin{array}{ccc} A^N & \stackrel{\pi_{F^N}}{\to} & (A/F)^N \\ \downarrow \boldsymbol{\theta}_A & & \downarrow \boldsymbol{\theta}_{A/F} \\ \mathcal{P}_N(A) & \stackrel{\pi_F^\sharp}{\to} & \mathcal{P}_N(A/F) \end{array} \tag{3.1}$$

(i.e., $\boldsymbol{\theta}_{A/F} \circ \pi_{F^N} = \pi_F^\sharp \circ \boldsymbol{\theta}_A$).

In what follows we will use the notation $\boldsymbol{\nu}_{A,F} = \boldsymbol{\theta}_{A/F} \circ \pi_{F^N}$ and call $\boldsymbol{\nu}_{A,F}(\boldsymbol{a})$ the (A,F)-*type* of $\boldsymbol{a}$. The (A,F)-type is exactly what is needed to describe orbits with respect to the action of the semidirect group $S_N \ltimes F^N$. Indeed, it is immediate to check that $\mathcal{P}_N(A/F)$ is in bijection with the quotient $A^N/(S_N \ltimes F^N)$: given $\boldsymbol{a}, \boldsymbol{b} \in A^N$, we have that

$$\exists (\sigma, \boldsymbol{g}) \in S_N \ltimes F^N \text{ s.t. } (\sigma, \boldsymbol{g})\boldsymbol{a} = \boldsymbol{b} \Leftrightarrow \boldsymbol{\nu}_{A,F}(\boldsymbol{a}) = \boldsymbol{\nu}_{A,F}(\boldsymbol{b}).$$

If $\boldsymbol{\nu} \in P_N(A/F)$, we will use the notation $A^N_{\boldsymbol{\nu}} := \{\boldsymbol{a} \in A^N \mid \boldsymbol{\nu}_{A,F}(\boldsymbol{a}) = \boldsymbol{\nu}\}$. Using the fact that $\boldsymbol{\nu}_{A,F} = \boldsymbol{\theta}_{A/F} \circ \pi_{F^N}$ we obtain that

$$|A^N_{\boldsymbol{\nu}}| = \tbinom{N}{N\boldsymbol{\nu}} \prod_{\alpha \in A/F} |\pi_F^{-1}(\alpha)|^{N\boldsymbol{\nu}(\alpha)}. \tag{3.2}$$

Now define $\mathcal{O}^N_{\boldsymbol{\nu}} := \{\boldsymbol{\theta} \in \mathcal{P}_N(A) \text{ s.t. } \pi_F^\sharp(\boldsymbol{\theta}) = \boldsymbol{\nu}\}$. For every given $\boldsymbol{\nu} \in \mathcal{P}(A/F)$, and N in $\mathbb{N}$, we have

$$A^N_{\boldsymbol{\nu}} = \bigcup_{\boldsymbol{\theta} \in \mathcal{O}^N_{\boldsymbol{\nu}}} A^N_{\boldsymbol{\theta}}, \tag{3.3}$$

the union being disjoint. Notice that we also have $\left|\mathcal{O}^N_{\boldsymbol{\nu}}\right| = \prod_{\alpha \in A/F} |\pi_F^{-1}(\alpha)|^{N\boldsymbol{\nu}(\alpha)}$.

3.2. A general framework for LDPC ensembles over Abelian groups. Fix an infinite subset $\mathcal{N} \subseteq \mathbb{N}$, a group U, two sequences of finite Abelian groups $Z^{(N)}$ and $Y^{(N)}$ (with $N \in \mathcal{N}$), and two sequences of homomorphisms

$$\Xi_o^N : U^N \to Z^{(N)}, \qquad \Xi_i^N : Z^{(N)} \to Y^{(N)}.$$

Consider, moreover, a sequence I_N of subgroups of $\mathrm{Aut}(Z^{(N)})$, and assume that the actions of I_N on $Z^{(N)}$ satisfy the following property: there exists a fixed finite set A and a sequence of invariant maps $\Theta_N : Z^{(N)} \to \mathcal{P}(A)$ such that $\boldsymbol{x}$, $\boldsymbol{y} \in Z^{(N)}$ are in the same orbit iff $\Theta_N(\boldsymbol{x}) = \Theta_N(\boldsymbol{y})$. In this way the quotient space $Z^{(N)}/I_N$ can be naturally identified with the image of Θ_N inside $\mathcal{P}(A)$.

Now let Π_N be a sequence of random variables uniformly distributed over I_N. For every $N \in \mathcal{N}$ define

$$\Phi_N := \Xi_i^N \Pi_N \Xi_o^N. \tag{3.4}$$

The triple (Ξ_o^N, Ξ_i^N, I_N) is called an *interconnected ensemble*, while $(\ker \Phi_N)$ will be the *random code sequence* associated with the ensemble. The set A will be called the *interconnection type alphabet* of the ensemble.

Now consider the type-enumerating function $W_N(\boldsymbol{\theta})$ for the ensemble. By taking the expectation with respect to our probability space, we get

$$\overline{W_N(\boldsymbol{\theta})} = \mathbb{E}\Big[\sum_{\boldsymbol{x} \in U^N_{\boldsymbol{\theta}}} \mathbb{1}_{\{\mathbf{0}\}}(\Phi_N \boldsymbol{x})\Big] = \sum_{\boldsymbol{x} \in U^N_{\boldsymbol{\theta}}} \mathbb{P}(\Phi_N \boldsymbol{x} = \mathbf{0}). \tag{3.5}$$

Put $Z^{(N)}_{\boldsymbol{\nu}} := \Theta_N^{-1}(\boldsymbol{\nu})$, and define the following sets: for every $\boldsymbol{\nu} \in \mathcal{P}(A)$, $\boldsymbol{\theta} \in \mathcal{P}(U)$

$$Z^{i,N}_{\boldsymbol{\nu}} := \left\{\boldsymbol{w} \in Z^{(N)}_{\boldsymbol{\nu}} \mid \Xi_i^N \boldsymbol{w} = \mathbf{0}\right\}, \qquad U^{o,N}_{\boldsymbol{\theta},\boldsymbol{\nu}} := \{\boldsymbol{x} \in U^N \mid \boldsymbol{\theta}_U(\boldsymbol{x}) = \boldsymbol{\theta},\ \Theta_N(\Xi_o^N \boldsymbol{x}) = \boldsymbol{\nu}\}. \tag{3.6}$$

We have the following simple result.

PROPOSITION 3.1. *For every* $\boldsymbol{\theta}$ *in* $\mathcal{P}_N(U)$

$$\overline{W_N(\boldsymbol{\theta})} = \sum_{\boldsymbol{v}\in\mathcal{P}(A)} \frac{|U^{o,N}_{\boldsymbol{\theta},\boldsymbol{v}}||Z^{i,N}_{\boldsymbol{v}}|}{|Z^{(N)}_{\boldsymbol{v}}|}. \tag{3.7}$$

Proof. If $\boldsymbol{x} \in U^{o,N}_{\boldsymbol{\theta},\boldsymbol{v}}$, using the fact that I_N acts transitively on $Z^{(N)}_{\boldsymbol{v}}$ and the class formula, we obtain

$$\mathbb{P}(\Phi_N \boldsymbol{x} = \mathbf{0}) = \mathbb{P}(\Pi_N \Xi^N_o \boldsymbol{x} \in Z^{i,N}_{\boldsymbol{v}}) = \frac{|Z^{i,N}_{\boldsymbol{v}}||\mathrm{Stab}_{I_N}(\Xi^N_o(\boldsymbol{x}))|}{|I_N|} = \frac{|Z^{i,N}_{\boldsymbol{v}}|}{|Z^{(N)}_{\boldsymbol{v}}|}.$$

Now using (3.5), (3.7) follows immediately. ∎

We now frame the LDPC ensembles introduced in section 2 into this more general setting. We use the notation introduced in section 2.4. Given $(c,d) \in \mathbb{N}^2$ and $N \in \mathcal{N}_{(c,d)}$, consider $L = Nc/d$. Take $U = G$, $Z^{(N)} = G^{Nc}$, $Y^{(N)} = G^L$. Also, take $\Xi^N_o = \mathrm{Rep}^N_c$, $\Xi^N_i = \mathrm{Sum}^N_d$, $I_N = S_{Nc} \ltimes F^{Nc}$. The ensemble $(\mathrm{Rep}^N_c, \mathrm{Sum}^N_d, S_{Nc} \ltimes F^{Nc})$ is the (c,d)-regular F-labelled ensemble. The type alphabet in this case is simply $A = G/F$.

Irregular ensembles can be framed into this setting by simply modifying the repetition and the sum operators. Also other interesting cases can be obtained by considering the interconnections among the inner and outer encoder done through some vector structured channels and allowing only independent permutations on the various channels. Finally, hybrid nonbinary LDPC codes can be considered in this framework by replacing the product group U^N with the product of copies of different Abelian groups $U^N_1 \times \cdots \times U^N_k$.

However, we will now focus on the evaluation of the type-spectra of the regular F-labelled LDPC G-code ensembles. This will be done in the following subsection by explicitly calculating the three terms entering in the formula (3.7).

3.3. The average type-spectrum of the (c,d)-regular F-labelled ensemble. In order to prove the main result of this section we will use some generating function techniques. For a finite set A, consider the ring of complex-coefficient multivariable polynomials (briefly multinomials) $\mathbb{C}[A]$. Given $p \in \mathbb{C}[A]$ and $\boldsymbol{k} \in \mathbb{Z}^A_+$, we denote by $\lfloor p(\boldsymbol{z}) \rfloor_{\boldsymbol{k}}$ the coefficient of the term $\boldsymbol{z}^{\boldsymbol{k}}$ in $p(\boldsymbol{z})$, i.e., $p(\boldsymbol{z}) = \sum_{\boldsymbol{k}\in\mathbb{Z}^A_+} \lfloor p(\boldsymbol{z}) \rfloor_{\boldsymbol{k}} \boldsymbol{z}^{\boldsymbol{k}}$. In particular, we will consider type-enumerating multinomials, i.e., homogeneous-degree multinomials of the form $p(\boldsymbol{z}) = \sum_{\boldsymbol{\theta}\in\mathcal{P}_N(A)} \lfloor p(\boldsymbol{z}) \rfloor_{N\boldsymbol{\theta}} \boldsymbol{z}^{N\boldsymbol{\theta}}$, where each coefficient $\lfloor p(\boldsymbol{z}) \rfloor_{N\boldsymbol{\theta}}$ equals the number of N-tuples $\boldsymbol{a} \in A^N$ of A-type $\boldsymbol{\theta}$, satisfying certain properties. The easiest case is provided by the multinomial $(\sum_{a\in A} z_a)^N = \sum_{\boldsymbol{\theta}\in\mathcal{P}_N(A)} \binom{N}{N\boldsymbol{\theta}} \boldsymbol{z}^{N\boldsymbol{\theta}}$, simply enumerating the N-tuples of different A-types. The following result, proved in [9], characterizes the asymptotic growth rate of the coefficients of powers of enumerating multinomials.

THEOREM 3.2. *Let A be a finite set and $p(\boldsymbol{z}) \in \mathbb{R}_+[A]$ be a homogeneous-degree, nonnegative, real-coefficient multinomial. For all $\boldsymbol{\theta} \in \mathcal{P}_{\mathbb{N}}(A)$ and $\boldsymbol{z} \in \mathcal{P}(A)$ such that* $\mathrm{supp}(\boldsymbol{z}) = \mathrm{supp}(\boldsymbol{\theta})$*, we have*

$$\lfloor p(\boldsymbol{z})^N \rfloor_{N\boldsymbol{\theta}} \le \frac{p(\boldsymbol{z})^N}{\boldsymbol{z}^{N\boldsymbol{\theta}}}, \qquad \lim_{N\in\mathcal{N}_{\boldsymbol{\theta}}} \frac{1}{N} \log \lfloor p(\boldsymbol{z})^N \rfloor_{N\boldsymbol{\theta}} = \inf_{\substack{\boldsymbol{z}\in\mathcal{P}(A):\\ \mathrm{supp}(\boldsymbol{z})=\mathrm{supp}(\boldsymbol{\theta})}} \log \frac{p(\boldsymbol{z})}{\boldsymbol{z}^{\boldsymbol{\theta}}}. \tag{3.8}$$

Moreover, the left-hand side of (3.8) *is a concave (and thus upper semicontinuous)* $[-\infty,+\infty)$*-valued function on* $\mathcal{P}(A)$.

Observe that, by considering $p(\boldsymbol{z}) = \sum_a z_a$, (2.1) can be deduced from Theorem 3.2.

The first type-enumerating multinomial which we will need in our derivations is the one enumerating the 0-sum d-tuples over a finite Abelian group G:

$$\beta_d(\boldsymbol{z}) \in \mathbb{C}[z_g,\, g \in G], \qquad \beta_d(\boldsymbol{z}) := \sum_{g_1,\dots,g_d} \mathbb{1}_{\{0\}}\left(\sum_{k=1}^{d} g_k\right) \prod_{1\le k\le d} z_{g_k}.$$

By introducing the group $\hat{G}$ of characters of G, i.e., homomorphisms of G in the multiplicative group $\mathbb{C}^*$ of nonzero complex numbers, it is possible to find an explicit expression for $\beta_d(\boldsymbol{z})$ as stated in the following lemma.

LEMMA 3.3. *For every finite Abelian group* G *and* $d \in \mathbb{N}$

$$\beta_d(\boldsymbol{z}) = \frac{1}{|G|} \sum_{\chi\in\hat{G}} \left(\sum_{g\in G} z_g \chi(g)\right)^d.$$

Proof. The inversion formula for the discrete Fourier transform (see [41, p. 168]) $f(g) = \frac{1}{|G|}\sum_\chi \langle f,\chi\rangle \chi(g)$, applied to $f = \delta_0 \in L^2(G)$, gives $\frac{1}{G}\sum_\chi \chi(g) = \mathbb{1}_{\{0\}}(g)$. Then

$$\begin{aligned}
\beta_d(\boldsymbol{z}) &= \sum_{g_1,\dots,g_d} \mathbb{1}_{\{0\}}\Big(\sum_{1\le k\le d} g_k\Big) \prod_{1\le k\le d} z_{g_k} \\
&= \sum_{g_1,\dots,g_d} \tfrac{1}{|G|}\sum_\chi \chi\Big(\sum_{1\le k\le d} g_k\Big) \prod_{1\le k\le d} z_{g_k} \\
&= \tfrac{1}{|G|}\sum_\chi \sum_{g_1,\dots,g_d} \prod_{1\le k\le d} \chi\left(g_k\right) z_{g_k} \\
&= \tfrac{1}{|G|}\sum_\chi \Big(\sum_g z_g \chi(g)\Big)^d. \qquad \square
\end{aligned}$$

Recall that, given any subgroup F of $\mathrm{Aut}(G)$ and a degree pair (c,d) in $\mathbb{N}^2$, the (c,d)-regular F-labelled ensemble of LDPC G-codes is described by the triple $\big(\mathrm{Rep}_c^N, \mathrm{Sum}_d^N, S_{Nc} \ltimes F^{Nc}\big)$. Let $\pi_F : G \to G/F$ be the canonical projection on the quotient and $\pi_F^\sharp : \mathcal{P}(G) \to \mathcal{P}(G/F)$ be the associated action on probabilities. Also, define

$$\boldsymbol{\varphi} : G/F \to \mathbb{N}, \qquad \boldsymbol{\varphi}(q) = \left|\pi_F^{-1}(q)\right| \tag{3.9}$$

to be the map giving the cardinalities of the orbits of G under the action of F.

