Bulletin of the Iranian Mathematical Society Vol. 31 *No. 2 (2005), pp 13-32.*

ON THE GRÖBNER BASIS OF A FAMILY OF QUASI-CYCLIC LDPC CODES

MARTA GIORGETTI*, MARTA ROSSI AND MASSIMILIANO SALA

Communicated by Teo Mora

Abstract. In [30] a class of quasi-cyclic LDPC codes has been proposed, whose information rate is 1/2. We generalize that construction to arbitrary rates $\frac{l-1}{l}$ and we provide a Gröbner basis for their dual codes, in some generic cases.

1. Introduction

In R. Bresnan's Master thesis [2], a class of quasi-cyclic LDPC codes has been proposed. The LDPC codes (see Section 2.2) are codes with an excellent decoding performance and are usually constructed via probabilistic algorithms, preventing an accurate study of their properties (see [4], [7], [18], [20], [21], [26], [27], [28], [34], [35], [36]). On the other hand, quasi-cyclic codes are algebraic codes and allow a rigorous study via the Gröbner basis approach introduced by K. Lally and P. Fitzpatrick [16]. In [30] it has been shown that some simple algebraic conditions on the Gröbner basis elements guarantee good decoding performance for the Bresnan codes. A Gröbner basis for the dual code has also been presented in some cases of interest. However, the codes in [30] are only 1/2-rate codes.

MSC(2000): Primary 11T71
Keywords: Generalized semi-direct product, Deficiency zero group, Factor pair, Cyclically presented group
Received: 21 July 2005
*Corresponding author

In this paper we generalize Bresnan's construction to $\frac{l-1}{l}$-rate codes and provide a Gröbner basis for their dual codes, in some cases of interest. In particular, we can determine their dimension. Moreover, suitable generator matrices from the parity-check matrices might then be deduced.

This paper is organized as follows:

- an introductory section;
- Section 2, where we provide our notation and recall some relevant well-known facts, particularly on quasi-cyclic and LDPC codes,
- Section 3, where we define our family of quasi-cyclic LDPC codes and show the Gröbner basis of their duals,
- Section 4, where we draw some conclusions and plan further research.

2. Preliminaries and notation

In this section we recall some known facts and give some notation. There are four sub-sections: one on circulant matrices and their polynomial representation, one on LDPC codes, one on the Gröbner basis representation of quasi-cyclic codes and one on the Bresnan codes.

2.1. Circulant matrices.

Binary circulant matrices are important for our goals, as they form the "bricks" with which we "build" our parity-check matrices.

Definition 2.1. Let $m \geq 3$. Let C be an $m \times m$ matrix over $\mathbb{Z}_2$. We say that C is *circulant* if its rows are obtained by successive shifts (on the right). We say that C is *weight*-2 if the weight of any row is 2.

The polynomial representation of the first row, $p(x) \in \mathbb{Z}_2[x]$, is called the *polynomial* of C.

Consider for example the following weight-2 circulant matrix

$$C = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Its polynomial is $p = x + 1$ and $m = 5$.

2.2. **LDPC codes.** The parity-check matrix $H = (h_{i,j})$ of any binary $[n, k, d]$ linear code C can be represented by a graph, known as the Tanner graph ([33, 34]). The Tanner graph is formed by two types of nodes: the "bit nodes" and the "check nodes". Bit nodes correspond to matrix columns and check nodes correspond to matrix rows, so that there are $r = n - k$ check nodes and n bit nodes. We connect the check node i to the bit node j if and only if the entry $h_{i,j} = 1$. There is no edge connecting two check nodes or two bit nodes (this kind of graph is called a *bipartite* graph).

Now we introduce LDPC codes (Low-Density Parity-Check) a class of linear error correcting codes. Historically, these codes were discovered by Gallager in 1963 in his PhD thesis [5]. These codes were largely ignored, because of some implementation issues. In the 1990's they were rediscovered by MacKay [18] and now the research continues vigorously, with dozens of papers published every year.

Definition 2.2. An LDPC code is a linear block code for which the parity-check matrix has a low density of non-zero entries.

An (r, c)-regular LDPC code is a linear code whose parity-check matrix H contains exactly c ones per column and r ones per row.

We do not specify what we mean by low density because it depends on the context. For example, for a typical (3,6)-regular binary code (rate 1/2) of block length n, there are only three ones in each column of H and so the fraction of ones in this matrix is $6/n$.

The LDPC codes have excellent decoding performance, near to the channel capacity ([5, 18, 26]), but their performance is heavily hindered by the presence of small cycles in the Tanner graph ([36]). In fact, the parameter that mostly affects the behaviour of their decoding algorithm is the *girth* of its Tanner graph.

Definition 2.3. In a graph, a *cycle* is a path that starts from a vertex v and ends in v. The *girth* of a graph is the smallest of its cycles.

Some structured LDPC codes have appeared (see [8], [9], [10], [13], [14], [15], [23], [24], [29], [33]).

2.3. **Quasi-cyclic codes and Gröbner bases.** In this subsection we summarize some algebraic properties of quasi-cyclic codes, which have

been investigated in [16, 17]. Since a quasi-cyclic code may be represented as a sub-module of a module over a polynomial ring, the main tools will be (module) Gröbner bases . We expect the reader to be familiar with Gröbner bases for modules and so we will use them without any further comment. In particular, we will use the standard abbreviation POT for the Position Over Term monomial ordering.

Quasi-cyclic codes of index ℓ over a (finite) field F are defined by the property that a cyclic shift of a codeword by ℓ places is another codeword and l is the smallest such natural number ([19], [3], [11], [12], [37]). Let $\mathcal{C}$ be a quasi-cyclic code of length ℓm and index ℓ. We may assume that each element of $\mathcal{C}$ can be represented as a vector $c = (c_1(x), \ldots, c_\ell(x))$ of polynomials of degree less than m. Let $R = F[x]/\langle x^m - 1\rangle$, where F is a finite field. It is possible to show that $\mathcal{C}$ is an R–submodule of R^ℓ and that the preimage $\tilde{\mathcal{C}}$ of $\mathcal{C}$ in $F[x]^\ell$ is an $F[x]$–submodule containing $\tilde{\mathcal{K}} = \langle (x^m - 1)e_i, i = 1, \ldots, \ell\rangle$, where e_i is the standard basis vector with 1 in position i and 0 elsewhere.

