High-Rate Girth-Eight Low-Density Parity-Check Codes on Rectangular Integer Lattices

High-Rate Girth-Eight Low-Density Parity-Check Codes on Rectangular Integer Lattices

Bane Vasic, *Senior Member, IEEE*, Karunakar Pedagani, and Milos Ivkovic

***Abstract*—This letter introduces a combinatorial construction of girth-eight high-rate low-density parity-check codes based on integer lattices. The parity-check matrix of a code is defined as a point-line incidence matrix of a 1-configuration based on a rectangular integer lattice, and the girth-eight property is achieved by a judicious selection of sets of parallel lines included in a configuration. A class of codes with a wide range of lengths and column weights is obtained. The resulting matrix of parity checks is an array of circulant matrices.**

***Index Terms*—Combinatorial designs, error-control coding, finite geometries, graph girth, iterative decoding, low-density parity-check (LDPC) codes.**

I. Introduction

CODES on graphs, especially low-density parity-check (LDPC) codes, is a research area of great current interest. The theory of codes on graphs has not only yielded capacity-approaching codes, it has also opened new research avenues for investigating alternative optimal and suboptimal decoding schemes based on belief propagation. Applied on a Tanner graph of a linear block code [6], [12], the belief-propagation algorithm gives an exact *a posteriori* probability mass function for a given probability density function of the observed variables, but only if the factor graph is cycle free. Extensive simulation results of MacKay and Neal [14] showed that the message-passing algorithm also performs well in graphs with cycles. However, the presence of short cycles hurts the performance.

In this letter, we address the problem of finding codes with good cycle properties. We are interested in "deterministic" sparse parity-check matrices, as opposed to the common "random code" assumption that has been widely used in recent research [13]. One of the first attempts to design a deterministic LDPC for iterative decoding is due to Kou *et al.* [3], and it is based on projective and Euclidean geometries. The codes given in [3] are one-step majority logic decodable, and therefore, the girth of the associated Tanner graph [6] is six. Lucas *et al.* showed that such LDPC codes can be efficiently decoded by belief-propagation algorithms [15]. A first attempt to construct deterministic codes with large girth is due to Margulis [18], who introduced an explicit construction of LDPC codes using k-regular graphs obtained as Caley graphs of $SL_2(\mathbb{F}_q)$, a special linear group, and $PGL_2(\mathbb{F}_q)$, a projective general linear group, of dimension two over $\mathbb{F}_q$, the finite field with q elements (q power of a prime). By careful selection of transformation matrices, the author was able to achieve good girth properties. This idea was further developed by Rosenthal and Vontobel [18]. They were able to construct a short code (of length less than 5000) with girth 12. Recently, the explicit construction of families of LDPC with girth at least six has been discussed in Kim *et al.* [17]. The authors extended Lazebnik and Ustimenko's [19] method for explicit construction of graphs with arbitrary large girth, based on regular graphs.

The code construction presented in this letter is based on balanced incomplete block designs (BIBD) [1]. More specifically, the codes are based on subdesigns of a 2-$(v, k, 1)$ design, where v is the number of parity bits, and k is the column weight of a parity-check matrix. The parity-check matrix is a point-block incidence matrix of the design (V, B), where V is a set of points and B is a set of blocks of size k. As we have shown in [7], the removal of certain blocks from a design can result in eliminating Pasch and generalized Pasch configurations and, consequently, in increasing minimum distance of a code. In this letter, we exploit the idea that a judicious selection of disregarded blocks can also increase the girth of a design. It is a desirable property of a bipartite graph to have a large girth, because in the message-passing decoding algorithm [10] on such graphs, it takes more iterations until extrinsic information originating from different nodes in the bipartite graph becomes correlated. The construction of designs with high girths appears to be a very difficult problem, in general [8]. However, the designs based on rectangular integer lattices introduced in [7] allow for a simple algorithm for finding a girth-eight subdesign. In [23], a condition for absence of cycles of lengths smaller than a given constant was given for array codes, but no explicit construction is given for girths larger than six. In this letter, we give an explicit construction for $k = 3$, using arithmetically constrained sequences.

In this letter, we are interested in very-high-rate codes ($R \geq 3/4$), for which the girth-eight property is much "rarer" than in low-rate codes. We present a construction based on sets of parallel lines on a rectangular integer lattice, which is conceptually simple and gives a large family of codes. The number of parity bits is equal to $v = m \cdot k$, $m > k$, and the blocks are defined as lines of different slopes connecting points of an $m \times k$ integer lattice.