Consider some admissible block-length N in $\mathcal{N}_{(c,d)}$. Formula (3.2) shows that $|Z_{\boldsymbol{v}}^{(N)}| = \binom{Nc}{Nc\boldsymbol{v}} \boldsymbol{\varphi}^{Nc\boldsymbol{v}}$ for every $\boldsymbol{v} \in \mathcal{P}_{Nc}(G/F)$. Moreover, in this case $|U_{\boldsymbol{\theta},\boldsymbol{v}}^{o,N}| = \binom{N}{N\boldsymbol{\theta}} \mathbb{1}_{\{\pi_F^\sharp\boldsymbol{\theta}\}}(\boldsymbol{v})$. Substituting into (3.7), and defining $\boldsymbol{v} := \pi_F^\sharp\boldsymbol{\theta}$, we obtain

$$\overline{W_N(\boldsymbol{\theta})} = \binom{N}{N\boldsymbol{\theta}}\binom{Nc}{Nc\boldsymbol{v}}^{-1} \boldsymbol{\varphi}^{-Nc\boldsymbol{v}} |Z_{\boldsymbol{v}}^{i,N}|. \tag{3.10}$$

It remains to evaluate the enumerating weights $|Z_{\boldsymbol{\upsilon}}^{i,N}|$ relative to the check summation operator. In order to do that, we introduce the multinomial

$$\alpha_{F,d}(\boldsymbol{t}) \in \mathbb{C}[t_q,\, q \in G/F], \qquad \alpha_{F,d}(\boldsymbol{t}) := \frac{1}{|G|}\sum_{\chi\in\hat{G}}\left(\sum_{q\in G/F}\frac{1}{\boldsymbol{\varphi}(q)}\sum_{g\in q}\chi(g)t_q\right)^d \tag{3.11}$$

and present the following result, stating that the Lth power of $\alpha_{F,d}(\boldsymbol{t})$ is the type-enumerating multinomial of the normalized weights $|Z_{\boldsymbol{\upsilon}}^{i,N}|/\boldsymbol{\varphi}^{Nc\boldsymbol{\upsilon}}$.

LEMMA 3.4. *For every* $N \in \mathcal{N}_{(c,d)}$

$$\sum_{\boldsymbol{\upsilon}\in\mathcal{P}_{Nc}(G/F)}\frac{|Z_{\boldsymbol{\upsilon}}^{i,N}|}{\boldsymbol{\varphi}^{Nc\boldsymbol{\upsilon}}}\boldsymbol{t}^{Nc\boldsymbol{\upsilon}} = \left(\alpha_{F,d}(\boldsymbol{t})\right)^L. \tag{3.12}$$

Proof. First, consider the type-enumerating multinomial $B(\boldsymbol{z}) \in \mathbb{C}[z_g,\, g \in G]$ for the kernel of the inner homomorphism $\Xi_i^N = \mathrm{Sum}_d^N$. Since any $\boldsymbol{x}$ in G^{Nc} belongs to $\ker \mathrm{Sum}_d^N$ iff it is the concatenation of L 0-sum d-tuples, from Lemma 3.3 we have $B(\boldsymbol{z}) = \left(\beta_d(\boldsymbol{z})\right)^L$. Now consider the map

$$\Psi : \mathbb{C}[z_g,\, g \in G] \to \mathbb{C}[t_q,\ q \in G/F], \qquad \Psi : p(\boldsymbol{z}) \mapsto p(t_{\pi_F(g)},\, g \in G).$$

It follows from (3.3) that, for all $\boldsymbol{\upsilon}$ in $\mathcal{P}(G/F)$, we have

$$\frac{|Z_{\boldsymbol{\upsilon}}^{i,N}|}{\boldsymbol{\varphi}^{Nc\boldsymbol{\upsilon}}} = \sum_{\boldsymbol{\theta}\in\mathcal{O}_{\boldsymbol{\upsilon}}^{Nc}}\frac{\lfloor B(\boldsymbol{z})\rfloor_{Nc\boldsymbol{\theta}}}{\boldsymbol{\varphi}^{Nc\boldsymbol{\upsilon}}} = \sum_{\boldsymbol{\upsilon}\in\mathcal{P}_{Nc}(G/F)}\frac{\lfloor \Psi B\,(\boldsymbol{t})\rfloor_{Nc\boldsymbol{\upsilon}}}{\boldsymbol{\varphi}^{Nc\boldsymbol{\upsilon}}} = \sum_{\boldsymbol{\upsilon}\in\mathcal{P}_{Nc}(G/F)}\left\lfloor \Psi B\left(\frac{\boldsymbol{t}}{\boldsymbol{\varphi}}\right)\right\rfloor_{Nc\boldsymbol{\upsilon}}. \tag{3.13}$$

Thus, the claim follows by observing that $\Psi B\left(\boldsymbol{t}/\boldsymbol{\varphi}\right) = \left(\Psi\beta_d\left(\boldsymbol{t}/\boldsymbol{\varphi}\right)\right)^L = \alpha_{F,d}(\boldsymbol{t})^L$. ∎

We are now ready to prove the main result of this section, stating that the average type-spectrum of the (c,d)-regular F-labelled ensemble of LDPC G-codes is given by

$$\Gamma_{(F,c,d)}(\boldsymbol{\theta}) := \mathrm{H}(\boldsymbol{\theta}) + \frac{c}{d}\inf_{\substack{\boldsymbol{t}\in\mathcal{P}(G/F):\\ \mathrm{supp}(\boldsymbol{t})=\mathrm{supp}(\pi_F^\sharp\boldsymbol{\theta})}}\left\{\log\alpha_{F,d}(\boldsymbol{t}) + dD\big(\pi_F^\sharp\boldsymbol{\theta}||\boldsymbol{t}\big)\right\}. \tag{3.14}$$

From Theorem 3.2 it follows that the spectrum $\Gamma_{(F,c,d)}(\boldsymbol{\theta})$ is an upper semicontinuous function on the probability simplex $\mathcal{P}(G)$. Notice that, by choosing $\boldsymbol{t} = \pi_F^\sharp\boldsymbol{\theta}$, we immediately obtain the estimate

$$\Gamma_{(F,c,d)}(\boldsymbol{\theta}) \le \frac{c}{d}\log\alpha_{F,d}\left(\pi_F^\sharp\boldsymbol{\theta}\right) + \mathrm{H}(\boldsymbol{\theta}).$$

THEOREM 3.5. *For the* (c,d)*-regular* F*-labelled ensemble of LDPC* G*-codes*

$$\lim_{N\in\mathcal{N}_{\boldsymbol{\theta}}\cap\mathcal{N}_{(c,d)}}\frac{1}{N}\log\overline{W_N(\boldsymbol{\theta})} = \Gamma_{(F,c,d)}(\boldsymbol{\theta}).$$

Proof. From (3.10), by recalling that $Nc = Ld$ and $\boldsymbol{\upsilon} = \pi_F^\sharp\boldsymbol{\theta}$, we get

$$\frac{1}{N}\log\overline{W_N(\boldsymbol{\theta})} = \frac{1}{N}\log\binom{N}{N\boldsymbol{\theta}} + \frac{c}{d}\frac{1}{L}\log\frac{|Z_{\boldsymbol{\upsilon}}^{i,N}|}{\binom{Ld}{Ld\boldsymbol{\upsilon}}\boldsymbol{\varphi}^{Ld\boldsymbol{\upsilon}}}.$$

From (2.1) we have $\lim \frac{1}{N} \log \binom{N}{N\boldsymbol{\theta}} = \mathrm{H}(\boldsymbol{\theta})$. Then we can first apply Lemma 3.4 and then Theorem 3.2 (notice that (3.12) with $L = 1$ implies that $\alpha_{F,d}(\boldsymbol{t})$ has nonnegative real coefficients and homogeneous degree), obtaining

$$\lim_N \frac{1}{L} \log \frac{|Z^{i,N}_{\boldsymbol{\upsilon}}|}{\binom{Ld}{Ld\boldsymbol{\upsilon}} \boldsymbol{\varphi}^{Ld\boldsymbol{\upsilon}}} = \lim_N \frac{1}{L} \log \frac{\left\lfloor \alpha_{F,d}(\boldsymbol{t})^L \right\rfloor_{Ld\boldsymbol{\upsilon}}}{\binom{Ld}{Ld\boldsymbol{\upsilon}} \boldsymbol{\varphi}^{Ld\boldsymbol{\upsilon}}}$$
$$= \inf_{\substack{\boldsymbol{t} \in \mathcal{P}(G/F): \\ \mathrm{supp}(\boldsymbol{t}) = \mathrm{supp}(\boldsymbol{\upsilon})}} \left\{ \log \frac{\alpha_{F,d}(\boldsymbol{t})}{\boldsymbol{t}^{d\boldsymbol{\upsilon}}} - d\,\mathrm{H}(\boldsymbol{\upsilon}) \right\}. \qquad \square$$

3.4. Special cases of Theorem 3.5. Now we particularize Theorem 3.5 to some important special cases, showing that all previously known results can be reobtained, while new interesting cases can be studied as well.

3.4.1. LDPC codes over Galois fields. Suppose $G \simeq \mathbb{Z}_p^r$ for some prime number p and positive integer r. First, let F coincide with the whole automorphism group $\mathrm{Aut}(\mathbb{Z}_p^r)$, which is isomorphic to the general linear group of $r \times r$ invertible matrices on $\mathbb{Z}_p$. In this case the probability that an N-tuple $\boldsymbol{x}$ in G^N belongs to the random LDPC code $\mathcal{C}_N = \ker\left(\mathrm{Sum}_d^N \, \Pi_N \, \mathrm{Rep}_c^N\right)$ depends only on the Hamming weight (i.e., number of nonzero entries) of $\boldsymbol{x}$. Indeed, it is easily seen that the action of $\mathrm{Aut}(\mathbb{Z}_p^r)$ on $\mathbb{Z}_p^r$ has only two orbits: one containing the zero element only and one containing all of the nonzero elements of $\mathbb{Z}_p^r$. Thus, the quotient space is $G/F = \{q_0, q_1\}$, with $\boldsymbol{\varphi}(q_0) = 1$, $\boldsymbol{\varphi}(q_1) = p^r - 1$. Moreover, since all nontrivial characters are orthogonal to the trivial one $\chi_0 \equiv 1$, it follows that $\sum_{g \in q_1} \chi(g) = -\chi(0) = -1$ for all $\chi \in \hat{G} \setminus \{\chi_0\}$. Then the average type-spectra of the (c,d)-regular $\mathrm{Aut}(\mathbb{Z}_p^r)$-labelled ensemble of LDPC $\mathbb{Z}_p^r$-codes are given by

(3.15)
$$\Gamma_{(\mathrm{Aut}(\mathbb{Z}_p^r),c,d)}(\boldsymbol{\theta}) = \mathrm{H}(\boldsymbol{\theta}) + \tfrac{c}{d} \inf_{t \in (0,1)} \left\{ \log\left(\tfrac{1}{p^r} + \tfrac{p^r-1}{p^r} \left(1 - \tfrac{p^r}{p^r-1} t\right)^d \right) + dD(\lambda||t) \right\},$$

where $\lambda := 1 - \boldsymbol{\theta}(0)$ and $D(\lambda||t) := \lambda \log \frac{\lambda}{t} + (1-\lambda) \log \frac{1-\lambda}{1-t}$.

Now consider the case $G \simeq \mathbb{Z}_p^r$ again, but now with label group $F \simeq \mathbb{F}_{p^r}^*$, the multiplicative group of nonzero elements of the Galois field $\mathbb{F}_{p^r}$. Observe that $\mathbb{F}_{p^r}^*$ can always be identified with a subgroup (proper if $r > 1$) of $\mathrm{Aut}(\mathbb{Z}_p^r)$. Nevertheless, the action of $\mathbb{F}_{p^r}^*$ on $\mathbb{Z}_p^r$ has the same two orbits as the action of the whole $\mathrm{Aut}(\mathbb{Z}_{p^r})$ on $\mathbb{Z}_p^r$. This shows that the (c,d)-regular $F_{p^r}^*$-labelled ensemble has the same average type-spectrum of the $\mathrm{Aut}(\mathbb{Z}_p^r)$-labelled ensemble, i.e.,

$$\Gamma_{(\mathbb{F}_{p^r}^*,c,d)}(\boldsymbol{\theta}) = \Gamma_{(\mathrm{Aut}(\mathbb{Z}_p^r),c,d)}(\boldsymbol{\theta}) \qquad \forall\, \boldsymbol{\theta} \in \mathcal{P}(\mathbb{Z}_p^r). \tag{3.16}$$

The expression (3.15) coincides with the spectrum of the $\mathbb{F}_{p^r}^*$-labelled ensemble obtained in [4, 17]. We observe that in [32] it was numerically observed that the density-evolution dynamical system [34] exhibits the same threshold value for the $\mathbb{F}_{p^r}^*$-labelled and the $\mathrm{Aut}(\mathbb{Z}_p^r)$-labelled ensembles over the BEC. Formula (3.16) shows that these ensembles have identical average type-spectra.

