Low density parity check codes over groups and rings

Deepak Sridhara and Thomas E. Fuja[1]
Department of Electrical Engineering
University of Notre Dame.
email: {dsridhar, tfuja}@nd.edu

Abstract — **The role of low density parity check principles in the design of group codes for coded modulation is examined. In this context, the structure of linear codes over certain rings $\mathbb{Z}_m$ and $\mathbb{G}_m$ is discussed, and LDPC codes over these ring structures are designed.**

I. Introduction

The re-discovery of low density parity check (LDPC) codes with near-capacity performance over binary channels has generated considerable activity in the coding community. The application of LDPC principles to bandwidth-efficient modulation has focused primarily on the use of binary codes within the context of multi-level codes and bit-interleaved coded modulation [1, 2]. This paper takes a completely different approach – the design of LDPC codes over groups and matching signal sets.

A signal set S is said to be *matched* to a group G if there exists a mapping μ from G onto S such that, for all $a, b \in G$, the following property holds:

$$d_E(\mu(a), \mu(b)) = d_E(\mu(b^{-1} \cdot a), \mu(e)) \qquad (1)$$

where $d_E(x, y)$ is the Euclidean distance between x and y, e is the identity element of the group G, and '$\cdot$' is the group operation [3]. This paper examines the performance of LDPC codes constructed over groups G and modulated over matching signal sets S. Of particular interest are codes over the additive groups in $\mathbb{Z}_8$ and $\mathbb{Z}_8 \oplus \mathbb{Z}_8$ modulated using the 8-PSK constellation as well as a three dimensional 8-point signal set S_o (Figure 1).

II. Signal sets matched to groups

Let $\mathbb{Z}_m$ denote the set of integers $\{0, 1, \ldots, m-1\}$. Then $\mathbb{Z}_m$ is a commutative group under addition modulo m, and there exists a matched mapping μ from $\mathbb{Z}_m$ to the m-ary PSK constellation:

$$\mu(k) = exp(j2\pi k/m) \qquad k \in \mathbb{Z}_m, \qquad (2)$$

where the m-PSK signal points are represented as complex numbers on the unit-circle. For even m, the group $\mathbb{Z}_m$ is also matched to the three dimensional constellation S_0 shown in Figure 1. This constellation is made up of two $(m/2)$-PSK constellations rotated by $2\pi/m$ radians relative to each other. The labeling in the figure indicates the matched mapping from $\mathbb{Z}_m$ to S_0.

[1]This work was supported by NSF Grant CCR 99-96222

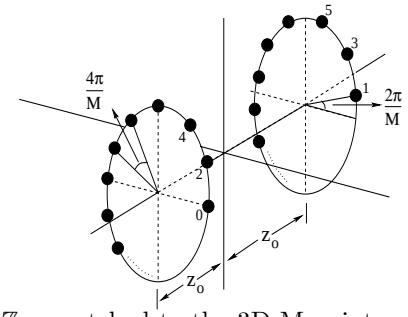

Figure 1: $\mathbb{Z}_M$ matched to the 3D M-point constellation.

Since $\mathbb{Z}_m$ has a natural ring structure, a linear block code of length n over $\mathbb{Z}_m$ can be seen as a $\mathbb{Z}$-submodule of $(\mathbb{Z}_m)^n$, and is a subgroup of $(\mathbb{Z}_m)^n$. The signal space code obtained after mapping is *geometrically uniform* in the sense of [4].

These mappings can be extended component-wise to the group of two-tuples (i.e., the direct sum group) $\mathbb{Z}_m \oplus \mathbb{Z}_m$. The group $\mathbb{Z}_m \oplus \mathbb{Z}_m$ is matched to the $2 \times m$-PSK and the $2 \times S_0$ constellations. Let $\mathbb{Z}_m R$ and $\mathbb{Z}_m I$ denote two rings, each with elements from $\mathbb{Z}_m \oplus \mathbb{Z}_m$. For the ring $\mathbb{Z}_m R$ we define addition and multiplication as simple component-wise application of the operation, while for $\mathbb{Z}_m I$ we define addition component-wise but multiplication is carried out[2] using complex arithmetic – i.e., $(a, b) \times (c, d) = (ac - bd, ad + bc)$. A linear block code of length n over the ring $\mathbb{Z}_m R$ [resp. $\mathbb{Z}_m I$] is a $\mathbb{Z}_m R$ [resp. $\mathbb{Z}_m I$] submodule of $(\mathbb{Z}_m \oplus \mathbb{Z}_m)^n$, and is a subgroup of $(\mathbb{Z}_m \oplus \mathbb{Z}_m)^n$.

