LDPC Codes from Matrix Equations

Ariel Amir, Abigail Mitchell and Joachim Rosenthal

***Abstract*— Different constructions of LDPC codes based on matrix equations are investigated. The parameters such as the dimension, rate and distance are computed. The classical Tanner graph representation known for LDPC codes are described. The main difference between standard LDPC codes and the LDPC codes based on matrix equations lies in the structure of their codewords. Whereas in the classical situation codewords are simply vectors, the codewords in this new setting will be two-dimensional vectors or matrices. This implies that the parity-check constraints must be satisfied in both perpendicular directions of the codeword. Therefore, a codeword may be interpreted as a two-dimensional array which is suitable for recording on two-dimensional pattern-oriented storage media.**

I. Motivation

Error-correcting codes play an important role in digital recording systems. Generally, their purpose is to increase the performance of the channel. The motivation for LDPC codes from matrix equations comes along with the new two-dimensional (2-D) data storage solutions. There the data is saved as a 2-D array or pattern. The main objective is to match the representation of the recorded data with the characteristics of the recording channel. Therefore, LDPC codes based on matrix equations might be naturally applied for recording on 2-D storage systems.

In order to obtain an example for coding consider binary matrices A_1, A_2, B_1, B_2 of sizes $r \times m$, $r \times n$, $s \times n$ and $s \times m$, respectively. Consider the matrix equation

$$A_1 X B_1^T + A_2 X^T B_2^T = 0\,.$$

The solution set of $m \times n$ defines a matrix code C as a subset of all $m \times n$ over the binaries. The matrix equation imposes parity checks on both the columns and rows of X and X^T.

An important advantage of codes from matrix equations versus standard LDPC codes is their compact description. We compare a LDPC code and a code from the matrix equation above, both of same length and nearly equal rate. For LDPC codes it is customary to have a length of several thousand bits. On the one hand, consider a rate $1/2$ binary $(3, 6)$-LDPC code of length 10000. Its parity-check matrix has size 5000 $\times$ 10000 with a column weight of 3, so after compression the data requires at least 30,000 bits to describe. On the other hand, let A_1, A_2, B_1 and B_2 be binary matrices, each of size 70 $\times$ 100 and a density of $1/2$, where X has size 100×100 and satisfies the matrix equation. It can be shown that C has rate $0.51 \approx 1/2$. The matrices A_1, A_2, B_1 and B_2 give a representation of the parity checks of the code C by 4 times 3500 bits or a total of 14 kilobits only. Of course if A_i and B_i are sparse matrices this would be further reduced – but we are interested in describing how a not too dense linear matrix equation translates to a traditional LDPC code. In general, we have a compact description of the code with a convenient equation.

In the following we present a catalog of possible linear matrix equations, deriving such parameters as distance, rate and dimension for each.

This work was supported by the Swiss National Science Foundation under grant numbers 112422 and 113251.

The authors are with the Institute of Mathematics, Winterthurerstrasse 190, CH-8057 Zürich, Switzerland. http://www.math.uzh.ch/aa/

II. Definitions and Examples

Throughout this paper let $\mathbb{F}$ denote a finite field, and $F^{m\times n}$ the vector space of $m \times n$ matrices over $\mathbb{F}$. Codes based on matrix equations are defined as subspaces of the vector space $\mathbb{F}^{m\times n}$. In this work we seek interesting codes $C \subseteq \mathbb{F}^{m\times n}$ with a low-density parity-check matrix [2]. We define a linear subspace $C \subseteq \mathbb{F}^{m\times n}$ as an $m \times n$ *matrix code*. Occasionally, we will switch from the matrix sense to the vector sense by concatenating the rows of a codeword vertically to form a vector. We denote by $\delta_{i,j}$ the Kronecker delta, and by I_n the *identity matrix* of size n (where if there is no confusion the subscript may be omitted.)

Definition 2.1: Let C be an $m \times n$ matrix code. We define a *parity-check matrix* of C as a matrix H such that for every codeword $X \in \mathbb{F}^{m\times n}$

$$X \in C \Leftrightarrow H \begin{bmatrix} x_1^T \\ x_2^T \\ \vdots \\ x_m^T \end{bmatrix} = 0\,,$$

where $x_1, x_2, \ldots, x_m$ denote the rows of X.

