

Nonbinary LDPC Codes on Cages: Structural Property and Code Optimization

Chao Chen, Baoming Bai, *Member, IEEE*, Guangming Shi, *Senior Member, IEEE*, Xiaotian Wang, and Xiaopeng Jiao

Abstract—A (v, g) -cage is a (not necessarily unique) smallest v -regular graph of girth g . On such a graph, a nonbinary $(2, v)$ -regular low-density parity-check (LDPC) code can be defined such that the Tanner graph has girth $2g$ and the code length achieves the minimum possible. In this paper, we focus on two aspects of this class of codes, structural property and code optimization. We find that, in addition to those found previously, many cages can be used to construct structured LDPC codes. We show that all cages with even girth can be structured as protograph-based codes, many of which have block-circulant Tanner graphs. We also find that four cages with odd girth can be structured as protograph-based codes with block-circulant Tanner graphs. For code optimization, we develop an ontology-based approach. All possible inter-connected cycle patterns that lead to low symbol-weight codewords are identified to put together the ontology. By doing so, it becomes handleable to estimate and optimize distance spectrum of equivalent binary image codes. We further analyze some known codes from the Consultative Committee for Space Data Systems recommendation and design several new codes. Numerical results show that these codes have reasonably good minimum bit distance and perform well under iterative decoding.

Index Terms—Nonbinary LDPC code, cage, protograph-based code, CCSDS recommendation, minimum distance.

I. INTRODUCTION

NONBINARY low-density parity-check (LDPC) codes were first introduced by Gallager in 1960s using modulo arithmetic [1]. In [2], Davey and MacKay introduced non-binary LDPC codes over finite fields. Recently, these codes have attracted a lot of attention [3]–[17]. Non-binary LDPC codes have the potential to outperform their binary counterparts under iterative decoding. For short block lengths, about 1 dB

performance gain can be achieved [8]–[13]. In practice, non-binary LDPC codes are being considered by the Consultative Committee for Space Data Systems (CCSDS) for telecommand applications [14].

An important class of non-binary LDPC codes are called $(2, v)$ -regular codes, whose parity-check matrices have column weight 2 and row weight v . This class of codes can attain optimal average bit-weight spectrum as the block length and field order become sufficiently large [3]. In [5], a design method of such codes was proposed based on their binary image. In [7], structural properties of this class of codes were analyzed from a graph-theoretical point of view.

For $(2, v)$ -regular LDPC codes, it is desirable to have large girth in the Tanner graph, which is highly beneficial to the error floor performance [5], [6]. To achieve this, several researchers have proposed to design codes on a special class of graphs, called cages. A prominent feature of such codes is that the code length achieves the minimum possible for the given code rate and girth. In [20], it was observed that the codes constructed for partial response channels in [19] can be obtained from some cages, and more cages were considered for code construction. Exploiting the relation between quasi-cyclic (QC) codes and convolutional codes, the authors in [21] developed a code search algorithm and obtained several QC-LDPC codes defined on cages. It was shown in [6] that a number of cages can be obtained using a modified Progressive Edge-Growth (PEG) algorithm. In [15], a class of non-binary QC-LDPC codes defined on cages were proposed based on Singer difference set. Using the fact that some cages are Hamiltonian graphs, it was shown in [16] and [17] that the induced codes have dual-diagonal structure that facilitates efficient encoding.

In contrast to binary LDPC codes, non-binary LDPC codes have an additional design freedom in terms of the selection of non-zero entries in the parity-check matrix [4]. For non-binary $(2, v)$ -regular LDPC codes, a design criterion for selecting non-zero entries was presented in [5], which targets for improving the distance properties associated with local topological structures in the Tanner graph, such as rows, cycles, and inter-connected cycles.

In this paper, we study non-binary $(2, v)$ -regular LDPC codes defined on cages. We will focus on two aspects, structural property and code optimization. It has been shown that some cages can be used to construct structured codes [13], [15], [21]. Since structured codes have advantages in terms of code description and implementation complexity, a natural question is whether more cages can lend themselves to the construction of structured codes. In fact, many cages themselves are constructed algebraically and have regular structures. In this paper,

Manuscript received April 26, 2014; revised September 9, 2014, November 29, 2014, and December 10, 2014; accepted December 23, 2014. Date of publication January 1, 2015; date of current version February 12, 2015. This work was supported in part by the 973 Program of China under Grants 2012CB316100 and 2010CB328300, by the NSFC under Grants 61101127, 61401333, 61471286, and 61471294, by the Research Fund for the Doctoral Program of Higher Education of China under Grant 20130203120009, by the Shaanxi Province Natural Science Foundation of China under Grant 2014JQ8296, by the China Postdoctoral Science Foundation under Grant 2014M560751, and by the Shaanxi Postdoctoral Science Foundation. The associate editor coordinating the review of this paper and approving it for publication was L. Dolecek.

C. Chen, G. Shi, and X. Wang are with the School of Electronic Engineering, Xidian University, Xi'an 710071, China (e-mail: chenchaoxidian@gmail.com; gmshi@xidian.edu.cn; xtwang@mail.xidian.edu.cn).

B. Bai is with the State Key Laboratory of Integrated Service Networks, School of Telecommunication Engineering, Xidian University, Xi'an 710071, China (e-mail: bmbai@mail.xidian.edu.cn).

X. Jiao is with the School of Computer Science and Technology, Xidian University, Xi'an 710071, China (e-mail: jiaozi1216@126.com).

Digital Object Identifier 10.1109/TCOMM.2014.2387341

we find that more cages can be used to construct structured codes. Specifically, we show that all cages with even girth can be structured as protograph-based codes, many of which have block-circulant Tanner graphs, and find that four cages with odd girth can be structured as protograph-based codes with block-circulant Tanner graphs.

Given the Tanner graph, code optimization involves the selection of non-zero entries in the parity matrix. Similar to the methodology in [36], we develop an ontology-based method. The method applies to general non-binary $(2, v)$ -regular LDPC codes and is not limited to the codes defined on cages. By investigating the influence of graph structure on distance property, we identify all possible subgraph patterns in the Tanner graph that lead to low symbol-weight codewords. The patterns of inter-connected short cycles collectively form the ontology, which is independent of any particular code. Based on the ontology, the identification of inter-connected short cycles can be greatly simplified for the given Tanner graph. Then we can efficiently estimate the distance spectrum of equivalent binary image codes for any given assignment of non-zero entries. As a result, good candidate codes may be obtained by comparing the bit-distance spectrum of numerous codes generated. We will apply the ontology-based method to the codes defined on cages and show that codes with good minimum bit-distance can be obtained.

The rest of the paper is organized as follows. Section II provides some preliminaries about LDPC codes and cages. In Section III, we explore the structures of codes on cages. In Section IV, we present the ontology-based approach for code optimization. In Section V, some code design examples are presented and numerical results are given. Finally, we conclude the paper in Section VI.

II. PRELIMINARIES

A. Graphical Representations of $(2, v)$ -Regular LDPC Codes

Let \mathbf{H} be the parity-check matrix of a non-binary LDPC code over some finite field. Let \mathbf{H}_b be the corresponding binary matrix obtained by replacing each non-zero entry of \mathbf{H} by '1.' Then \mathbf{H}_b can be graphically represented by a *Tanner graph* [18], a bipartite graph. The two subsets of nodes, called variable nodes and check nodes, correspond to the columns and rows of \mathbf{H}_b , respectively. A variable node is adjacent to a check node if and only if the entry in the corresponding column and row is '1.' Therefore, \mathbf{H}_b is the *bi-adjacency matrix* of the Tanner graph.

If \mathbf{H}_b has column weight 2, there is an alternative graphical representation, called the *associated graph*.¹ Each vertex corresponds to a row and each edge to a column. An edge is incident to a vertex if and only if the entry in the corresponding row and column is '1.' Therefore, \mathbf{H}_b is the *incidence matrix* of the associated graph. For a $(2, v)$ -regular LDPC code, the associated graph is a v -regular graph, i.e., each vertex is of degree v .

¹Here, we follow the terminology in [7]. Note that it is called a cycle graph in [17] and a distance graph in [20].

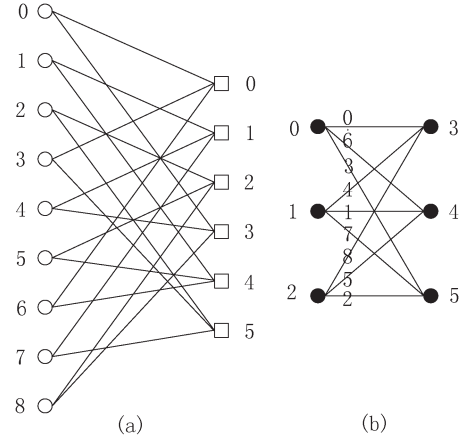


Fig. 1. Two graphical representations of \mathbf{H}_b . (a) Tanner graph. (b) The associated graph.

For a given \mathbf{H} , the resultant \mathbf{H}_b serves simultaneously as the bi-adjacency matrix of the Tanner graph and the incidence matrix of the associated graph. The associated graph has girth g if and only if the Tanner graph has girth $2g$.