III. Structure of linear codes over rings

Let:

- $\mathbb{Z}_m$ be the ring of integers modulo m. (More precisely, $\mathbb{Z}_m$ is the quotient ring $\mathbb{Z}/m\mathbb{Z}$.)
- $\mathbb{G}_m$ be the quotient ring $\mathbb{G}/(m + j0)\mathbb{G}$, where $\mathbb{G} = \{a + jb \mid a, b \in \mathbb{Z}\}$ is the ring of Gaussian integers[3].

The following theorem from [5] describes the structure of a linear code over $\mathbb{Z}_m$:

Theorem III.1 *Let $C \subset (\mathbb{Z}_m)^n$. Then the following statements are equivalent:*

1. C is a subgroup of $(\mathbb{Z}_m)^n$.

[2]All operations are defined modulo m.

[3]$\mathbb{G}_m$ is isomorphic to $\mathbb{Z}_m I$; hence, the two are used interchangeably.

2. *There exists an integer r $(0 \leq r \leq n)$, a set of linearly independent vectors $\{\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_r\} \subset (\mathbb{Z}_m)^n$, and a set of nested ideals of $\mathbb{Z}_m$ (not necessarily distinct)*

$$\mathbb{Z}_m \ > \ a_1\mathbb{Z}_m \ > \ a_2\mathbb{Z}_m \ > \ \ldots \ > \ a_r\mathbb{Z}_m \ > \ \{0\}$$

such that C can be written as the direct sum

$$C = \bigoplus_{i=1}^{r} a_i \mathbb{Z}_m \mathbf{x}_i$$

Moreover, the ideals and r are uniquely determined by C and m.

3. *There exists a unique lattice Λ, $m\mathbb{Z}^n < \Lambda < \mathbb{Z}^n$, such that $C \simeq \Lambda/m\mathbb{Z}^n$. Given any set $[\Lambda/m\mathbb{Z}^n]$ of coset representatives, C can be written as $C = [\Lambda/m\mathbb{Z}^n] mod\ m$.*

A consequence of this theorem is the following corollary for a linear block code over the ring $\mathbb{G}_m$:

Corollary III.2 *Let $C \subset (\mathbb{G}_m)^n$. Then the following statements are equivalent:*

1. *C is a $\mathbb{G}$-submodule of $(\mathbb{G}_m)^n$.*
2. *There exists an integer r $(0 \leq r \leq n)$, a set of linearly independent vectors $\{\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_r\} \subset (\mathbb{G}_m)^n$, and a set of nested ideals of $\mathbb{G}_m$ (not necessarily distinct)*

$$\mathbb{G}_m \ > \ a_1\mathbb{G}_m \ > \ a_2\mathbb{G}_m \ > \ \ldots \ > \ a_r\mathbb{G}_m \ > \ \{0\}$$

such that C can be written as the direct sum

$$C = \bigoplus_{i=1}^{r} a_i \mathbb{G}_m \mathbf{x}_i$$

The ideals and r are uniquely determined by C and m. Here, $a_i \in \mathbb{G}$.

3. *There exists a unique complex lattice Λ, $m\mathbb{G}^n < \Lambda < \mathbb{G}^n$, such that $C \simeq \Lambda/m\mathbb{G}^n$. Given any set $[\Lambda/m\mathbb{G}^n]$ of coset representatives, C can be written as $C = [\Lambda/m\mathbb{G}^n]$ mod $(m + j0)$. (Here, $m\mathbb{G}^n = (m + j0)\mathbb{G}^n$.)*

The above corollary requires that C be not only closed under addition, but also that C form a $\mathbb{G}$-module, i.e., $jC \subseteq C$. The proof of the theorem uses the fact that $\mathbb{Z}$ is a principal ideal domain. Since $\mathbb{G}$ is a Euclidean domain (and hence, a principal ideal domain), the proof of the corollary follows quite naturally.