Regarding a codeword X as a vertical concatenation of its rows, this definition describes the code C as the right kernel of the parity-check matrix H in $\mathbb{F}^{m\times n}$.

Example 2.2: Let C consist of the set

$$C = \{X \in \mathbb{F}^{m\times n} \mid AX = 0\,, A \in \mathbb{F}^{l\times m}\}\,.$$

Let $X = \big[x_1, x_2, \ldots, x_n\big]$, where x_i denotes the i-th column of X. We may write $AX = \big[Ax_1, Ax_2, \ldots, Ax_n\big] = 0$. We know that for each single homogeneous equation the dimension of the solution space is equal to $m - \operatorname{rank} A$. By taking the direct sum of n copies of A and vertically concatenating the n columns of X we can equivalently write

$$\begin{bmatrix} A & & & \\ & A & & \\ & & \ddots & \\ & & & A \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = 0_{nl\times 1}\,.$$

ISBN 978-963-311-370-7

The matrix on the left has rank $(n \operatorname{rank} A)$. Accordingly, we derive the parameters of the code C. The dimension of C is given by $\dim C = mn - (n \operatorname{rank} A) = n(m - \operatorname{rank} A)$. The rate is $R = \frac{mn-(n \operatorname{rank} A)}{mn} = \frac{m-\operatorname{rank} A}{m}$. Let $C_A = \{x \in \mathbb{F}^m \,|\, Ax = 0\}$. Then the distance of C is equal to the distance of C_A, $d(C) = d(C_A)$. Let $A = (a_{ij})$ and $X = (x_{ij})$; then a parity check matrix for C is given by $H = (h_{ij})$, where for $1 \le i \le l$, $1 \le u \le m$ and $1 \le j, v \le n$,

$$h_{(i-1)n+j,(u-1)n+v} = a_{i,u}\, \delta_{j,v}\,.$$

III. Product Codes

Given two matrices $A \in \mathbb{F}^{r\times m}$ and $B \in \mathbb{F}^{s\times n}$, consider the code

$$C = \{X \in \mathbb{F}^{m\times n} \,|\, AX = 0 \text{ and } XB^T = 0\}\,.$$

The two conditions

$$AX = 0 \text{ and } XB^T = 0 \tag{1}$$

impose parity checks on the columns and rows of X, respectively, which may be made explicit as follows:

$$(AX)_{i,j} = \sum_{k=1}^{m} a_{i,k}x_{k,j} = 0\,,\ \text{for } 1 \le i \le r, 1 \le j \le n \tag{2}$$

$$(XB^T)_{i,j} = \sum_{l=1}^{n} b_{j,l}x_{i,l} = 0\,,\ \text{for } 1 \le i \le m, 1 \le j \le s, \tag{3}$$

The resulting parity check matrix $H = (h_{ij}) \in \mathbb{F}^{(nr+ms)\times mn}$ is given by

$$h_{(i-1)n+j,(u-1)n+v} = a_{i,u}\,\delta_{j,v}\,,\ \text{for } 1 \le i \le r, 1 \le j \le n\,,$$

$$h_{rn+(i-1)s+j,(u-1)n+v} = b_{j,v}\,\delta_{i,u}\,,\ \text{for } 1 \le i \le m, 1 \le j \le s\,.$$

Note that the first rn rows contain the constraints for Equation (2) and the subsequent ms rows contain the constraints for Equation (3).

To determine the dimension of C, we begin with the following lemma which will be stated without proof:

Lemma 3.1: Let $M \in \mathbb{F}^{m\times n}$. If $S \in \mathbb{F}^{m\times m}$ and $T \in \mathbb{F}^{n\times n}$ are invertible matrices, then the map

$$\mu : \mathbb{F}^{m\times n} \to \mathbb{F}^{m\times n}\,, \quad M \mapsto SMT\,,$$

is an automorphism and, in particular, preserves dimension of subspaces.