To make more clear the correspondence between the two graphical representations, we give an example. Consider a $(2, 3)$ -regular LDPC code over the finite field $\text{GF}(2^2) = \{0, \alpha^0, \alpha^1, \alpha^2\}$ where α is a primitive element. The parity-check matrix is given by

$$\mathbf{H} = \begin{bmatrix} \alpha^0 & 0 & 0 & \alpha^2 & 0 & 0 & \alpha^0 & 0 & 0 \\ 0 & \alpha^1 & 0 & 0 & \alpha^0 & 0 & 0 & \alpha^2 & 0 \\ 0 & 0 & \alpha^2 & 0 & 0 & \alpha^2 & 0 & 0 & \alpha^1 \\ \alpha^2 & 0 & 0 & 0 & \alpha^1 & 0 & 0 & 0 & \alpha^0 \\ 0 & \alpha^0 & 0 & 0 & 0 & \alpha^0 & \alpha^2 & 0 & 0 \\ 0 & 0 & \alpha^2 & \alpha^0 & 0 & 0 & 0 & \alpha^0 & 0 \end{bmatrix}, \quad (1)$$

where the rows are indexed by $i (i = 0, \dots, 5)$ and the columns are indexed by $j (j = 0, \dots, 8)$. Fig. 1 illustrates the two graphical representations of the resultant \mathbf{H}_b . In the Tanner graph, open circles and squares correspond respectively to the columns and rows of the \mathbf{H}_b , while in the associated graph, edges and filled circles correspond respectively to the columns and rows of \mathbf{H}_b . It can be checked that the Tanner graph has girth 8 and the associated graph has girth 4.

A complete bipartite graph, denoted by $K_{J,L}$, is a special bipartite graph such that each vertex in one vertex set consisting of J vertices is adjacent to all vertices of the other vertex set consisting of L vertices. From this definition, we see that the graph in Fig. 1(b) is the complete bipartite graph $K_{3,3}$.

B. Cages

A v -regular graph of girth g is called a (v, g) -graph. The number of vertices in a (v, g) -graph is lower bounded by the Moore bound [29]

$$M(v, g) = \begin{cases} \frac{v(v-1)^{(g-1)/2} - 2}{v-2}, & \text{for } g \text{ odd} \\ \frac{2(v-1)^{g/2} - 2}{v-2}, & \text{for } g \text{ even} \end{cases}.$$

A (v, g) -graph that achieves the Moore bound is called a Moore graph.

TABLE I
CURRENTLY KNOWN CAGES

Girth	(v, g)	$m(v, g)$	Comments	Tanner graph
Even	$(v \geq 2, g = 4)$	$2v$	are complete bipartite graphs	block-circulant *
	$(q + 1, 6)$ (q a prime power)	$2(q^2 + q + 1)$	from finite projective planes [32]	block-circulant [15], [21], *
	$(q + 1, 8)$ (q a prime power)	$2(q + 1)(q^2 + 1)$	from generalized quadrangles [32]	block-circulant *
	$(q + 1, 12)$ (q a prime power)	$2(q^3 + 1)(q^2 + q + 1)$	from generalized hexagons [32]	protograph-based *
	$(3, 6)$	14	named Heawood graph	block-circulant [15], [21], *
	$(3, 8)$	30	named Tutte-Coxeter graph	block-circulant [21], *
	$(3, 10)$	70	there are three (3,10)-cages	block-circulant [21]
	$(3, 12)$	126	named Benson graph	block-circulant [21]
	$(7, 6)$	90	from Baker elliptic semiplane [31]	block-circulant *
	$(v = 2, g \geq 3)$	g	are cycles	
Odd	$(v \geq 2, g = 3)$	$v + 1$	are complete graphs	
	$(3, 5)$	10	named Petersen graph	block-circulant [13], *
	$(3, 7)$	24	named McGee graph	
	$(3, 9)$	58	there are eighteen (3,9)-cages	
	$(3, 11)$	112	named Balaban 11-cage	
	$(4, 5)$	19	named Robertson graph	
	$(5, 5)$	30	there are four (5,5)-cages	block-circulant *
	$(6, 5)$	40	--	block-circulant *
	$(7, 5)$	50	named Hoffman-Singleton graph	block-circulant *
	$(4, 7)$	67	the uniqueness is unknown	

Definition: A (v, g) -cage is a (v, g) -graph that has the minimum possible number of vertices.

The graph given in Fig. 1(b) is the (3,4)-cage, which is also a Moore graph. Let $m(v, g)$ be the number of vertices in a (v, g) -cage, then $m(v, g) \geq M(v, g)$. Note that in many cases the Moore bound is not achievable even with cages.

Table I lists the known cages, including six infinite families and 14 small examples [30]. We arrange the cages according to the oddity of their girths. Note that the (3,6)-cage, (3,8)-cage, and (3,12)-cage are three specific cases of the three infinite families with girth 6, 8, and 12, respectively. Given parameter (v, g) , there may exist more than one cage up to graph isomorphism. More properties of these cages can be found in [30]. Structural properties of some of Tanner graphs are shown in the last column. Some results have been obtained in [13], [15], and [21]. We mark with * the results given in the present paper. If a (v, g) -cage is used as the associated graph of a code, then the parity-check matrix has $m(v, g)$ rows and $\frac{v \cdot m(v, g)}{2}$ columns, implying that the design rate of the code is $1 - \frac{2}{v}$.

C. Protograph-Based LDPC Codes

A protograph-based LDPC code is an LDPC code constructed from a *protograph*, a small bipartite graph where parallel edges are allowed [22]. By applying a "copy-and-permutation" operation on the protograph, a larger graph can be derived, which serves as the Tanner graph of the LDPC code. The operation is called the *lifting* of the protograph. To obtain a non-binary code, we also need to assign non-zero field elements to the edges of the derived Tanner graph.

The above construction can be interpreted from a matrix perspective. First define the base matrix corresponding to the protograph, and then replace each entry by a sum of permutation matrices, where the number of permutation matrices is equal to the value taken by the entry (the empty sum is read as a zero matrix). The expanded matrix serves as the bi-adjacency matrix of the Tanner graph. The protograph-based construction can be seen as a special case of the superposition construction

of LDPC codes [23], where the replacement matrices can even be non-square.

To facilitate the implementation, circulant-based lifting is usually adopted, i.e., the replacement matrices are chosen to be circulant matrices. A Tanner graph is said to be block-circulant if it is obtained through circulant-based lifting of some protograph. Let \mathbf{P} be the $p \times p$ matrix

$$\mathbf{P} = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & \cdots & 0 \end{bmatrix},$$

then \mathbf{P}^i forms a circulant permutation matrix. Conventionally, \mathbf{P}^0 is used to denote the identity matrix. We see that the code defined by (1) forms a protograph-based LDPC code with block-circulant Tanner graph. The protograph is the complete bipartite graph $K_{2,3}$, with the base matrix

$$\mathbf{B} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}.$$

Through circulant-based lifting, we obtain the Tanner graph in Fig. 1(a), with the bi-adjacency matrix

$$\mathbf{H}_b = \begin{bmatrix} \mathbf{P}^0 & \mathbf{P}^0 & \mathbf{P}^0 \\ \mathbf{P}^0 & \mathbf{P}^1 & \mathbf{P}^2 \end{bmatrix},$$

where \mathbf{P} is of size 3×3 . By assigning non-zero elements of $\text{GF}(2^2)$ to \mathbf{H}_b , we obtain the parity-check matrix \mathbf{H} in (1).

For some protographs, simple circulant-based lifting has some limitations in terms of the upper bounds on the girth or the minimum distance. For example, if the protograph contains the complete bipartite graph $K_{2,3}$ as a subgraph, then the derived Tanner graph has girth at most 12 [24]. If the protograph is the complete bipartite graph $K_{J,L}$, the minimum distance of the (binary) code is upper bounded by $(J + 1)!$ [25]. To overcome these limitations, a two-round circulant-based lifting was proposed in [28], and a multiple-round lifting was adopted in [27], where the last round is restricted to be circulant-based.

III. STRUCTURES OF CODES ON CAGES

We consider LDPC codes that take cages as their associated graphs. We investigate the structural properties of the corresponding Tanner graphs. The key is how to map a cage to the Tanner graph. Considering that cages with even girth and odd girth have different properties, we deal with the two cases separately.

A. Codes on Cages With Even Girth

In [29], Wong conjectured that cages with even girth are regular bipartite graphs. All known cages with even girth conform with this conjecture.

A v -regular bipartite graph with m vertices can be represented by its bi-adjacency matrix \mathbf{A} , which is a square matrix of size $\frac{m}{2} \times \frac{m}{2}$ having v ones in each row and each column. Based on Hall's marriage theorem [35], \mathbf{A} can be decomposed into v permutation matrices \mathbf{A}_k such that

$$\mathbf{A} = \sum_{k=0}^{v-1} \mathbf{A}_k. \quad (2)$$

For example, the bi-adjacency matrix of the 3-regular bipartite graph in Fig. 1(b) is given by

$$\mathbf{A} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix},$$

which can obviously be written as

$$\mathbf{A} = \mathbf{P}^0 + \mathbf{P}^1 + \mathbf{P}^2,$$

where \mathbf{P} is of size 3×3 .