3.4.2. Unlabelled LDPC ensembles over cyclic groups. We now consider the case when $G \simeq \mathbb{Z}_m$ and $F = \{1\}$. In this case, the characters of $\mathbb{Z}_m$ are given by $\chi_k(h) := e^{\frac{2\pi}{m} hki}$ for $h, k \in \mathbb{Z}_m$, while, trivially, the quotient space $\mathbb{Z}_m/F$ coincides

with $\mathbb{Z}_m$ itself and $\boldsymbol{\varphi} \equiv 1$ (see (3.9)). It follows that

$$\alpha_{\{1\},d}(\boldsymbol{t}) = \beta_d(\boldsymbol{t}) = \tfrac{1}{m} \sum_{1 \le k \le m} \left(\sum_{1 \le h \le m} e^{\frac{2\pi}{m} hki} z_h \right)^d .$$

Then the average type-spectrum takes the following form:

(3.17)
$$\Gamma_{(\{1\},c,d)}(\boldsymbol{\theta}) = \mathrm{H}(\boldsymbol{\theta}) + \frac{c}{d} \inf_{\substack{\boldsymbol{z} \in \mathcal{P}(\mathbb{Z}_m) \\ \mathrm{supp}(\boldsymbol{z}) = \mathrm{supp}(\boldsymbol{\theta})}} \left\{ \log\left(\frac{1}{m} \sum_k \left(\sum_h e^{\frac{2\pi}{m} hki} z_h \right)^d \right) + dD\big(\boldsymbol{\theta} || \boldsymbol{z}\big) \right\}.$$

The above spectrum coincides with the one obtained in [4] (see also [19, p. 49]).

3.4.3. Uniformly labelled ensembles over cyclic groups. Finally, consider the case when $G \simeq \mathbb{Z}_m$ again, but this time with F isomorphic to $\mathbb{Z}_m^*$, the multiplicative group of units of $\mathbb{Z}_m$. Notice that $\mathbb{Z}_m^*$ acts by multiplication on the ring $\mathbb{Z}_m$. It is immediate to see that two $a, b \in \mathbb{Z}_m$ are in the same orbit with respect to this group action iff $(m, a) = (m, b)$, where (k, h) denotes the greatest common divisor of two naturals k and h. The quotient space $\mathbb{Z}_m / \mathbb{Z}_m^*$ can be identified with the set of divisors of m, $\mathbb{D}_m := \{l \in \mathbb{N} \text{ s.t. } l \mid m\}$. We have $|\mathbb{Z}_m^*| = \varphi(m)$, where $\varphi : \mathbb{N} \to \mathbb{N}$, $\varphi(n) = \big|\big\{m \in \mathbb{N} \text{ s.t. } m \le n,\, (n, m) = 1\big\}\big|$, is the Euler φ-function. The projection map is

$$\pi_{\mathbb{Z}_m^*} : \mathbb{Z}_m \to \mathbb{D}_m, \qquad \pi_{\mathbb{Z}_m^*}(a) = \frac{m}{(m, a)}.$$

Notice that, for every $l \in \mathbb{D}_m$, the orbit $\pi^{-1}_{\mathbb{Z}_m^*}(l)$ coincides with $\frac{m}{l}\mathbb{Z}_m^*$ and it is in bijection with $\mathbb{Z}_l^*$ through the map $h \mapsto \frac{m}{l} h$. Then $\boldsymbol{\varphi}(l) = |\pi^{-1}_{\mathbb{Z}_m^*}(l)| = |\mathbb{Z}_l^*| = \varphi(l)$.

In order to evaluate the average-type spectra of the (c, d)-regular $\mathbb{Z}_m^*$-labelled ensemble of LDPC $\mathbb{Z}_m$-codes, it is convenient to introduce the so-called Ramanujan sums

$$r_l(k) := \sum_{j \in \mathbb{Z}_l^*} e^{\frac{2\pi}{l} jki}, \qquad l, k \in \mathbb{N}.$$

The Ramanujan sums are well known in number theory and can be explicitly evaluated in terms of both the Euler φ-function and Möbius function:

$$\mu : \mathbb{N} \to \mathbb{Z}, \qquad \mu(n) = \begin{cases} 1 & \text{if} \quad n = 1, \\ 0 & \text{if} \quad p^2 \mid n \text{ for some prime } p, \\ (-1)^k & \text{if} \quad m = p_1 p_2 \dots p_k \text{ for distinct primes } p_i. \end{cases}$$

For every $l, k \in \mathbb{N}$ it holds [21, p. 237] that

$$r_l(k) = \mu\left(\frac{l}{(l, k)} \right) \frac{\varphi(l)}{\varphi\left(\frac{l}{(l,k)} \right)}. \tag{3.18}$$

We can now explicitly evaluate the multinomial $\alpha_{\mathbb{Z}_m^*,d}(\boldsymbol{t})$, obtaining

$$\begin{aligned}\alpha_{\mathbb{Z}_m^*,d}(\boldsymbol{t}) &= \tfrac{1}{m}\sum_{1\le k\le m}\left(\sum_{l|m}\tfrac{1}{\varphi(l)}\sum_{j\in\mathbb{Z}_l^*}e^{\frac{2\pi}{l}jki}t_l\right)^d\\ &= \tfrac{1}{m}\sum_{1\le k\le m}\left(\sum_{l|m}\tfrac{1}{\varphi(l)}r_l(k)t_l\right)^d\\ &= \tfrac{1}{m}\sum_{k|m}\varphi\left(\tfrac{m}{k}\right)\left(\sum_{l|m}\frac{\mu\left(\frac{l}{(l,k)}\right)}{\varphi\left(\frac{l}{(l,k)}\right)}t_l\right)^d.\end{aligned}$$

It follows that the average type-spectrum of the (c,d)-regular $\mathbb{Z}_m^*$-labelled LDPC ensemble of $\mathbb{Z}_m$-codes is given by

(3.19)
$$\Gamma_{(\mathbb{Z}_m^*,c,d)}(\boldsymbol{\theta})=\mathrm{H}(\boldsymbol{\theta})+\frac{c}{d}\inf_{\boldsymbol{t}}\left\{\log\left(\frac{1}{m}\sum_{k|m}\varphi\left(\frac{m}{k}\right)\left(\sum_{l|m}\frac{\mu\left(\frac{l}{(l,k)}\right)}{\varphi\left(\frac{l}{(l,k)}\right)}t_l\right)^d\right)+dD\big(\pi_{\mathbb{Z}_m^*}\boldsymbol{\theta}||\boldsymbol{z}\big)\right\},$$

where the above infimum has to be considered with respect to all $\boldsymbol{t}$ in $\mathcal{P}(\mathbb{D}_m)$ such that $\mathrm{supp}(\boldsymbol{t})=\mathrm{supp}(\pi_{\mathbb{Z}_m^*}\boldsymbol{\theta})$. Of course, when m is prime, formula (3.19) reduces to (3.15). In particular, when $m=2$, (3.15), (3.17), and (3.19) coincide. For nonprime m instead, (3.19) is novel, to the best of our knowledge.

4. On low-weight type-spectra. In this section we will deal with estimations of the average type-spectra of the regular F-labelled LDPC G-code ensembles for G-types very close to the all-zero type δ_0. We will consider the variational distance on $\mathcal{P}(G)$, $||\boldsymbol{\theta}-\boldsymbol{\theta}'||:=\sup_{B\subseteq G}\{\boldsymbol{\theta}(B)-\boldsymbol{\theta}'(B)\}$.

Recall that, since we are dealing with LDPC G-codes, the all-zero N-tuple is always a codeword. Then $W_N(\delta_0)=1$ deterministically, i.e., for any realization of Π_N in the interconnection group $S_{Nc}\ltimes F^{Nc}$. Hence clearly $\Gamma_{(F,c,d)}(\delta_0)=0$. The main result of this section is that there exists a punctured neighborhood of δ_0 in $\mathcal{P}(G)$, over which the spectra $\Gamma_{(F,c,d)}(\boldsymbol{\theta})$ are strictly negative. Actually, much more precise results will be derived, characterizing the exact rate of decay (asymptotically in N) of the sum of the average enumerating coefficients over all G-types $\boldsymbol{\theta}$ such that $0<||\boldsymbol{\theta}-\delta_0||<\frac{2}{d}$.

Throughout this section we will often use the following notation: for a,t in $\mathbb{N}$ we define the discrete intervals $I_t^a:=[(t-1)a+1,ta]\cap\mathbb{N}$. Notice that, given a degree pair (c,d), for every admissible block-length N in $\mathcal{N}_{(c,d)}$ we have $\{1,2,\dots,Nc\}=\bigcup_{1\le t\le L}I_t^d=\bigcup_{1\le s\le N}I_s^c$.

4.1. An upper bound to low-weight spectra. We start by deriving an upper bound to low-weight type-enumerating coefficients for the inner encoder $|Z_{\boldsymbol{\theta}}^{i,N}|:=\left|G_{\boldsymbol{\theta}}^{Nc}\cap\ker\mathrm{Sum}_d^N\right|$.

LEMMA 4.1. *Let (c,d) be a degree pair, and let $N\in\mathcal{N}_{(c,d)}$. For every $\boldsymbol{\theta}$ in $\mathcal{P}_{Nc}(G)$ such that*

$$||\boldsymbol{\theta}-\delta_0||\le\frac{2}{d},\tag{4.1}$$

we have

$$\left|Z_{\boldsymbol{\theta}}^{i,N}\right|\le\binom{L}{\lfloor w/2\rfloor}\binom{\lfloor w/2\rfloor\, d}{w}\binom{w}{\boldsymbol{\omega}},\tag{4.2}$$

where $\boldsymbol{\omega} \in \mathbb{N}^{G\setminus\{0\}}$ *is defined by* $\boldsymbol{\omega}(k) := Nc\,\boldsymbol{\theta}(k)$*, and* $w := \sum_{k=1}^{m-1} \boldsymbol{\omega}(k)$ *is the number of nonzero entries in an* Nc*-tuple of type* $\boldsymbol{\theta}$*.*

Proof. Let $\boldsymbol{y}$ in $G_{\boldsymbol{\theta}}^{Nc}$ be any Nc-tuple of type $\boldsymbol{\theta}$. A necessary condition for $\boldsymbol{y}$ to be in $\ker \mathrm{Sum}_d^N$ is that each of the first L intervals I_t^d contains either none or at least two nonzero entries of $\boldsymbol{y}$. It follows from (4.2) that $\left|\left\{t \le L : \left|\mathrm{supp}(\boldsymbol{y}) \cap I_t^d\right| \ge 2\right\}\right| \le \lfloor w/2 \rfloor$, while, for any choice of a dissection $1 \le t_1 < \cdots < t_{\lfloor w/2 \rfloor} \le L$ (notice that (4.1) implies $w/2 \le L$), we have $|\{\boldsymbol{y} \in G_{\boldsymbol{\theta}}^{Nc} : \mathrm{supp}(\boldsymbol{y}) \subseteq \bigcup_{j=1}^{\lfloor w/2 \rfloor} I_{t_j}^d\}| \le \binom{d\lfloor w/2 \rfloor}{w}\binom{w}{\boldsymbol{\omega}}$. It follows that

$$\begin{aligned}
|Z_{\boldsymbol{\theta}}^{i,N}| &\le \left| \bigcup_{1\le t\le L} \left\{\boldsymbol{y} \in G_{\boldsymbol{\theta}}^{Nc} : \left|\mathrm{supp}(\boldsymbol{y}) \cap I_t^d\right| \ne 1\right\} \right| \\
&\le \left| \bigcup_{1\le t_1<\cdots<t_{\lfloor w/2 \rfloor}\le L} \left\{ \boldsymbol{y} \in G_{\boldsymbol{\theta}}^{Nc} : \mathrm{supp}(\boldsymbol{y}) \subseteq \bigcup_{j=1}^{\lfloor w/2 \rfloor} I_{t_j} \right\} \right| \\
&\le \binom{L}{\lfloor w/2 \rfloor}\binom{d\,\lfloor w/2 \rfloor}{w}\binom{w}{\boldsymbol{\omega}}. \qquad \square
\end{aligned}$$

We now obtain an estimation for the average low-weight type-enumerators.

LEMMA 4.2. *Let* (c,d) *be a degree pair,* $F \le \mathrm{Aut}(G)$*, and* $N \in \mathcal{N}_{(c,d)}$*. For every* $\boldsymbol{\theta} \in \mathcal{P}_N(G)$ *satisfying* (4.1) *the average type-enumerator function of the* (c,d)*-regular* F*-labelled ensemble satisfies*

$$\overline{W_N(\boldsymbol{\theta})} \le \binom{N}{N\boldsymbol{\theta}}\binom{L}{\lfloor w/2 \rfloor}\left(\frac{w}{2L}\right)^w, \tag{4.3}$$

where $w := Nc(1-\boldsymbol{\theta}(0))$*.*

Proof. Consider the projection map $\pi_F : G \to G/F$ and the associated map for types $\pi_F^\sharp : G \to G/F$. Define $\boldsymbol{\upsilon} := \pi_F^\sharp \boldsymbol{\theta}$, and $\boldsymbol{u} \in \mathbb{Z}_+^{G/F\setminus\{0\}}$ by $\boldsymbol{u}(k) = Nc\boldsymbol{\upsilon}(k)$. Also, for every $\boldsymbol{\theta}'$ in $\mathcal{P}(G)$, define $\boldsymbol{\omega}'$ in $\mathbb{Z}_+^{G\setminus\{0\}}$ by $\boldsymbol{\omega}'(k) := Nc\,\boldsymbol{\theta}'(k)$. Notice that $\sum_{\boldsymbol{\theta}' \in \mathcal{O}_{\boldsymbol{\upsilon}}^{Nc}} \binom{w}{\boldsymbol{\omega}'} = \binom{w}{Nc\,\boldsymbol{u}}\boldsymbol{\varphi}^{Nc\boldsymbol{\upsilon}}$. From (3.10), (3.13), and (4.2) we get

$$\begin{aligned}
\overline{W_N(\boldsymbol{\theta})} &= \binom{N}{N\boldsymbol{\theta}}\binom{Nc}{Nc\,\boldsymbol{\upsilon}}^{-1} \boldsymbol{\varphi}^{-Nc\,\boldsymbol{\upsilon}} \sum_{\boldsymbol{\theta}' \in \mathcal{O}_{\boldsymbol{\upsilon}}^{Nc}} |Z_{\boldsymbol{\theta}'}^{i,N}| \\
&\le \binom{N}{N\boldsymbol{\theta}}\binom{Nc}{w}^{-1}\binom{L}{\lfloor w/2 \rfloor}\binom{\lfloor w/2 \rfloor\, d}{w}\binom{w}{Nc\,\boldsymbol{u}}^{-1} \boldsymbol{\varphi}^{-Nc\,\boldsymbol{\upsilon}} \sum_{\boldsymbol{\theta}' \in \mathcal{O}_{\boldsymbol{\upsilon}}^{Nc}} \binom{w}{\boldsymbol{\omega}'} \\
&= \binom{N}{N\boldsymbol{\theta}}\binom{L}{\lfloor w/2 \rfloor}\binom{Nc}{w}^{-1}\binom{\lfloor w/2 \rfloor\, d}{w} \\
&= \binom{N}{N\boldsymbol{\theta}}\binom{L}{\lfloor w/2 \rfloor}\frac{\lfloor w/2 \rfloor d(\lfloor w/2 \rfloor d-1)\ldots(\lfloor w/2 \rfloor d-w+1)}{Ld(Ld-1)\ldots(Ld-w+1)} \\
&\le \binom{N}{N\boldsymbol{\theta}}\binom{L}{\lfloor w/2 \rfloor}\left(\frac{w}{2L}\right)^w. \qquad \square
\end{aligned}$$

A first consequence of Lemma 4.2 is the following upper bound on the average type-spectra of the F-labelled LDPC ensembles.