If A and B are of full rank, then there exist invertible matrices S and T such that we can write

$$AS^{-1} = \begin{bmatrix} I_r & 0 \end{bmatrix} \text{ and } T^{-1}B^T = \begin{bmatrix} I_s \\ 0 \end{bmatrix}\,.$$

This gives us an alternative description of the code $C = \{X \in \mathbb{F}^{m\times n} \,|\, AX = 0 \text{ and } XB^T = 0\}$, namely that

$$C = \{X \in \mathbb{F}^{m\times n} \,|\, (AS^{-1})(SX) = 0 \text{ and } (XT)(T^{-1}B^T) = 0\}\,.$$

Next, we compute the dimension of C. Without loss of generality, let $\tilde{A} = \begin{bmatrix} I_r & 0 \end{bmatrix}$ and $\tilde{B}^T = \begin{bmatrix} I_s \\ 0 \end{bmatrix}$. Consider the set $\{X \in \mathbb{F}^{m\times n} \,|\, \tilde{A}X = 0 \text{ and } X\tilde{B}^T = 0\}$. It follows that X must be of the form

$$X = \begin{bmatrix} 0_{r\times s} & 0 \\ 0 & * \end{bmatrix}\,,$$

and the dimension of the code C is then equal to the size of the lower right non-zero block of X. Thus, we arrive at the following proposition.

Proposition 3.2: Let $A \in \mathbb{F}^{r\times m}$ and $B \in \mathbb{F}^{s\times n}$ have full rank. Then, the dimension of the matrix code $C = \{X \in \mathbb{F}^{m\times n} \,|\, AX = 0 \text{ and } XB^T = 0\}$ is given by

$$\dim C = (m - \operatorname{rank} A)(n - \operatorname{rank} B) = (m - r)(n - s)\,,$$

the rate is $R = \frac{(m-r)(n-s)}{mn}$, and its distance is $d(C) = \dim\ker A \cdot \dim\ker B$.

Note that $R = R_A R_B$, i.e. the rate of C is the product of rates of the two smaller codes with parity-check matrices A and B. This means that small codes with high rates are required to produce a reasonable product code; however, codes with high rate tend to have small distance, resulting in a product code with low distance as well. It can also be shown that Tanner graphs of these codes have girth $\gamma = \min\{\gamma_A, \gamma_B, 8\}$.

Remark 3.3: As discussed above, we can write down all parity-check equations, form the Tanner graph based on those equations and proceed with LDPC iterative decoding. However, the structure of product codes also permits a more efficient decoding procedure, e.g. the soft-decision algorithm of Reddy and Robinson [4].

Example 3.4: We choose the matrices

$$A\,,\, B = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \end{bmatrix}\,.$$

As parity-check matrices, A and B each describe a $[7, 4, 2]$ code whose Tanner graph forms a tree. Then the code C has the parameters $[49, 16, 4]$ and $\gamma = 8$. The density of the parity-check matrix H is computed as approximately 0.06. Figure 1 shows the conventional decoding performance over the AWGN channel.

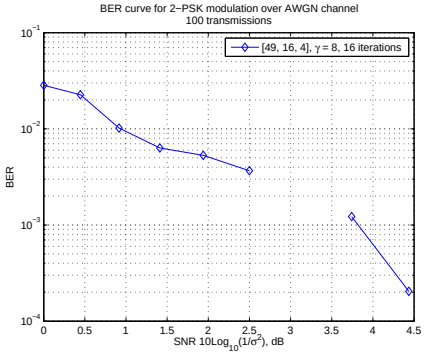

Fig. 1. BER Performance

IV. $A_1XB_1^T + A_2X^TB_2^T$

Given the matrices $A_1 \in \mathbb{F}^{r\times m}$, $A_2 \in \mathbb{F}^{r\times n}$, $B_1 \in \mathbb{F}^{s\times n}$ and $B_2 \in \mathbb{F}^{s\times m}$, consider the matrix code

$$C = \{X \in \mathbb{F}^{m\times n} \,|\, A_1XB_1^T + A_2X^TB_2^T = 0\}\,. \quad (4)$$

We will first consider some special cases of (4) and then head to the general case.

