www.ietdl.org

Published in IET Communications
Received on 27th October 2011
Revised on 12th March 2012
doi: 10.1049/iet-com.2011.0791

ISSN 1751-8628

Approach to the construction of regular low-density parity-check codes from group permutation matrices

R. Sobhani

Department of Mathematics, University of Isfahan, 81746-73441 Isfahan, Iran
E-mail: r.sobhani@sci.ui.ac.ir

Abstract: In this study, a new method for constructing low-density parity-check (LDPC) codes is presented. This construction is based on permutation matrices which come from a finite abstract group and hence the codes constructed in this manner are called group permutation low-density parity-check (GP-LDPC) codes. A necessary and sufficient condition under which a GP-LDPC code has a cycle is given and some properties of these codes are investigated. A class of flexible-rate GP-LDPC codes without cycles of length four is also introduced. Simulation results show that GP-LDPC codes perform very well with the iterative decoding and can outperform their random-like counterparts.

1 Introduction

Recently, there is much interest in the class of low-density parity-check (LDPC) codes, since for sufficiently large lengths, they can achieve near Shannon limit performance with the iterative message-passing decoding [1, 2]. Although the constructed codes in [1, 2] have performance very close to the Shannon limit, their length is too large (10^6 and 10^7) and they have been constructed with random techniques. On the other hand, for many practical applications we need to design well-structured LDPC codes with shorter lengths. In this direction, several algebraic constructions for LDPC codes can be found in the literature. From among these constructions we refer to those given in [3–10, 13–24]. These constructions can be divided into two types. One type is based on finite geometries ([3, 5, 13–19]) and another type, which initially proposed by Gallager [6], is based on circulant matrices [4, 6–10, 20–24].

The LDPC codes obtained from circulant matrices, are (J, L)-regular quasi-cyclic (QC) LDPC codes. Note that a (J, L)-regular LDPC code is one with a parity-check matrix of column weight J and row weight L. It can be deduced from Theorem 2 of [7] that, the minimum distance of these LDPC codes is bounded from above by $(J+1)!$. Consequently, when the column weight is small and the rate is low, any long-length LDPC code obtained from circulant matrices has poor minimum distance. This may cause the occurrence of error floors in the performance curve of these codes. On the other hand, evidences obtained from simulating such codes (when the column weight is three) confirm the existence of long error floors in the performance curve of them (see Fig. 3). Therefore the main disadvantage of LDPC codes obtained from circulant matrices is that, in this class of LDPC codes we cannot design a good long-length low-rate LDPC code of small column weight.

In this paper we introduce a new method based on permutation matrices which come from a finite abstract group, to construct (J, L)-regular LDPC codes. The codes constructed in this manner are called group permutation low-density parity-check (GP-LDPC) codes. When the underlying group is cyclic, the group permutation matrices coincide with circulant matrices and hence this method generalises many of the previous constructions for QC LDPC codes, for example those given [8–10]. More precisely, QC LDPC codes based on circulant matrices are indeed GP-LDPC codes based on cyclic groups.

The main significance of this method is that, based on non-abelian groups, we can design good long-length low-rate GP-LDPC codes of column weight three. Recall that we are not able to construct such codes when we deal with cyclic groups. Also, based on non-abelian groups, we can design GP-LDPC codes of column weight three and various rates, that can outperform their random-like counterparts and QC LDPC codes obtained from circulant matrices (see Section 4). Another advantage of this method is that we can construct GP-LDPC codes with girths greater than 12. Note that, from Theorem 2.5 of [9], the girth of an LDPC code constructed from circulant matrices is bounded from above by 12. Finally, the method enables us to introduce a class of flexible-rate GP-LDPC codes which are free of cycles of length four.

The paper is organised as follows. In Section 2 we introduce our construction method and define a GP-LDPC code. We present a necessary and sufficient condition under which a GP-LDPC code has a cycle and show that when the underlying group is abelian, the girth of a GP-LDPC code is bounded from above by 12 and its minimum distance is bounded from above by $(J+1)!$. Section 3 is devoted to a special case of flexible-rate GP-LDPC codes which are free of four cycles. The performance of some classes of GP-LDPC codes of column weight three on an AWGN channel with iterative message-passing decoding is examined in Section 4. Finally we close the paper with Section 5 which summarises the results and concludes the paper.

2 Construction

In this section, we introduce our construction method and derive some properties of the codes obtained from the method. Assume that $\mathcal{G} = \{g_1, g_2, \ldots, g_n\}$ is a finite abstract group of size n. For $1 \leq t \leq n$, let us define the permutation matrix $\mathcal{I}(g_t)$ to be the $n \times n$ matrix whose (i, j)th element is equal to 1 if $g_j = g_i g_t$ and 0 otherwise. When the group $\mathcal{G}$ is known and $g_j = g_i g_t$ we write $j = p(g_i g_t)$ or equivalently $i = p(g_j g_t^{-1})$. Hence for all $1 \leq i \leq n$ entries $(i, p(g_i g_t))$ of $\mathcal{I}(g_t)$ are 1 and others are 0. Equivalently, for all $1 \leq j \leq n$ the entries $(p(g_j g_t^{-1}), j)$ of $\mathcal{I}(g_t)$ are 1 and others are 0. Now, let $\boldsymbol{H}$ be the following $nJ \times nL$ matrix

$$\boldsymbol{H} := \begin{pmatrix} \mathcal{I}(g_{1,1}) & \mathcal{I}(g_{1,2}) & \cdots & \mathcal{I}(g_{1,L}) \\ \mathcal{I}(g_{2,1}) & \mathcal{I}(g_{2,2}) & \cdots & \mathcal{I}(g_{2,L}) \\ \vdots & & \ddots & \vdots \\ \mathcal{I}(g_{J,1}) & \mathcal{I}(g_{J,2}) & \cdots & \mathcal{I}(g_{J,L}) \end{pmatrix} \tag{1}$$

where $g_{i,j} \in \mathcal{G}$ for $1 \leq i \leq J$ and $1 \leq j \leq L$. The code C associated with the parity-check matrix $\boldsymbol{H}$ is called group-permutation LDPC code and is denoted by GP-LDPC code. Also the $J \times L$ matrix

$$\begin{pmatrix} g_{1,1} & g_{1,2} & \cdots & g_{1,L} \\ g_{2,1} & g_{2,2} & \cdots & g_{2,L} \\ \vdots & & \ddots & \vdots \\ g_{J,1} & g_{J,2} & \cdots & g_{J,L} \end{pmatrix} \tag{2}$$

is called the base group matrix of $\boldsymbol{H}$ and is denoted by BGM($\boldsymbol{H}$).