Theorem III.1 and its corollary lead to the following results:

• A non-trivial linear code C of block length n over a ring of the type $\mathbb{Z}_{p^a}$, for p a prime and a a positive integer, can be represented by a generator matrix of the form:

$$G = \begin{bmatrix} I_{k_0} & A_{01} & A_{02} & \ldots & A_{0,a-1} & A_{0a} \\ 0 & pI_{k_1} & pA_{12} & \ldots & pA_{1,a-1} & pA_{1a} \\ 0 & 0 & p^2 I_{k_2} & \ldots & p^2 A_{2,a-1} & p^2 A_{2a} \\ . & . & . & \ldots & . & . \\ 0 & 0 & 0 & \ldots & p^{a-1} I_{k_{a-1}} & p^{a-1} A_{a-1,a} \end{bmatrix}$$

where the columns are grouped into blocks of sizes k_0, k_1, ..., k_{a-1}, k_a, the k_i are non-negative integers summing to n, and I_{k_i} is the $k_i \times k_i$ identity matrix [6]. The code C then consists of codewords

$$[v_0\ v_1\ v_2\ \ldots\ v_{a-1}]G,$$

where each v_i is a vector of length k_i with components from $\mathbb{Z}_{p^{a-i}}$, so that C contains p^k codewords, where $k = \sum_{i=0}^{a-1}(a-i)k_i$. The code C with generator matrix G is said to have a dual code $C^\perp$ whose generator matrix is of the form:

$$G^\perp = \begin{bmatrix} B_{0a} & B_{0,a-1} & . & B_{02} & B_{01} & I_{k_a} \\ pB_{1a} & pB_{1,a-1} & . & pB_{12} & pI_{k_{a-1}} & 0 \\ p^2 B_{2a} & p^2 B_{2,a-1} & . & p^2 I_{k_{a-2}} & 0 & 0 \\ . & . & . & . & . & . \\ p^{a-1} B_{a-1,a} & p^{a-1} I_{k_1} & . & 0 & 0 & 0 \end{bmatrix}$$

The dual code $C^\perp$ is defined to be the set $C^\perp = \{\mathbf{x} \in (\mathbb{Z}_{p^a})^n \mid \mathbf{x} \cdot \mathbf{y} = 0,\ \forall \mathbf{y} \in C\}$, where the dot product $\mathbf{x} \cdot \mathbf{y} = x_1 y_1 + \ldots + x_n y_n$.(Addition and multiplication are as defined for the ring $\mathbb{Z}_{p^a}$.)

• A non-trivial linear code C of block length n over rings of the type $\mathbb{G}_{p^a}$ can be represented by a generator matrix of the form:

$$G = \begin{bmatrix} I_{k_0} & A_{01} & A_{02} & \ldots & A_{0,a-1} & A_{0a} \\ 0 & b_1 I_{k_1} & b_1 A_{12} & \ldots & b_1 A_{1,a-1} & b_1 A_{1a} \\ 0 & 0 & b_2 I_{k_2} & \ldots & b_2 A_{2,a-1} & b_2 A_{2a} \\ 0 & 0 & 0 & \ldots & b_3 A_{3,a-1} & b_3 A_{3a} \\ . & . & . & \ldots & . & . \\ 0 & 0 & 0 & \ldots & b_{a-1} I_{k_{a-1}} & b_{a-1} A_{a-1,a} \end{bmatrix}$$

where the columns are grouped into blocks of sizes k_0, k_1, ..., k_{a-1}, k_a, the k_i are non-negative integers adding to n, and the b_i are non-units in $\mathbb{G}_{p^a}$ with the property that $b_i | b_{i+1}$ for $i = 1, 2, \ldots, a-2$ and $b_{a-1} | p^a$. The code C then consists of codewords

$$[v_0\ v_1\ v_2\ \ldots\ v_{a-1}]G,$$

where each v_i is a vector of length k_i with components from $\mathbb{G}_{p^a/b_i}$. The dual of C is defined in an analogous manner. The cardinality of C is determined easily from the b_i's and the k_i's. For instance, in the case of $p = 2$, we have $b_1 = 1 + j$, $b_2 = 2$, $b_3 = 2 + 2j$, $b_4 = 4$, ...

IV. Group LDPC codes

Codes over $\mathbb{Z}_8$: A group LDPC code over $\mathbb{Z}_8$ is designed by constructing an LDPC matrix H with non-zero elements chosen from $\mathbb{Z}_8$. The matrix H can be transformed to the form of $G^\perp$ above by elementary row and column operations. A generator matrix G for the group code is then obtained from $G^\perp$. A *uniform* Euclidean-space code is obtained by mapping the code elements onto the 8-PSK signal set using (2).