PROPOSITION 4.3. *For every degree pair* (c,d) *such that* $c \ge 3$ *we have*

$$\Gamma_{(F,c,d)}(\boldsymbol{\theta}) \le f_{c,d}(x) \qquad \forall\, \boldsymbol{\theta} : \|\boldsymbol{\theta} - \delta_0\| \le \frac{2}{d},$$

where $x := 1 - \boldsymbol{\theta}(0)$*, and*

$$f_{c,d}(x) := \mathrm{H}(x) + x\log(|G|-1) + \tfrac{c}{d}\,\mathrm{H}\left(\tfrac{d}{2}x\right) + cx\log\left(\tfrac{d}{2}x\right),$$

with $\mathrm{H}(x) := -x\log x - (1-x)\log(1-x)$ *denoting the binary entropy.*

Proof. From (4.3) it follows that, for every $||\boldsymbol{\theta} - \delta_0|| < \frac{2}{d}$, for the F-labelled (c,d)-regular ensemble we have

$$\begin{aligned}\frac{1}{N}\log\overline{W_N(\boldsymbol{\theta})} \quad &\leq \quad \frac{1}{N}\log\binom{N}{N\boldsymbol{\theta}} + \frac{1}{N}\log\binom{L}{\lfloor xN\frac{c}{2}\rfloor} + \frac{1}{N}\log\left(\frac{cNx}{2L}\right)^{cNx} \\ &\overset{N\in\mathcal{N}_{(c,d)}}{\longrightarrow} \ \mathrm{H}(\boldsymbol{\theta}) + \frac{c}{d}\,\mathrm{H}\left(\frac{d}{2}x\right) + +cx\log\left(\frac{d}{2}x\right) \\ &\leq \quad \mathrm{H}(x) + x\log(|G|-1) + cx\log\left(\frac{d}{2}x\right). \qquad \square\end{aligned}$$

It is easy to see that, whenever $c > 2$, $\frac{\mathrm{d}}{\mathrm{d}x} f_{c,d}\big|_{x=0} = -\infty$. Therefore, Proposition 4.3 implies that the spectra $\Gamma_{(F,c,d)}(\boldsymbol{\theta})$ are strictly negative in a sufficiently small punctured neighborhood of δ_0 in $\mathcal{P}(G)$. In section 5 this fact will be used in order to show that the minimum $\boldsymbol{\Delta}$-distance grows linearly with N with high probability. Here we derive more precise estimations for the average type-enumerating functions.

PROPOSITION 4.4. *Let F be any subgroup of* $\mathrm{Aut}(G)$*, (c,d) a degree pair, and $N \in \mathcal{N}_{(c,d)}$. There exists a positive constant K such that the type-enumerator function of the (c,d)-regular F-labelled ensemble satisfies*

$$\sum_{\frac{2}{N}\leq||\delta_0-\boldsymbol{\theta}||\leq\frac{2}{d}} \overline{W_N(\boldsymbol{\theta})} \leq KN^{2-c}.$$

Proof. For every N in $\mathcal{N}_{(c,d)}$ we define the quantities

$$g_w(N) := \sum_{||\delta_0-\boldsymbol{\theta}||=\frac{w}{N}} \overline{W_N(\boldsymbol{\theta})}, \qquad w \in \mathbb{N}.$$

For $\boldsymbol{\theta}$ in $\mathcal{P}_N(G)$ define $\boldsymbol{\omega}$ as in Lemma 4.1. For all $w = 2, \dots, \lfloor \frac{2}{d}N \rfloor$, (4.3) implies

$$g_w(N) \leq \sum_{\boldsymbol{\theta}(0)=\frac{N-w}{N}} \binom{N}{N\boldsymbol{\theta}}\binom{L}{\lfloor c\frac{w}{2}\rfloor}\left(\frac{wc}{2L}\right)^{wc} = \binom{L}{\lfloor c\frac{w}{2}\rfloor}\left(\frac{wc}{2L}\right)^{wc}\binom{N}{w}(|G|-1)^w =: g'_w(N).$$

We have, for every $2 \leq w \leq \lfloor 2dN \rfloor$,

$$\frac{g'_{w+2}(N)}{g'_w(N)} \leq (|G|-1)^2\left(\frac{N-w}{w}\right)^2\left(\frac{L-\lfloor c\frac{w}{2}\rfloor}{\lfloor c\frac{w}{2}\rfloor\, 2L}\right)^c\left(1+\frac{2}{w}\right)^{(w+2)c} \leq (|G|-1)^2(3e)^{2c}N^{2-c}.$$

It follows that if $c \geq 3$, then there exists N_0 in $\mathbb{N}$ such that, for all N in $\mathcal{N}_{(c,d)}$ such that $N \geq N_0$, $\frac{g'_{w+2}(N)}{g'_w(N)} \leq \frac{1}{2}$ for all $1 \leq w \leq \lfloor \frac{2}{d}N \rfloor$. Then we have

$$\sum_{\frac{2}{N}\leq||\delta_0-\boldsymbol{\theta}||\leq\frac{2}{d}} \overline{W_N(\boldsymbol{\theta})} \leq g'_2(N)\sum_{w=2}^{\lfloor\frac{2}{d}N\rfloor} 2^{-w} + g'_3(N)\sum_{w=2}^{\lfloor\frac{2}{d}N\rfloor} 2^{-w} \leq 2g'_2(N) + 2g'_3(N) \leq KN^{2-c}$$

for some positive constants K', K'', K, all independent of N. $\square$

4.2. On weight-one codewords. We now derive a more precise estimation of the average enumerating functions for G-types of N-tuples with all but one entry equal to zero. Fixed any N in $\mathbb{N}$, k in G we define the G-type

$$\boldsymbol{\tau}_k := \left(1 - \frac{1}{N}\right)\delta_0 + \frac{1}{N}\delta_k \in \mathcal{P}_N(G),$$

and we look for upper bounds on the average spectra $\overline{W_N(\boldsymbol{\tau}_k)}$ for the (c,d)-regular F-labelled LDPC ensembles. We will show how these estimations depend on the choice of F among the subgroups of the automorphism group $\mathrm{Aut}(G)$.

We start with a few elementary considerations about closed walks and cycles in directed graphs. A closed walk of length n in a directed graph $\mathcal{G} = (V, E)$ (where V is a finite set and $E \subseteq V^2$) is a $\mathbb{Z}_n$-labelled string of vertices $\boldsymbol{v} \in V^{\mathbb{Z}_n}$ such that any two consecutive vertices are adjacent, i.e., $(v_k, v_{k+1}) \in E$ for all $k \in \mathbb{Z}_n$. A cycle of length n is a closed walk $\boldsymbol{v} \in V^{\mathbb{Z}_n}$ such that $v_k \neq v_j$ for all $k \neq j \in \mathbb{Z}_n$. A self-loop is a cycle of length 1. Every closed walk $\boldsymbol{v}$ of length n is the concatenation of k cycles $\boldsymbol{v}^1, \dots, \boldsymbol{v}^k$ such that the sum of the lengths of $\boldsymbol{v}^1, \dots, \boldsymbol{v}^k$ equals n. Observe that in general $k \leq n$, while $k \leq \lfloor n/2 \rfloor$, provided that the directed graph $\mathcal{G}$ contains no self-loops.

Given a finite Abelian group G and a subset S of G, we denote by $\mathcal{G}(G, S)$ the directed Cayley graph with vertex set G and edge set $\{(g, g+s) \,|\, g \in G,\, s \in S\}$. It is straightforward that closed walks $\boldsymbol{v}$ of length n in an Abelian Cayley graph $\mathcal{G}(G, S)$ starting in any fixed vertex $g \in G$ (i.e., such that $v_0 = g$) are in one-to-one correspondence with 0-sum n-tuples $\boldsymbol{x}$ in S^n.

For a subset $S \subseteq G$ and a positive integer n, consider a closed walk $\boldsymbol{v}$ of length n in $\mathcal{G}$. By the previous considerations, $\boldsymbol{v}$ is the concatenation of $k(\boldsymbol{v})$ cycles. We put $b(S, n)$ equal to the maximum of $k(\boldsymbol{v})$ over all possible closed walks $\boldsymbol{v}$ of length n in $\mathcal{G}(G, S)$, with the agreement that $b(S, n) = 0$ whenever no closed walk in $\mathcal{G}(G, S)$ has length n. The reason for this notation becomes evident with the following result.

LEMMA 4.5. *Let F be any subgroup of* $\mathrm{Aut}(G)$, *(c, d) a degree pair, and $N \in \mathcal{N}_{(c,d)}$. Then, for all k in G, the type-enumerator function of the (c, d)-regular F-labelled ensemble satisfies*

$$\overline{W_N(\boldsymbol{\tau}_k)} \leq N \binom{L}{b(Fk, c)} \left[\frac{b(Fk, c)}{L}\right]^c. \tag{4.4}$$

Proof. Define $\boldsymbol{v} := \pi_F^\sharp \boldsymbol{\tau}_k \in \mathcal{P}(G/F)$. Let $\boldsymbol{y}$ be any element of $G_{\boldsymbol{v}}^{Nc}$. Then for $\mathrm{Sum}_d^N \boldsymbol{y} = \boldsymbol{0}$ in G^L it is necessary that $\sum_{1 \leq j \leq Nc} y_j = 0$ in G. Since $\boldsymbol{y} \in G_{\boldsymbol{v}}^{Nc}$ has exactly c nonzero entries all belonging to Fk, it follows that $\left|Z_{\boldsymbol{v}}^{i,N}\right| = 0$ iff there are no closed walks of length c in the Cayley graph $\mathcal{G}(G, Fk)$. Then (4.4) immediately follows in the case $b(Fk, c) = 0$.

Now assume that there exist closed walks of length c in $\mathcal{G}(G, Fk)$. By the previous considerations, each such walk decomposes in at most $b(Fk, c)$ cycles. If we consider the intervals I_t^d, for $1 \leq t \leq L$, and put $\mathrm{supp}(\boldsymbol{y}) \cap I_t^d := \{j_1^t, j_2^t, \dots, j_{n_t}^t\}$, we have

$$\left(\mathrm{Sum}_d^N \boldsymbol{y}\right)_t = \sum_{j \in I_t^d} y_j = \sum_{1 \leq i \leq n_t} y_{j_i^t} \qquad \forall\, 1 \leq t \leq L.$$

Therefore, if $\mathrm{Sum}_d^N \boldsymbol{y} = \boldsymbol{0}$, then it is necessary that $\boldsymbol{v} \in G^{\mathbb{Z}_{n_t}}$, $v_l := \sum_{1 \leq i \leq l} y_{j_i^t}$ is a closed walk in $\mathcal{G}(G, Fk)$ for all t such that $\mathrm{supp}(\boldsymbol{y}) \cap I_t^d$ is nonempty. It follows that

$\mathrm{supp}(\boldsymbol{y}) \cap I_t^d$ is nonempty for at most $b(Fk,c)$ values of t. Therefore, by taking into account the $\binom{L}{b(Fk,c)}$ possible choices of $b(Fk,c)$ intervals out of L possible ones, the $\binom{b(Fk,c)}{c}$ choices of c positions out of $b(Fk,c)d$ available ones, and the $\boldsymbol{\varphi}(Fk)^c$ choices of an ordered c-tuple with entries from the orbit Fk, we get

$$\left|Z_{\boldsymbol{v}}^{i,N}\right| = \left|\ker \mathrm{Sum}_d^N \cap G_{\boldsymbol{v}}^{Nc}\right| \leq \binom{L}{b(Fk,c)}\binom{b(Fk,c)d}{c}\boldsymbol{\varphi}(Fk)^c.$$

Then from (3.10) it follows that

$$\begin{aligned}\overline{W_N(\boldsymbol{\tau}_k)} = \frac{N\left|Z_{\boldsymbol{v}}^{i,N}\right|}{\binom{Nc}{c}\boldsymbol{\varphi}(Fk)^c} &\leq \frac{N}{\binom{Nc}{c}}\binom{L}{b(Fk,c)}\binom{b(Fk,c)d}{c} \\ &\leq N\binom{L}{b(Fk,c)}\left[\frac{b(Fk,c)}{L}\right]^c. \qquad \square\end{aligned}$$

4.3. Main result. Building on the results of sections 4.1 and 4.2, we are now ready to present the main result of this section. For a subgroup F of $\mathrm{Aut}(G)$ and a positive integer c we define

$$a(F,c) := 1 - c + \max\left(\{1\} \cup \{b(Fk,c) |\, k \in G \setminus \{0\}\}\right), \tag{4.5}$$

where we recall that $b(S,c)$ was defined in section 4.2 as the minimum number of cycles in $\mathcal{G}(G,S)$ of total length c, with the agreement that $b(S,c) = 0$ when no closed walk in $\mathcal{G}(G,S)$ has length c.

Before stating the main result, we need a simple property of $a(F,c)$. For every $k \neq 0$, Fk does not contain 0, so that there are no self-loops in $\mathcal{G}(G,Fk)$, and then $b(Fk,c) \leq \lfloor c/2 \rfloor$. It immediately follows that

$$2 - c \leq a(F,c) \leq 1 - \lceil c/2 \rceil. \tag{4.6}$$

THEOREM 4.6. *For every degree pair (c,d) such that $c \geq 3$, and every subgroup F of $\mathrm{Aut}(G)$, there exists a positive constant K such that for the (c,d)-regular F-labelled ensemble it holds that*

$$\sum_{0<||\delta_0 - \boldsymbol{\theta}||\leq \frac{2}{d}} \overline{W_N(\boldsymbol{\theta})} \leq K N^{a(F,c)}, \qquad N \in \mathcal{N}_{(c,d)}.$$

Proof. First, we consider weight-one types. From (4.4) we have

$$\sum_{\boldsymbol{\theta}(0)=\frac{N-1}{N}} \overline{W_N(\boldsymbol{\theta})} \leq \sum_{k\in G\setminus\{0\}} N\binom{L}{b(Fk,c)}\frac{b(Fk,c)^c}{L^c} \leq K' \sum_{k\in G\setminus\{0\}} N^{1+b(Fk,c)-c} \leq K'|G|N^{a(F,c)}$$

for some positive constant K'. The claim then follows by combining Proposition 4.4 with the previous estimation and observing that $a(F,c) \leq 2 - c \leq -1$. $\square$

Now we explicitly evaluate $a(F,c)$ for the three examples studied in the previous section.