The following theorem describes the structure of a Gröbner basis of $\tilde{\mathcal{C}}$.

Theorem 2.1. ([16]) *Each submodule $\tilde{\mathcal{C}}$ of $F[x]^\ell$ containing $\tilde{\mathcal{K}}$ has a POT reduced Gröbner basis of the form*

$$\tilde{\mathcal{G}} = \{g_i = (g_{i1}, g_{i2}, \ldots, g_{i\ell}), i = 1, \ldots, \ell\}\,, \tag{2.1}$$

where

(i) $g_{ij} = 0$ *for all* $j < i$,
(ii) $\deg(g_{ki}) < \deg(g_{ii})$ *for* $k < i$,
(iii) *if the left-most non-zero component of an element of $\tilde{\mathcal{C}}$ lies in the i-th place then it is divisible by g_{ii}; in particular, g_{ii} divides $x^m - 1$,*
(iv) *if* $g_{ii} = x^m - 1$ *then* $g_i = (x^m - 1)e_i$,
(v) *the F-dimension of $F[x]^\ell/\tilde{\mathcal{C}}$ is* $\sum_{i=1}^{\ell} \deg(g_{ii})$.

The code $\mathcal{C}$ is the image of $\tilde{\mathcal{C}}$ under the natural homomorphism

$$\varphi : F[x]^\ell \to R^\ell, (c_1, \ldots, c_\ell) \mapsto (c_1 + \langle x^m - 1\rangle, \ldots, c_\ell + \langle x^m - 1\rangle)\,.$$

Dropping the coset notation we see immediately that $\mathcal{C}$ has an R-generating set $\mathcal{G}$ comprising the elements of a Gröbner basis $\tilde{\mathcal{G}}$ not mapped to zero under φ. We refer to this set of generators as a *GB generating set* of $\mathcal{C}$. This can be used to determine the dimension of $\mathcal{C}$.

Theorem 2.2. ([16]) *The dimension of the code $\mathcal{C}$ with GB generating set $\{\varphi(g_i), i = 1, \ldots, \ell\}$ is given by*

$$\ell m - \sum_{i=1}^{\ell} \deg(g_{ii}) = \sum_{i=1}^{\ell} (m - \deg(g_{ii}))\,.$$

Remark 2.1. In [16] it has been shown that from $\tilde{\mathcal{G}}$ other results can be obtained, e.g. Gröbner bases for the dual code, classification and counting codes with given parameters and efficient search for optimal codes.

Although some code properties can always be deduced by "ad hoc" arguments on the generator matrix (as for example the dimension) and hence the introduction of Gröbner bases is not strictly necessary in understanding quasi-cyclic codes, the Gröbner basis approach gives straightforward techniques to compute the desired properties in a methodical, consistent way and, as such, it is highly preferable. Moreover:

- the notation of RGB generating set (the image of the Gröbner basis in to $\mathbb{F}_q[x]/(x^m + 1)$) is more meaningful that of "generators" in classical sense, since for example there is no obvious way to get the dimension of "1-generator" codes from the classical generator (instead it is straightforward with an RGB generating set). It is also easy to classify and count quasi-cyclic codes with some given parameters using RGB generating sets.
- Decades of research on cyclic codes have shown the huge importance of their generator polynomials, that allow for example very good bounds on the distance (starting from polynomial roots, [1], [19], [25]); although similar results are still lacking for quasi-cyclic codes, we think that Gröbner bases for a quasi-cyclic code may play the same role as generator polynomials for cyclic codes (and there are partial results providing an extension of the BCH bound to quasi-cyclic codes), and that it will become clear as researchers in the field will become familiar with this (still recent) point of view.

2.4. **Bresnan codes.** In this subsection we recall the Bresnan codes and their properties, that have been introduced and investigated in [30].

Definition 2.4. ([30]) Let α, m be positive integers such that $\alpha \geq 4, m \geq 3$. We denote by $\mathcal{H}_{m,\alpha}$ the class of the $(m\alpha \times 2m\alpha)$ matrices of

the form

$$H = \left[\begin{array}{ccccc|ccccc} H_1^1 & 0 & \dots & 0 & I & H_1^2 & I & 0 & \dots & 0 \\ I & H_2^1 & 0 & \dots & 0 & 0 & H_2^2 & I & & \vdots \\ 0 & I & \ddots & \ddots & \vdots & \vdots & 0 & \ddots & \ddots & 0 \\ \vdots & & \ddots & \ddots & 0 & 0 & & \ddots & \ddots & I \\ 0 & \dots & 0 & I & H_\alpha^1 & I & 0 & \dots & 0 & H_\alpha^2 \end{array}\right],$$

where every H_h^i, with $i \in \{1,2\}$ and $h \in \{1,2,..,\alpha\}$, is an $m \times m$ binary weight-2 circulant matrix. We denote by p_h^i the polynomial of H_h^i.

A code with a parity-check matrix $H \in \mathcal{H}_{m,\alpha}$ will be called from now on a "Bresnan code". Given a Bresnan code, the following condition is important in our context:

$$\gcd(x^m + 1, 1 + \prod_{1 \le h \le 4} p_h^1) = 1. \tag{2.2}$$

In [30] three main results for the Bresnan codes have been found:

- Theorem 7.35 [30] provides necessary and sufficient conditions on a Bresnan code to have girth $g \ge 8$;
- Theorem 7.2 [30] shows the Gröbner basis of dual codes for Bresnan codes under condition (2.2); this result is generalized in the present paper (Theorem 3.1);
- Corollary 7.3 [30] gives the dimension of the Bresnan codes, under the hypotheses of Theorem 7.2 [30]; this will be generalized in the present paper (Corollary 3.1).