Section II introduces some definitions necessary for dealing with BIBDs. Section III introduces a construction of LDPC codes using rectangular integer lattices, and construction of

Paper approved by M. Fossorier, the Editor for Coding and Communication Theory of the IEEE Communications Society. Manuscript received March 11, 2002; revised October 4, 2002 and December 2, 2003. This work was supported by the National Science Foundation under Grant CCR 0208597.

B. Vasic and K. Pedagani are with the Department of Electrical and Computer Engineering, University of Arizona, Tucson, AZ 85721 USA (e-mail: vasic@ece.arizona.edu; karun@ece.arizona.edu).

M. Ivkovic was with the Instituto de Matemática, Estatística e Computação Científica, 13083-970 Campinas-SP, Brazil. He is now with the Department of Mathematics, University of Arizona, Tucson, AZ 85721 USA.

girth-eight codes. It also gives the bit-error rate (BER) performance of these codes in additive white Gaussian (AWGN) channels, obtained by computer simulations.

II. BIBDs and LDPC Codes

In this section, we introduce some definitions. A BIBD is a pair (V, B) where V is a v-element set and B is a collection of b k-subsets of V, called blocks, such that each element of V is contained in exactly r blocks, and any 2-subset of V is contained in exactly λ blocks. The parameter r is called the *replication number*. The notation 2-(v, k, λ) design is used for a BIBD on *v points, block size k*, and index λ. We consider a slightly different class of combinatorial designs called λ-configurations. A λ-configuration is an incidence structure of v points and b blocks such that each block contains k points, each point is incident with r blocks, and two different points are contained in *at most* λ blocks. A λ-configuration can be obtained from a 2-(v, k, λ) design by removing some of its blocks. Two blocks in a design are referred to as *parallel* if they are disjoint. A design is called *resolvable* if there exists a partition of its block set B into parallel classes, each of which partitions the set V. As we will show, the lines on a lattice introduced in [7] and analyzed in [19] and [20] form a resolvable 1-configuration.

We define the point-block incidence matrix of (V, B) as a $v \times b$ matrix $H = (h_{ij})$, in which $h_{ij} = 1$ if the ith element of V occurs in the jth block of B, and $h_{ij} = 0$, otherwise. It is easy to see that H is a matrix of parity checks of a Gallager code [2]. The row weight is r, column weight is k, and the code rate is $R \geq (b - \min(v, b))/b$. We are interested in designs in which no more than one block contains the same pair of points. Such codes are one-step majority logic decodable, or equivalently, there are no cycles of length four in a bipartite graph [6]. The main idea of this letter is that a 1-configuration with large girth can be constructed by removing whole classes of parallel blocks, rather than removing individual blocks.

III. Lattice Construction of 2-$(v, k, 1)$ Girth-Eight 1-Configurations

In this section, we address the problem of construction of resolvable l-configurations with a wide range of block sizes. 2-$(v, k, 1)$ designs naturally come as girth-six designs, because no pair of points occurs in more than one block. In other words, if $|B| = b = \binom{v}{2}/\binom{k}{2}$ (i.e., if the design has the maximum possible number of blocks), then the girth is $g(V, B) = 6$. As we will show, for every design (V, B), there exists a 1-configuration (V, B'), $B' \subset B$, such that $g(V, B') \geq 8$. In a 1-configuration, there exist a pair of points that are disconnected, i.e., there is no line incident with both of them. This is why the girth of a 1-configuration can be larger than six. Our construction is based on the integer lattice construction given in [7], and briefly summarized as follows.

We define a class of 1-configurations as sets of lines connecting the points of a rectangular integer lattice. Consider a rectangular integer lattice $L = \{(x, y) : 0 \leq x \leq k-1, 0 \leq y \leq m-1\}$, where m is a prime. The construction can be readily generalized to the case when m is a prime power (i.e., $m = p^l$). Let $l : L \to V$ be a one-to-one mapping of the lattice L to the point set V. An example of such mapping is a simple linear mapping $l(x, y) = m \cdot x + y + 1$. The numbers $l(x, y)$ are referred to as lattice-point labels.