Example 1: Let $\mathcal{G} = \langle \varepsilon, \rho | \varepsilon^2 = \rho^3 = 1, \varepsilon\rho = \rho^2\varepsilon \rangle$ be the dihedral group of size 6 which is the only non-abelian group of this size and is isomorphic to the symmetric group S_3 consisting of all permutations on three symbols. Assume that, elements of $\mathcal{G}$ are ordered as follows

$$\begin{array}{lll} g_1 := 1 & g_2 := \rho & g_3 := \rho^2 \\ g_4 := \varepsilon & g_5 := \varepsilon\rho & g_6 := \varepsilon\rho^2 \end{array}$$

Clearly $\mathcal{I}(g_1) = \mathcal{I}(1) = \mathcal{I}_6$ is the identity matrix of order 6. To compute the permutation matrix $\mathcal{I}(g_2) = \mathcal{I}(\rho)$ we need to calculate $p(g_i g_2)$, for $1 \leq i \leq 6$. On the other hand, we have

$$\begin{array}{ll} p(g_1 g_2) = p(\rho) = 2 & p(g_2 g_2) = p(\rho^2) = 3 \\ p(g_3 g_2) = p(\rho^3) = p(1) = 1 & p(g_4 g_2) = p(\varepsilon\rho) = 5 \\ p(g_5 g_2) = p(\varepsilon\rho^2) = 6 & p(g_6 g_2) = p(\varepsilon\rho^3) = p(\varepsilon) = 4 \end{array}$$

Now, for $1 \leq i \leq 6$, entries $(i, p(g_i g_2))$ of the permutation matrix $\mathcal{I}(\rho)$ are 1 and the others are 0. Therefore we have

$$\mathcal{I}(\rho) = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

Recall that another way for determining $\mathcal{I}(\rho)$ is to calculate $p(g_j g_2^{-1}) = p(g_j \rho^2)$, for $1 \leq i \leq 6$. In this case, the entries $(p(g_j \rho^2), j)$ of the permutation matrix $\mathcal{I}(\rho)$ are 1 and the others are 0. Anyway, the result would be the same as that obtained previously. Other permutation matrices corresponding to the elements of $\mathcal{G}$ are as follows

$$\mathcal{I}(\rho^2) = \begin{pmatrix} 001 & 000 \\ 100 & 000 \\ 010 & 000 \\ 000 & 001 \\ 000 & 100 \\ 000 & 010 \end{pmatrix}, \quad \mathcal{I}(\varepsilon) = \begin{pmatrix} 000 & 100 \\ 000 & 001 \\ 000 & 010 \\ 100 & 000 \\ 001 & 000 \\ 010 & 000 \end{pmatrix}$$

$$\mathcal{I}(\varepsilon\rho) = \begin{pmatrix} 000 & 010 \\ 000 & 100 \\ 000 & 001 \\ 010 & 000 \\ 100 & 000 \\ 001 & 000 \end{pmatrix}, \quad \mathcal{I}(\varepsilon\rho^2) = \begin{pmatrix} 000 & 001 \\ 000 & 010 \\ 000 & 100 \\ 001 & 000 \\ 010 & 000 \\ 100 & 000 \end{pmatrix}$$

It can be easily seen that when $\mathcal{G} = \langle g \rangle$ is a cyclic group of order n and $g_i = g^i$, then the permutation matrix $\mathcal{I}(g_t)$ is the $n \times n$ circulant permutation matrix $\mathcal{I}(t)$ and the code associated with $\boldsymbol{H}$ will be a QC code. QC LDPC codes of this type have been extensively studied in [8, 9].

Like the QC LDPC codes constructed from circulant permutation matrices, a cycle of length $2v$ in $\boldsymbol{H} = [h_{x,y}]$ is defined by $2v + 1$ positions $h_{x,y} = 1$ such that two consecutive positions are obtained by changing alternatively of row or column only and all positions are distinct, except the first and last ones which are equal. It follows that two consecutive positions in any cycle belong to distinct group permutation matrices which are either in the same row, or in the same column. Hence, a cycle of length $2v$ can be associated with an ordered series of group permutation matrices

$$\mathcal{I}(g_{j_0,l_0}), \mathcal{I}(g_{j_1,l_0}), \mathcal{I}(g_{j_1,l_1}), \ldots, \mathcal{I}(g_{j_{v-1},l_{v-1}}), \mathcal{I}(g_{j_0,l_{v-1}}), \mathcal{I}(g_{j_0,l_0})$$

in which for $1 \leq k \leq v - 1$, $j_k \neq j_{k-1}$ and $l_k \neq l_{k-1}$. Hence, any cycle C of length $2v$ in the Tanner graph of $\boldsymbol{H}$ can be represented by the ordered series

$$(j_0, l_0); (j_1, l_0); (j_1, l_1); (j_1, l_2); \cdots; (j_{v-1}, l_{v-1}); (j_0, l_{v-1}); (j_0, l_0)$$

where for $1 \leq k \leq v - 1$, $j_k \neq j_{k-1}$ and $l_k \neq l_{k-1}$. This is called the block sequence of C. Now, we have the following theorem.