For comparison, we recall:

Corollary 2.1. (Corollary 7.3 [30]) *Let m be a positive integer such that $m \ge 3$. Let H be in $\mathcal{H}_{m,4}$. Let C be the Bresnan code admitting H as a parity-check matrix. If condition (2.2) holds, then the dimension of C is $k = 4m$ (and hence it is a code with rate $1/2$).*

3. A class of quasi-cyclic LDPC codes

In this section we propose a new family of quasi-cyclic LDPC codes.

Definition 3.1. Let α, m be positive integers such that $\alpha \ge 4$, $m \ge 3$. Let $2 \le i \le \alpha$. We denote by $\mathcal{H}^{i,\alpha,m}$ the family of all binary matrices of

type

$$\begin{bmatrix}
H_1^i & 0 & \dots & \dots & \dots & \dots & \dots & 0 & I_1^i & 0 & \dots & \dots & 0 \\
0 & H_2^i & 0 & \dots & \dots & \dots & \dots & \dots & 0 & I_2^i & 0 & \dots & 0 \\
\vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\
\vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & 0 \\
0 & \ddots & \ddots & \ddots & H_{\alpha-i+1}^i & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & I_{\alpha-i+1}^i \\
I_{\alpha-i+2}^i & \ddots & \ddots & \ddots & \ddots & H_{\alpha-i+2}^i & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & 0 \\
0 & I_{\alpha-i+3}^i & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\
\vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\
\vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\
\vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\
\vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\
\vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & 0 \\
0 & \dots & \dots & \dots & \dots & \dots & 0 & I_\alpha^i & 0 & \dots & \dots & 0 & H_\alpha^i
\end{bmatrix},$$

where

- H_h^i, with $h \in \{1, \dots \alpha\}$, is an $m \times m$ binary weight-2 circulant matrix,
- I_h^i, with $h \in \{1, \dots \alpha\}$, is the $m \times m$ identity matrix,
- sub-matrix I_1^i is in position $(1, i)$ and the others shift consecutively on the right.

We denote by p_h^i the polynomial of H_h^i.

Remark 3.1. In previous definition we adopted notation "I_h^i" to denote the (same) $m \times m$ identity matrix, but in different positions. It would be more usual to denote it simply by "I", but we choose this notation because the location of those matrices is of utmost importance in our context.

Definition 3.2. Let α, m, l be positive integers such that $\alpha \geq 4$, $m \geq 3$ and $2 \leq l \leq \alpha - 1$. Let $S = \{s_1, \dots, s_l\}$ be any l-element sub-set of $\{2, \dots \alpha\}$ s.t. $s_1 = \alpha$. We denote by $\mathcal{B}_{m,\alpha,S}$ the set of all matrices of kind

$$\left[\ A_{s_1} \,\middle|\, \dots \,\middle|\, A_{s_l}\ \right], \tag{3.1}$$

with $A_{s_j} \in \mathcal{H}^{s_j,\alpha,m}$.

Observe that any matrix in $\mathcal{B}_{m,\alpha,S}$ can be a parity-check matrix for a quasi-cyclic LDPC code. These codes are the object of our present study. The Bresnan codes form a sub-class of our codes, since clearly

$$\mathcal{H}_{m,\alpha} = \mathcal{B}_{m,\alpha,\{\alpha,2\}}\,.$$

The next definition is essential to describe the Gröbner basis of the dual codes of our codes.

Definition 3.3. Let α, m be positive integers such that $\alpha \geq 4$, $m \geq 3$. Let $S = \{s_1, s_2, \ldots, s_l\} \subset \{2, \ldots, \alpha\}$, with $s_1 = \alpha$. Let B be in $\mathcal{B}_{m,\alpha,S}$ of type $B = [A_{s_1}|\ldots|A_{s_l}]$. Let $p_h^{s_j}$ be the polynomial of $H_h^{s_j}$ in A_{s_j}, for $s_j \in S$ and $h = 1, \ldots, \alpha$. For any $0 \leq k \leq \alpha$, we define the following polynomials:

$$\mathbb{P}_k(B) = \begin{cases} \prod_{h=1}^{k} p_h^{\alpha} & \text{if } k \neq 0 \\ 1 & \text{if } k = 0, \end{cases} \tag{3.2}$$

$$\mathbb{S}_k^{s_j}(B) = \begin{cases} 0 & if \quad k = 0 \\ \mathbb{P}_{k-s_j+\alpha} + p_k^{s_j}\,\mathbb{P}_{k-1} & if \quad 1 \leq k \leq s_j \\ \mathbb{P}_{k-s_j} + p_k^{s_j}\,\mathbb{P}_{k-1} & if \quad k > s_j. \end{cases} \tag{3.3}$$

When B is understood we will shorten $\mathbb{P}_k(B)$ and $\mathbb{S}_k^{s_j}(B)$ to $\mathbb{P}_k$ and $\mathbb{S}_k^{s_j}$, respectively. Given B in $\mathcal{B}_{m,\alpha,S}$, the following condition is important in our context:

$$\gcd(1 + \mathbb{P}_\alpha, x^m + 1) = 1. \tag{3.4}$$

The next theorem is our main result and describes completely the Gröbner basis of dual codes of our codes (under condition (3.4)).

Theorem 3.1. *Let α, m be positive integers such that $\alpha \geq 4$, $m \geq 3$. Let $S = \{s_1, s_2, \ldots, s_l\} \subset \{2, \ldots, \alpha\}$, with $s_1 = \alpha$. Let B be in $\mathcal{B}_{m,\alpha,S}$, $B = [A_{s_1}|\ldots|A_{s_l}]$. Let C be the code with parity-check matrix B. Let D be the dual code of C. Let $p_h^{s_j}$ be as in Definition 3.1. Suppose that (3.4) holds and let*

$$\mu,\ \lambda \in \mathbb{Z}_2[x] \quad s.t. \quad \mu(1 + \mathbb{P}_\alpha) + \lambda(x^m + 1) = 1. \tag{3.5}$$