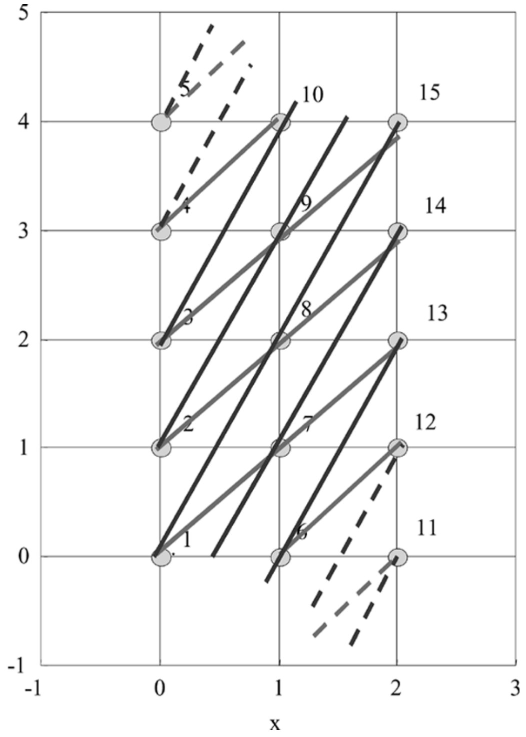

Fig. 1. Example of the rectangular grid for $m = 5$ and $k = 3$.

A line with slope s, $0 \leq s \leq m-1$, starting at the point (0, a), is the m set of points $\{(x, a + s\ x \bmod m) : 0 \leq x \leq k-1\}$, where $0 \leq a \leq m-1$. We are concerned with a 1-configuration which is an incidence structure comprised of points on the integer lattice and all lines of slopes s, $0 \leq s \leq m-1$. As mentioned earlier, two lines are referred to as parallel if they do not have any common points. There are, therefore, m classes of parallel lines in our 1-configuration corresponding to m different slopes. Each class of parallel lines comprises m lines.

Example 3.1: Fig. 1 depicts the rectangular integer lattice with $m = 5$ and $k = 3$. It also shows two classes of parallel lines (with slopes $s = 1$ and $s = 2$).

In our example, the lines of slope one are {1,7,13}, {2,8,14}, {3,9,15}, etc. We assume that the lattice labels are periodic in the vertical (y) dimension, and therefore, the line comprising points {4,10,11} also has the slope one. The examples of lines with slope two are {1,8,15} and {2,9,11}. The slopes $3, 4, \ldots, m-1$ can be defined analogously. Notice that no vertical line belongs to the design. Each column in Table I gives a set of parallel lines with slope s. A set of parallel lines defines a resolvability class.

Remark 3.1: Notice that in general, there are m parallel classes of blocks (lines), each corresponding to a different slope.

Lemma 3.1: A set B of all m k-element sets of V obtained by taking the labels of the points along the lines with slopes s, $0 \leq s \leq m-1$, is a 1-configuration.

TABLE I
RESOLVABILITY CLASSES OF LATTICE DESIGN IN FIG. 1

s=0	s=1	s=2	s=3	s=4
{1, 6, 11}	{1, 7, 13}	{1, 8, 15}	{1, 9, 12}	{1, 10, 14}
{2, 7, 12}	{2, 8, 14}	{2, 9, 11}	{2, 10, 13}	{2, 6, 15}
{3, 8, 13}	{3, 9, 15}	{3, 10, 12}	{3, 6, 14}	{3, 7, 11}
{4, 9, 14}	{4, 10, 11}	{4, 6, 13}	{4, 7, 15}	{4, 8, 12}
{5, 10, 15}	{5, 6, 12}	{5, 7, 14}	{5, 8, 11}	{5, 9, 13}

Proof: The design B containing all m k-element sets of points in V obtained by taking labels of points along the lines with slopes s, $0 \leq s \leq m-1$, is a 1-configuration. It can be readily verified by noticing that because m is a prime, for each lattice point (x, y) there cannot be more than one line with slope s that passes through (x, y).

Q.E.D.

Remark 3.2: The generalization to the case when m is a power of prime is straightforward.

Remark 3.3: The block size is k, number of blocks is $b = m^2$ and each point in the design occurs in exactly m blocks. The matrix of parity checks of a lattice code can be written in the form

$$H = \begin{bmatrix} H_{1,1} & H_{1,2} & \dots & H_{1,m} \\ H_{2,1} & H_{2,2} & \dots & H_{2,m} \\ \vdots & \vdots & & \vdots \\ H_{k,1} & H_{k,2} & \dots & H_{k,m} \end{bmatrix}$$

wherein each submatrix $H_{i,j}$ is a circulant with column weight equal to one. H is a line-point incidence matrix of a 1-configuration defined by the integer lattice defined above.

The position of the only nonzero position in the first column of $H_{i,j}$ can be found by using $c_i^{(j-1)}$, the ith element of the first base block in the class of blocks corresponding to the jth slope (see [7]).