We have the following result.

Theorem 1: If the associated graph is a v -regular bipartite graph with bi-adjacency matrix \mathbf{A} in (2), then the resulting code is a protograph-based code, whose Tanner graph is specified by the bi-adjacency matrix

$$\mathbf{H}_b = \begin{bmatrix} \mathbf{P}^0 & \mathbf{P}^0 & \cdots & \mathbf{P}^0 \\ \mathbf{A}_0 & \mathbf{A}_1 & \cdots & \mathbf{A}_{v-1} \end{bmatrix}. \quad (3)$$

Proof: We define a mapping from the associated graph to the Tanner graph of the code. For the matrix \mathbf{A} , we use i ($i = 0, 1, \dots, \frac{m}{2} - 1$) and j ($j = 0, 1, \dots, \frac{m}{2} - 1$) to index the rows and columns, respectively. From (2), we know that the associated graph can be decomposed into v bipartite graphs with bi-adjacency matrix \mathbf{A}_k . Assume that vertex j and vertex i are connected in the bipartite graph defined by some \mathbf{A}_k . As illustrated in Fig. 2, vertex j is mapped to check node j , vertex i is mapped to check node $i + \frac{m}{2}$, and the edge is mapped to variable node $j + k\frac{m}{2}$. With the mapping, the resulting Tanner graph has the bi-adjacency matrix \mathbf{H}_b given in (3). ■

Remark: For the associated graph, \mathbf{A} is the bi-adjacency matrix and \mathbf{H}_b is the incidence matrix. As will be seen later through an example, the decomposition of \mathbf{A} in (2) is not necessarily unique, which indicates that different \mathbf{H}_b may be obtained. We also notice that the above construction has some similarity to the class-I superposition construction in [23], where the matrix

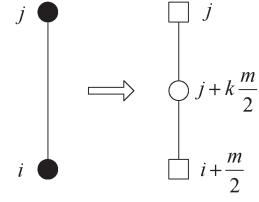


Fig. 2. Mapping from the associated graph to the Tanner graph.

decomposition is applied to the point-line incidence matrices of finite geometry planes.

Theorem 1 only assumes that the associated graph of the code is a regular bipartite graph. Based on Wong's conjecture, we have

Conjecture: Codes on cages with even girth can be structured as protograph-based LDPC codes.

Now we show that for three infinite families of cages and the (7,6)-cage in Table I, the protograph-based LDPC codes have block-circulant Tanner graphs.

The $(v \geq 2, g = 4)$ family of cages are complete bipartite graphs $K_{v,v}$. The bi-adjacency matrix \mathbf{A} is the $v \times v$ all-one matrix, which can be written as

$$\mathbf{A} = \sum_{k=0}^{v-1} \mathbf{P}^k.$$

Therefore, the constructed code has a block-circulant Tanner graph of girth 8, which has $2v$ check nodes and v^2 variable nodes.

For the $(q+1, 6)$ family of cages where q is a prime power, the bi-adjacency matrix \mathbf{A} is a $(q^2 + q + 1) \times (q^2 + q + 1)$ circulant matrix with row weight $v = q + 1$ [33]. Let a_k , $k = 0, 1, \dots, v-1$, be the column coordinate of the k -th 1 in the first row, \mathbf{A} can be decomposed as

$$\mathbf{A} = \sum_{k=0}^{v-1} \mathbf{P}^{a_k}.$$

Therefore, the constructed code has a block-circulant Tanner graph of girth 12, which has $2(q^2 + q + 1)$ check nodes and $v(q^2 + q + 1)$ variable nodes. Note that using a different proof method, [15] obtained the same result based on Singer difference set. In Table II, we list the values of a_k for some cages.

For the $(q+1, 8)$ family of cages where q is a prime power, the bi-adjacency matrix \mathbf{A} is a $(q+1)(q^2+1) \times (q+1)(q^2+1)$ matrix with row and column weights $v = q+1$. In [34, Proposition 2], it was shown that \mathbf{A} is a block matrix

$$\mathbf{A} = \begin{bmatrix} \mathbf{A}_{0,0} & \mathbf{A}_{0,1} & \cdots & \mathbf{A}_{0,L-1} \\ \mathbf{A}_{1,0} & \mathbf{A}_{1,1} & \cdots & \mathbf{A}_{1,L-1} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{A}_{L-1,0} & \mathbf{A}_{L-1,1} & \cdots & \mathbf{A}_{L-1,L-1} \end{bmatrix}, \quad (4)$$

where each sub-matrix $\mathbf{A}_{i,j}$ is either an all-zero square matrix or a circulant matrix, and if q is even, $L = q+1$, $\mathbf{A}_{i,j}$ is of size $(q^2+1) \times (q^2+1)$; otherwise, $L = 2(q+1)$, $\mathbf{A}_{i,j}$ is of size $\frac{(q^2+1)}{2} \times \frac{(q^2+1)}{2}$. We have the following result.

TABLE II
THE VALUES OF a_k FOR SOME $(v, g = 6)$ -CAGES

v	$q^2 + q + 1$	$\{a_0, a_1, \dots, a_{v-1}\}$
3	7	$\{0, 1, 3\}$
4	13	$\{0, 1, 4, 6\}$
5	21	$\{0, 1, 4, 14, 16\}$
6	31	$\{0, 1, 4, 10, 12, 17\}$
8	57	$\{0, 1, 3, 13, 32, 36, 43, 52\}$
9	73	$\{0, 1, 3, 7, 15, 31, 36, 54, 63\}$
10	91	$\{0, 1, 6, 10, 23, 26, 34, 41, 53, 55\}$
12	133	$\{0, 1, 10, 58, 60, 64, 82, 87, 98, 101, 113, 126\}$
14	183	$\{0, 1, 9, 12, 22, 45, 50, 106, 110, 112, 126, 141, 158, 165\}$
17	273	$\{0, 1, 3, 7, 15, 31, 63, 90, 116, 127, 136, 181, 194, 204, 233, 238, 255\}$

Proposition 2: The bi-adjacency matrix \mathbf{A} in (4) can be decomposed as $\mathbf{A} = \sum_{k=0}^{v-1} \mathbf{A}_k$, where \mathbf{A}_k is a block matrix consisting of $L \times L$ sub-matrices. Each sub-matrix has the same size as $\mathbf{A}_{i,j}$ and is either an all-zero square matrix or a circulant permutation matrix.

Proof: Define the weight matrix

$$\mathbf{W} = \begin{bmatrix} w_{0,0} & w_{0,1} & \cdots & w_{0,L-1} \\ w_{1,0} & w_{1,1} & \cdots & w_{1,L-1} \\ \vdots & \vdots & \ddots & \vdots \\ w_{L-1,0} & w_{L-1,1} & \cdots & w_{L-1,L-1} \end{bmatrix},$$

where $w_{i,j}$ is the row weight of $\mathbf{A}_{i,j}$. The row weight of \mathbf{W} is $v = q+1$. Based on Birkhoff's theorem [35], \mathbf{W} can be decomposed as

$$\mathbf{W} = \sum_{k=0}^{v-1} \mathbf{W}_k,$$

where \mathbf{W}_k is a permutation matrix. The entry $w_{i,j}$ in \mathbf{W} gives the number of \mathbf{W}_k whose (i, j) entry is 1. Each circulant matrix $\mathbf{A}_{i,j}$ can be written as a sum of $w_{i,j}$ circulant permutation matrices. By substituting these circulant permutation matrices for the 1's as the (i, j) entries of \mathbf{W}_k and substituting all-zero matrices for 0's, we obtain the block matrices \mathbf{A}_k as desired. ■

The constructed code has a block-circulant Tanner graph of girth 16, which has $2(q+1)(q^2+1)$ check nodes and $v(q+1)(q^2+1)$ variable nodes. From the proof we see that a two-round lifting is employed in the code construction. To make this more clear, we give an example. Consider the (3,8)-cage, whose bi-adjacency matrix is given by

$$\mathbf{A} = \begin{bmatrix} \mathbf{P}^0 + \mathbf{P}^1 & \mathbf{P}^0 & \mathbf{0} \\ \mathbf{P}^0 & \mathbf{P}^2 & \mathbf{P}^2 \\ \mathbf{0} & \mathbf{P}^1 & \mathbf{P}^0 + \mathbf{P}^2 \end{bmatrix},$$

where \mathbf{P} is of size 5×5 . Then we can write the weight matrix as

$$\mathbf{W} = \begin{bmatrix} 2 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 2 \end{bmatrix},$$

which can be decomposed as

$$\begin{aligned} \mathbf{W} &= \mathbf{W}_0 + \mathbf{W}_1 + \mathbf{W}_2 \\ &= \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} + \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}. \end{aligned}$$

Correspondingly, \mathbf{A} can be (not uniquely) decomposed as

$$\begin{aligned} \mathbf{A} &= \mathbf{A}_0 + \mathbf{A}_1 + \mathbf{A}_2 \\ &= \begin{bmatrix} \mathbf{P}^0 & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{P}^2 & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{P}^0 \end{bmatrix} + \begin{bmatrix} \mathbf{P}^1 & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{P}^2 \\ \mathbf{0} & \mathbf{P}^1 & \mathbf{0} \end{bmatrix} + \begin{bmatrix} \mathbf{0} & \mathbf{P}^0 & \mathbf{0} \\ \mathbf{P}^0 & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{P}^2 \end{bmatrix}. \end{aligned}$$