Following the approach used for LDPC codes over non-binary *fields* in [7], the iterative message passing decoder for the LDPC code is modified to decode a code over $\mathbb{Z}_8$. The non-zero entries of H are chosen from the non-zero-divisors in $\mathbb{Z}_8$. The performance of group LDPC codes of block lengths 991, 1991, and 2991 (8-PSK) symbols, constructed thus, is shown in Figure 2. The figure also shows the performance of bit-interleaved coded modulation schemes that use binary LDPC codes with Gray mapping. All the curves shown correspond to regular $(3, 9)$

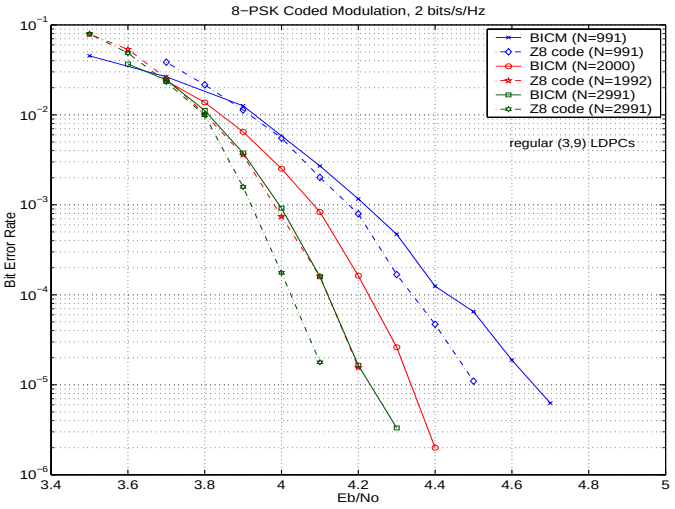

Figure 2: Group based vs bit-interleaved LDPC with 8-PSK modulation. (rate = 2 bits/symbol)

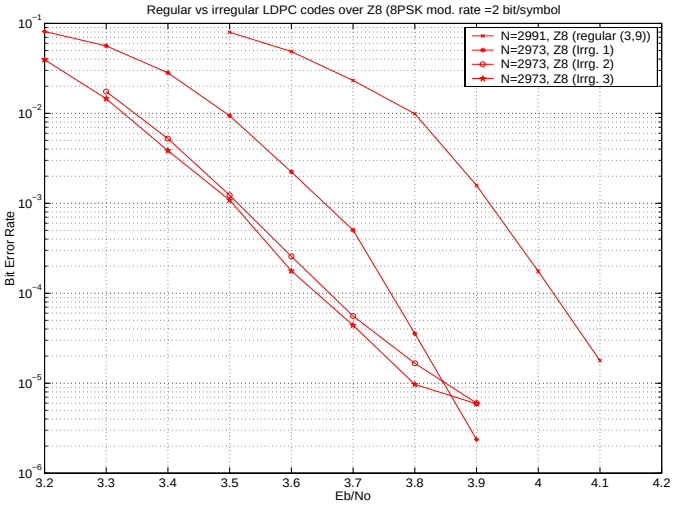

Figure 3: Regular vs irregular LDPCs over Z8 with 8PSK modulation (rate = 2 bits/symbol)

LDPC codes[4]. The non-binary group based codes are found to consistently outperform bit-interleaved coded modulation using binary LDPCs; a gain of 0.10-0.15 dB is observed.

Thresholds and code optimization: The performance of the message passing decoder on an LDPC constraint graph has been shown to depend on the degree-profile of the nodes in the graph [8]. In particular, a parameter known as the "threshold" has been found to characterize the convergence behavior of the decoder; the decoder is guaranteed to converge on a cycle-free constraint graph when the signal to noise ratio (SNR) of the channel exceeds the threshold. Similar analyses can, in principle, be extended to LDPCs over non-binary alphabets and modulation schemes. However, such an analysis may involve the computation of the probability density function of the extrinsic messages exchanged within the graph as a function of the decoding round. With LDPC codes over $\mathbb{Z}_m$, an extrinsic message is an $m-1$ dimensional parameter, and so for large m (such as $m = 8$), this task becomes computationally infeasible. As we haven't yet found an analytical approach to this problem, an "approximate" threshold for the message passing decoder on LDPC constraint graphs over $\mathbb{Z}_m$ is determined through simulations.