A. $A(X + X^T)$

Consider a special case of Equation (4) where $A_1 = A_2 = A \in \mathbb{F}_2^{r\times n}$ is of full rank and $B_1 = B_2 = I_n$, i.e. the matrix code

$$C = \{X \in \mathbb{F}_2^{n\times n} \,|\, A(X + X^T) = 0\}\,.$$

We remark that any X with a single 1 on the diagonal and zeros elsewhere satisfies the constraint $A(X + X^T) = 0$, and therefore the distance is $d(C) = 1$. Let us consider the parity-check equations

$$(A(X + X^T))_{i,j} = \sum_{t=1}^{n} a_{i,t}(x_{t,j} + x_{j,t}) = 0\,, \quad (5)$$

for $1 \le i, \le r$ and $1 \le j, \le n$. For particular i and j in Equation (5) we get a parity-check equation which corresponds to a row in the parity-check matrix $H \in \mathbb{F}^{rn\times n^2}$ of C. Entries of H are given by the coefficients of $x_{u,v}$, $1 \le u, v \le n$, in Equation (5). Then, for $1 \le i, \le r$, $1 \le j, u, v \le n$ the parity-check matrix $H \in \mathbb{F}^{rn\times n^2}$,

$$\begin{aligned} h_{(i-1)n+j,(u-1)n+v} &= \begin{cases} 2a_{i,j} & \text{if } j = u = v\,, \\ a_{i,v} & \text{if } j = u\,, \\ a_{i,u} & \text{if } j = v\,, \\ 0 & \text{otherwise} \end{cases} \\ &= a_{i,v}\,\delta_{j,u} + a_{i,u}\,\delta_{j,v}\,. \end{aligned}$$

(Note that as an $rn \times n^2$ matrix with row weight at most $2n - 1$, H is sparse for large n.)

By examining H more closely, we see that the 1st, $(n+2)$nd, $(2n+3)$th, $(3n+4)$th, …, $((n-1)n+n) = n^2$th columns are equal to the all-zero column over $\mathbb{F}_2$. An immediate consequence is the existence, as remarked earlier, of a weight one codeword in C.

Without loss of generality, we may let

$$\tilde{A} = \begin{bmatrix} I_r & 0 \end{bmatrix}$$

and consider the code $\{X \in \mathbb{F}_2^{n\times n} \,|\, \tilde{A}(X+X^T) = 0\}$, which will have the same dimension as C. Results thus obtained are summarized as follows:

Proposition 4.1: Let $A \in \mathbb{F}_2^{r\times n}$. The matrix code

$$C = \{X \in \mathbb{F}_2^{n\times n} \,|\, A(X + X^T) = 0\}$$

has distance $d(C) = 1$, dimenstion $n^2 - r(n-r) - \left(\frac{r^2-r}{2}\right)$ and rate $R = \frac{1}{n^2}\left(n^2 - r(n-r) - \frac{1}{2}(r^2-r)\right)$.

B. AXB^T

Let $A \in \mathbb{F}^{r\times m}$ and $B \in \mathbb{F}^{s\times n}$. Consider the matrix code

$$C = \{X \in \mathbb{F}^{m\times n} \,|\, AXB^T = 0\}\,.$$

Let us first derive the parity-check matrix of C. Consider parity-check equations

$$(AXB^T)_{i,j} = \sum_{k=1}^{n}(AX)_{i,k}\,b_{k,j}^T = \sum_{k=1}^{n}\sum_{l=1}^{m} a_{i,l}\,b_{j,k}\,x_{l,k} = 0\,, \quad (6)$$

for $1 \le i \le r$ and $1 \le j \le s$. For particular i and j in Equation (6) we get a parity-check equation which corresponds to a row in the parity-check matrix $H \in \mathbb{F}^{rs\times mn}$ of C. Hence, for $1 \le i \le r$, $1 \le j \le s$, $1 \le l \le m$ and $1 \le k \le n$ H is given by

$$h_{(i-1)s+j,(l-1)n+k} = a_{i,l}\,b_{j,k}\,.$$

Note that H may be expected to be dense.

Assume A and B have full rank, and let $S \in \mathbb{F}^{m\times m}$ and $T \in \mathbb{F}^{n\times n}$ be invertible matrices such that

$$AS^{-1} = \begin{bmatrix} I_r & 0 \end{bmatrix} \text{ and } T^{-1}B^T = \begin{bmatrix} I_s \\ 0 \end{bmatrix}\,.$$

We have

$$AXB^T = 0 \quad \Rightarrow \quad (AS^{-1})(SXT)(T^{-1}B^T) = 0\,.$$

The mapping $X \mapsto SXT$ is an automorphism so without loss of generality set $\tilde{A} = AS^{-1}$ and $\tilde{B}^T = T^{-1}B^T$, and consider the set $\{X \in \mathbb{F}^{m\times n} \,|\, \tilde{A}X\tilde{B}^T = 0\}$. Then X must have the following shape to satisfy $\tilde{A}X\tilde{B}^T = 0$

$$X = \begin{bmatrix} 0_{r\times s} & * \\ * & * \end{bmatrix}\,.$$

The dimension of the code C is then equal to the size of the non-zero portion of X denoted by asterisks, and we obtain the following proposition.