Then the reduced Gröbner basis G of D w.r.t. POT ordering is:

$$\begin{bmatrix} \tilde{E}_{s_1} & \tilde{E}_{s_2} & \dots & \dots & \dots & \tilde{E}_{s_l} \\ 0 & M & 0 & \dots & \dots & 0 \\ \vdots & 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & 0 \\ 0 & \dots & \dots & \dots & 0 & M \end{bmatrix}, \tag{3.6}$$

where

- *$\tilde{E}_{s_1} = \tilde{E}_\alpha$ is an $\alpha \times \alpha$ matrix that has the main diagonal composed of 1's, the second main superior diagonal composed of p_h^α, $h = 2, \dots, \alpha$ and any other entry is zero, as follows:*

$$\begin{bmatrix} 1 & p_2^\alpha & 0 & \dots & \dots & \dots & 0 \\ 0 & 1 & p_3^\alpha & 0 & \ddots & \ddots & \vdots \\ \vdots & 0 & 1 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & p_\alpha^\alpha \\ 0 & \dots & \dots & \dots & \dots & 0 & 1 \end{bmatrix},$$

- *$\tilde{E}_{s_j}$, for $j = 2, \dots, l$, is the following $\alpha \times \alpha$ matrix:*

$$
\begin{bmatrix}
0 & p_2^{s_j} & 0 & \dots & \dots & \dots & \dots & \dots & 0 & \overset{\overset{s_j+1}{\downarrow}}{1} & 0 & \dots & 0 \\
\vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\
\vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & 0 \\
0 & \ddots & \ddots & \ddots & p_{\alpha-s_j+1}^{s_j} & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & 1 \\
1 & \ddots & \ddots & \ddots & \ddots & p_{\alpha-s_j+2}^{s_j} & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & 0 \\
0 & 1 & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\
\vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\
\vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\
\vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\
\vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\
\vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & 0 \\
0 & \dots & \dots & \dots & \dots & \dots & 0 & 1 & 0 & \dots & \dots & 0 & p_\alpha^{s_j} \\
\mu\mathbb{S}_1^{s_j} & \mu\mathbb{S}_2^{s_j} & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \mu\mathbb{S}_\alpha^{s_j}
\end{bmatrix},
$$

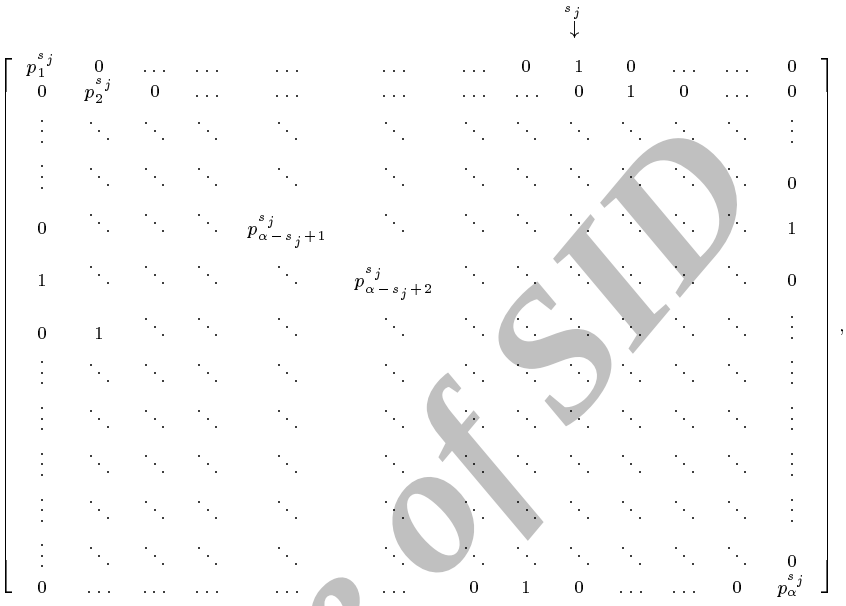
- *M is the diagonal $\alpha \times \alpha$ matrix with polynomial x^m+1 on the (main) diagonal:*

$$
\begin{bmatrix}
x^m+1 & 0 & \dots & \dots & 0 \\
0 & \ddots & \ddots & \ddots & \vdots \\
\vdots & \ddots & \ddots & \ddots & \vdots \\
\vdots & \ddots & \ddots & \ddots & 0 \\
0 & \dots & \dots & 0 & x^m+1
\end{bmatrix}.
$$

Proof. We start from a basis (3.7) for the $\mathbb{Z}_2[x]$ sub-module $\tilde{\mathrm{D}}$ in $(\mathbb{Z}_2[x])^{l\alpha}$, obtained from matrix B plus the generators of $\tilde{\mathcal{K}}$ (see 2.3)

$$
\begin{bmatrix}
E_{s_1} & E_{s_2} & \dots & \dots & E_{s_l} \\
M & 0 & \dots & \dots & 0 \\
0 & M & 0 & \dots & \vdots \\
\vdots & \ddots & \ddots & \ddots & \vdots \\
\vdots & \ddots & \ddots & \ddots & 0 \\
0 & 0 & \dots & 0 & M
\end{bmatrix}. \tag{3.7}
$$

Clearly, E_{s_j} is (we recall $s_1 = \alpha$) as follows



where in the first row polynomial 1 is in position $(1, s_j)$ and in the last row (the α-th) polynomial 1 is in position $(\alpha, s_j - 1)$.

We will denote by $\mathbf{r}_1$ the first row vector of (3.7), by $\mathbf{r}_2$ the second and so on. Note that the length of any vector $\mathbf{r}_k$ is $l\alpha$. We will perform some operations on (3.7), but we will rename the rows accordingly. For example, if we swap row $\mathbf{r_i}$ and row $\mathbf{r_j}$, after the operation we will refer to the old row $\mathbf{r_j}$ as to "row $\mathbf{r_i}$".