Example 4. Consider the case when $G \simeq \mathbb{Z}_p^r$ and either $F \simeq \mathrm{Aut}(\mathbb{Z}_p^r)$ or $F \simeq \mathbb{F}_{p^r}^*$. In both cases $Fk = \mathbb{Z}_p^r \setminus \{0\}$ for all $k \in \mathbb{Z}_p^r \setminus \{0\}$. Then $\mathcal{G}(\mathbb{Z}_p^r, Fk) = \mathcal{G}(\mathbb{Z}_p^r, \mathbb{Z}_p^r \setminus \{0\})$ is the complete graph with p^r vertices. It follows that $\mathcal{G}(\mathbb{Z}_p^r, \mathbb{Z}_p^r \setminus \{0\})$ contains closed walks of any length $n \geq 2$ whenever $p^r \neq 2$, while $\mathcal{G}(\mathbb{Z}_2, \{1\})$ contains closed walks

of even length only. Therefore, for $G \simeq \mathbb{Z}_p^r$ with $p^r \neq 2$, $a(F,c) = 1 - \lceil c/2 \rceil$ for all c, while for $G \simeq \mathbb{Z}_2$, $a(F,c) = 1 - c/2$ for even c and $2 - c$ for odd c.

Example 5. Consider the unlabelled ensemble over the cyclic group, i.e., $G \simeq \mathbb{Z}_m$ with $F = \{1\}$. If $(m,c) = 1$, then $m|ck$ iff $m|k$. Then, for all $k \in \mathbb{Z}_m \setminus \{0\}$, the Cayley graph $\mathcal{G}(\mathbb{Z}_m, Fk) = \mathcal{G}(\mathbb{Z}_m, \{k\})$ has no closed walks of length c. In this case clearly $a(\{1\}, c) = 2 - c$.

Then consider the case when $(m,c) > 1$, and let $\mathrm{lpcf}(c,m)$ be the smallest prime common factor between c and m. Consider any k in $\mathbb{Z}_m \setminus \{0\}$ such that $\mathcal{G}(\mathbb{Z}_m, \{k\})$ has a closed walk of length c, i.e., such that $m \mid ck$. The length of the shortest such walk is given by $\frac{m}{(m,k)} = \frac{(m,ck)}{(m,k)} = (\frac{m}{(m,k)}, c)$. Thus, $\frac{m}{(m,k)} \mid c$, while clearly $\frac{m}{(m,k)} \mid m$. But $(m,k) < m$, so that necessarily the shortest cycle in $\mathcal{G}(\mathbb{Z}_m, \{k\})$ $\frac{m}{(m,k)}$ is not less than $\mathrm{lpcf}(m,c)$, with equality iff $k \in \frac{m}{\mathrm{lpcf}(m,c)}\mathbb{Z}_m \setminus \{0\}$. Thus, $b(\{k\}, c) = \frac{c}{\mathrm{lpcf}(m,c)}$ for $k \in \frac{m}{\mathrm{lpcf}(m,c)}\mathbb{Z}_m \setminus \{0\}$, and $b(\{k\}, c) < \frac{c}{\mathrm{lpcf}(m,c)}$ for $k \in \mathbb{Z}_m \setminus \frac{m}{\mathrm{lpcf}(m,c)}\mathbb{Z}_m$. It immediately follows that, whenever $(m,c) > 1$, $a(\{1\}, c) = 1 - c + \frac{c}{\mathrm{lpcf}(m,c)}$.

Example 6. Consider the uniformly labelled ensemble over the cyclic group, i.e., $G \simeq \mathbb{Z}_m$ with $F \simeq \mathbb{Z}_m^*$. First, we claim, for $n \geq 2$, the following:

- if n is even, then all closed walks in $\mathcal{G}(\mathbb{Z}_n, \mathbb{Z}_n^*)$ have even length and there exists a 2-cycle;
- if n is odd, then there exist both a 2-cycle and a 3-cycle.

To see this, first, since $1, -1 \in \mathbb{Z}_n^*$, $(0,1)$ is a 2-cycle in $\mathcal{G}(\mathbb{Z}_n, \mathbb{Z}_n^*)$, both for even and odd n. Then consider the case when n is even: clearly all $k \in \mathbb{Z}_n^*$ are odd, so that the modulo-n sum of an odd number of elements of $\mathbb{Z}_n^*$ cannot be equal to 0 modulo n. Thus every closed walk in $\mathcal{G}(\mathbb{Z}_n, \mathbb{Z}_n^*)$ must be of even length. On the other hand, if n is odd, then $2 \in \mathbb{Z}_n^*$, so that $(0,2,1)$ is a 3-cycle in $\mathcal{G}(\mathbb{Z}_n, \mathbb{Z}_n^*)$.

Let us now consider some $k \in \mathbb{Z}_m \setminus \{0\}$. Then, by applying the previous observation with $n = \frac{m}{(m,k)}$, one gets that, if c is odd and $\frac{m}{(m,k)}$ is even, there are no closed walks of length c in $\mathcal{G}(\mathbb{Z}_m, \mathbb{Z}_m^* k)$ so that $b(\mathbb{Z}_m^* k, c) = 0$, while otherwise, if c is even or $\frac{m}{(m,k)}$ is odd, $b(\mathbb{Z}_m^* k, c) = \lfloor c/2 \rfloor$. It thus follows that $a(\mathbb{Z}_m^*, c) = 1 - \lceil c/2 \rceil$ unless c is odd and m is an integer power of 2; in the latter case $a(\mathbb{Z}_m^*, c) = 2 - c$.

4.4. Lower bounds on low-weight type-enumerators. In this section we present some results, of independent interest, which show that the estimations given by Theorem 4.6 are tight. All of the proofs are deferred to the appendix.

First, we deal with weight-one type-enumerators.

PROPOSITION 4.7. *Let (c,d) be a degree pair such that $c \geq 3$, and let F be any subgroup of* $\mathrm{Aut}(G)$. *Then there exists a constant $K > 0$ such that for all k in $G \setminus \{0\}$ such that $a(F,c) = 1 - c + b(Fk, c)$ the type-enumerator function of the (c,d)-regular F-labelled LDPC ensemble satisfies*

$$\mathbb{P}\left(W_N(\boldsymbol{\tau}_k) \geq 1\right) \geq K N^{a(F,c)}, \qquad N \in \mathcal{N}_{(c,d)}. \tag{4.7}$$

Finally, we propose a lower bound on weight-two type-enumerators. For every k in G define

$$\hat{\boldsymbol{\tau}}_k := \frac{1}{N}\delta_k + \frac{1}{N}\delta_{-k} + \frac{N-2}{N}\delta_0 \in \mathcal{P}(G).$$

PROPOSITION 4.8. *For every degree pair (c,d) there exists a constant $K > 0$ such that for every k in $G \setminus \{0\}$ the type-enumerator function of the (c,d)-regular F-labelled LDPC ensemble satisfies*

$$\mathbb{P}\left(W_N(\hat{\boldsymbol{\tau}}_k) \geq 1\right) \geq K N^{2-c} \qquad \forall\, N \in \mathcal{N}_{(c,d)}. \tag{4.8}$$

5. Asymptotic lower bounds on the typical minimum distance. Throughout this section we will assume we have fixed a G-symmetric MC $(\mathcal{X}, \mathcal{Y}, P)$ with associated Bhattacharyya distance $\boldsymbol{\Delta}$ and weight $\boldsymbol{\delta}$, and we study the asymptotics of the minimum $\boldsymbol{\Delta}$-distance of regular LDPC G-code ensembles.

Given a degree pair (c, d), a natural candidate for the typical normalized minimum $\boldsymbol{\Delta}$-distance of the (c, d)-regular F-labelled ensemble is the quantity

$$\gamma_{(F,c,d)} := \inf\left\{\langle \boldsymbol{\delta}, \boldsymbol{\theta}\rangle \,\middle|\, \boldsymbol{\theta} \in \mathcal{P}(G) \setminus \{\delta_0\} \text{ s.t. } \Gamma_{(F,c,d)}(\boldsymbol{\theta}) \geq 0\right\}. \tag{5.1}$$

It turns out that $\gamma_{(F,c,d)}$ actually is a lower bound on the asymptotic normalized minimum distance for the (c, d)-regular F-labelled ensemble. This does not follow directly from Theorem 3.5 since $\lim_{\boldsymbol{\theta}\to\delta_0} \Gamma_{(F,c,d)}(\boldsymbol{\theta}) = 0$. However, using both Theorems 3.5 and 4.6 the following result can be proved.

THEOREM 5.1. *Let (c, d) be a degree pair such that $a(F, c) < -1$. Then for the (c, d)-regular F-labelled LDPC ensemble the following holds:*

$$\mathbb{P}\left(\liminf_{N\in\mathcal{N}_{(c,d)}} \tfrac{1}{N} \mathrm{d}_{\min}(\ker \Phi_N) \geq \gamma_{(F,c,d)}\right) = 1.$$

Proof. By (2.3) we have that

$$\frac{1}{N}\mathrm{d}_{\min}(\ker \Phi_N) = \inf\left\{\langle \boldsymbol{\delta}, \boldsymbol{\theta}\rangle \,\middle|\, \boldsymbol{\theta} \in \mathcal{P}(G) \setminus \{\delta_0\} \text{ s.t. } W_N(\boldsymbol{\theta}) \geq 1\right\} = \min\left\{\kappa'_N, \kappa''_N\right\},$$

where for every N in $\mathcal{N}_{(c,d)}$ we define

$$\begin{aligned}\kappa'_N &:= \inf\left\{\langle \boldsymbol{\delta}, \boldsymbol{\theta}\rangle \,\middle|\, 0 < ||\boldsymbol{\theta} - \delta_0|| < \tfrac{2}{d} \,:\, W_N(\boldsymbol{\theta}) \geq 1\right\},\\ \kappa''_N &:= \inf\left\{\langle \boldsymbol{\delta}, \boldsymbol{\theta}\rangle \,\middle|\, ||\boldsymbol{\theta} - \delta_0|| \geq \tfrac{2}{d} \,:\, W_N(\boldsymbol{\theta}) \geq 1\right\}.\end{aligned}$$

Clearly, $\liminf_N \frac{1}{N}\mathrm{d}_{\min}(\ker \Phi_N) = \min\{\rho', \rho''\}$, where we put $\rho' := \liminf_N \kappa'_N$ and $\rho'' := \liminf_N \kappa''_N$.

We start by establishing a lower bound on ρ''. Define $\Omega := \left\{\boldsymbol{\theta} : ||\boldsymbol{\theta} - \delta_0|| \geq \frac{2}{d}\right\}$ and, for each x in $\mathbb{R}$, the set

$$\Omega_x := \left\{\boldsymbol{\theta} \in \Omega \cap \mathcal{P}_{\mathbb{N}}(G) \text{ s.t. } \Gamma_{(F,c,d)}(\boldsymbol{\theta}) < x\right\}. \tag{5.2}$$

Now consider the quantity $\eta(x) := \inf\left\{\langle \boldsymbol{\delta}, \boldsymbol{\theta}\rangle \,\middle|\, \boldsymbol{\theta} \in \Omega \setminus \Omega_x\right\}$. Since $\Gamma_{(F,c,d)}(\boldsymbol{\theta})$ is an upper semicontinuous function of $\boldsymbol{\theta}$ and Ω is a closed subset of $\mathcal{P}(G)$, standard analytical arguments (see Lemma 8.1 in the appendix) allow us to conclude that η is a nondecreasing and lower semicontinuous function.

Let us now fix some arbitrary $\varepsilon > 0$. By successively applying a union bound estimation, the Markov inequality, Theorem 3.5, and (5.2), we get

$$\mathbb{P}\left(\bigcup_{\boldsymbol{\theta}\in\Omega_{-\varepsilon}} \{W_N(\boldsymbol{\theta}) \geq 1\}\right) \leq \sum_{\boldsymbol{\theta}\in\Omega_{-\varepsilon}} \mathbb{P}\left(W_N(\boldsymbol{\theta}) \geq 1\right) \leq \sum_{\boldsymbol{\theta}\in\Omega_{-\varepsilon}} \overline{W_N(\boldsymbol{\theta})} \leq \exp(-N(\varepsilon - f(N))),$$

with $\lim_N f(N) = 0$. It follows that $\sum_N \mathbb{P}\big(\bigcup_{\boldsymbol{\theta}\in\Omega_{-\varepsilon}} \{W_N(\boldsymbol{\theta}) \geq 1\}\big) < +\infty$, and thus the Borel–Cantelli lemma implies that with probability one the event $\bigcup_{\boldsymbol{\theta}\in\Omega_{-\varepsilon}} \{W_N(\boldsymbol{\theta}) \geq 1\}$ occurs only for finitely many N in $\mathcal{N}_{(c,d)}$. Hence,

$$\mathbb{P}\left(\rho'' < \eta(-\varepsilon)\right) \leq \mathbb{P}\left(\left\{\bigcup_{\boldsymbol{\theta}\in\Omega_{-\varepsilon}} \{W_N(\boldsymbol{\theta}) > 0\}\right\} \text{ i. o. } N \in \mathcal{N}_{(c,d)}\right) = 0 \qquad \forall\, \varepsilon > 0,$$

where i. o. stands for infinitely often. Notice that $\gamma_{(F,c,d)} = \eta(0)$. Hence, monotonicity and lower semicontinuity of the function η allow us to conclude that

(5.3)
$$\mathbb{P}\left(\rho'' < \gamma_{(F,c,d)}\right) = \mathbb{P}\left(\rho'' < \eta(0)\right) \leq \mathbb{P}\left(\rho'' < \lim_k \eta\left(-\tfrac{1}{k}\right)\right) = \lim_k \mathbb{P}\left(\rho'' < \eta\left(-\tfrac{1}{k}\right)\right) = 0.$$