To give a different decomposition, \mathbf{A} can also be written as

$$\mathbf{A} = \begin{bmatrix} \mathbf{P}^1 & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{P}^2 & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{P}^2 \end{bmatrix} + \begin{bmatrix} \mathbf{P}^0 & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{P}^2 \\ \mathbf{0} & \mathbf{P}^1 & \mathbf{0} \end{bmatrix} + \begin{bmatrix} \mathbf{0} & \mathbf{P}^0 & \mathbf{0} \\ \mathbf{P}^0 & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{P}^0 \end{bmatrix}.$$

Therefore, the code construction involves a two-round lifting,

$$\begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \xrightarrow{\text{lifting}} \begin{bmatrix} \mathbf{I}_1 & \mathbf{I}_1 & \mathbf{I}_1 \\ \mathbf{W}_0 & \mathbf{W}_1 & \mathbf{W}_2 \end{bmatrix} \xrightarrow{\text{lifting}} \begin{bmatrix} \mathbf{I}_2 & \mathbf{I}_2 & \mathbf{I}_2 \\ \mathbf{A}_0 & \mathbf{A}_1 & \mathbf{A}_2 \end{bmatrix}$$

where \mathbf{I}_1 is the 3×3 identity matrix and \mathbf{I}_2 is the 15×15 identity matrix. Note that the second lifting is a circulant-based lifting while the first lifting is not.

We now investigate the code defined on the (7,6)-cage. The cage is the incidence graph of the elliptic semiplane discovered in [31]. We find that the bi-adjacency matrix of the cage can be written as (5), shown at the bottom of the next page, where \mathbf{P} is of size 3×3 . If we replace each zero matrix in \mathbf{A} by 0 and each circulant permutation matrix in \mathbf{A} by 1, we obtain a 15×15 circulant matrix $\mathbf{W} = \sum_{k=0}^6 \mathbf{W}_k$, with $\mathbf{W}_k = \mathbf{P}^{a_k}$ where \mathbf{P} is of size 15×15 and $\{a_0, \dots, a_6\} = \{0, 5, 7, 10, 11, 13, 14\}$. As in the proof of Proposition 2, we can easily obtain each \mathbf{A}_k from \mathbf{W}_k and \mathbf{A} . Therefore, based on Theorem 1, we can obtain a protograph-based LDPC code with block-circulant Tanner graph of girth 12, using a two-round circulant-based lifting.

B. Codes on Cages With Odd Girth

Since cages with odd girth are in general not regular bipartite graphs, we do not have a general result as in the case of cages with even girth. Here, we find that with appropriate mapping, four independent examples in Table I can be structured as protograph-based LDPC codes with block-circulant Tanner graphs of girth 10. These cages are (3,5)-cage, one of (5,5)-cages (known as the Robertson-Wegner graph [30]), (6,5)-cage, and (7,5)-cage, respectively.

The (3,5)-cage shown in Fig. 3 is used as the associated graph of the code. By labeling the vertices and edges in the cage,

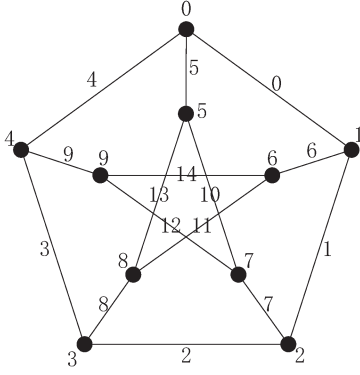


Fig. 3. The (3,5)-cage as the associated graph of the code.

we obtain the Tanner graph with bi-adjacency matrix

$$\mathbf{H}_b = \begin{bmatrix} \mathbf{P}^0 + \mathbf{P}^4 & \mathbf{P}^0 & \mathbf{0} \\ \mathbf{0} & \mathbf{P}^0 & \mathbf{P}^0 + \mathbf{P}^3 \end{bmatrix},$$

where \mathbf{P} is of size 5×5 . The base matrix corresponding to the protograph is given by

$$\mathbf{B} = \begin{bmatrix} 2 & 1 & 0 \\ 0 & 1 & 2 \end{bmatrix}.$$

Note that essentially the same result has been obtained in [13, Example 2].

Due to space limitations, we do not show how to label the vertices and edges for the other three cages. We only give the bi-adjacency matrices of the corresponding Tanner graph. For the (5,5)-cage, the corresponding Tanner graph has the bi-adjacency matrix given in (6), shown at the bottom of the page,

where \mathbf{P} is of size 5×5 . For the (6,5)-cage, the corresponding Tanner graph has the bi-adjacency matrix

$$\mathbf{H}_b = [\mathbf{H}_1 \quad \mathbf{H}_2],$$

where \mathbf{H}_1 and \mathbf{H}_2 are respectively given by (7) and (8), shown at the bottom of the next page, where \mathbf{P} is of size 5×5 . For the (7,5)-cage, the corresponding Tanner graph has the bi-adjacency matrix

$$\mathbf{H}_b = [\mathbf{H}_3 \quad \mathbf{H}_4],$$

where \mathbf{H}_3 and \mathbf{H}_4 are respectively given by (9) and (10), shown at the bottom of the next page, where \mathbf{P} is of size 5×5 .

IV. AN ONTOLOGY-BASED APPROACH TO CODE OPTIMIZATION

In this section, we present an ontology-based approach to the optimization of non-zero entries of the parity-check matrix. The goal is to improve the bit-distance property of the codes, i.e., the distance property of the equivalent binary image codes. The method only assumes a given Tanner graph, and is applicable to general non-binary $(2, v)$ -regular LDPC codes, not limited to the codes defined on cages.

Low bit-weight codewords in the binary image code are most likely induced by low symbol-weight codewords in the original code. Therefore, to improve the bit-distance property, we first need to eliminate low symbol-weight codewords.

In [5], the authors showed that, for non-binary $(2, v)$ -regular LDPC codes, low symbol-weight codewords are caused by short cycles and inter-connected short cycles in the Tanner

$$\mathbf{A} = \begin{bmatrix} \mathbf{P}^2 & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{P}^2 & \mathbf{0} & \mathbf{P}^0 & \mathbf{0} & \mathbf{0} & \mathbf{P}^1 & \mathbf{P}^0 & \mathbf{0} & \mathbf{P}^0 & \mathbf{P}^0 \\ \mathbf{P}^0 & \mathbf{P}^0 & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{P}^2 & \mathbf{0} & \mathbf{P}^0 & \mathbf{0} & \mathbf{0} & \mathbf{P}^0 & \mathbf{P}^1 & \mathbf{0} & \mathbf{P}^2 \\ \mathbf{P}^0 & \mathbf{P}^1 & \mathbf{P}^0 & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{P}^2 & \mathbf{0} & \mathbf{P}^2 & \mathbf{0} & \mathbf{0} & \mathbf{P}^0 & \mathbf{P}^0 & \mathbf{0} \\ \mathbf{0} & \mathbf{P}^1 & \mathbf{P}^0 & \mathbf{P}^2 & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{P}^2 & \mathbf{0} & \mathbf{P}^0 & \mathbf{0} & \mathbf{0} & \mathbf{P}^1 & \mathbf{P}^0 \\ \mathbf{P}^0 & \mathbf{0} & \mathbf{P}^2 & \mathbf{P}^0 & \mathbf{P}^1 & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{P}^0 & \mathbf{0} & \mathbf{P}^2 & \mathbf{0} & \mathbf{0} & \mathbf{P}^0 \\ \mathbf{P}^2 & \mathbf{P}^1 & \mathbf{0} & \mathbf{P}^1 & \mathbf{P}^1 & \mathbf{P}^0 & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{P}^0 & \mathbf{0} & \mathbf{P}^1 & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{P}^1 & \mathbf{P}^2 & \mathbf{0} & \mathbf{P}^1 & \mathbf{P}^1 & \mathbf{P}^1 & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{P}^0 & \mathbf{0} & \mathbf{P}^1 & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{P}^1 & \mathbf{P}^1 & \mathbf{0} & \mathbf{P}^1 & \mathbf{P}^2 & \mathbf{P}^1 & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{P}^0 & \mathbf{0} & \mathbf{P}^0 \\ \mathbf{P}^1 & \mathbf{0} & \mathbf{0} & \mathbf{P}^2 & \mathbf{P}^1 & \mathbf{0} & \mathbf{P}^1 & \mathbf{P}^1 & \mathbf{P}^0 & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{P}^1 & \mathbf{0} \\ \mathbf{0} & \mathbf{P}^1 & \mathbf{0} & \mathbf{0} & \mathbf{P}^1 & \mathbf{P}^1 & \mathbf{0} & \mathbf{P}^0 & \mathbf{P}^1 & \mathbf{P}^2 & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{P}^1 \\ \mathbf{P}^1 & \mathbf{0} & \mathbf{P}^2 & \mathbf{0} & \mathbf{0} & \mathbf{P}^0 & \mathbf{P}^2 & \mathbf{0} & \mathbf{P}^2 & \mathbf{P}^2 & \mathbf{P}^1 & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{P}^1 & \mathbf{0} & \mathbf{P}^2 & \mathbf{0} & \mathbf{0} & \mathbf{P}^2 & \mathbf{P}^0 & \mathbf{0} & \mathbf{P}^1 & \mathbf{P}^2 & \mathbf{P}^2 & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{P}^1 & \mathbf{0} & \mathbf{P}^1 & \mathbf{0} & \mathbf{0} & \mathbf{P}^2 & \mathbf{P}^2 & \mathbf{0} & \mathbf{P}^2 & \mathbf{P}^0 & \mathbf{P}^2 & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{P}^1 & \mathbf{0} & \mathbf{P}^2 & \mathbf{0} & \mathbf{0} & \mathbf{P}^0 & \mathbf{P}^2 & \mathbf{0} & \mathbf{P}^2 & \mathbf{P}^2 & \mathbf{P}^1 & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{P}^2 & \mathbf{0} & \mathbf{P}^1 & \mathbf{0} & \mathbf{0} & \mathbf{P}^2 & \mathbf{P}^2 & \mathbf{0} & \mathbf{P}^1 & \mathbf{P}^2 & \mathbf{P}^0 \end{bmatrix} \quad (5)$$