We insert the first row between the α-th and the $(\alpha+1)$-th row. The matrix E_{s_j} becomes E'_{s_j}:

$$\begin{array}{c} \hspace{9em}\overset{s_j+1}{\downarrow} \\ \left[\begin{array}{ccccccccccccc}
0 & p_2^{s_j} & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & 0 & 1 & 0 & \cdots & 0 \\
\vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\
\vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & 0 \\
0 & \ddots & \ddots & \ddots & p_{\alpha-s_j+1}^{s_j} & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & 1 \\
1 & \ddots & \ddots & \ddots & \ddots & p_{\alpha-s_j+2}^{s_j} & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & 0 \\
0 & 1 & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\
\vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\
\vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\
\vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\
\vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\
\vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & 0 \\
0 & \cdots & \cdots & \cdots & \cdots & \cdots & 0 & 1 & 0 & \cdots & \cdots & 0 & p_\alpha^{s_j} \\
p_1^{s_j} & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & 0 & 1 & 0 & \cdots & \cdots & 0
\end{array}\right], \end{array}$$

and, in particular, $E_{s_1} = E_\alpha$ is now E'_{s_1}:

$$\left[\begin{array}{cccccc}
1 & p_2^\alpha & 0 & \cdots & \cdots & 0 \\
0 & 1 & p_3^\alpha & 0 & \cdots & 0 \\
\vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\
\vdots & \ddots & \ddots & \ddots & \ddots & 0 \\
0 & \ddots & \ddots & 0 & 1 & p_\alpha^\alpha \\
p_1^\alpha & 0 & \cdots & \cdots & 0 & 1
\end{array}\right].$$

The Buchberger algorithm w.r.t. POT in this case reduces to row reductions. It is not difficult to see that performing the first α reductions is equivalent to the following operation:

$$\mathbf{r}_\alpha \to \mathbf{r}_\alpha + \sum_{i=1}^{\alpha-1} \mathbb{P}_i \mathbf{r}_\mathbf{i}, \tag{3.8}$$

where $\mathbb{P}_i$ is as in Definition 3.3.
To show what happens, for the moment we consider only the first α columns of our matrix. We will use a prime to denote the matrix rows truncated to the first α columns.

We have:

$$
\begin{array}{lcccccccccccc}
\mathbf{r}_1'\mathbb{P}_1 & \to (& \mathbb{P}_1 & p_2^\alpha\mathbb{P}_1 & 0 & \dots & \dots & \dots & \dots & \dots & 0 &)+ \\
\mathbf{r}_2'\mathbb{P}_2 & \to (& 0 & \mathbb{P}_2 & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & 0 &)+ \\
\vdots & & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots & \vdots \\
\mathbf{r}_{k-1}'\mathbb{P}_k & \to (& 0 & \ddots & \ddots & \ddots & p_k^\alpha\mathbb{P}_{k-1} & 0 & \dots & \dots & 0 &)+ \\
\mathbf{r}_k'\mathbb{P}_k & \to (& 0 & \ddots & \ddots & 0 & \mathbb{P}_k & p_{k+1}^\alpha\mathbb{P}_k & 0 & \dots & 0 &)+ \\
\vdots & & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots & \vdots \\
\vdots & & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & 0 & \vdots \\
\mathbf{r}_{\alpha-1}'\mathbb{P}_{\alpha-1} & \to (& 0 & \dots & \dots & 0 & 0 & \dots & \dots & \mathbb{P}_{\alpha-1} & p_\alpha^\alpha\mathbb{P}_{\alpha-1} &)+ \\
\mathbf{r}_\alpha' & \to (& p_1^\alpha & 0 & \dots & 0 & 0 & \dots & \dots & 0 & 1 &) = \\
\mathbf{r}_\alpha' & \to (& 0 & 0 & \dots & 0 & 0 & \dots & \dots & 0 & 1+\mathbb{P}_\alpha &),
\end{array}
$$

where we have used the obvious facts that

$$p_k^\alpha\mathbb{P}_{k-1} = \mathbb{P}_k,\ 1 \le k \le \alpha, \quad \text{and} \quad \mathbb{P}_1 = p_1^\alpha.$$

At this stage, row vector $\mathbf{r}_\alpha{}'$ has all components equal to 0, except for the α-th which is equal to $1+\mathbb{P}_\alpha$.

Using hypothesis (3.5) we can perform the following substitutions

$$\mathbf{r}_\alpha \to \mu\mathbf{r}_\alpha + \lambda\mathbf{r}_{2\alpha}, \tag{3.9}$$

$$\mathbf{r}_{2\alpha} \to (1+\mathbb{P}_\alpha)\mathbf{r}_{2\alpha} + (x^m+1)\mathbf{r}_\alpha. \tag{3.10}$$

The effects on the first α columns of operations (3.9) and (3.10) are respectively:

$$
\begin{array}{rcccccccc}
\mu\mathbf{r}_\alpha{}' & \to & (& 0 & \dots & \dots & 0 & \mu(1+\mathbb{P}_\alpha) &) + \\
\lambda\mathbf{r_2}_\alpha{}' & \to & (& 0 & \dots & \dots & 0 & \lambda(x^m+1) &) = \\
\hline
\mathbf{r}_\alpha{}' & \to & (& 0 & \dots & \dots & 0 & 1 &)
\end{array}
$$

$$
\begin{array}{rcccccccc}
(1+\mathbb{P}_\alpha)\mathbf{r}_{2\alpha}' & \to & (& 0 & \dots & \dots & 0 & (1+\mathbb{P}_\alpha)(x^m+1) &) + \\
(x^m+1)\mathbf{r}_\alpha' & \to & (& 0 & \dots & \dots & 0 & x^m+1 &) = \\
\hline
\mathbf{r}_{2\alpha}' & \to & (& 0 & \dots & \dots & 0 & (x^m+1)\mathbb{P}_\alpha &).
\end{array}
$$

These substitutions leave the module invariant, because the determinant of matrix

$$\begin{bmatrix} \mu & \lambda \\ x^m+1 & 1+\mathbb{P}_\alpha \end{bmatrix}$$

is equal to 1 by (3.5).

In this way the top left $\alpha\times\alpha$ minor has the main diagonal composed by 1's and the second superior diagonal composed by p_h^α with $h = 2, \dots, \alpha$, i.e. the top left $\alpha \times \alpha$ minor is actually $\tilde{E}_{s_1} = \tilde{E}_\alpha$.