Theorem 1: $\boldsymbol{H}$ has a cycle of length $2v$ with block sequence

$$(j_0, l_0); (j_1, l_0); (j_1, l_1); (j_1, l_2); \cdots; (j_{v-1}, l_{v-1}); (j_0, l_{v-1}); (j_0, l_0)$$

if and only if in the group $\mathcal{G}$ we have

$$\prod_{e=0}^{v-1} g_{j_e,l_e} g_{j_{e+1},l_e}^{-1} = 1$$

where 1 is the identity of $\mathcal{G}$ and $j_v = j_0$.

Proof: Assume that $\boldsymbol{H}$ has a cycle C of length $2v$ with block sequence

$$(j_0, l_0); (j_1, l_0); (j_1, l_1); (j_1, l_2); \cdots; (j_{v-1}, l_{v-1}); (j_0, l_{v-1}); (j_0, l_0)$$

Let C be started with a 1 at $(i, p(g_i g_{j_0,l_0}))$th entry of the block $\mathcal{I}(g_{j_0,l_0})$. The next position of C must be a 1 at $(p(g_{p(g_i g_{j_0,l_0})} g_{j_1,l_0}^{-1}), p(g_i g_{j_0,l_c}))$th entry of the block $\mathcal{I}(g_{j_1,l_0})$. On the other hand

$$p(g_{p(g_i g_{j_0,l_0})} g_{j_1,l_0}^{-1}) = p(g_i g_{j_0,l_0} g_{j_1,l_0}^{-1})$$

Continuing this procedure, the $2v$th position of C must be a 1 at the

$$(p(g_i g_{j_0,l_0} g_{j_1,l_0}^{-1} \cdots g_{j_{v-1},l_{v-1}} g_{j_0,l_{v-1}}^{-1}), p(g_i g_{j_0,l_0} g_{j_1,l_c}^{-1} \cdots g_{j_{v-1},l_{v-1}}))$$

entry of the block $\mathcal{I}(g_{j_0,l_{v-1}})$. Now the last position of C must be the first one and hence we must have $i = p(g_i g_{j_0,l_0} g_{j_1,l_0}^{-1} \cdots g_{j_{v-1},l_{v-1}} g_{j_0,l_{v-1}}^{-1})$ or equivalently we must have

$$\prod_{e=0}^{v-1} g_{j_e,l_e} g_{j_{e+1},l_e}^{-1} = 1$$

where 1 is the identity of $\mathcal{G}$ and $j_v = j_0$. Proceeding similar steps, one can prove the converse of the theorem and the proof is completed. □

The following lemma, which can be easily proved, may reduce the complexity involved in the calculation of the girth of $\boldsymbol{H}$.

Lemma 1: $\boldsymbol{H}$ has a cycle of type $(j_0, j_1, \ldots, j_{v-1})$ if and only if it has a cycle of the following types:

- $(j_l, j_{l+1}, \ldots, j_{v-1}, j_0, j_1, \ldots, j_{l-1})$, for $1 \le l \le v-1$, where subscribes are calculated modulo v.
- $(j_l, j_{l-1}, \ldots, j_1, j_0, j_{v-1}, \ldots, j_{l+1})$, for $0 \le l \le v-1$, where subscribes are calculated modulo v. □

In the case where $\mathcal{G}$ is abelian, the following two corollaries describes some bounds on the girth of $\boldsymbol{H}$ and the minimum distance of the code corresponding to $\boldsymbol{H}$.

Corollary 1: If $\mathcal{G}$ is abelian then the girth of $\boldsymbol{H}$ is upper bounded by 12, regardless of the matrix BGM($\boldsymbol{H}$).

Proof: The result follows from Theorem 2.5 of [9] and the fact that any abelian group $\mathcal{G}$ is a direct product of cyclic groups. □

Corollary 2: If $\mathcal{G}$ is abelian and C is the code corresponding to $\boldsymbol{H}$ then $d(C)$ is upper bounded by $(J+1)!$, where J is the column weight of $\boldsymbol{H}$.

Proof: The result follows from Theorem 2 of [7] and the fact that, as two finite groups, we have $\mathcal{G} \cong \mathcal{I}(\mathcal{G})$, where $\mathcal{I}(\mathcal{G}) = \{\mathcal{I}(g) \mid g \in \mathcal{G}\}$. □

Note that Corollaries 1 and 2 urge us to consider non-abelian groups for constructing GP-LDPC codes.

3 Special case for the base group matrix

In this section we consider a special case for the base group matrix and design a class of flexible-rate GP-LDPC codes without cycles of length four. Let $\mathcal{G} = \langle a, b \rangle$ be a finite group with two generators a and b of orders O_a and O_b, respectively. Assume that $L \le O_a$, $J \le O_b$ and $\boldsymbol{H}(a, b)$ is the parity-check matrix for a GP-LDPC code whose base group matrix is

$$\mathrm{BGM}(\boldsymbol{H}(a,b)) = \begin{pmatrix} 1 & a & \cdots & a^{L-1} \\ b & ab & \cdots & a^{L-1}b \\ \vdots & & \ddots & \vdots \\ b^{J-1} & ab^{J-1} & \cdots & a^{L-1}b^{J-1} \end{pmatrix} \quad (3)$$

Assume that $(j_0, l_0); (j_1, l_0); (j_1, l_1); (j_1, l_2); \ldots; (j_{v-1}, l_{v-1}); (j_0, l_{v-1}); (j_0, l_0)$ is the block sequence of a length-$2v$ cycle C in $\boldsymbol{H}(a, b)$. In this case, we say that C has type $(j_0, j_1, \ldots, j_{v-1}, j_0)$. The following lemma helps us to determine the girth of $\boldsymbol{H}(a, b)$.