Now let us consider the term ρ'. By sequentially applying a union bound estimation, the Markov inequality, and Theorem 4.6, we get for every N in $\mathcal{N}_{(c,d)}$

$$\mathbb{P}\left(\bigcup_{0<||\boldsymbol{\theta}-\delta_0||<\frac{2}{d}} \{W_N(\boldsymbol{\theta}) \geq 1\}\right) \leq \sum_{0<||\boldsymbol{\theta}-\delta_0||<\frac{2}{d}} \overline{W_N(\boldsymbol{\theta})} \leq K N^{a(F,c)}, \tag{5.4}$$

where K is a positive constant independent of N. Since $a(F,c) < -1$, we get

$$\sum_N \mathbb{P}\left(\bigcup_{0<||\boldsymbol{\theta}-\delta_0||<\frac{2}{d}} \{W_N(\boldsymbol{\theta}) \geq 1\}\right) \leq K \sum_N N^{a(F,c)} < +\infty.$$

By the Borel–Cantelli lemma we get that the event $\bigcup_{0<||\boldsymbol{\theta}-\delta_0||<\frac{2}{d}} \{W_N(\boldsymbol{\theta}) \geq 1\}$ occurs only for finitely many N in $\mathcal{N}_{(c,d)}$ with probability one. This yields $\mathbb{P}(\rho' = +\infty) = 1$, which, together with (5.3), implies the claim. ∎

We have proved the previous theorem under the assumption $a(F,c) < -1$. In fact, for $c = 2$ it is known, since Gallager's work [19], that deterministically the minimum distance cannot grow faster than logarithmically with the block-length N. From (4.6) it follows that if $c \geq 5$, then $a(F,c) < -1$ for any F, and if $c = 3$, then $a(F,c) = -1$ for any F, while, when $c = 4$, $a(F,c) < -1$ for some choices of F. However, one can weaken the assumption $a(F,c) < -1$ requiring only that $a(F,c) < 0$ (thus including the cases $c = 3$ and $c = 4$ for some F). In these cases, $\gamma_{(F,c,d)}$ still gives an asymptotic lower bound for the normalized minimum distances $\frac{1}{N}\,\mathrm{d}_{\min}(\ker \Phi_N)$ in a weaker probabilistic sense. In fact, a more detailed analysis enlightens a nonconcentration phenomenon. In order to describe it, first, for every degree pair (c,d) and every subgroup F of $\mathrm{Aut}(G)$, we define the following quantity:

(5.5)
$$\zeta_{(F,c)} := \begin{cases} \min\{\boldsymbol{\delta}(k) |\, k \in G \setminus \{0\} : a(F,c) = 1 - c + b(Fk,c)\} & \text{if} \quad a(F,c) \neq 2-c, \\ \min\{(2 - b(Fk,c))\boldsymbol{\delta}(k) |\, k \in G \setminus \{0\}\} & \text{if} \quad a(F,c) = 2-c. \end{cases}$$

We have the following result.

THEOREM 5.2. *Let (c,d) be a degree pair such that $a(F,c) = -1$. Then*

$$\lim_{N \in \mathcal{N}_{(c,d)}} \mathbb{P}\left(\frac{1}{N}\,\mathrm{d}_{\min}(\ker \Phi_N) \geq \gamma_{(F,c,d)}\right) = 1.$$

Moreover, if the random variables Π_N defining the (c,d)-regular unlabelled LDPC ensemble are mutually independent, we have

$$\mathbb{P}\left(\liminf_{N \in \mathcal{N}_{(c,d)}} \mathrm{d}_{\min}(\ker \Phi_N) = \zeta_{(F,c)}\right) = 1.$$

Theorem 5.2 is proved in the appendix. The probabilistic interpretation is as follows. In the case $a(F,c) = -1$, with probability one, the sequence of the unnormalized minimum distances $(\mathrm{d}_{\min}(\ker \Phi_N))$ contains a subsequence converging to $\zeta_{(F,c)}$.

Thus, while with increasing probability the minimum $\mathbf{\Delta}$-distance is growing linearly with the block-length N, almost surely a subsequence with constant minimum distance shows up. We observe that, for irregular binary LDPC ensembles, even more evident nonconcentration phenomena are known to arise; see [15, 31].

6. Numerical results. In this section we present some numerical results for the minimum distances of the LDPC ensembles which have been studied in this paper. We focus on a particular channel, the $\mathbb{Z}_8$-symmetric 8-PSK AWGN channel, and we compare the average distance-spectra of the regular unlabelled and uniformly labelled LDPC $\mathbb{Z}_8$-code ensembles. Our results indicate a strong superiority of the uniformly labelled (i.e., the one with label group $F \simeq \mathbb{Z}_8^*$) ensemble with respect to the unlabelled one (i.e., $F = \{1\}$). Then we compare these results with some contradicting analysis of the average error probability of these ensembles and discuss how this seeming paradox can be explained by invoking so-called expurgation arguments.

6.1. Numerical results for the average distance-spectra. Let us start with some general considerations. Suppose we are given any ensemble of G-codes with average type-spectrum $\Gamma(\boldsymbol{\theta})$. Let $\gamma := \inf\{\langle \boldsymbol{\theta}, \boldsymbol{\delta}\rangle | \, \boldsymbol{\theta} \in \mathcal{P}(G) \setminus \{\delta_0\} \text{ s.t. } \Gamma(\boldsymbol{\theta}) \geq 0\}$ be its designated typical normalized minimum distance which we are interested in computing. Notice that Γ is a map defined over the $(|G|-1)$-dimensional simplex $P(G)$ and therefore in general of difficult visualization whenever $|G| > 2$. It is then convenient and natural to introduce the average distance-spectrum as a one-dimensional projection of Γ:

(6.1)
$$\Upsilon : [0, \max\{\boldsymbol{\delta}(x) | \, x \in G\}] \to [-\infty, +\infty), \qquad \Upsilon(t) := \sup\left\{\Gamma(\boldsymbol{\theta}) \middle| \, \boldsymbol{\theta} \in \mathcal{P}(G) : \langle \boldsymbol{\delta}, \boldsymbol{\theta}\rangle = t\right\}.$$

It is immediate to verify that $\gamma = \inf\{t \in [0, \max\{\boldsymbol{\delta}(x) | \, x \in G\}] \, : \Upsilon(t) \geq 0\}$. Notice also that, for $|G| = 2$ and $|G| = 3$, all Bhattacharyya distances are proportional to the Hamming distance, so that the average distance spectrum Υ is independent (up to a rescaling factor) of the chosen G-symmetric channel. For $|G| \geq 4$ instead, Υ really depends on the choice of the Bhattacharyya distance $\mathbf{\Delta}$.

In Figure 6.1 the average distance-spectra of two regular LDPC $\mathbb{Z}_8$-code ensembles are reported. We considered the Bhattacharyya distance $\mathbf{\Delta}$ of the 8-PSK AWGN channel and normalized it in such a way that $\max\{\boldsymbol{\delta}(x) | \, x \in \mathbb{Z}_8\} = \mathbf{\Delta}(0, 4) = 1$. In each picture a degree pair (c, d) is fixed. The dash-dotted curve is the graph of the distance-spectrum $\Upsilon_{(\{1\},c,d)}(t)$ of the (c, d)-regular unlabelled LDPC ensemble, while the solid curve is the graph of the distance-spectrum $\Upsilon_{(\mathbb{Z}_8^*,c,d)}(t)$ of the (c, d)-regular uniformly labelled LDPC ensemble.

As a reference two dotted curves are also plotted in each picture. The one taking the value 0 for $t = 0$ is the distance spectrum of the binary (c, d)-regular LDPC ensemble $\Upsilon^2_{(c,d)}(t)$. It is straightforward to check that it is a lower bound for the distance spectrum of any $\mathbb{Z}_8$-LDPC ensemble: it suffices to restrict the optimization in (6.1) to $\mathbb{Z}_8$-types $\boldsymbol{\theta}$ supported on the binary subgroup $4\mathbb{Z}_8$.

The second dotted curve instead, taking value $\frac{1}{2}\log\frac{1}{2}$ for $t = 0$, corresponds to the distance-spectra of the $\mathbb{Z}_8$-code ensemble (with no sparsity constraints) of the same rate $R = \frac{1}{2}\log 8$. This ensemble is defined as a sequence of kernels of random homomorphisms $(\ker \Phi_N)$, each Φ_N being uniformly distributed over $\mathrm{Hom}(\mathbb{Z}_8^N, \mathbb{Z}_8^{N/2})$, the group of all homomorphisms from $\mathbb{Z}_8^N$ to $\mathbb{Z}_8^{N/2}$, with no sparsity constraint. $\mathbb{Z}_8$-code ensembles of codes are a natural generalization of the traditional linear-coding ensembles over finite fields [20, 2] and have been considered in [10] and [11] in order to characterize the capacity achievable by Abelian group codes over symmetric channels.

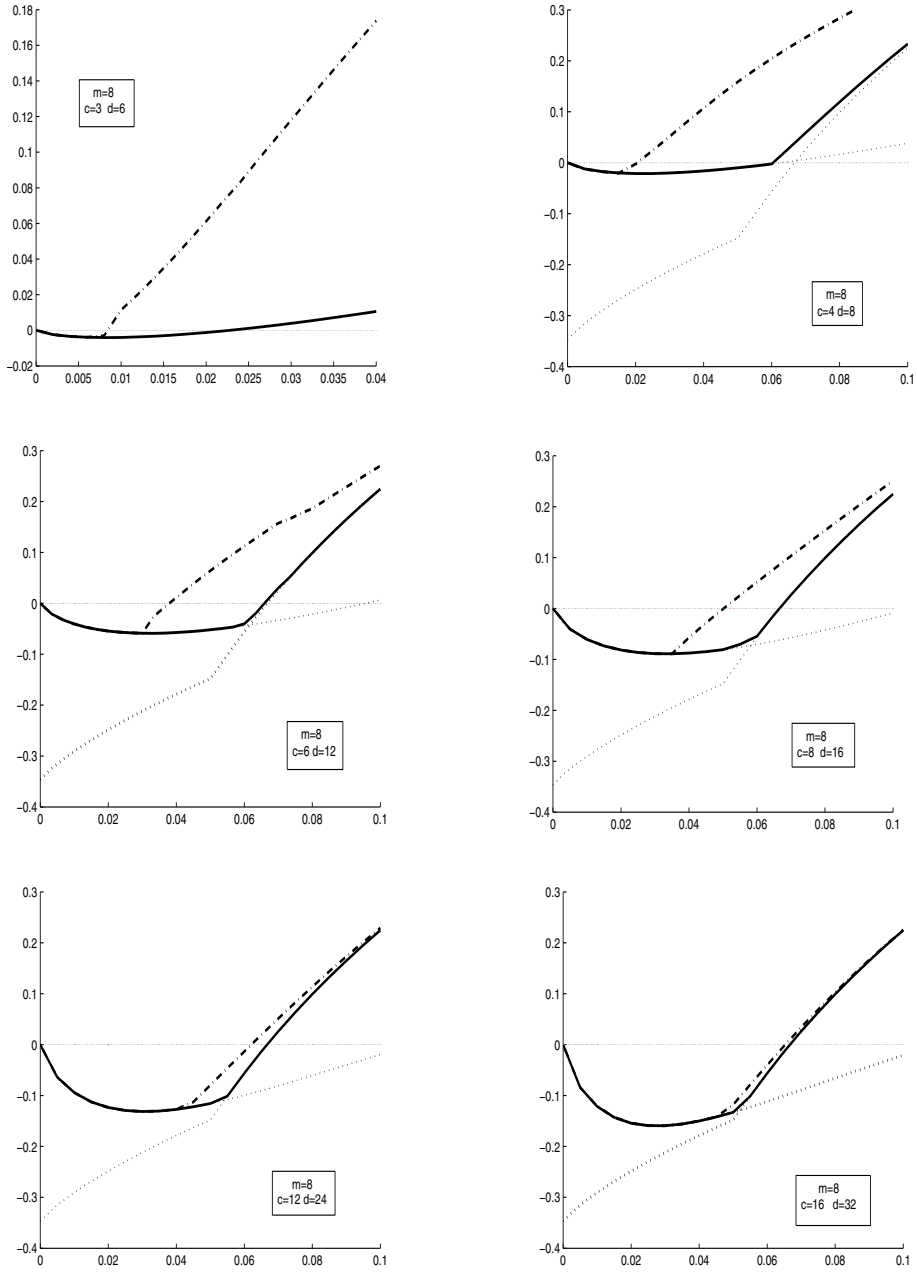

FIG. 6.1. *Bhattacharyya distance spectra of* (c, d)*-regular LDPC ensembles over* $\mathbb{Z}_8$ *for the* 8*-PSK AWGN channel: the solid curve corresponds to the uniformly labelled ensemble, the dash-dotted one corresponds to the unlabelled ensemble, and the two dotted curves correspond, respectively, to the* $\mathbb{Z}_8$*-linear ensemble and to the binary LDPC ensemble.*

In [12] their average type-spectra have been characterized; for the $\mathbb{Z}_8$-code ensemble of rate $\frac{1}{2}\log 8$ this is given by

$$\Gamma_{\mathbb{Z}_8}(\boldsymbol{\theta}) := \mathrm{H}(\boldsymbol{\theta}) - \frac{1}{2}\log l_8(\boldsymbol{\theta}), \qquad l_8(\boldsymbol{\theta}) := \frac{8}{\gcd\left(\mathrm{supp}\left(\boldsymbol{\theta}\right)\right)}.$$

Notice that $\Gamma_{\mathbb{Z}_8}(\boldsymbol{\theta})$ is an upper semicontinuous function over the simplex $\mathcal{P}(\mathbb{Z}_8)$, and its discontinuities correspond to types supported on the subgroups $2\mathbb{Z}_8$ and $4\mathbb{Z}_8$. In fact a salient point is easily recognizable in the graphs reported around the abscissa $t = 0.05$, corresponding to the intersection between the average spectrum of the binary subchannel and that of the $\mathbb{Z}_8$-subchannel. This salient point occurs before the curve crosses the t-axis, which is coherent with the fact, proved in [12], that the typical normalized minimum distance of the $\mathbb{Z}_8$-code ensemble equals the corresponding Gilbert–Varshamov bound. In other words, while for low values of t the distance spectrum of the $\mathbb{Z}_8$-code ensemble is dominated by the term corresponding to the smallest nontrivial subgroup (a phenomenon generally observable for Abelian group code ensembles), the value of the typical minimum distance is determined by types which are not supported in any proper subgroup of $\mathbb{Z}_8$ (this is instead related to the particular constellation chosen, although it is conjectured to be true for many constellations of interest).