We now want to eliminate rows $\mathbf{r}_{\alpha+j}$, $j = 1, \ldots, \alpha$. We first perform

$$\mathbf{r}_{\alpha+j} \to \mathbf{r}_{\alpha+j} + (x^m + 1)\mathbf{r}_j \,, \quad \text{for} \quad 1 \le j \le \alpha \,,$$

so that, for any $j = 1, \ldots, \alpha$, we have

$$\mathbf{r}_{\alpha+j} = \big(0, \ldots, 0, \underset{\substack{\uparrow \\ j+1}}{(x^m + 1)(*)}, \ldots, \underset{\substack{\uparrow \\ l\alpha}}{(x^m + 1)(*)}\big) \,,$$

where $*$ stands for any polynomial in $\mathbb{Z}_2[x]$. But it is obvious that, for any $1 \le j \le \alpha$, $\mathbf{r}_{\alpha+j}$ may be reduced to the zero vector, via reduction w.r.t. the remaining basis vectors

$$\{\mathbf{r}_{\alpha+j+i} \mid \alpha + j + i \le l\alpha, 1 \le i\} \,.$$

We come back to operations (3.8) and (3.9) to see their effect on all columns. They transform E'_{s_j} in $\overline{E}_{s_j}$ as follows:

$$\left[\begin{array}{ccccccccccccc}
0 & p_2^{s_j} & 0 & \ldots & \ldots & \ldots & \ldots & \ldots & 0 & \overset{\substack{s_j+1 \\ \downarrow}}{1} & 0 & \ldots & 0 \\
\vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\
\vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & 0 \\
0 & \ddots & \ddots & \ddots & p^{s_j}_{\alpha-s_j+1} & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & 1 \\
1 & \ddots & \ddots & \ddots & \ddots & p^{s_j}_{\alpha-s_j+2} & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & 0 \\
0 & 1 & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\
\vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\
\vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\
\vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\
\vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\
\vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & 0 \\
0 & \ldots & \ldots & \ldots & \ldots & \ldots & 0 & 1 & 0 & \ldots & \ldots & 0 & p_\alpha^{s_j} \\
* & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & *
\end{array}\right],$$

where $*$ means, as usual, a generic polynomial in $\mathbb{Z}_2[x]$.

Since clearly any further row reduction will not affect the first α rows, we may safely deduce (Theorem 2.1) that the reduced Gröbner basis will be

$$\left[\begin{array}{cccccc}
\tilde{E}_{s_1} & \overline{E}_{s_2} & \ldots & \ldots & \ldots & \overline{E}_{s_l} \\
0 & \overline{M}_2 & \# & \ldots & \ldots & \# \\
\vdots & 0 & \overline{M}_3 & \ddots & \ddots & \vdots \\
\vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\
\vdots & \ddots & \ddots & \ddots & \ddots & \# \\
0 & \ldots & \ldots & \ldots & 0 & \overline{M}_l
\end{array}\right],$$

where # stands for any $\alpha \times \alpha$ matrix over $\mathbb{Z}_2[x]$ and $\overline{M}_j$ stands for any $\alpha \times \alpha$ upper-triangular matrix of type

$$\begin{bmatrix} g_{(j-1)\alpha+1} & * & \dots & \dots & \dots & * \\ 0 & g_{(j-1)\alpha+2} & * & \dots & \dots & \vdots \\ \vdots & 0 & g_{(j-1)\alpha+3} & \ddots & \ddots & \vdots \\ \vdots & \ddots & 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & * \\ 0 & \dots & \dots & \dots & 0 & g_{j\alpha} \end{bmatrix},$$

for some $g_k \in \mathbb{Z}_2[x]$, with $\alpha+1 \le k \le l\alpha$, s.t. either $\deg(g_k) \le m-1$ or $g_k = x^m + 1$. In the latter case the k-th row is

$$(0, \dots, 0, x^m + 1, 0, \dots, 0)$$

where $x^m + 1$ is in position k.
The dimension of D is then (Theorem 2.2)

$$\dim(D) = \left[\alpha m + \sum_{k=\alpha+1}^{\alpha l} (m - \deg(g_k)) \right] \ge \alpha m \tag{3.11}$$

but its generator matrix B has αm rows, so that

$$\dim(D) \le \alpha m. \tag{3.12}$$

From (3.11) and (3.12) we see that

$$\dim(D) = \alpha m \quad \text{and} \quad \deg(g_k) = m, \quad k = \alpha+1, \dots, \alpha l,$$

and hence

$$g_k = x^m + 1, \quad k = \alpha+1, \dots, \alpha l\,.$$

As a consequence, our basis must have the following shape:

$$\begin{bmatrix} \tilde{E}_{s_1} & \overline{E}_{s_2} & \dots & \dots & \dots & \overline{E}_{s_l} \\ 0 & M & 0 & \dots & \dots & 0 \\ 0 & 0 & M & \dots & \dots & 0 \\ 0 & \dots & \vdots & \ddots & 0 & 0 \\ 0 & \dots & \vdots & \ddots & \ddots & 0 \\ 0 & \dots & \dots & \dots & 0 & M \end{bmatrix}, \tag{3.13}$$

for some $\overline{E}_{s_2}, \dots, \overline{E}_{s_l}$.

We now consider the remaining $\alpha(l-1)$ columns of the first α rows, i.e. matrices $\{\overline{E}_{s_2}, \ldots, \overline{E}_{s_l}\}$. We want to determine what happens performing reduction operations (3.8) and (3.9) on E'_{s_j} $(2 \leq j \leq l)$. Matrix E'_{s_j} has α columns and in any column (say the k-th) there are only two row positions that have a non zero-value, one containing 1 (position $h_k^{s_j}$) and another containing $p_k^{s_j}$ (position $l_k^{s_j}$). By circularity, we have

$$h_k^{s_j} = \begin{cases} k - s_j + \alpha & \text{if} \quad k \leq s_j \\ k - s_j & \text{if} \quad k > s_j, \end{cases} \qquad l_k^{s_j} = \begin{cases} k-1 & \text{if} \quad k \neq 1 \\ \alpha & \text{if} \quad k = 1. \end{cases}$$