Lemma 2: If $O_b = J$ then $\boldsymbol{H}(a, b)$ has a cycle of type $(j_0, j_1, \ldots, j_{v-1})$ if and only if it has a cycle of type

- $(\overline{j_0 + k}, \overline{j_1 + k}, \ldots, \overline{j_{v-1} + k})$, for $1 \le k \le J-1$, where $\overline{l} = l \bmod J$,

Proof: Assume that $(j_0, l_0); (j_1, l_0); (j_1, l_1); (j_1, l_2); \ldots; (j_{v-1}, l_{v-1}); (j_0, l_{v-1}); (j_0, l_0)$ is the block sequence of a length-$2v$ cycle C in $\boldsymbol{H}(a, b)$. Then according to Theorem 1, we must have

$$\prod_{e=0}^{v-1} (a^{l_e} b^{j_e})(a^{l_e} b^{j_{e+1}})^{-1} = 1 \quad (4)$$

Recall that in a group $\mathcal{G}$ we have $g_1 g_2 = 1$ if and only if $g_2 g_1 = 1$. Hence (4) is true if and only if

$$a^{l_0} \left(\prod_{e=0}^{v-2} b^{j_e - j_{e+1}} a^{l_{e+1} - l_e} \right) b^{j_{v-1} - j_0} a^{-l_{v-1}} = 1$$

which is true if and only if

$$\prod_{e=0}^{v-1} b^{j_e - j_{e+1}} a^{l_{e+1} - l_e} = 1$$

Now the assertion can be easily deduced. □

Proposition 1: Assume that O_a and O_b are two prime numbers. Then $\boldsymbol{H}(a, b)$ is 4-cycle free if and only if $ab \ne ba$ or equivalently $\mathcal{G}$ is non-abelian.

Proof: Assume that $\boldsymbol{H}(a, b)$ has a cycle C of length 4. Using Lemma 2, we may assume that C is of type $(0, r)$ for some $1 \le r \le J-1$. Hence we must have

$$a^{l_0}(a^{l_0} b^r)^{-1}(a^{l_1} b^r)(a^{l_1})^{-1} = 1$$

for some $0 \le l_0$ and $l_1 \le L-1$ with $l_0 \ne l_1$. On the other hand, setting $t := l_0 - l_1$, s to be the inverse of t modulo O_a

doi: 10.1049/iet-com.2011.0791

and u to be the inverse of r modulo O_b, then we have

$$\begin{aligned} a^{l_0}(a^{l_0}b^r)^{-1}(a^{l_1}b^r)(a^{l_1})^{-1} = 1 &\Rightarrow b^{-r}a^t b^r = a^t \\ &\Rightarrow (b^{-r}a^t b^r)^s = a^{st} \\ &\Rightarrow b^{-r}ab^r = a \\ &\Rightarrow ab^r a^{-1} = b^r \\ &\Rightarrow (ab^r a^{-1})^u = b^{ur} \\ &\Rightarrow aba^{-1} = b \\ &\Rightarrow ab = ba \end{aligned}$$

The converse of the claim is clear and the proof is now completed. □

Proposition 1 provides a large class of flexible-rate GP-LDPC codes which are free of cycles of length four. To construct a (J, L)-regular GP-LDPC code without cycles of length four, it suffices to choose a non-abelian group $\mathcal{G}$ generated by elements a and b of prime orders $O_a \geq L$ and $O_b \geq J$. This is almost always possible. For example, if p and q are two primes such that $q|p-1$, one may choose the metacyclic group $\mathcal{G}$ of order pq where

$$\mathcal{G} = \langle a, b | a^p = b^q = 1, bab^{-1} = a^r \rangle$$

and $1 \leq r \leq p-1$ has order q in the multiplicative group of the field $\mathbb{Z}_p$.

Example 2: Again, let $\mathcal{G}$ be the dihedral group of size 6 described in the previous example. Note that $\mathcal{G}$ is a metacyclic group with $p = 3$ and $q = r = 2$. Assume that $a = \rho$ and $b = \varepsilon$. The order of a is 3 and the order of b is 2. The matrix $\boldsymbol{H}(a, b)$ is the following 12×18 binary parity check matrix

$$\boldsymbol{H}(a, b) = \begin{pmatrix} \mathcal{I}(1) & \mathcal{I}(\rho) & \mathcal{I}(\rho^2) \\ \mathcal{I}(\varepsilon) & \mathcal{I}(\varepsilon\rho^2) & \mathcal{I}(\varepsilon\rho) \end{pmatrix}$$

According to Proposition 1, the girth of $\boldsymbol{H}(a, b)$ is at least 6. Note that, the exact girth of $\boldsymbol{H}(a, b)$ is equal to 8.

Remark 1: One may consider the random method for constructing the matrix BGM($\boldsymbol{H}$). Indeed, one may choose a random element of the group $\mathcal{G}$ for the (i, j)th entry of BGM($\boldsymbol{H}$). For some small groups, random method results in better GP-LDPC codes from the girth and performance perspective. However, in many cases I have checked, the codes constructed from the method described above are superior to the random ones from the girth and performance viewpoint.

4 Simulation results

In this section, the performance obtained with some of the GP-LDPC codes of column weight three is presented. The followings can be verified from the results of this section:

- GP-LDPC codes can outperform their random-like counterparts at different lengths and rates.
- GP-LDPC codes based on non-abelian groups can outperform QC LDPC codes based on circulant matrices (corresponding to GP-LDPC codes based on cyclic groups).
- At large lengths and low rates, QC LDPC codes based on circulant matrices have long error floors while GP-LDPC codes based on non-abelian groups perform very well.

For our computations, we use GAP (Groups, Algorithms, Programming) program available online at [11] which is a system for computational discrete algebra, with particular emphasis on computational group theory.

We consider simple groups including alternating groups of order n consisting of even permutations on n symbols, denoted by A_n, and projective special linear groups of those $d \times d$ matrices over the field with q elements whose determinant is the identity of the field, modulo the centre, denoted by PSL(d, q), as the underlying groups of our GP-LDPC codes. Note that the GAP program uses some permutation representations of the group PSL(d, q).

Our simulation results are over BPSK-modulated AWGN channel and have been obtained using the software available online at [12]. The BP decoder was allowed a maximum of 50 decoding iterations. The BP decoder stops when either a valid codeword is found or the maximum number of decoding iterations is reached. In each simulation, at least 500 blocks have been transmitted. The results are compared with regular randomly constructed LDPC codes and QC LDPC codes based on circulant matrices, of similar rates and block lengths.