$$\mathbf{H}_b = \begin{bmatrix} \mathbf{P}^0 & \mathbf{0} & \mathbf{0} & \mathbf{P}^0 & \mathbf{0} & \mathbf{P}^0 & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{P}^0 + \mathbf{P}^2 & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{P}^0 & \mathbf{0} & \mathbf{0} & \mathbf{P}^0 & \mathbf{0} & \mathbf{0} & \mathbf{P}^0 & \mathbf{0} & \mathbf{0} & \mathbf{P}^0 + \mathbf{P}^2 & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{P}^0 & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{P}^0 & \mathbf{0} & \mathbf{P}^0 & \mathbf{0} & \mathbf{0} & \mathbf{P}^0 + \mathbf{P}^2 & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{P}^0 & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{P}^0 & \mathbf{P}^0 & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{P}^0 + \mathbf{P}^4 & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{P}^4 & \mathbf{0} & \mathbf{P}^0 & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{P}^3 & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{P}^0 + \mathbf{P}^4 & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{P}^1 & \mathbf{0} & \mathbf{P}^3 & \mathbf{P}^0 & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{P}^0 + \mathbf{P}^4 \end{bmatrix} \quad (6)$$

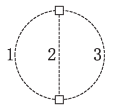
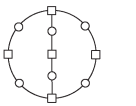
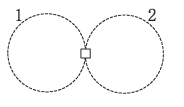
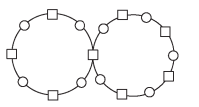
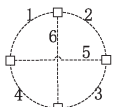
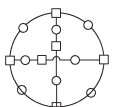
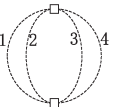
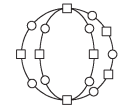
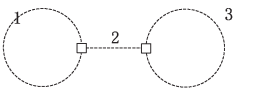
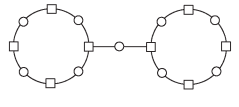
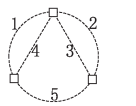
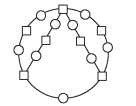
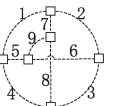
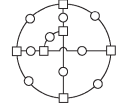
Patterns	Examples
 $A - (n_1, n_2, n_3)$	 $A - (2, 2, 2)$
 $B - (n_1, n_2)$	 $B - (4, 5)$
 $C - (n_1, n_2, n_3, n_4, n_5, n_6)$	 $C - (1, 1, 1, 1, 2, 2)$
 $D - (n_1, n_2, n_3, n_4)$	 $D - (2, 2, 2, 3)$
 $E - (n_1, n_2, n_3)$	 $E - (4, 1, 4)$
 $F - (n_1, n_2, n_3, n_4, n_5)$	 $F - (2, 2, 2, 2, 1)$
 $G - (n_1, n_2, n_3, n_4, n_5, n_6, n_7, n_8, n_9)$	 $G - (1, 1, 1, 1, 1, 1, 1, 1, 1)$

Fig. 4. Ontology of inter-connected short cycles.

inter-connected short cycles. This can be efficiently done once the submatrices are identified. Now the key is how to identify these submatrices, or equivalently the corresponding subgraphs.

For a given Tanner graph, short cycles can be easily identified. In contrast, it is more difficult to identify inter-connected cycles. To address this problem, we follow the methodology in [36] and develop an ontology, which consists of all possible patterns of inter-connected cycles that lead to low symbol-weight codewords. The ontology is illustrated in Fig. 4, where each pattern is denoted by an uppercase letter followed by a tuple, e.g., $A - (n_1, n_2, n_3)$. The i -th element n_i of the tuple represents the number of variable nodes in the edge i . For these inter-connected cycles, the number of variable nodes is given by $w = \sum_i n_i$, strictly larger than that of check nodes. For some codes, e.g., the codes defined on cages with even girth, all cycles in the Tanner graph have lengths divisible by 4. We categorize all inter-connected cycles into two types. An inter-connected cycle is called Type-I if all cycles involved have lengths divisible by 4; otherwise, it is called Type-II.

Based on the ontology, we create a database, as shown in Table III. The database enumerates all possible inter-connected cycles that lead to codewords of symbol weight up to $\lceil \frac{3}{4}g_T \rceil + 3$, where $g_T = 8, 10, \dots, 16$ is the girth of the Tanner graph. For Tanner graphs with $g_T > 16$, codewords of symbol weight up to $\lceil \frac{3}{4}g_T \rceil + 3$ are only caused by the $A - (n_1, n_2, n_3)$ pattern. Due to space limitations, we do not include them in Table III. The reader can easily figure them out.

Given the database, we are aware of searching for which inter-connected cycles. Once all short cycles are obtained, the intended inter-connected short cycles can be easily identified.

Therefore, the ontology-based approach makes the optimization of bit-distance spectrum handleable. To accelerate the code search process, however, we need to consider some more detailed problems encountered in practice. There are two major factors that may slow down the code search process.

The first factor is about how much effort should be paid on the cancellation of short cycles. The number of short cycles we can cancel depends on the number of short cycles and the field order. For large fields, for example $\text{GF}(2^8)$, it is usually easy to cancel all short cycles of lengths less than or equal to $2 \times \lceil \frac{3}{4}g_T \rceil$. For most Tanner graphs, this means that the minimum symbol-weight codewords are collectively provided by short cycles and inter-connected short cycles. If it becomes time-consuming to cancel cycles of larger lengths, we stop the cycle cancellation procedure.

The second factor is that there may be a huge number of inter-connected cycles, which makes the estimation of bit-distance spectrum very time-consuming. We address the problem based on the observation that minimum bit-weight codewords tend to be induced by minimum symbol-weight codewords. We first coarsely estimate the minimum bit-distance of each code by only using the inter-connected cycles that lead to the minimum symbol-weight codewords. Empirically, the number of these inter-connected cycles is far less than that of all identified inter-connected cycles. In this way, we can quickly filter out the codes that have less minimum bit-distance and keep some candidate codes that potentially have large minimum bit-distance. For these candidate codes, we make a refined estimation of bit-distance spectrum based on all identified cycles and inter-connected cycles. Then we select the best code from these candidate codes.

For cycle cancellation, we follow the method presented in [5]. Non-zero field elements are replaced randomly in a row manner, on the premise that more short cycles will be cancelled. Some good candidate rows have been tabulated in [5].

V. CODE DESIGN EXAMPLES AND NUMERICAL RESULTS

In this section, we use the proposed ontology-based method to analyze some known codes and design some new codes defined on cages. Numerical results are presented. We assume that BPSK is used over the AWGN channel and the maximum number of iterations for decoding is set to be 100.