Proposition 4.2: Let $A \in \mathbb{F}^{r\times m}$ have full rank r and $B \in \mathbb{F}^{s\times n}$ have full rank s. The matrix code

$$C = \{X \in \mathbb{F}^{m\times n} \,|\, AXB^T = 0\}$$

has distance $d(C) \le \min\{d(\ker A), d(\ker B)\}$, dimenstion $\dim C = mn - rs$ and rate $R = \frac{mn-rs}{mn}$.

Proof: The dimension and rate follow from the discussion above. For the distance consider first a codeword in $\ker A$ of minimal weight as a column of X, where the remaining entries are set to zero. Then, multiplication from left by A already satisfies the constraint $AXB^T = 0$. The same holds for a minimal-weight codeword in $\ker B$ as a row of X, where we interchange the roles of A and B. Therefore, any codeword in $\ker A$ and $\ker B$ will also be reproduced in C. So, $\min\{d(\ker A), d(\ker B)\}$ is an upper bound on the distance of C. ∎

C. $A_1XB_1^T + A_2X^TB_2^T$

Eventually, we reach the general case. Recall $A_1 \in \mathbb{F}^{r\times m}$, $A_2 \in \mathbb{F}^{r\times n}$, $B_1 \in \mathbb{F}^{s\times n}$ and $B_2 \in \mathbb{F}^{s\times m}$. Assume that A_1, A_2 have full rank r, and B_1, B_2 have full rank s. We consider the matrix code

$$C = \{X \in \mathbb{F}^{m\times n} \,|\, A_1XB_1^T + A_2X^TB_2^T = 0\}\,.$$

The left side of Equation (4) writes as

$$\begin{aligned}(A_1XB_1^T + A_2X^TB_2^T)_{i,j} &= \sum_{k=1}^{n}\sum_{l=1}^{m} a_{1\,i,l}\, x_{l,k}\, b^T_{1\,k,j} + \sum_{p=1}^{m}\sum_{q=1}^{n} a_{2\,i,q}\, x^T_{q,p}\, b^T_{2\,p,j} \\ &= \sum_{k=1}^{n}\sum_{l=1}^{m} a_{1\,i,l}\, b_{1\,j,k}\, x_{l,k} + a_{2\,i,k}\, b_{2\,j,l}\, x_{l,k}\,,\end{aligned}$$

for $1 \le i \le r$ and $1 \le j \le s$. In the second equation we joined the summations and applied the transposition of the matrices. We are now able to write down the parity-check matrix $H \in \mathbb{F}^{rs\times mn}$ of C. For $1 \le i \le r$, $1 \le j \le s$, $1 \le u \le m$ and $1 \le v \le n$ we get

$$h_{(i-1)s+j,(u-1)n+v} = a_{1\,i,u}\, b_{1\,j,v} + a_{2\,i,v}\, b_{2\,j,u}\,.$$

Now we compute the dimension of C. If A_1, B_1 have full rank, we may choose invertible matrices $S \in \mathbb{F}^{m\times m}$ and $T \in \mathbb{F}^{n\times n}$ such that

$$AS^{-1} = \begin{bmatrix} I_r & 0\end{bmatrix},\; T^{-1}B_1^T = \begin{bmatrix} I_s \\ 0\end{bmatrix},$$

and as before the transformation $X \mapsto SXT$ is an automorphism, thus the code

$$C' = \{X \in \mathbb{F}^{m\times n} \,|\, \begin{bmatrix} I_r & 0\end{bmatrix} X \begin{bmatrix} I_s \\ 0\end{bmatrix} + \tilde{A}_2X^T\tilde{B}_2^T = 0\},$$

where $\tilde{A} = A_2(T^{-1})^T$ and $\tilde{B} = B_2S^{-1}$, has the same dimension as C.