Example 3: Assume that p is a prime such that $p-1$ is divisible by both J and L. Let α and β be positive integers less than or equal to $p-1$ such that the orders of α and β in the multiplicative group of the field $\mathbb{F}_p$ are L and J, respectively. Assume that $\mathcal{G} = \langle g \rangle$ is a cyclic group of size p. Consider the $pJ \times pL$ parity-check matrix $\boldsymbol{H}$ for which the (i, j)th entry of the matrix BGM($\boldsymbol{H}$) is $g^{\alpha^i \beta^j}$. The (J, L)-regular GP-LDPC codes obtained from this method are indeed QC LDPC codes introduced in [8, 10]. In the rest of the paper, a QC LDPC code of length n and rate r, obtained from this construction method, has been denoted by Tan(n, r, J, L, p).

Example 4: Let $\mathcal{G} = A_5$. We have $|\mathcal{G}| = 60$ and $\mathcal{G} = \langle a, b \rangle$, where $a = (1, 2, 3, 4, 5)$ and $b = (3, 4, 5)$. The orders of a and b are 5 and 3, respectively. The (3,5)-regular GP-LDPC code corresponding to the parity-check matrix $\boldsymbol{H}(a, b)$ (recall that BGM($\boldsymbol{H}(a, b)$) has the form given in (3)) has girth 8. The matrix $\boldsymbol{H}(a, b)$ has 10 redundant checks and therefore the rate of the code is approximately 0.433. The performance of this code (with the label $GP(300, 0.433, A_5)$) has been shown in Fig. 1. The code has also been compared with Tan(305, 0.4, 3, 5, 61) and a random-like (3, 5)-regular LDPC code of length 300 (with the label $R(300, 0.4)$). The figure shows that, while we have a rate gain at $\sim$0.033, the GP-LDPC code obtained from A_5 outperforms the random-like and QC LDPC code.

Example 5: Consider the finite group

$$\mathcal{G} = \langle (1, 5, 2, 4, 3)(6, 8, 7), (1, 4, 2, 5, 3)(6, 7, 8) \rangle$$

of size 180. This group is isomorphic to $GL(2, 4)$ consisting of all invertible 4×4 matrices over the field $\mathbb{F}_2$. All of the (3, 5)-regular GP-LDPC codes with parity-check matrices of the form $\boldsymbol{H}(a, b)$, have girth at most 8. However, the (3, 5)-regular GP-LDPC code corresponding to the parity-check matrix $\boldsymbol{H}$ such that BGM($\boldsymbol{H}$) is the randomly chosen

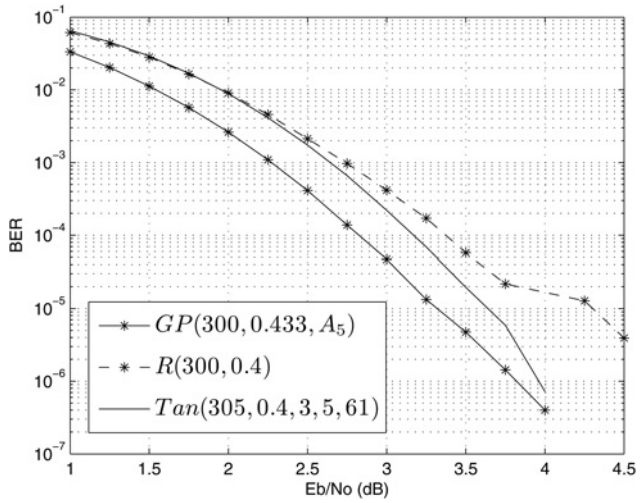

Fig. 1 *Performance of the short-length (3, 5)-regular GP-LDPC code obtained from non-abelian group A_5, against QC and random-like LDPC codes*

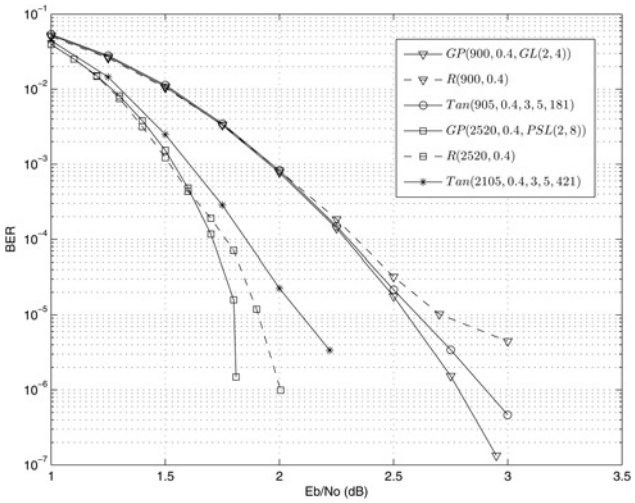

Fig. 2 *Performance of two moderate-length (3, 5)-regular GP-LDPC codes, against QC and random-like LDPC codes*

matrix

$$\begin{pmatrix} g_{1,1} & g_{1,2} & g_{1,3} & g_{1,4} & g_{1,5} \\ g_{2,1} & g_{2,2} & g_{2,3} & g_{2,4} & g_{2,5} \\ g_{1,5} & g_{2,5} & g_{3,5} & g_{4,5} & g_{5,5} \end{pmatrix}$$