Performing operation (3.8) we obtain in position (α, k) the polynomial given by the sum of just two addenda:

$$\mathbb{P}_{l_k^{s_j}} = \mathbb{P}_{k-1} p_k^{s_j} \quad \text{and} \quad \mathbb{P}_{h_k^{s_j}}.$$

The sum of these two polynomials is exactly polynomial $\mathbb{S}_k^{s_j}$ (Definition 3.3),

$$\mathbb{S}_k^{s_j} = \mathbb{P}_{k-1} p_k^{s_j} + \mathbb{P}_{h_k^{s_j}} = \begin{cases} \mathbb{P}_{k-1} p_k^{s_j} + \mathbb{P}_{\alpha - s_j + k} & \text{if} \quad 1 \leq k \leq s_j \\ \mathbb{P}_{k-1} p_k^{s_j} + \mathbb{P}_{k-s_j} & \text{if} \quad s_j < k \leq \alpha. \end{cases}$$

Performing operation (3.9) we multiply each $\mathbb{S}_k^{s_j}$ by μ and we add it to a vector that has only a non-zero component, i.e. the α-th. All the other reduction operations do not touch the α-th row so that it is:

$$(0, 0, \ldots, 0, 1, \mu\mathbb{S}_1^{s_2}, \ldots, \mu\mathbb{S}_\alpha^{s_2}, \cdots, \mu\mathbb{S}_1^{s_l}, \ldots, \mu\mathbb{S}_\alpha^{s_l}). \tag{3.14}$$

Then the α-th row of any $\overline{E}_{s_j}$ is given by

$$\left(\mu\mathbb{S}_1^{s_j}, \mu\mathbb{S}_2^{s_j}, \ldots, \mu\mathbb{S}_\alpha^{s_j}\right), \tag{3.15}$$

In other words, our basis (3.13) has become exactly (3.6). From Theorem 3.1 it is immediate to determine the dimension of our codes.

Corollary 3.1. *Let α, m be positive integers such that $\alpha \geq 4$, $m \geq 3$. Let $S = \{s_1, \ldots, s_l\} \subset \{2, \ldots, \alpha\}$ with $s_1 = \alpha$. Let B be in $\mathcal{B}_{m,\alpha,S}$, $B = [A_{s_1}|\ldots|A_{s_l}]$. Let $\mathbb{C}$ be the code with parity-check matrix B. Let p_h^i be as in Definition 3.1. If (3.4) holds then the dimension of C is $\alpha m(l-1)$ and its rate is $\frac{l-1}{l}$.*

Proof. The dimension k' of the dual code D of C follows directly from Theorem 3.1 and Theorem 2.2: $k' = \alpha m$. The length n of both codes is

$n = l\alpha m$. Then the dimension of C is $k = n - k' = (l-1)\alpha m$ and the rate is

$$\frac{k}{n} = \frac{(l-1)\alpha m}{l\alpha m} = \frac{l-1}{l}.$$

Remark 3.2. Condition (3.4) deserves some considerations.

First of all, observe that $1 + x$ is always a factor of $x^m + 1$. But $\mathbb{P}_\alpha$ is the product of α 2-weight polynomials and hence it is always 0 in 1. As a consequence, $1 + \mathbb{P}_\alpha$ is always 1 in 1 and hence $1 + x$ never divides $1 + \mathbb{P}_\alpha$. In particular, if $m = 2^r$ for some r, then $x^m + 1 = (x + 1)^m$ and condition (3.4) is always satisfied. These values of m are very important for implementation issues and rarely other values are used.

It is well-known that the probability that two random polynomials over $\mathbb{Z}_2$ have a common factor is slightly more than 1/2 [22]. If, as a first approximation, we assume $1 + \mathbb{P}_\alpha$ and $x^m + 1$ as two random polynomials, condition (3.4) is satisfied for (slightly) more than 50% of cases. Even if there is no apparent limitation on the factorization of $1 + \mathbb{P}_\alpha$ (apart from what discussed previously), the factorization of $x^m + 1$ is special and deeply studied. The worst case for us is when m is of the form $m = 2^r - 1$ for some r, the best case for us is when m is a prime, since in the former there are many factors of small degree (more likely to divide a generic polynomial), and in the latter there are only a few factors, mostly with high degree (unlikely to divide a generic polynomial).

In conclusion, there are many values of m that can be chosen in order to maximize the probability that condition (3.4) holds and so in previous papers we have referred to this condition as a "non-restrictive" hypothesis (since we are free to construct our codes as we like).

4. Conclusions and further research

The codes introduced by R. Bresnan are interesting, both from a mathematical point of view and from an engineering point of view. In this paper we have generalized his construction to $\frac{l-1}{l}$-rate codes, improving on previous results ([6], [31]). With the Bresnan codes, the codes so obtained share similar dimension properties and the same ease of implementation ([32]). Although we believe they share also similar girth conditions, this issue is still under active investigation.

Acknowledgments

The first two authors would like to thank the third author (their supervisor). The authors would like to thank P. Fitzpatrick and C. Traverso, for many useful comments and discussions. The authors wish to thank an anonymous referee, whose comments have greatly improved the paper's presentation.

References

[1] E. Betti, M. Sala, A new bound for the minimum distance of a cyclic code from its defining set, *IEEE Trans. on Inf. Th.* **52** (8) (2006), 3700-3706.

[2] R. Bresnan, *Novel code construction and decoding techniques for LDPC codes*, Master's thesis, Dept. of Elec. Eng., UCC Cork, 2004.

[3] C. L. Chen, W. W. Peterson and E. J. Weldon, Jr., Some results on quasi-cyclic Codes, *Inform. Contr.* **15** (1969), 407-423.

[4] S.-Y. Chung, G. D. Forney, T. J. Richardson, and R. Urbanke, On the design of low-density parity-check codes within 0.0045 dB of the Shannon limit, *IEEE Comm. Lett.* **5** (2) (2001), 58-60.

[5] R. G. Gallager, *Low-Density Parity-Check Codes*, PhD thesis, Dept. of Elec. Eng., M.I.T., 1963.