Now we would like to apply a further dimension-preserving transformation, using invertible matrices taken from the stabilizers of $\begin{bmatrix} I_r & 0\end{bmatrix}$ and $\begin{bmatrix} I_s \\ 0\end{bmatrix}$ respectively:

$$\begin{aligned} Stab_L\left(\begin{bmatrix} I_r & 0\end{bmatrix}\right) &= \left\{\begin{bmatrix} I_r & 0 \\ * & P_4\end{bmatrix} \,|\, P_4 \in GL(m-r,\mathbb{F})\right\} \\ Stab_R\left(\begin{bmatrix} I_s \\ 0\end{bmatrix}\right) &= \left\{\begin{bmatrix} I_s & * \\ 0 & Q_4\end{bmatrix} \,|\, Q_4 \in GL(n-s,\mathbb{F})\right\}.\end{aligned}$$

Take $P \in Stab_L\left(\begin{bmatrix} I_r & 0\end{bmatrix}\right)$ and $Q \in Stab_R\left(\begin{bmatrix} I_s \\ 0\end{bmatrix}\right)$, the transformation $X \mapsto P^{-1}XQ^{-1}$ preserves dimension, i.e. the code

$$C'' = \{X \in \mathbb{F}^{m\times n} \,|\, \begin{bmatrix} I_r & 0\end{bmatrix} X \begin{bmatrix} I_s \\ 0\end{bmatrix} + \tilde{\tilde{A}}_2X^T\tilde{\tilde{B}}_2^T = 0\},$$

where $\tilde{\tilde{A}} = \tilde{A}Q^T = A_2(T^{-1})^TQ^T$ and $\tilde{\tilde{B}} = \tilde{B}P = B_2S^{-1}P$, has the same dimension as C' and C. (Note that if A_2 and B_2 have full rank, then the derived matrices $\tilde{\tilde{A}}$ and $\tilde{\tilde{B}}$ have full rank as well.)

Examining this code we obtain a lower bound on the dimension of $mn-rs$, giving rise to the following proposition.

Proposition 4.3: Let $A_1 \in \mathbb{F}^{r\times m}$, $A_2 \in \mathbb{F}^{r\times n}$ and $B_1 \in \mathbb{F}^{s\times n}$, $B_2 \in \mathbb{F}^{s\times m}$ have full rank r and s, respectively. Then the matrix code

$$C = \{X \in \mathbb{F}^{m\times n} \,|\, A_1XB_1^T + A_2X^TB_2^T = 0\}\,.$$

has dimension $\dim(C) \ge mn - rs$ and rate $R \ge \frac{mn-rs}{mn}$.

Example 4.4: Table I lists distance computations for some matrix codes C. The girth is also listed but in all our test it was equal to 4. The matrices A_1, A_2, B_1 and B_2 describing the code C were chosen at random and therefore have a density of approximately 0.5.

TABLE I
DISTANCE COMPUTATIONS

R	C	$d(C)$
0.51	$A_1, A_2, B_1, B_2 \in \mathbb{F}^{7\times 10}$	9
0.64	$A_1 \in \mathbb{F}^{8\times 10}, A_2 \in \mathbb{F}^{8\times 20}, B_1 \in \mathbb{F}^{9\times 20}, B_2 \in \mathbb{F}^{9\times 10}$	7
0.65	$A_1 \in \mathbb{F}^{7\times 10}, A_2 \in \mathbb{F}^{7\times 20}, B_1 \in \mathbb{F}^{10\times 20}, B_2 \in \mathbb{F}^{10\times 10}$	9
0.75	$A_1, A_2, B_1, B_2 \in \mathbb{F}^{5\times 10}$	3
0.84	$A_1, A_2, B_1, B_2 \in \mathbb{F}^{4\times 10}$	2

Example 4.5: Figure 2 compares the decoding performance of a matrix code C with random matrices $A_1, A_2, B_1, B_2 \in \mathbb{F}^{7\times 10}$ and a $(3,6)$-regular LDPC code both of girth $\gamma = 4$ over the AWGN channel.

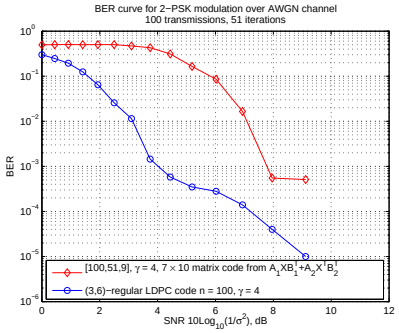

Fig. 2. BER Performance

V. COMMUTATOR CODES

For a given square matrix $A \in \mathbb{F}^{m\times m}$, the set of all matrices $X \in \mathbb{F}^{m\times m}$ which commute with A forms the matrix code

$$C = \{X \in \mathbb{F}^{m\times m} \,|\, [X, A] = 0\}\,, \tag{7}$$

where $[X, A] := XA - AX$ is the Lie bracket.