Example 1: In the CCSDS recommendation [14], there are three (16,8) non-binary LDPC codes over $\text{GF}(2^8)$. The first code was designed by DLR, while the other two codes were designed by NASA-JPL. As a QC code, the third code is called

TABLE III
A DATABASE OF SMALL-SIZE INTER-CONNECTED CYCLES

g_T	w	Type-I	Type-II
8	6	$A - (2, 2, 2)$	
	7	$A - (1, 3, 3)$	$A - (2, 2, 3)$
	8	$A - (2, 2, 4), B - (4, 4), C - (1, 1, 1, 1, 2, 2),$ $D - (2, 2, 2, 2)$	$A - (1, 3, 4), A - (2, 3, 3)$
	9	$A - (1, 3, 5), A - (3, 3, 3), C - (1, 1, 2, 2, 2, 1),$ $E - (4, 1, 4), F - (2, 3, 1, 2, 1),$ $G - (1, 1, 1, 1, 1, 1, 1, 1, 1)$	$A - (1, 4, 4), A - (2, 2, 5), A - (2, 3, 4), B - (4, 5),$ $C - (1, 1, 1, 1, 2, 3), C - (1, 2, 1, 2, 1, 2),$ $D - (2, 2, 2, 3), F - (2, 2, 2, 2, 1)$
10	8		$A - (2, 3, 3)$
	9	$A - (3, 3, 3)$	$A - (1, 4, 4), A - (2, 3, 4)$
	10	$A - (2, 4, 4)$	$A - (1, 4, 5), A - (2, 3, 5), A - (3, 3, 4), B - (5, 5),$ $C - (2, 2, 2, 2, 1, 1)$
	11	$A - (1, 5, 5), A - (3, 3, 5)$	$A - (1, 4, 6), A - (2, 3, 6), A - (2, 4, 5),$ $A - (3, 4, 4), B - (5, 6), C - (2, 2, 2, 2, 1, 2),$ $C - (3, 2, 2, 2, 1, 1), C - (1, 3, 2, 2, 1, 2),$ $D - (2, 3, 3, 3), E - (5, 1, 5), F - (2, 3, 2, 3, 1)$
12	9	$A - (3, 3, 3)$	
	10	$A - (2, 4, 4)$	$A - (3, 3, 4)$
	11	$A - (1, 5, 5), A - (3, 3, 5)$	$A - (2, 4, 5), A - (3, 4, 4)$
	12	$A - (2, 4, 6), A - (4, 4, 4), B - (6, 6),$ $C - (2, 2, 2, 2, 2, 2), C - (1, 2, 1, 2, 3, 3),$ $D - (3, 3, 3, 3)$	$A - (1, 5, 6), A - (2, 5, 5), A - (3, 3, 6),$ $A - (3, 4, 5)$
14	11		$A - (3, 4, 4)$
	12	$A - (4, 4, 4)$	$A - (2, 5, 5), A - (3, 4, 5)$
	13	$A - (3, 5, 5)$	$A - (1, 6, 6), A - (2, 5, 6), A - (3, 4, 6),$ $A - (4, 4, 5)$
	14	$A - (2, 6, 6), A - (4, 4, 6)$	$A - (2, 5, 7), A - (3, 4, 7), A - (3, 5, 6),$ $A - (1, 6, 7), A - (4, 5, 5), B - (7, 7),$ $C - (2, 2, 2, 2, 3, 3), C - (3, 3, 3, 3, 1, 1)$
16	12	$A - (4, 4, 4)$	
	13	$A - (3, 5, 5)$	$A - (4, 4, 5)$
	14	$A - (2, 6, 6), A - (4, 4, 6)$	$A - (3, 5, 6), A - (4, 5, 5)$
	15	$A - (1, 7, 7), A - (3, 5, 7), A - (3, 6, 6),$ $A - (5, 5, 5)$	$A - (2, 6, 7), A - (4, 4, 7), A - (4, 5, 6)$

a graph cover non-binary protograph-based code [10], [11]. Based on the ontology-based approach, we estimate the bit-distance spectrum of the three codes and design a new QC code.

Up to column permutations, all the three codes in the CCSDS recommendation can be viewed as codes defined on the (4,4)-cage. We denote these codes (after column permutation) by C_1 , C_2 and C_3 , respectively. Our designed code is also defined on this cage and denoted by C_4 . The Tanner graph has the bi-adjacency matrix

$$\mathbf{H}_b = \begin{bmatrix} \mathbf{P}^0 & \mathbf{P}^0 & \mathbf{P}^0 & \mathbf{P}^0 \\ \mathbf{P}^0 & \mathbf{P}^1 & \mathbf{P}^2 & \mathbf{P}^3 \end{bmatrix},$$

where \mathbf{P} is of size 4×4 . The cycle distribution of the Tanner graph is given by $36x^8 + 96x^{12} + 72x^{16}$. Table IV gives the number of inter-connected short cycles in the Tanner graph. In [39], we list the identified short cycles and inter-connected short cycles in the Tanner graph.

The non-zero elements of the parity-check matrices for C_1 , C_2 , C_3 and C_4 are given in Table V, where each element is represented by the power of a primitive element of $\text{GF}(2^8)$. The field is generated using the primitive polynomial $f(x) = 1 + x^2 + x^3 + x^4 + x^8$. The positions of these non-zero entries are known from \mathbf{H}_b .

With the non-zero entries given in Table V, all cycles have been cancelled for C_1 and C_2 . For C_3 and C_4 , all cycles of length 8 and 16 have been cancelled, and some cycles of length 12 are not cancelled. Note that whether a code with a block-circulant Tanner graph is a quasi-cyclic code depends on the selection of

TABLE IV
INTER-CONNECTED SHORT CYCLES FOR THE
TANNER GRAPH FROM THE (4,4)-CAGE

Pattern	Number
$A - (2, 2, 2)$	48
$A - (1, 3, 3)$	288
$A - (2, 2, 4)$	288
$B - (4, 4)$	144
$C - (1, 1, 1, 1, 2, 2)$	144
$D - (2, 2, 2, 2)$	12
$A - (1, 3, 5)$	432
$A - (3, 3, 3)$	96
$C - (1, 1, 2, 2, 2, 1)$	192
$E - (4, 1, 4)$	144
$F - (2, 3, 1, 2, 1)$	576
$G - (1, 1, 1, 1, 1, 1, 1, 1, 1)$	16

non-zero entries. It can be proved [15] that due to the constraint of the quasi-cyclicity on C_3 and C_4 , those un-cancelled cycles of length 12 cannot be cancelled by selecting non-zero entries.

Based on the ontology-based method, the bit-weight spectrum is estimated, as shown in Table VI. The estimated minimum bit-distances of these codes are 13, 14, 15, and 15, respectively. We see that C_4 has a reduced multiplicity of minimum bit-weight codewords compared to C_3 . In [39], we provide the minimum bit-weight codewords of the four codes. It was reported in [12] that, using the algorithm in [37], one codeword of weight 13 and seven codewords of weight 14 were found for C_1 . Here, we found fifteen codewords of weight 14 for C_1 . Therefore, the ontology-based method gives a better estimation result for the codes.

TABLE V
NON-ZERO ENTRIES OF THE PARITY-CHECK MATRICES

C_1				C_2			
173	0	182	8	183	173	0	8
9	81	89	0	0	88	8	80
182	8	0	173	0	167	40	127
173	0	8	182	0	182	8	173
0	8	88	80	0	89	9	81
127	40	169	0	8	0	173	182
40	0	169	128	173	8	183	0
88	0	8	80	8	0	80	88
C_3				C_4			
89	9	81	0	183	173	0	8
89	9	81	0	183	173	0	8
89	9	81	0	183	173	0	8
89	9	81	0	183	173	0	8
0	80	8	88	0	8	183	173
0	80	8	88	0	8	183	173
0	80	8	88	0	8	183	173
0	80	8	88	0	8	183	173

TABLE VI
ESTIMATED BIT-WEIGHT DISTRIBUTIONS FOR THE FOUR CODES

	13	14	15	16	17	18	19	20	21
C_1	1	15	36	185	658	2057	6192	17727	45506
C_2	-	17	53	177	633	2085	6455	17431	45502
C_3	-	-	60	200	644	2114	6376	17910	45600
C_4	-	-	8	172	664	2124	6016	17220	46448

TABLE VII
INTER-CONNECTED SHORT CYCLES FOR THE
TANNER GRAPH FROM THE (4,6)-CAGE

Pattern	Number
$A - (3, 3, 3)$	468
$A - (2, 4, 4)$	2808
$A - (1, 5, 5)$	8424
$A - (3, 3, 5)$	2808
$A - (2, 4, 6)$	14976
$A - (4, 4, 4)$	936
$B - (6, 6)$	5616
$C - (2, 2, 2, 2, 2, 2)$	468
$C - (1, 2, 1, 2, 3, 3)$	2808
$D - (3, 3, 3, 3)$	117

The FER performance curves for C_1 , C_2 , and C_3 can be found in [14] (see also [12] and [11]). In the low-to-moderate signal-to-noise ratio (SNR) region, the three codes have almost the same FER performance. In the high SNR region ($\text{FER} \approx 10^{-8}$), C_1 and C_2 perform slightly better than C_3 , which may be explained as follows: The advantage of C_3 over C_1 and C_2 in terms of minimum bit-distance is not sufficient to cancel out the influence of quasi-cyclicity restriction on C_3 . Our simulation shows that C_4 has almost the same FER performance as C_1 and C_2 , and we do not provide the performance curve for C_4 here.

Example 2: We consider the (52,26) codes over $\text{GF}(2^8)$, which are defined on the (4,6)-cage. The Tanner graph has the bi-adjacency matrix

$$\mathbf{H}_b = \begin{bmatrix} \mathbf{p}^0 & \mathbf{p}^0 & \mathbf{p}^0 & \mathbf{p}^0 \\ \mathbf{p}^0 & \mathbf{p}^1 & \mathbf{p}^4 & \mathbf{p}^6 \end{bmatrix},$$

where \mathbf{P} is of size 13×13 . The cycle distribution is given by $234x^{12} + 702x^{16} + 5616x^{20} + 21060x^{24} + \dots$. Table VII gives the number of inter-connected short cycles in the Tanner graph.