Typically, in these simulations, the apriori messages are generated either by approximating the log-likelihood ratios (in the case of binary LDPCs) to be Gaussian random variables or by sampling the probability density function of the apriori's computed at that instant of decoding. However, we obtain the apriori's directly from the extrinsics generated at the previous decoding round by simulating a number of realizations of the basic constraint node(s); the apriori's are chosen randomly from among the extrinsics obtained in different realizations, at each decoding round. The quality of the extrinsics is measured by a suitable parameter and an approximate threshold limit for decoder-convergence is determined. This limit agrees reasonably well with the corresponding waterfall behavior of the codes that were simulated. The degree profile of the nodes of the constraint graph were optimized based on this parameter, and, subsequently, a few good irregular LDPC constraint graphs were found.

Figure 3 shows the performance of three irregular and one regular LDPC codes over $\mathbb{Z}_8$ of block lengths close to 3000 symbols. The codes marked Irg. 2 and Irg. 3 were found by optimizing the node-degrees of an LDPC over $\mathbb{Z}_8$. Both of these have a maximum variable-node degree of 12 and an average constraint-node degree of 8.5; their thresholds under belief propagation, as determined through simulation, is approximately 3.15 dB.

LDPC codes over $\mathbb{Z}_8R$ and $\mathbb{G}_8$: LDPC codes over $\mathbb{Z}_8R$ and $\mathbb{G}_8$ are designed in a way similar to the codes described above. A rate-3/4 $(3, 12)$ regular LDPC code of block length 1000 is constructed over the rings $\mathbb{Z}_8R$ and $\mathbb{G}_8$ respectively and mapped onto the 6D $2 \times S_o$ constellation. Similarly, a $(3, 6)$ rate 1/2 and block length 1500 LDPC code constructed over the two ring structures is mapped onto the 4D $2 \times$ 8-PSK constellation. The two ring structures yield codes that perform quite differently with the same modulation scheme. With the former ring structure, no benefit is derived from going to higher dimensions due to the fact that ring operations are defined component-wise. A block length N LDPC code over $\mathbb{Z}_8$ with S_o modulation would therefore perform similar to a block length N LDPC code over $\mathbb{Z}_8R$ with $2 \times S_o$ modulation. However, some benefit can be accrued by designing a code over $\mathbb{G}_8$.

Figure 4 compares the performance of these codes with that of an LDPC code over $\mathbb{Z}_8$ that is mapped to the 2D 8-PSK constellation and two binary LDPC codes that are used in bit-interleaved coded modulation (BICM), with

[4]The code-constraint graph for a (j, k) LDPC code contains only variable nodes of degree j and constraint nodes of degree k.

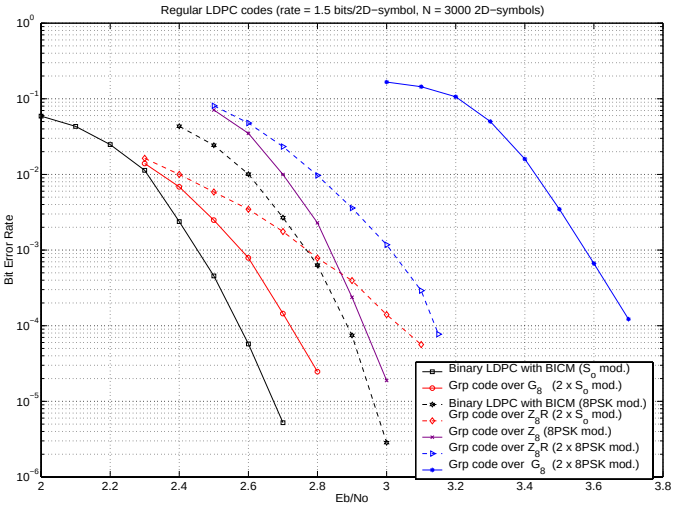

Figure 4: Group LDPCs matched to multi-dimensional constellations. (rate=1.5 bits/2D-symbol)