For $A = (a_{i,j})$ and $X = (x_{i,j})$, the parity-check equations defining such a code are given by the entries of the Lie bracket

$$([X, A])_{i,j} = \sum_{k=1}^{m} x_{i,k}a_{k,j} - a_{i,k}x_{k,j} = 0\,, \tag{8}$$

for $1 \leq i, j \leq m$. These are m^2 parity-check equations in the m^2 unknowns corresponding to the entries of X, and thus the entries of the square parity-check matrix $H \in \mathbb{F}^{m^2 \times m^2}$ for the code C are as follows:

$$h_{(i-1)m+j,(u-1)m+v} = a_{v,j}\,\delta_{i,u} - a_{i,u}\,\delta_{j,v}\,.$$

Note that if A is regular and sparse, i. e., with a small constant number r of non-zero entries in every row and column, then H is also sparse, with $2r$ nonzero entries per row and column (over a matrix of size $m^2 \times m^2$.)

Consider the commutative ring of polynomials in A:

$$\mathbb{F}[A] = \left\{ \sum_{i=0}^{k} a_i A^i \mid a_i \in \mathbb{F} \right\}\,.$$

Note that in general $\mathbb{F}[A] \subseteq C$, and in fact $\mathbb{F}[A] = C$ if and only if the characteristic and minimal polynomials of A are identical. A proof of this result is given in [1] (Theorem 5.19).

Theorem 5.1 ([1]): For generic matrices A, $C = \mathbb{F}[A]$ if and only if the minimal polynomial of A is identical to the characteristic polynomial of A.

Moreover, we have Schur's Theorem (see e. g. [3]), which states that the maximal number of linearly independent matrices commuting with a given matrix $A \in \mathbb{F}^{m\times m}$ is $\left\lfloor \frac{m^2}{4} \right\rfloor + 1$. Such vectors form a basis for C, allowing us to state the following proposition.

Proposition 5.2: Let $A \in \mathbb{F}^{m\times m}$. If the characteristic polynomial $\chi_A(x)$ is irreducible, then the matrix code

$$C = \{X \in \mathbb{F}_q^{m\times m} \mid [X, A] = 0\}$$

has distance $d(C) = m$ and the rate is bounded by $R \leq 1/4 + 1/m^2$.

Proof: We know that $\mathbb{F}_q[A] \supseteq C$. Since $\chi_A(x)$ is irreducible it is identical to the minimal polynomial of A, and thus by Theorem 5.1 $\mathbb{F}_q[A] = C$. Certainly the identity matrix $I_m \in C$ with $\operatorname{wt} I_m = m$ and so $d(C) \leq m$. By the irreducibility of $\chi_A(x)$ we have $\mathbb{F}_q[A] \cong \mathbb{F}_q[x]/(\chi_A(x)) \cong \mathbb{F}_{q^{\deg \chi_A(x)}}$. Since $\mathbb{F}_q[A]$ is isomorphic to a field, every non-zero element $X \in \mathbb{F}_q[A]$ is invertible, i.e. has at least one nonzero entry in every row, and thus $d(C) \geq m$. We conclude that $d(C) = m$, and the rate follows from the discussion above. ∎

References

[1] C. G. Cullen. *Matrices and linear transformations*. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., second edition, 1972.

[2] R.G. Gallager. *Low-Density Parity Check Codes*. M.I.T. Press, Cambridge, MA, 1963. Number 21 in Research monograph series.

[3] N. Jacobson. Schur's theorems on commutative matrices. *Bull. Amer. Math. Soc.*, 50:431–436, 1944.

[4] S. M. Reddy and J. P. Robinson. Random error and burst correction by iterated codes. *IEEE Trans. Information Theory*, IT-18:182–185, 1972.

[5] W. E. Ryan. An introduction to LDPC codes. In B. Vasic, editor, *CRC Handbook for Coding and Signal Processing for Recoding Systems*. CRC Press, 2004.