where

$$g_{1,1} = (1, 2)(4, 5)(6, 8, 7)$$
$$g_{1,2} = (1, 2)(4, 5)$$
$$g_{1,3} = (2, 5, 4)(6, 7, 8)$$
$$g_{1,4} = (1, 3, 5, 4, 2)$$
$$g_{1,5} = (1, 5, 4, 2, 3)(6, 8, 7)$$
$$g_{2,1} = (1, 2)(3, 5)$$
$$g_{2,2} = (1, 3, 5, 4, 2)(6, 8, 7)$$
$$g_{2,3} = (1, 3, 4)(6, 8, 7)$$
$$g_{2,4} = (1, 2)(3, 5)(6, 7, 8)$$
$$g_{2,5} = (1, 4)(3, 5)(6, 8, 7)$$
$$g_{3,1} = (1, 2, 3, 4, 5)(6, 7, 8)$$
$$g_{3,2} = (1, 3, 2, 5, 4)$$
$$g_{3,3} = (1, 2, 3)(6, 8, 7)$$
$$g_{3,4} = (2, 5)(3, 4)$$
$$g_{3,5} = (1, 4, 5, 3, 2)(6, 7, 8)$$

has girth 10. The performance of this code (with the label GP(900, 0.4, GL(2, 4))) is shown in Fig. 2. The code has also been compared with Tan(905, 0.4, 3, 5, 181) and a random-like (3, 5)-regular LDPC code of length 900 (with the label $R(900, 0.4)$).

Example 6: Let $\mathcal{G} = PSL(2, 8)$. We have $|\mathcal{G}| = 504$ and $\mathcal{G} = \langle a, b \rangle$, where

$$a = (3, 4, 5, 6, 7, 8, 9)$$
$$b = (1, 2, 3)(4, 7, 5)(6, 9, 8)$$

The orders of a and b are 7 and 3, respectively. The (3, 5)-regular GP-LDPC code corresponding to the parity-check matrix $\boldsymbol{H}(a, b)$ has girth 12. The performance of this code (with the label $GP(2520, 0.4, \text{PSL}(2, 8))$) has been shown in Fig. 2. The code also has been compared with Tan(2105, 0.4, 3, 5, 421) and a random-like (3,5)-regular LDPC code of length 2520 (with the label $R(2520, 0.4)$).

Example 7: Let $\mathcal{G} = A_7$. We have $|\mathcal{G}| = 2520$ and $\mathcal{G} = \langle a, b \rangle$, where

$$a = (1, 2, 3, 4, 5, 6, 7)$$
$$b = (2, 3)(4, 5, 6, 7)$$

The orders of a and b are 7 and 4, respectively. The (3, 5)-regular GP-LDPC code corresponding to the parity-check matrix $\boldsymbol{H}(a, b)$ has girth 10. The performance of this code (with the label $GP(12600, 0.4, A_7)$) has been shown in Fig. 3. The code also has been compared with Tan(12605, 0.4, 3, 5, 2521) and a random-like (3,5)-regular LDPC code of length 12600 (with the label $R(12600, 0.4)$). The figure shows that the performance curve of Tan(12605, 0.4, 3, 5, 2521) has long error floors. This does not depend on the choice of p. For some primes $p > 2521$ of the form $15k + 1$, I have simulated the codes Tan($5p$, 0.4, 3, 5, p). In all of them, long error floors have been observed. This confirms that, long-length low-rate QC LDPC codes of column weight three, based on circulant matrices, are not good.

Note that there are other representations for A_7 with different generators for which the girth of the corresponding (3, 5)-regular GP-LDPC code is greater than 10. For example we have $A_7 = \langle c, d \rangle$, where $c = (3, 4, 5, 6, 7)$ and $d = (1, 2, 3)(5, 6, 7)$. The orders of c and d are 5 and 3, respectively. The (3, 5)-regular GP-LDPC code corresponding to the the parity-check matrix $\boldsymbol{H}(c, d)$ has girth 14. However, from the performance perspective, the

doi: 10.1049/iet-com.2011.0791

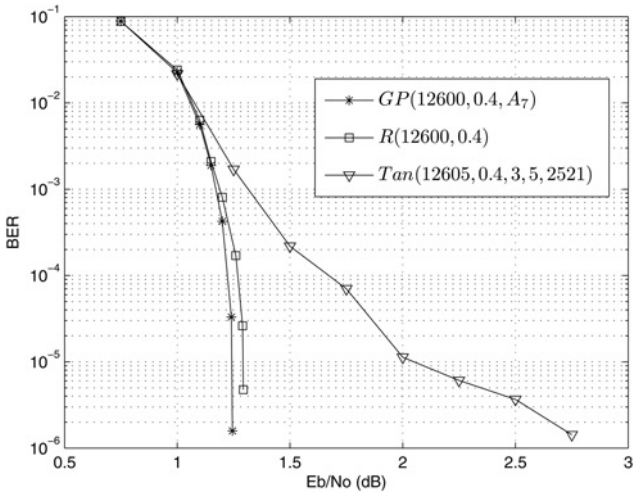

Fig. 3 *Performance of the long-length (3, 5)-regular GP-LDPC code obtained from non-abelian group A_7, against QC and random-like LDPC codes*

(3, 5)-regular GP-LDPC code corresponding to the the parity-check matrix $\boldsymbol{H}(a, b)$ is slightly better than that of $\boldsymbol{H}(c, d)$.

Example 8: Let $\mathcal{G} = PSL(2, 31)$. We have $|\mathcal{G}| = 14880$ and $\mathcal{G} = \langle a, b \rangle$, where

$$\begin{array}{lccccc} a = & (2, & 3, & 27, & & \\ & 4, & 21, & 23, & 28, & 31, \\ & 15, & 5, & 17, & 26, & 22, \\ & 14, & 25, & 24, & 9, & 10, \\ & 29, & 7, & 11, & 32, & 20, \\ & 30, & 16, & 13, & 8, & 6, \\ & & & 19, & 12, & 18) \end{array}$$

Also $b = \prod_{i=1}^{6} \alpha_i$ where

$$\begin{aligned} \alpha_1 &= (1, 2, 3, 7, 11) \\ \alpha_2 &= (5, 18, 12, 24, 21) \\ \alpha_3 &= (6, 28, 19, 14, 13) \\ \alpha_4 &= (8, 31, 30, 25, 16) \\ \alpha_5 &= (9, 23, 20, 32, 26) \\ \alpha_6 &= (15, 22, 29, 17, 27) \end{aligned}$$