Analogous considerations can be made about the LDPC distance-spectra based on the simulations reported. In particular, for distances close to 0, the average distance-spectra of both the unlabelled and the uniformly labelled $\mathbb{Z}_8$-LDPC ensembles are dominated by the binary-subgroup supported types. However, these components do affect the value of the typical normalized minimum distances ($\gamma_{(\{1\},c,d)}$ and $\gamma_{(\mathbb{Z}_8^*,c,d)}$, respectively) only for low values of the degrees ($c = 3, 4$). For all of the other values of the parameters, the typical minimum distance is instead determined by types which are not supported in any proper subgroup of $\mathbb{Z}_8$. Another observation which can be made is that, not surprisingly, as the values of the degrees (c, d) are increased while keeping their ratio constant, the distance-spectra of both the unlabelled and the uniformly labelled ensembles approach the one of the $\mathbb{Z}_8$-linear ensemble.

However, the most important conclusion which can be drawn from the graphics reported concerns the different behaviors of the unlabelled and the uniformly labelled ensembles. Indeed, it appears evident that the latter drastically outperforms the former at the distance level. In particular, already for relatively low values of the degrees ($c = 8$, $d = 16$) the uniformly labelled ensemble typical minimum distance $\gamma_{(\mathbb{Z}_8^*,c,d)}$ is very close (practically equal) to the Gilbert–Varshamov bound. For the same values of the degrees instead, the unlabelled ensemble suffers from a remarkable gap; this gap seems to be slowly filled up as the values of the degrees are increased, but it still remains significant for relatively high values of c and d. This indicates that structural properties of these two ensembles are remarkably different. Some prudence is nevertheless justified by the fact that ours are only lower bounds on the typical asymptotic normalized minimum distance, while, as already mentioned in the introduction, a concentration result for the type-spectra is needed in order to prove their tightness. However, while this phenomenon appears here only at the distance level, computer simulations of the performance of these codes reveal that a drastic superiority of the labelled ensemble with respect to the unlabelled one is evident also under belief-propagation decoding. We observe that this is coherent with Monte Carlo simulations reported in [4], where the labelled ensemble was shown to be closer to capacity than the unlabelled ensemble.

6.2. The average word error probability of the LDPC codes ensembles. In our analysis of the minimum distance properties of LDPC G-code ensembles, the quantities $\zeta_{(F,c)}$ show up as an almost sure lim inf for the unnormalized minimum distance only when $a(F,c) = -1$. However, these quantities characterize the asymptotic ML average performance of these ensembles for all values of $a(F,c)$.

For instance, let us consider in some detail the case $G \simeq \mathbb{Z}_{p^r}$ for some prime p and some positive integer r. Let us fix an admissible degree pair (c,d), and denote by $\overline{p_e(\mathcal{C}_N)}^{(F,c,d)}$ the average ML error probability of the (c,d)-regular F-labelled ensemble of LDPC $\mathbb{Z}_{p^r}$-codes over an arbitrary $\mathbb{Z}_{p^r}$-symmetric MC. Then it is possible to show that there exists a threshold $(1-\frac{c}{d})\log p^r < C_{(F,c,d)} < \log p^r$ such that, for every $\mathbb{Z}_{p^r}$-symmetric channel whose $\mathbb{Z}_{p^r}$-capacity (2.5) exceeds $C_{(F,c,d)}$, the average error probability $\overline{p_e(\mathcal{C}_N)}^{(F,c,d)}$ goes to zero in the limits of large N. Moreover, if one considers an increasing sequence of degree pairs (c_n,d_n) with a given designed rate $(1-\frac{c_n}{d_n})\log p^r$ converging to R, then the corresponding LDPC thresholds $C_{(c_n,d_n,F)}$ converge to R.

More precisely, it is possible to show that over any $\mathbb{Z}_{p^r}$-symmetric channel whose $\mathbb{Z}_{p^r}$-capacity exceeds $C_{(F,c,d)}$ we have

$$K_1 N^{a(F,c)} \leq \overline{p_e(\mathcal{C}_N)}^{(F,c,d)} \leq K_2 N^{a(F,c)} \tag{6.2}$$

for some positive constants K_1, K_2 both independent of N. Moreover, it can be proved that

$$\limsup_{N\in\mathcal{N}_{(c,d)}} \frac{\overline{p_e(\mathcal{C}_N)}^{(F,c,d)}}{N^{a(F,c)}} \leq K_3 \exp(\zeta_{(F,c)}) \tag{6.3}$$

for some positive constants K_3 independent of the channel (and thus from $\mathbf{\Delta}$). The results (6.2) are known in the binary case (see [29]); (6.2) was presented in [10] for the unlabelled LDPC ensemble. Proofs of (6.2), (6.3) in their full generality can be gathered coupling the estimations of section 4 with the standard bounding techniques used in [28, 39, 29, 4] and will be given elsewhere.

Observe that if $F \leq F' \leq \mathrm{Aut}(G)$, then

$$a(F,c) \leq a(F',c), \qquad \zeta_{(F,c)} \geq \zeta_{(F',c)}. \tag{6.4}$$

Thus, from the point of view of the average performance, the smaller the label group, the better the parameters. This stands in contrast with the numerical results presented in the previous paragraph, indicating that at the distance level the uniformly labelled ensembles perform much better than their unlabelled counterparts. An explanation for this seeming paradox can be obtained by invoking so-called expurgation arguments. Indeed, it can be proved that, while the average error probability of the LDPC ensembles is affected by a vanishingly small fraction of codes with low minimum distance and decays to zero only as a negative power of N, almost surely a sequence of codes sampled from the same ensemble has error probability decreasing to zero exponentially fast with N. It is this typical exponential behavior that has to be considered representative of the ensemble, rather than the one of the average error probability. It is also worth mentioning that the typical error exponent can be estimated in terms of the average type-spectra, using techniques presented in [39]. This phenomenon is well known in the LDPC code literature [19, 29]; proofs for LDPC codes over Galois fields can be found in [17, 4].

7. Conclusions. The following issues are left for future research:

- proving concentration results for the spectra of the LDPC ensembles for instance using a second-order method (see [33]);
- giving an analytical explanation of the different behavior of the labelled and unlabelled ensembles;
- generalizing the analysis to irregular ensembles following the approach of [15, 31];
- considering generalizations of the so-called stopping sets and pseudoweight distributions which in the binary case characterize the iterative decoding performance of LDPC codes (see [31, 43, 24]); while the distribution of stopping sets has been studied for binary LDPC ensembles, the distribution of pseudocodewords is unknown even in the binary case.

8. Appendix.

8.1. A semicontinuity lemma. Let E be a compact metric space. It is a standard fact that any lower semicontinuous function $f : E \to (-\infty, +\infty]$ achieves its minimum on every closed nonempty subset C of E, i.e.,

$$\exists\ \overline{x} \in C \text{ s.t. } f(\overline{x}) \leq f(x) \qquad \forall\ x \in C. \tag{8.1}$$

In the proof of Theorem 5.1 we used the following fact.

LEMMA 8.1. *Let $g, h : E \to (0, +\infty]$ both be lower semicontinuous. Then*

$$f : \mathbb{R} \to (-\infty, +\infty], \qquad f(y) := \inf\big\{g(x)\big|x \in E \text{ s.t. } h(x) \leq y\big\}$$

is nonincreasing and lower semicontinuous.

Proof. That f is nonincreasing immediately follows from its definition. In order to prove semicontinuity, assume we are given a sequence $(y_n) \subset (-\infty, +\infty]$ converging to some $y \in [-\infty, +\infty]$. We want to show that

$$\liminf_n f(y_n) \geq f(y). \tag{8.2}$$

Observe that with no loss of generality we can restrict ourselves to the case when $y_n \geq \min\{h(x) \,|\, x \in E\}$, since otherwise the set $\{x \in E \text{ s.t. } h(x) \leq y_n\}$ is empty and $f(y_n) = +\infty$. Since h is lower semicontinuous we have that the sets $\{x \in E \text{ s.t. } h(x) \leq y_n\}$ are closed in E. Therefore, since the function g is lower semicontinuous as well, from (8.1) we have that there exists x_n in E such that $f(y_n) = g(x_n)$ and $h(x_n) \leq y_n$. Since the space E is compact, from the sequence (x_n) we can extract a subsequence (x_{n_k}) converging to some $\overline{x}$ in E. From the lower semicontinuity of h we get

$$h(\overline{x}) \leq \liminf_k h\,(x_{n_k}) \leq \liminf_k y_{n_k} = y.$$

It immediately follows that $g(\overline{x}) \geq f(y)$. Finally, from the lower semicontinuity of g we get

$$\liminf_n f(y_n) = \liminf_k g\,(x_{n_k}) \geq g(\overline{x}),$$

which, together with the previous inequality, implies (8.2). ∎

8.2. Proofs for section 4.4. Recall that the interconnection group for the F-labelled ensemble is $S_{Nc} \ltimes F^{Nc}$. We will write the random variable $\Pi_N = (\Pi'_N, \Lambda)$, where Π'_N is uniformly distributed over S_{Nc} and Λ is uniformly distributed over F^{Nc}. For all $s = 1, \ldots, N$, and $k \in G$, let e_s^k in G^N be the vector whose components are all zero but for the sth, which is equal to k.

8.2.1. Proof of Proposition 4.7. Let k in $G \setminus \{0\}$ be such that $a(F,c) = 1 - c + b(Fk,c)$, and define the event $E_s^N := \{e_s^k \in \ker \Phi_N\}$. We have $W_N(\boldsymbol{\tau}_k) = \sum_{s=1}^N \mathbb{1}_{\ker \Phi_N}(e_s^k) = \sum_{s=1}^N \mathbb{1}_{E_s^N}$.

For $1 \leq t \leq L$, define the random variable $N_t := |\Pi'_N(I_s^c) \cap I_t^d|$. Define the event

$$\tilde{E}_s^N := \bigcap_{1 \leq t \leq L} \{N_t = 0\} \cup \{N_t > 0 \text{ and } \exists \text{ closed walk of length } N_t \text{ in } \mathcal{G}(G, Fk)\}.$$

It is not hard to check that $\tilde{E}_s^N \supseteq E_s^N$. Moreover, $\mathbb{P}(E_s^N | \tilde{E}_s^N) \geq |F|^{-c}$, since, given $\tilde{E}_s^N$, there exists at least one realization of the c entries $\Lambda_{(s-1)c+1}, \ldots, \Lambda_{sc}$ in F such that $\Phi_N e_s^k = \mathbf{0}$.

Observe that $\Pi_N(I_s^c)$ is uniformly distributed over the class of all subsets of $\{1, \ldots, Nc\}$ of cardinality c and that there exist at least $\binom{L}{b(Fk,c)}$ possible realizations of $\Pi_N(I_s^c)$ such that, for all $1 \leq t \leq L$, N_t is either 0 or equals the length of a closed walk in $\mathcal{G}(G, Fk)$. It follows that

$$\mathbb{P}(E_s^N) \geq \frac{1}{|F|^c} \mathbb{P}\left(\tilde{E}_s^N\right) \geq \frac{1}{|F|^c} \binom{Nc}{c}^{-1} \binom{L}{b(Fk,c)} \geq K' N^{b(Fk,c)-c} \tag{8.3}$$

for some $K' > 0$ independent of N.

We now estimate the probability of the intersections $E_s^N \cap E_r^N$ for $1 \leq r \neq s \leq N$. We have that, given that E_r^N occurred, $\Pi'_N(I_s^c)$ is uniformly distributed over the class of subsets of of cardinality c of $\{1, \ldots, Nc\} \setminus \Pi'_N(I_r^c)$. It follows that

(8.4)

$$\mathbb{P}(E_s^N | E_r^N) \leq \mathbb{P}(\tilde{E}_s^N | E_r^N) \leq \binom{(N-1)c}{c}^{-1} \binom{L}{b(Fk,c)} \binom{b(Fk,c)d}{c} \leq K'' N^{b(Fk,c)-c}$$

for some $K'' > 0$ independent of N. By applying a union-intersection bound, and using (8.3) and (8.4), we get

$$\begin{aligned} \mathbb{P}\left(W_N(\boldsymbol{\tau}_k) \geq 1\right) &\geq \sum_s \mathbb{P}\left(E_s^N\right) - \sum_{r \neq s} \mathbb{P}\left(E_s^N \cap E_r^N\right) \\ &\geq K' N^{a(F,c)} - K'' N^{2a(F,c)} \geq K N^{a(Fk,c)}, \end{aligned}$$

the last equality holding true for some constant $K > 0$ and N large enough, since $a(F,c) < 0$. ∎

8.2.2. Proof of Proposition 4.8. For $1 \leq s \neq r \leq N$ and $1 \leq t \leq L$, define the event

$$E_{r,s}^N := \bigcap_{t=1}^L \left\{ \left|\Pi_N(I_r^c) \cap I_t^d\right| = \left|\Pi_N(I_s^c) \cap I_t^d\right| \right\}.$$

In the unlabelled (c,d)-regular ensemble $E_{r,s}^N$ is sufficient for the N-tuple $e_r^k - e_s^k$ (whose G-type is $\hat{\boldsymbol{\tau}}_k$) to be in $\ker \Phi_N$. Indeed, in this case each check ends up summing an equal amount of entries equal to k and $-k$. For the F-labelled ensemble it is easy to see that $\mathbb{P}\left(e_r^k - e_s^k \in \ker \Phi_N \middle| E_{r,s}^N\right) \geq |F|^{-2c}$, since, given that $E_{r,s}^N$ occurred, for $\Phi_N(e_r^k - e_s^k)$ to be $\mathbf{0}$ it is sufficient that the $2c$ corresponding labels equal the identity automorphism. Thus,

$$\mathbb{P}\left(W_N\left(\hat{\boldsymbol{\tau}}_k\right) \geq 1\right) \geq \mathbb{P}\left(\sum_{s>r} \mathbb{1}_{\ker \Phi_N}(e_r^k - e_s^k) \geq 1\right) \geq |F|^{-2c} \mathbb{P}\left(\bigcup_{s>r}^N E_{r,s}^N\right).$$

Now we introduce the events $F_r^N := \bigcup_{t=1}^L \left\{ \left|\Pi_N(I_r^c) \cap I_t^d\right| > \frac{d}{2} \right\}$. We have

$$\mathbb{P}\left(F_r^N\right) \leq L \sum_{a=\lfloor d/2 \rfloor + 1}^{c} \binom{c}{a}\binom{d}{a}\binom{dL}{a}^{-1} \leq AN^{-\lfloor d/2 \rfloor}$$

for some positive A independent of N and r. Clearly, we have that F_r^N implies $\overline{E_{r,s}^N}$, so that $\mathbb{P}\left(E_{r,s}^N \middle| F_r^N\right) = 0$. Instead, we have $\mathbb{P}(E_{r,s}^N | \overline{F_r^N}) \geq \binom{(N-1)c}{c}^{-1} \geq (cN)^{-c}$. Thus, there exist some positive N_0 and K' such that, for every $N \geq N_0$,

$$\mathbb{P}\left(E_{r,s}^N\right) \geq \mathbb{P}\left(E_{r,s}^N \middle| \overline{F_r^N}\right)\mathbb{P}\left(\overline{F_r^N}\right) \geq (cN)^{-c}\left(1 - AN^{-\lfloor d/2 \rfloor}\right) \geq K'N^{-c}.$$