TABLE VIII
THE NONZERO FIELD ELEMENTS OF THE PARITY-CHECK MATRIX

8	173	183	0
81	0	89	9
183	0	172	8
167	127	40	0
169	40	127	0
169	40	128	0
8	173	183	0
8	182	173	0
172	0	182	8
0	80	8	88
40	127	0	169
0	8	183	173
0	80	88	8
0	172	8	183
88	8	80	0
80	88	0	8
0	80	8	88
81	89	9	0
167	127	40	0
182	172	8	0
0	169	40	127
40	167	127	0
169	40	0	128
40	167	127	0
127	40	0	167
183	173	8	0

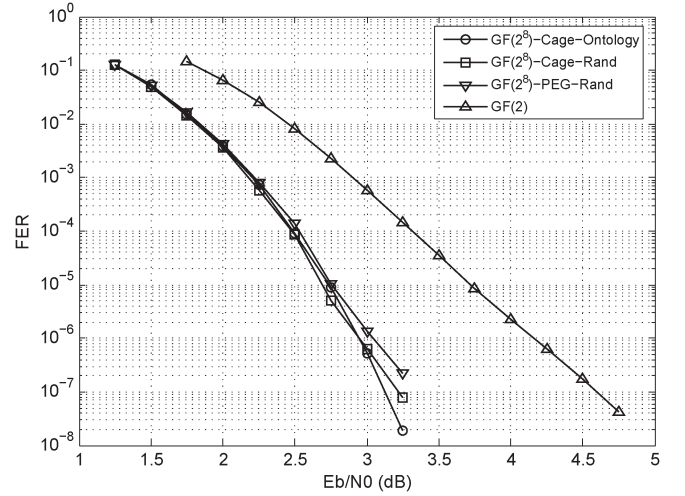


Fig. 5. The FER performances of the simulated LDPC codes.

Based on the ontology-based method, we obtain a code for which the non-zero elements of the parity-check matrix are given in Table VIII. The element representation is the same as in Example 1. All cycles of length 12 and 16 have been cancelled. The minimum bit-distance of the code is estimated as 22 and the bit-weight spectrum is estimated as $4x^{22} + 46x^{23} + 108x^{24} + 322x^{25} + 695x^{26} + 1540x^{27} + 3255x^{28} + \dots$.

Fig. 5 shows the FER performance of the code. For comparison, the performance curves of three other codes are also included in Fig. 5. The first two codes are (52,26) (2,4)-regular LDPC codes over $\text{GF}(2^8)$. The first code is defined on the (4,6)-cage. The second code has a Tanner graph of girth 12, which is generated based on the PEG algorithm [38]. For both codes, the non-zero elements of the parity-check matrices are randomly selected. Using the ontology-based method, the minimum bit-distances of the two codes are estimated as 16 and 13, respectively. The third code is the (414,209) binary regular LDPC

TABLE IX
INTER-CONNECTED SHORT CYCLES FOR THE
TANNER GRAPH FROM THE (4,8)-CAGE

Pattern	Number
$A - (4, 4, 4)$	4320
$A - (3, 5, 5)$	25920
$A - (2, 6, 6)$	77760
$A - (4, 4, 6)$	25920

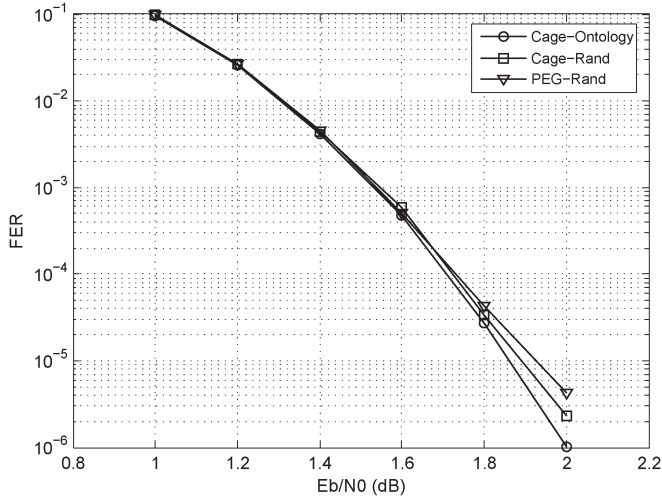


Fig. 6. The FER performances of three (160,80) LDPC codes over $GF(2^8)$.

code in [25, Table II]. The parity-check matrix of the binary code has row weight 6 and column weight 3 and the Tanner graph has girth 8. The code has the minimum distance 22.

It can be seen that all the three non-binary codes perform significantly better than the binary code. In the low-to-moderate SNR region, the three non-binary codes have almost the same performance. In the high SNR region, the two codes defined on cages perform better than the PEG-based code. Furthermore, our designed code has the best performance and no error floor is observed.

Example 3: We consider the (160,80) codes over $GF(2^8)$, which are defined on the (4,8)-cage. The cycle distribution is given by $1620x^{16} + 5184x^{20} + 43200x^{24} + \dots$. Table IX gives the number of inter-connected short cycles in the Tanner graph.

Using the ontology-based method, we obtain a code whose parity-check matrix is given in [39]. For this code, all cycles of length 16 and 20 have been cancelled. The minimum bit-distance of the code is estimated as 30 and the bit-weight spectrum is estimated as $21x^{30} + 54x^{31} + 183x^{32} + 480x^{33} + \dots$.

Fig. 6 shows the FER performance of the code. For comparison, we also simulated two other (160,80) (2,4)-regular LDPC codes over $GF(2^8)$. The first code is defined on the (4,8)-cage. The second code has a Tanner graph of girth 12, which is generated based on the PEG algorithm [38]. For both codes, the non-zero elements of the parity-check matrices are randomly selected. Using the ontology-based method, the minimum bit-distances of the two codes are estimated as 20 and 16, respectively. Compared to the two codes, our designed code has a much better minimum bit-distance. From Fig. 6, it can be seen that in the low-to-moderate SNR region, the three codes have almost the same performance. In the high SNR region,

our designed code has better performance as expected, since selective instead of random assignment of non-zero entries is performed using ontology-based method.

VI. CONCLUSION

In this paper, we studied non-binary $(2, \nu)$ -regular LDPC codes defined on cages. We found that many cages can be structured as protograph-based codes and most of these codes have block-circulant Tanner graphs. For code optimization, we developed an ontology-based method for general $(2, \nu)$ -regular LDPC codes (not limited to the codes defined on cages). The bit-distance spectrum can be effectively estimated. When applying the method to cages, codes with good minimum bit-distance have been found. Simulation results showed that these codes perform well under iterative decoding.

As a future work, it would be interesting to investigate whether the infinite family of cages from generalized hexagons in Table I can be structured as codes with block-circulant Tanner graphs. As a specific case, the (3,12)-cage has been shown to have this property in [21].

ACKNOWLEDGMENT

The first author would like to thank Dr. Tao Huang and Dr. Pingping Chen for helpful discussion, Prof. Weigang Chen for providing the copy of [16], and Prof. Xiao Ma for polishing the paper. The authors would like to thank the three anonymous reviewers and the Editor for their valuable comments that help improve the manuscript.

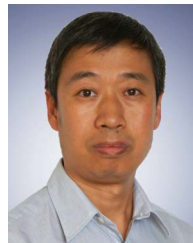
REFERENCES

- [1] R. G. Gallager, *Low-Density Parity-Check Codes*. Cambridge, MA, USA: MIT Press, 1963.
- [2] M. C. Davey and D. J. C. MacKay, "Low-density parity check codes over $GF(q)$," *IEEE Commun. Lett.*, vol. 2, no. 6, pp. 165–167, Jun. 1998.
- [3] X.-Y. Hu and E. Eleftheriou, "Binary representation of cycle Tanner-graph $GF(2^b)$ codes," in *Proc. IEEE Int. Conf. Commun.*, Paris, France, Jun. 2004, pp. 528–532.
- [4] D. J. C. MacKay, Optimizing Sparse Graph Codes Over $GF(q)$, Aug. 2003. [Online]. Available: <http://www.inference.phy.cam.ac.uk/mackay/CodesGallager.html>
- [5] C. Poulliat, M. Fossorier, and D. Declercq, "Design of regular $(2, d_c)$ -LDPC codes over $GF(q)$ using their binary images," *IEEE Trans. Commun.*, vol. 56, no. 10, pp. 1626–1635, Oct. 2008.
- [6] A. Venkiah, D. Declercq, and C. Poulliat, "Design of cages with a randomized progressive edge growth algorithm," *IEEE Commun. Lett.*, vol. 12, no. 4, pp. 301–303, Apr. 2008.
- [7] J. Huang, S. Zhou, and P. Willett, "Structure, property, and design of nonbinary regular cycle codes," *IEEE Trans. Commun.*, vol. 58, no. 4, pp. 1060–1071, Apr. 2010.
- [8] B.-Y. Chang, L. Dolecek, and D. Divsalar, "EXIT chart analysis and design of non-binary protograph-based LDPC codes," in *Proc. IEEE Military Communications Conference (Milcom)*, Baltimore, MD, USA, Nov. 2011, pp. 566–571.
- [9] B.-Y. Chang, D. Divsalar, and L. Dolecek, "Non-binary protograph-based LDPC codes for short block-lengths," in *Proc. ITW*, Sep. 2012, pp. 282–286.
- [10] D. Divsalar and L. Dolecek, "Graph cover ensembles of non-binary protograph LDPC codes," in *Proc. IEEE ISIT*, Cambridge, MA, USA, 2012, pp. 2526–2530.
- [11] L. Dolecek, D. Divsalar, Y. Sun, and B. Amiri, "Non-binary protograph-based LDPC codes: Enumerators, analysis, and designs," *IEEE Trans. Inf. Theory*, vol. 60, no. 7, pp. 3913–3941, Jul. 2014.