The orders of a and b are 31 and 5, respectively. The (3, 5)-regular GP-LDPC code corresponding to the parity-check matrix $\boldsymbol{H}(a, b)$ has girth 12. The performance of this code (with the label GP(74400, 0.4, PSL(2, 31))) together the performance of its random-like counterpart (with the label R(74400, 0.4)) are shown in Fig. 4. Again we should mention that there are other representations for $PSL(2, 31)$ with different generators for which the girth of the corresponding (3, 5)-regular GP-LDPC code is greater than 12. For example, if $c = \prod_{i=1}^{6} \alpha_i$ where

$$\begin{aligned} \alpha_1 &= (3, 9, 15, 21, 27) \\ \alpha_2 &= (4, 10, 16, 22, 28) \\ \alpha_3 &= (5, 11, 17, 23, 29) \\ \alpha_4 &= (6, 12, 18, 24, 30) \\ \alpha_5 &= (7, 13, 19, 25, 31) \\ \alpha_6 &= (8, 14, 20, 26, 32) \end{aligned}$$

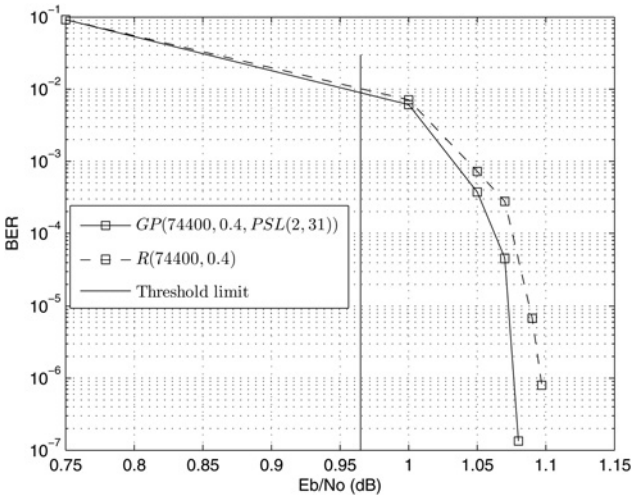

Fig. 4 *Performance of a long-length (3, 5)-regular GP-LDPC code, against its random-like counterpart*

and $d = \prod_{i=1}^{10} \beta_i$ where

$$\begin{aligned} \beta_1 &= (1, 3, 10), & \beta_2 &= (2, 6, 13) \\ \beta_3 &= (4, 28, 14), & \beta_4 &= (5, 27, 9) \\ \beta_5 &= (7, 19, 11), & \beta_6 &= (8, 31, 15) \\ \beta_7 &= (12, 32, 18), & \beta_8 &= (16, 20, 29) \\ \beta_9 &= (17, 26, 30), & \beta_{10} &= (22, 24, 23) \end{aligned}$$

Then the (3, 5)-regular GP-LDPC code corresponding to the parity-check matrix $\boldsymbol{H}(c, d)$ has girth 16. However, from the performance perspective, the (3, 5)-regular GP-LDPC code corresponding to the the parity-check matrix $\boldsymbol{H}(a, b)$ is a bit better than that of $\boldsymbol{H}(c, d)$.

Example 9: Again, let $\mathcal{G} = A_7$ and assume that a, b are the same as those given in Example 7. The (3, 7)-regular GP-LDPC code corresponding to the parity-check matrix $\boldsymbol{H}(a, b)$ has girth 10. The performance of this code (with the label GP(17640, 0.57143, A_7)) has been shown in Fig. 5. The code also has been compared with Tan(17647, 0.57143, 3, 7, 2521) and a (3, 7)-regular random-like LDPC code of length 17640 (with the label R(17640, 0.57143)).

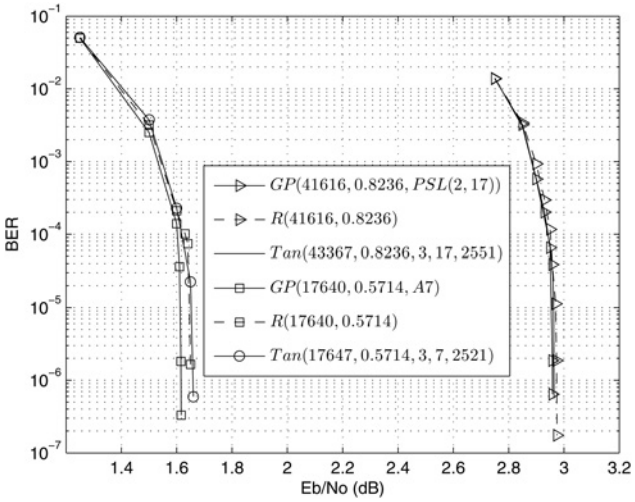

Fig. 5 *Performance of two GP-LDPC codes with different rates, against QC and random-like LDPC codes*

Example 10: Let $\mathcal{G} = \mathrm{PSL}(2, 17)$. We have $|\mathcal{G}| = 2448$ and $\mathcal{G} = \langle a, b \rangle$, where

$$a = \begin{matrix} (2, & 3, & 17, & 4, & 15, \\ 8, & 18, & 14, & 13, & 5, \\ 6, & 10, & 16, & 7, & 12, \\ & & & 9, & 11,) \end{matrix}$$

Also $b = \alpha_1\alpha_2$ where

$$\alpha_1 = (1, 2, 3, 10, 9, 17, 16, 7)$$
$$\alpha_2 = (5, 11, 14, 8, 13, 18, 12, 15)$$

The orders of a and b are 17 and 8, respectively. The (3, 17)-regular GP-LDPC code corresponding to the parity-check matrix $\boldsymbol{H}(a, b)$ has girth 8. The performance of this code (with the label GP(41616, 0.82353, *PSL*(2, 17))) has been shown in Fig. 5. The code has also been compared with Tan(43367, 0.82353, 3, 17, 2551) and a (3, 17)-regular random-like LDPC code of length 41616 (with the label R(41616, 0.82353)).