For every unordered triple $\{q,r,s\} \subseteq \{1,\dots,N\}$ we consider the event

$$E_{q,r,s}^N := \bigcap_{t=1}^L \left\{ \left|\Pi_N(I_q^c) \cap I_t^d\right| = \left|\Pi_N(I_r^c) \cap I_t^d\right| = \left|\Pi_N(I_s^c) \cap I_t^d\right| \right\}.$$

We have that

$$\mathbb{P}\left(E_{q,r,s}^N\right) \leq (d-1)^c c! \binom{(N-1)c}{c}^{-1} (d-2)^c c! \binom{(N-2)c}{c}^{-1} \leq K''N^{-2c}$$

for some positive K'' independent of N. For every unordered 4-tuple $\{p,q,r,s\}$ define

$$E_{p,q,r,s}^N := \bigcap_{t=1}^L \left\{ \left|\Pi_N(I_p^c) \cap I_t^d\right| = \left|\Pi_N(I_q^c) \cap I_t^d\right| = \left|\Pi_N(I_r^c) \cap I_t^d\right| = \left|\Pi_N(I_s^c) \cap I_t^d\right| \right\}.$$

We have that

$$\mathbb{P}\left(E_{p,q,r,s}^N\right) \leq (d-1)^c c! \binom{(N-1)c}{c}^{-1} (d-2)^c c! \binom{(N-2)c}{c}^{-1} (d-3)^c c! \binom{(N-3)c}{c}^{-1} \leq K'''N^{-3c}$$

for some positive K'' independent of N. It follows that

$$\begin{aligned}
\mathbb{P}\left(W_N\left(\hat{\boldsymbol{\tau}}_k\right) \geq 1\right) &\geq |F|^{-2c}\mathbb{P}\left(\bigcup_{s>r} E_{r,s}^N\right) \\
&\geq \sum_{r<s}\mathbb{P}\left(E_{r,s}^N\right) - \sum_{q<r<s}\mathbb{P}\left(E_{q,r,s}^N\right) - \sum_{p<q<r<s}\mathbb{P}\left(E_{p,q,r,s}^N\right) \\
&\geq \tbinom{N}{2}K'N^{-c} - \tbinom{N}{3}K''N^{-2c} - \tbinom{N}{4}K'''N^{-3c} \\
&\geq KN^{2-c}
\end{aligned}$$

for some positive K independent of N and $N \in \mathcal{N}_{(c,d)}$ large enough. ∎

8.3. Proof of Theorem 5.2. In order to show the first part of the claim, one follows the steps of the proof of Theorem 5.1 until obtaining (5.3) and (5.4). Then (5.3) implies that $\lim_N \mathbb{P}\left(\kappa_N'' < \gamma_{(F,c,d)}\right) = 0$, while from (5.4), since $a(F,c) \leq -1$, one gets $\lim_N \mathbb{P}\left(\kappa_N' < \gamma_{(F,c,d)}\right) \leq KN^{a(F,c)} = 0$.

For the second part of the claim, we first show that

$$\mathbb{P}\left(\liminf_N \mathrm{d}_{\min}\left(\ker \Phi_N\right) \leq \zeta_{(F,c)}\right) = 1. \tag{8.5}$$

Indeed, let us first consider the case $a(F,c) = -1 > 2 - c$. From Proposition 4.7 it follows that, for every $k \in G \setminus \{0\}$ such that $b(Fk,c) = a(F,c) - 1 + c = c - 2$,

$$\sum_{N \in \mathcal{N}_{(c,d)}} \mathbb{P}(W_N(\boldsymbol{\tau}_k) \geq 1) \geq \sum_{N \in \mathcal{N}_{(c,d)}} KN^{a(F,c)} = K \sum_{N \in \mathcal{N}_{(c,d)}} N^{-1} = +\infty.$$

We now recall that by assumption (Π_N) is a sequence of independent random variables, so that the events $\{W_N(\hat{\boldsymbol{\tau}}_k) \geq 1\}$, for N in $\mathcal{N}_{(c,d)}$, are independent. We can thus apply the converse part of the Borel–Cantelli lemma [7] to conclude that with probability one the event $\{W_N(\hat{\boldsymbol{\tau}}_k) \geq 1\}$ occurs for infinitely many $N \in \mathcal{N}_{(c,d)}$. It follows that, for all $K \in G \setminus \{0\}$ such that $b(Fk,c) = c - 2$,

$$\mathbb{P}\big(\liminf_N \mathrm{d}_{\min}(\ker \Phi_N) \leq \boldsymbol{\delta}(k)\big) \geq \mathbb{P}\big(\{W_N(\hat{\boldsymbol{\tau}}_k) \geq 1\} \text{ i. o. } N \in \mathcal{N}_{(c,d)}\big) = 1, \tag{8.6}$$

so that (8.5) follows. The case when $c = 3$ can be treated similarly using Propositions 4.7 and 4.8 and the converse part of the Borel–Cantelli lemma.

It remains to prove that $\liminf_N \mathrm{d}_{\min}(\ker \Phi_N) \geq \zeta_{(F,c)}$ with probability one. First, consider the case $c = 3$. For every k such that $b(Fk,c) = 0$ we have $W_N(\boldsymbol{\tau}_k) = 0$ for every realization of Π_N in the interconnection group $S_{Nc} \ltimes F^{Nc}$. It follows that deterministically

$$\mathrm{d}_{\min}(\ker \Phi_N) \geq \min\big\{(2 - \mathbb{1}_{\{1\}}(b(Fk,c)))\boldsymbol{\delta}(k) \big| k \in G \setminus \{0\}\big\} = \zeta_{(F,c)}.$$

When $c \geq 4$, for every k in $G \setminus \{0\}$ such that $b(Fk,c) < 2 - c$, Lemma 4.5 and the Borel–Cantelli lemma imply that with probability one $\{W_N(\boldsymbol{\tau}_k) = 0\}$ occurs only finitely often. Then using an argument similar to that in the proof of Proposition 4.4 it is possible to show that $\sum_{\frac{1}{N} < ||\boldsymbol{\theta} - \delta_0|| < \frac{2}{d}} \overline{W_N(\boldsymbol{\theta})} \leq KN^{-2}$, and then $\sum_{\frac{1}{N} < ||\boldsymbol{\theta} - \delta_0|| < \frac{2}{d}} W_N(\boldsymbol{\theta}) = 0$ for all but a finitely many N. This implies (8.5). ∎

Acknowledgments. Part of the work was done while the first author was visiting Yale University. We thank the Electrical Engineering Department and Professor Sekhar Tatikonda for their hospitality.

REFERENCES

[1] M. A. Armand, *Decoding LDPC codes over integer residue rings*, IEEE Trans. Inform. Theory, 52 (2006), pp. 4680–4686.

[2] A. Barg and G. D. Forney, Jr., *Random codes: Minimum distances and error exponents*, IEEE Trans. Inform. Theory, 48 (2002), pp. 2568–2573.

[3] S. Benedetto, R. Garello, M. Mondin, and G. Montorsi, *Geometrically uniform TCM codes over groups based on $L \times$ MPSK constellations*, IEEE Trans. Inform. Theory, 40 (1994), pp. 137–152.

[4] A. Bennatan and D. Burshtein, *On the application of LDPC codes to arbitrary discrete memoryless channels*, IEEE Trans. Inform. Theory, 50 (2004), pp. 417–438.

[5] A. Bennatan and D. Burshtein, *Design and analysis of nonbinary LDPC codes for arbitrary discrete memoryless channels*, IEEE Trans. Inform. Theory, 52 (2006), pp. 549–583.

[6] R. Blahut, *Composition bounds for channel block codes*, IEEE Trans. Inform. Theory, 23 (1977), pp. 656–674.

[7] V. S. Borkar, *Probability Theory: An Advanced Course*, Springer, New York, 1995.

[8] J. J. Boutros, A. Ghaith, and Y.-W. Yi, *Non-binary adaptive LDPC codes for frequency selective channels: Code construction and iterative decoding*, in Proceedings of the IEEE Information Theory Workshop, Chengdu, China, 2006, pp. 184–188.

[9] D. Burshetein and U. Miller, *Asymptotic enumeration methods for analyzing LDPC codes*, IEEE Trans. Inform. Theory, 50 (2004), pp. 1115–1131.

[10] G. Como and F. Fagnani, *Ensembles of codes over Abelian groups*, in Proceedings of the IEEE International Symposium on Information Theory, Adelaide, Australia, 2005, pp. 1788–1792.

[11] G. Como and F. Fagnani, *The capacity of finite Abelian group codes over memoryless symmetric channels*, IEEE Trans. Inform. Theory, submitted.
[12] G. Como and F. Fagnani, *On the Gilbert-Varshamov distance of Abelian group codes*, in Proceedings of the IEEE International Symposium on Information Theory, Nice, France, 2007, pp. 2651–2655.
[13] M. C. Davey and D. J. C. MacKay, *Low density parity check codes over GF(q)*, IEEE Comm. Lett., 2 (1998), pp. 159–166.
[14] A. Dembo and A. Montanari, *Finite size scaling for the core of large random hypergraphs*, Ann. Appl. Probab., to appear.
[15] C. Di, T. J. Richardson, and R. Urbanke, *Weight distribution of low-density parity-check codes*, IEEE Trans. Inform. Theory, 52 (2006), pp. 4839–4855.
[16] R. L. Dobrushin, *Asymptotic optimality of group and systematic codes for some channels*, Theor. Probab. Appl., 8 (1963), pp. 47–59.
[17] U. Erez and G. Miller, *The ML decoding performance of LDPC ensembles over $\mathbb{Z}_q$*, IEEE Trans. Inform. Theory, 51 (2005), pp. 1871–1879.
[18] G. D. Forney, Jr., *Geometrically uniform codes*, IEEE Trans. Inform. Theory, 37 (1991), pp. 1241–1260.
[19] R. G. Gallager, *Low Density Parity Check Codes*, MIT Press, Cambridge MA, 1963.
[20] R. G. Gallager, *Information Theory and Reliable Communication*, Wiley, New York, 1968.
[21] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 5th ed., Oxford University Press, New York, 1979.
[22] J. Hou, P. H. Siegel, L. B. Milstein, and H. D. Pfister, *Capacity-approaching bandwidth-efficient coded modulation schemes based on low-density parity-check codes*, IEEE Trans. Inform. Theory, 49 (2003), pp. 2141–2155.
[23] T. W. Hungerford, *Algebra*, Springer-Verlag, New York, 1974.
[24] R. Koetter, W.-C. W. Li, P. O. Vontobel, and J. L. Walker, *Characterizations of pseudo-codewords of (low-density) parity-check codes*, Adv. Math., 213 (2007), pp. 205–229.
[25] S.-L. Litsyn and V. Shevelev, *On ensembles of low-density parity-check codes: Asymptotic distance distributions*, IEEE Trans. Inform. Theory, 48 (2002), pp. 887–908.
[26] S.-L. Litsyn and V. Shevelev, *Distance distributions in ensembles of irregular low-density parity-check codes*, IEEE Trans. Inform. Theory, 49 (2003), pp. 3140–3159.
[27] H.-A. Loeliger, *Signal sets matched to groups*, IEEE Trans. Inform. Theory, 37 (1991), pp. 1675–1679.
[28] D. J. C. MacKay, *Good error correcting codes based on very sparse matrices*, IEEE Trans. Inform. Theory, 45 (1999), pp. 399–431.
[29] G. Miller and D. Burshetein, *Bounds on the maximum likelihood decoding error probability of low-density parity-check codes*, IEEE Trans. Inform. Theory, 47 (2001), pp. 2696–2710.
[30] K. S. Ng and M. A. Armand, *LDPC codes over mixed alphabets*, Electron. Lett., 42 (2006), pp. 1290–1291.
[31] A. Orlitsky, K. Viswanathan, and J. Zhang, *Stopping set distribution of LDPC code ensembles*, IEEE Trans. Inform. Theory, 51 (2005), pp. 929–953.
[32] V. Rathi and R. Urbanke, *Density evolution, thresholds and the stability condition for non-binary LDPC codes*, IEE Proc. Commun., 152 (2005), pp. 1069–1074.
[33] V. Rathi, *On the asymptotic weight and stopping set distribution of regular LDPC ensembles*, IEEE Trans. Inform. Theory, 52 (2006), pp. 4212–4218.
[34] T. J. Richardson and R. Urbanke, *The capacity of low-density parity-check codes under message-passing decoding*, IEEE Trans. Inform. Theory, 47 (2001), pp. 599–618.
[35] T. J. Richardson, M. A. Shokrollahi, and R. Urbanke, *Design of capacity-approaching irregular low-density parity-check codes*, IEEE Trans. Inform. Theory, 47 (2001), pp. 619–637.
[36] T. J. Richardson and R. Urbanke, *Modern Coding Theory*, Cambridge University Press, Cambridge, UK, 2007.
[37] I. Sason and R. Urbanke, *Parity-check density versus performance of binary linear block codes over memoryless symmetric channels*, IEEE Trans. Inform. Theory, 49 (2003), pp. 1611–1635.
[38] L. Sassatelli and D. Declercq, *Non-binary hybrid LDPC codes: Structure, decoding and optimization*, in Proceedings of the IEEE Information Theory Workshop, Chengdu, China, 2006, pp. 71–75.
[39] N. Shulman and M. Feder, *Random coding techniques for nonrandom codes*, IEEE Trans. Inform. Theory, 45 (1999), pp. 2001–2004.
[40] D. Sridhara and T. E. Fuja, *LDPC codes over rings for PSK modulation*, IEEE Trans. Inform. Theory, 51 (2005), pp. 3209–3220.

[41] A. Terras, *Fourier Analysis on Finite Groups and Applications*, Cambridge University Press, Cambridge, UK, 1999.
[42] Various Authors, *Special issue on iterative decoding*, IEEE Trans. Inform. Theory, 47 (2001).
[43] P. O. Vontobel and R. Koetter, *Graph-cover decoding and finite-length analysis of message-passing iterative decoding of LDPC codes*, IEEE Trans. Inform. Theory, to appear.
[44] C. C. Wang, S. R. Kulkarni, and H. V. Poor, *Finite-dimensional bounds on $\mathbb{Z}_m$ and binary LDPC codes with belief propagation decoders*, IEEE Trans. Inform. Theory, 53 (2007), pp. 56–81.