- [12] G. Liva, E. Paolini, T. D. Cola, and M. Chiani, "Codes on high-order fields for the CCSDS next generation uplink," in *Proc. 6th ASMS 12th SPSC*, Sep. 2012, pp. 44–48.
- [13] G. Liva, E. Paolini, B. Matuz, S. Scalise, and M. Chiani, "Short turbo codes over high order fields," *IEEE Trans. Commun.*, vol. 61, no. 6, pp. 2201–2211, Jun. 2013.
- [14] Short Blocklength LDPC Codes for TC Synchronization and Channel Coding, Recommendation for Space Data System Standards, CCSDS 231.0-O-y.y, Oct. 2012.
- [15] C. Chen, B. Bai, and X. Wang, "Construction of nonbinary quasi-cyclic LDPC cycle codes based on Singer perfect difference set," *IEEE Commun. Lett.*, vol. 14, no. 2, pp. 181–183, Feb. 2010.
- [16] W. Chen, C. Poulliat, D. Declercq, and J. Lu, "Structured high-girth non-binary cycle codes," in *Proc. 15th APCC*, Shanghai, China, Oct. 2009, pp. 462–466.
- [17] G. Liva, E. Paolini, B. Matuz, and M. Chiani, "Short non-binary IRA codes on large-girth Hamiltonian graphs," in *Proc. IEEE Int. Conf. Commun.*, 2012, pp. 2616–2620.
- [18] R. M. Tanner, "A recursive approach to low-complexity codes," *IEEE Trans. Inf. Theory*, vol. IT-27, no. 6, pp. 533–547, Nov. 1981.
- [19] H. Song, J. Liu, and B. V. K. V. Kumar, "Large girth cycle codes for partial response channels," *IEEE Trans. Magn.*, vol. 40, no. 4, pp. 3084–3086, Jul. 2004.
- [20] G. Malema and M. Liebelt, "High girth column-weight-two LDPC codes based on distance graphs," *EURASIP J. Wireless Commun. Netw.*, vol. 2007, no. 1, 2007, Art. ID. 48158.
- [21] I. E. Bocharova, B. D. Kudryashov, and R. V. Satyukov, "Graph-based convolutional and block LDPC codes," *Problems Inf. Transmiss.*, vol. 45, no. 4, pp. 357–377, 2009.
- [22] J. Thorpe, "Low-Density Parity-Check (LDPC) codes constructed from protographs," Jet Propulsion Laboratory, Pasadena, CA, USA, IPN Progr. Rep. 42-154, Aug. 2003.
- [23] J. Xu, L. Chen, L. Zeng, L. Lan, and S. Lin, "Construction of low-density parity-check codes by superposition," *IEEE Trans. Commun.*, vol. 53, no. 2, pp. 243–251, Feb. 2005.
- [24] M. P. C. Fossorier, "Quasi-cyclic low-density parity-check codes from circulant permutation matrices," *IEEE Trans. Inf. Theory*, vol. 50, no. 8, pp. 1788–1793, Aug. 2004.
- [25] D. J. C. MacKay and M. C. Davey, "Evaluation of Gallager codes for short block length and high rate applications," *IMA Volumes Math. Appl.*, vol. 123, pp. 113–130, 2001.
- [26] I. E. Bocharova, F. Hug, R. Johannesson, B. D. Kudryashov, and R. V. Satyukov, "Searching for voltage graph-based LDPC tailbiting codes with large girth," *IEEE Trans. Inf. Theory*, vol. 58, no. 4, pp. 2265–2279, Apr. 2012.
- [27] D. G. M. Mitchell, R. Smarandache, and D. J. Costello, Jr., "Quasi-cyclic LDPC codes based on pre-lifted protographs," in *Proc. IEEE Inf. Theory Workshop*, Paraty, Brazil, Oct. 2011, pp. 350–354.
- [28] Y. Wang, S. C. Draper, and J. S. Yededia, "Hierarchical and high-girth QC LDPC codes," *IEEE Trans. Inf. Theory*, vol. 59, no. 7, pp. 4553–4583, Jul. 2013.
- [29] P. Wong, "Cages—A survey," *J. Graph Theory*, vol. 6, no. 1, pp. 1–22, 1982.
- [30] G. Exoo and R. Jajcay, "Dynamic cage survey," *Electron. J. Combinatorics*, vol. 16, 2008.
- [31] R. D. Baker, "An elliptic semiplane," *J. Combin. Theory Ser. A*, vol. 25, pp. 193–195, 1978.
- [32] H. van Maldeghem, *Generalized Polygons*. Basel, Switzerland: Birkhauser-Verlag, 1998.
- [33] 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. Inf. Theory*, vol. 47, no. 7, pp. 2711–2736, Nov. 2001.
- [34] Z. Liu and D. A. Pados, "LDPC codes from generalized polygons," *IEEE Trans. Inf. Theory*, vol. 51, no. 11, pp. 3890–3898, Nov. 2005.
- [35] J. H. van Lint and R. M. Wilson, *A Course in Combinatorics*, 2nd ed. Cambridge, U.K.: Cambridge Univ. Press, 2001.
- [36] B. Vasic, S. K. Chilappagari, D. V. Nguyen, and S. K. Planjery, "Trapping set ontology," in *Proc. Allerton Conf. Commun., Control, Comput.*, Monticello, IL, USA, Sep. 30–Oct. 2, 2009, pp. 1–7.
- [37] X.-Y. Hu, M. P. C. Fossorier, and E. Eleftheriou, "On the computation of the minimum distance of low-density parity-check codes," in *Proc. IEEE Int. Conf. Communi.*, Paris, France, Jun. 2004, pp. 767–771.
- [38] X.-Y. Hu, E. Eleftheriou, and D. M. Arnold, "Regular and irregular progressive edge-growth Tanner graphs," *IEEE Trans. Inf. Theory*, vol. 51, no. 1, pp. 386–398, Jan. 2005.
- [39] C. Chen, "An Ontology-Based Approach to the Optimization of Non-Binary $(2, v)$ -Regular LDPC Codes," Tech. Rep. [Online]. Available: <http://arxiv.org/abs/1409.2019>



Chao Chen received the Ph.D. degree from Xidian University, Xi'an, China, in 2010. He is currently with the School of Electronic Engineering, Xidian University. His research interests include information theory, channel coding, and network coding.



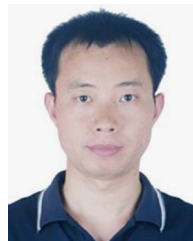
Baoming Bai (S'98–M'00) received the B.S. degree from the Northwest Telecommunications Engineering Institute, Xi'an, China, in 1987, and the M.S. and Ph.D. degrees in communication engineering from Xidian University, Xi'an, in 1990 and 2000, respectively. From 2000 to 2003, he was a Senior Research Assistant at the Department of Electronic Engineering, City University of Hong Kong. Since April 2003, he has been with the State Key Laboratory of Integrated Services Networks, School of Telecommunication Engineering, Xidian University, where he is currently a Professor. In 2005, he was with the University of California, Davis, CA, USA, as a Visiting Scholar. His research interests include information theory and channel coding, wireless communication, and quantum communication.



Guangming Shi (SM'10) received the B.S. degree in automatic control, the M.S. degree in computer control, and the Ph.D. degree in electronic information technology from Xidian University, Xi'an, China, in 1985, 1988, and 2002, respectively. He joined the School of Electronic Engineering, Xidian University, in 1988. From 1994 to 1996, he was a Research Assistant with the Department of Electronic Engineering, University of Hong Kong, Hong Kong. Since 2003, he has been a Professor with the School of Electronic Engineering, Xidian University. In 2004, he was the Head of the National Instruction Base of Electrician and Electronics, Xidian University. In 2004, he was with the Department of Electronic Engineering, University of Illinois at Urbana-Champaign, Champaign, IL, USA. He is currently the Deputy Director of the School of Electronic Engineering, Xidian University, and the Academic Leader in the subject of circuits and systems. He has authored or co-authored over 60 research papers. His research interests include compressed sensing, theory and design of multirate filter banks, image denoising, low-bit rate image/video coding, and implementation of algorithms for intelligent signal processing (using DSP and FPGA).



Xiaotian Wang received the B.S. degree in electronic engineering and the Ph.D. degree in electronic science and technology from Xidian University, Xi'an, China, in 2005 and 2011, respectively. She is currently a Lecturer at the School of Electronic Engineering, Xidian University. Her current research interests include image quality evaluation and enhancement, EEG signal modeling, and detection.



Xiaopeng Jiao received the B.S. and Ph.D. degrees from Xidian University, Xi'an, China, in 2004 and 2009, respectively. He is currently an Associate Professor at the School of Computer Science and Technology, Xidian University. His research area is information and coding theory.