[6] M. Giorgetti, M. Sala, On the Groebner basis of a family of quasi-cyclic LDPC codes, *poster presented at CoCOA summer school*, 2005.

[7] X. Y. Hu, E. Eleftheriou, D. M. Arnold, and A. Dholakia, Efficient implementations of the sum-product algorithm for decoding LDPC codes, *GLOBECOM, The Evolving Global Communications Network*, San Antonio, Texas, 2001.

[8] S. J. Johnson and S. R. Weller, Quasi-cyclic LDPC codes from difference families, *Australian Communications Theory Workshop*, Canberra, Australia, 2002, 18-22.

[9] S. J. Johnson and S. R. Weller, A family of irregular LDPC codes with low encoding complexity, *IEEE Comm. Lett.* **7** (2) (2003), 79-81.

[10] S. J. Johnson and S. R. Weller, Codes for iterative decoding from partial geometries, *IEEE Trans. on Comm.* **52** (2) (2004), 236-243.

[11] M. Karlin, New binary coding results by circulants, *IEEE Trans. an Inf. Th.* **15** (1) (1969), 81-92.

[12] M. Karlin, Decoding of circulant codes, *IEEE Trans. on Inf. Th.* **16** (6) (1970), 797-802.

[13] J.-L. Kim, U. N. Peled, I. Perepelitsa, V. Pless, and S. Friedland, Explicit construction of families of LDPC codes with no 4-cycles, *IEEE Trans. on Inf. Th.* **50** (10) (2004), 2378-2388.

[14] Y. Kou, S. Lin, and M. P. C. Fossorier, Low-density parity-check codes based on finite geometries: A rediscovery and new results, *IEEE Trans. on Inf. Th.* **47** (7) (2001), 2711-2736.

[15] Y. Kou, J. Xu, H. Tang, S. Lin, and K. Abdel-Ghaffar, On circulant low density parity-check codes, *IEEE ISIT*, Lausanne, Switzerland, 2002, p. 200.

[16] K. Lally and P. Fitzpatrick, Algebraic structure of quasi-cyclic codes, *Discr. Appl. Math.* **111** (1-2) (2001), 157–175.

[17] K. Lally and P. Fitzpatrick, Construction and classification of quasi-cyclic codes, *Proc. WCC*, INRIA, Paris, 1999, 11–20.
[18] D. J. C. MacKay and R. M. Neal, Good codes based on very sparse matrices, *Cryptography and Coding*, 5th IMA Conference, 1995.
[19] F. J. MacWilliams, N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North Holland, 1977.
[20] Y. Mao and A. H. Banihashemi, Decoding low-density parity-check codes with probabilistic scheduling, *IEEE Trans. on Inf. Th.* **5** (10) (2001), 414–416.
[21] Y. Mao and A. H. Banihashemi, A heuristic search for good low-density parity-check codes at short block lengths, *IEEE ICC2001*, Helsinki, Finland, 2001.
[22] K. E. Morrison, Random Polynomial over Finite Field, preprint, available at `www.calpoly.edu/~kmorriso`, 1999.
[23] E. Orsini, *Construction of a family of LDPC Goppa codes*, Master's thesis MAMI, Dept. of Math., Univ. of Milan-Bicocca, 2004.
[24] M. O'Sullivan, Algebraic Construction of Sparse Graphs with Large Girth, *BCRI Workshop on Coding and Cryptography*, 2005.
[25] W. W. Peterson, E. J. Weldon, Jr., *Error Correcting Codes*, MIT Press, 1972.
[26] T. J. Richardson, M. A. Shokrollahi, and R. L. Urbanke, Design of capacity-approaching irregular low-density parity-check codes, *IEEE Trans. on Inf. Th.* **47** (2) (2001), 619–637.
[27] T. J. Richardson and R. L. Urbanke, The capacity of low-density parity-check codes under message passing decoding, *IEEE Trans. on Inf. Th.* **47** (2) (2001), 599–618.
[28] T. J. Richardson and R. L. Urbanke, Efficient encoding of low-density parity-check codes, *IEEE Trans. on Inf. Th.* **47** (2) (2001), 638–656.
[29] J. Rosenthal, P. O. Vontobel, Construction of LDPC Codes using Ramanujan Graphs and Ideas from Margulis, *Proc. of Allerton Conf. on Comm., Con. and Comp.*, 2000, 248-257.
[30] M. Rossi, M. Sala, On a class of quasi-cyclic LDPC codes, BCRI preprint, available at `www.bcri.ucc.ie`, 2005.
[31] M. Rossi, M. Sala, On a class of quasi-cyclic LDPC codes, MEGA05, Alghero, Italy, 2005.
[32] C. Spagnol, E. M. Popovici, W. P. Marnane, Reduced complexity,FPGA implementation of quasi-cyclic LDPC decoder, ECCTD2005, Cork, 2005.
[33] R. M. Tanner, D. Sridhara, and T. Fuja, A class of group-structured LDPC codes, *ISCTA 2001*, Ambleside, England, 2001.
[34] R. M. Tanner, A recursive approach to low complexity codes, *IEEE Trans. on Inf. Th.* **27** (5) (1981), 533547.
[35] T. Tian, C. Jones, J. D. Villasenor, and R. D. Wesel, Construction of irregular LDPC codes with low error floors, *IEEE International Conference on Communications (ICC 2003)*, vol. 5, Anchorage, Alaska, 2003, 3125–3129.
[36] T. Tian, C. Jones, J. D. Villasenor, and R. D. Wesel, Selective avoidance of cycles in irregular LDPC codes construction, *IEEE Trans. on Comm.* **52** (8) (2004), 1242 - 1247.
[37] http://rimula.hkr.se/∼chen/research/codes/searchqc2.htm.

Marta Giorgetti
Department of Mathematics
University of Milan
Italy
e-mail:giorge@mat.unimi.it

Marta Rossi
Department of Mathematics and Applications
University of Milan-Bicocca
Italy
e-mail:marta.rossi@posso.dm.unipi.it

Massimiliano Sala
Boole Centre for Research in Informatics
UCC Cork
Ireland
e-mail:msala@bcri.ucc.ie