5 Conclusion

Based on a class of permutation matrices which come from a finite abstract group, a new class of algebraically structured (J, L)-regular LDPC codes, called GP-LDPC codes, has been introduced. This new method generalises many of the previous constructions for QC LDPC codes based on circulant matrices. Although long-length low-rate QC LDPC codes (based on circulant matrices) of column weight three are not good, we have designed good long-length low-rate GP-LDPC codes of column weight three. Based on non-abelian groups, we also have designed GP-LDPC codes of column weight three and various rates, that outperform their random-like counterparts and QC LDPC codes obtained from circulant matrices. Finally, based on metacyclic groups, we have introduced a class of flexible-rate GP-LDPC codes which are free of cycles of length four.

6 Acknowledgments

This work was partially supported by the Center of Excellence for Mathematics, University of Isfahan. Also, the author thank the referees whose comments greatly improved the manuscript.

7 References

1 Chung, S.Y., Forney, G.D., Richardson, T.J., Urbanke, R.: 'On the design of low-density parity-check codes within 0.0045 dB of the Shannon limit', *IEEE Commun. Lett.*, 2001, **5**, pp. 58–60
2 Richardson, T.J., Shokrollahi, A., Urbanke, R.: 'Design of capacity-approaching low-density parity-check codes', *IEEE Trans. Inf. Theory*, 2001, **47**, pp. 619–637
3 Vontobel, P.O., Tanner, R.M.: 'Construction of codes based on finite generalized quadrangles for iterative decoding'. Proc. IEEE Int. Symp. on Information Theory, June 2001, p. 223
4 Nguyen, D.V., Vasić, B., Marcellin, M., Chilappagari, S.K.: 'Structured LDPC codes from permutation matrices free of small trapping sets'. Information Theory Workshop (ITW), September 2010, pp. 1–5
5 Zhang, L., Huang, Q., Lin, S., Abdel-Ghaffar, K.: 'Quasi-cyclic LDPC codes: An algebraic construction, rank analysis, and codes on latin squares', *IEEE Trans. Commun.*, 2010, **58**, (10), pp. 3126–3139
6 Gallager, R.G.: 'Low-density parity-check codes' (MIT Press, Cambridge, MA, 1963)
7 MacKay, D.J.C., Davey, M.: 'Evaluation of Gallager codes for short block length and high rate applications'. Proc. IMA Workshop Codes, Systems and Graphical Models, 1999
8 Tanner, R.M., Sridhara, D., Fuja, T.: 'A class of group-structured LDPC codes'. Proc. ISTA, Ambleside, England, 2001
9 Fossorier, M.P.C.: 'Quasi-cyclic low-density parity-check codes from circulant permutation matrices', *IEEE Trans. Inf. Theory*, 2004, **50**, (8), pp. 1788–1793
10 Tanner, R.M.: 'LDPC block and convolutional codes based on circulant matrices', *IEEE Trans. Inf. Theory*, 2004, **50**, (12), pp. 2966–2984
11 ⟨http://www.gap-system.org⟩
12 ⟨http://www.cs.toronto.edu/Radford/ldpc.software.html⟩
13 Kou, Y., Lin, S., Fossorier, M.: 'Low-density parity-check codes based on finite geometries: a rediscovery and new results', *IEEE Trans. Inf. Theory*, 2001, **47**, pp. 2711–2736
14 Johnson, S.J., Weller, S.R.: 'Codes for iterative decoding from partial geometries'. Proc. IEEE Int. Symp. Inform. Theory, Lausanne, Switzerland, July 2002, p. 310
15 Ammar, B., Honary, B., Kou, Y., Xu, J., Lin, S.: 'Construction of low-density parity-check codes based on balanced incomplete block designs', *IEEE Trans. Inf. Theory*, 2004, **50**, (6), pp. 1257–1568
16 Xu, J., Chen, L., Djurdjevic, I., Lin, S., Abdel-Ghaffar, K.: 'Construction of regular and irregular LDPC codes: geometry decomposition and masking', *IEEE Trans. Inf. Theory*, 2007, **53**, (1), pp. 121–134
17 Ländner, S., Milenkovic, O.: 'LDPC codes based on Latin squares: cycle structure, stopping set, and trapping set analysis', *IEEE Trans. Commun.*, 2007, **55**, (2), pp. 303–307
18 Kamiya, N.: 'High-rate quasi-cyclic low-density parity-check codes derived from finite affine planes', *IEEE Inf. Theory*, 2007, **53**, (4), pp. 1444–1459
19 Lan, L., Tai, Y.Y., Lin, S., Memari, B., Honary, B.: 'New construction of quasi-cyclic LDPC codes based on special classes of BIBDs for the AWGN and binary erasure channels', *IEEE Trans. Commun.*, 2008, **56**, (1), pp. 39–48
20 Fan, J.L.: 'Array codes as low-density parity-check codes'. Proc. Second Int. Symp. Turbo Codes, Brest, France, September 2000, pp. 545–546
21 Vasic, B.: 'Combinatorial constructions of low-density parity check codes for iterative decoding'. Proc. IEEE Int. Symp. Information Theory, Lausanne, Switzerland, July 2002, p. 312
22 Kim, J.L., Peled, U.N., Perepelitsa, I., Pless, V.: 'Explicit construction of families of LDPC codes with girth at least six'. Proc. 40th Annual Allerton Conf. Communication, Control and Computing, Monticello, IL, 2002
23 Gabidulin, E., Moinian, A., Honary, B.: 'Generalized construction of quasi-cyclic regular LDPC codes based on permutation matrices'. Proc. IEEE Int. Symp. Inf. Theory, July 2006, pp. 679–683
24 Liva, G., Rayan, W.E., Chiani, M.: 'Quasi-cyclic generalized LDPC codes with low error floors', *IEEE Trans. Commun.*, 2008, **56**, (1), pp. 49–57

doi: 10.1049/iet-com.2011.0791