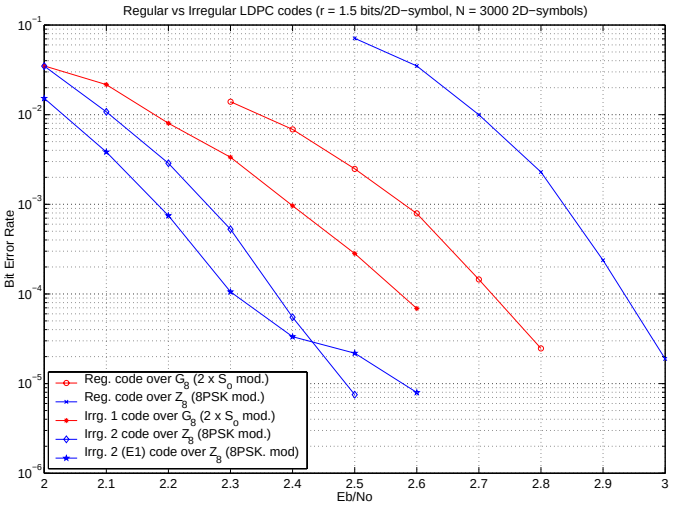

Figure 5: Regular vs Irregular Group LDPCs (rate=1.5 bits/2D-symbol)

one of them mapped to S_o and the other mapped to the 8-PSK signal set. The BICM codes are decoded in a turbo fashion wherein the BICM decoder uses the demapper and the LDPC-decoder as component decoders of a serial-concatenated turbo code. All codes shown in the figure have block lengths of 3000 2D symbols and spectral efficiency of 1.5 bits/2D-symbol.

The rate-3/4 code designed over $\mathbb{G}_8$ and mapped to $2\times S_o$ performs quite well when compared with an analogous code designed over $\mathbb{Z}_8R$. Further, the codes mapped to $2\times S_o$ perform substantially better than codes mapped to the 2×8-PSK constellation. Surprisingly, a rate 1/2 code over $\mathbb{G}_8$ that is mapped to the $2\times$ 8-PSK constellation performs poorly in comparison with an analogous code designed over $\mathbb{Z}_8R$.

The LDPC constraint graphs of some of these codes were optimized further by extending the threshold techniques described previously. Consequently, two irregular LDPC codes were designed:

- a code over $\mathbb{Z}_8$ with degree profile[5] $\lambda(x) = 0.374904x + 0.2x^2 + 0.425096x^9$ and $\rho(x) = 0.22919x^5 + 0.77081x^6$, used with 8PSK modulation;
- a code over $\mathbb{G}_8$ with degree profile $\lambda(x) = 0.29091x + 0.70909x^2$ and $\rho(x) = 0.5x^9 + 0.5x^{10}$, used with $2\times S_o$ modulation.

Figure 5 shows the performance of these irregular LDPC codes. The code over $\mathbb{Z}_8$ is found to perform significantly well in comparison with the regular LDPC codes of Figure 4. So far, the entries of the LDPC matrix H of the codes described, were chosen uniformly from among the non-zero-divisors of the corresponding ring. However, by a more careful selection of the entries of H, the code's performance can be enhanced further. The curve marked `E1` in Figure 5 shows the performance of one such code whose H matrix is similar to that of the code Irrg. 2, differing only in the choice of non-zero entries. The new code performs well at low to moderate SNRs in comparison with the original code.

References

[1] K. Narayanan and J. Li, "Bandwidth efficient low density parity check coding using multilevel coding and iterative multistage decoding," in *Proceedings of the International Symposium on Turbo Codes and Related Topics*, September 2000.

[2] J. Hou, P. H. Siegel, B. Milstein, and H. D. Pfister, "Design of low-density parity-check codes for bandwidth efficient modulation," in *Proceedings of IEEE Information Theory Workshop*, Oct 2001.

[3] H. A. Loeliger, "Signal sets matched to groups," *IEEE Transactions on Information Theory*, Nov 1991.

[4] G. D. Forney, "Geometrically uniform codes," *IEEE Transactions on Information Theory*, Sept 1991.

[5] G. Caire and E. M. Biglieri, "Linear block codes over cyclic groups," *IEEE Transactions on Information Theory*, Sept 1995.

[6] A. R. Calderbank and N. J. A. Sloane, "Modular and p-adic cyclic codes," *Designs, Codes, and Cryptography*, no. 6, pp. 21–35, 1995.

[7] D. J. C. Mackay and M. Davey, "Low density parity check codes over $GF(q)$," *IEEE Communication Letters*, June 1998.

[8] T. Richardson and R. Urbanke, "The capacity of low-density parity check codes under message-passing decoding," *IEEE Transactions on Information Theory*, Feb 2001.

[9] G. D. Forney, "Coset codes—Part I: Introduction and geometrical classification," *IEEE Transactions on Information Theory*, Sept. 1988.

[5]The degree profiles λ and ρ are defined as in [8].