Remark 3.4: Notice a similarity of the structure of the above parity-check matrix with that obtained in [17]. The codes denoted by $LU(2, q)$ in [17] have a square matrix of parity checks, while our codes have rectangular matrices of parity checks. This is not surprising, since it was shown in [17] that $LU(2; 4)$ and $LU(2; 8)$ are equivalent to Euclidean geometry codes [3], while a square lattice design (which includes the lines with infinity slope) is equivalent to the Euclidean plane. Notice also the similarity with a parity-check matrix of array codes [23].

Remark 3.5: The ensemble of integer-lattice codes defined by matrices of parity checks obtained by random selection of slopes and starting points has well-defined asymptotic distance distribution. Litsyn and Shevelev [21] showed that such an ensemble (they called it "Ensemble A") has superior distance distribution, compared with other ensembles they considered in [21].

Denote by $B(s)$ a resolvability class corresponding to slope s, and by B', a set of blocks of a subdesign composed of resolvability classes corresponding to the slopes from the set S, i.e., $B' = \bigcup_{s \in S} B(s)$. We are interested in the following problem. Find a maximum cardinality slope set S, such that B' is a girth-eight design. We are concerned with finding a set of slopes of maximal cardinality, because the slope-set cardinality directly influences the code rate, i.e., the larger the slope-set cardinality, the higher the code rate.

The problem of finding a set of maximal cardinality for given integers m and k is generally difficult, i.e., the complexity of the algorithm for finding such a set of slopes is exponential in $m \cdot k$. Instead of solving the hard problem of finding the maximal slope set, we give a polynomial algorithm that constructs a set of slopes S, resulting in a girth-eight 1-configuration (V, B'). The algorithm is based on a select, check, and disregard procedure.

```
$s = 0$,  $S = \{s\}$,  $B' = B(s)$,  $S' = \{1, \dots, m-1\}$.
while $S' \neq \emptyset$
$s = s + 1$
if $g(V, B' \cup B(s)) \geq 8$
  $S = S \cup \{s\}$
  $S' = S' \backslash \{s\}$
   $B' = B' \cup B(s)$
 else
  $S' = S' \backslash \{s\}$
 end
end
```

The function $g : (V, B) \rightarrow \mathrm{Z}_+$ gives the girth of a graph for a (V, B) design, and can be computed in time $O((v+b) \cdot vk)$ time (e.g., Dijkstra or Bellman–Ford algorithm; for more details, see [16]).

Clearly, the algorithm is greedy in the sense that if a slope s does not satisfy the girth-eight criterion, it checks for the immediate next slope $s+1$. Although this method does not result in a maximal slope set, the simulation results of the different codes obtained through this method have shown to yield good performance (discussed later).

In [23], Fan gave a condition for the absence of cycles of an arbitrary length in a Tanner graph of an array code, in terms of a relation among powers of a permutation matrix used as blocks in H. Notice, however, that this condition still requires a search for finding a desired set of powers, and is equivalent to a "triangle" condition in this letter (see the Appendix).

Note that finding a set of slopes for $k = 2$ is trivial, because $S = \{1, \dots, v/2-1\}$ is always a solution. However, for $k = 3$, we deduce a simple way of generating a slope set S, such that $B' = \bigcup_{s \in S} B(s)$ is a girth-eight design. The simplification stems from the interesting relationship between the elements of S with the "arithmetic-constrained" sequences (see [22]).

Definition 3.1: Given a fixed positive integer q, we define the arithmetically constrained sequence as the sequence $Y(q)$ of positive integers $0 = a_0 < a_1 < a_2 < \cdots$ by the conditions:

1) $a_1 = q$;
2) having chosen $a_0, a_1, a_2, \dots, a_n$ ($n > 0$), let a_{n+1} be the least integer such that $a_{n+1} > a_n$, and such that the sequence $a_0, a_1, a_2, \dots, a_n, a_{n+1}$ contains no three terms (not necessarily consecutive) in an arithmetic progression.

Furthermore, we define the "earliest" sequence $A : a_0, a_1, a_2, \dots, a_n, \dots$ such that $a_0 = 0, a_{2n} = 3a_n, a_{2n+1} = a_{2n+1}$. It can be verified [23] that A is an arithmetically constrained sequence with the property that the ternary expansion of $a_n = \sum t_i 3^i$ has $t_i = 0$ or 1 [22, Th. 2] ("Earliest" corresponds to

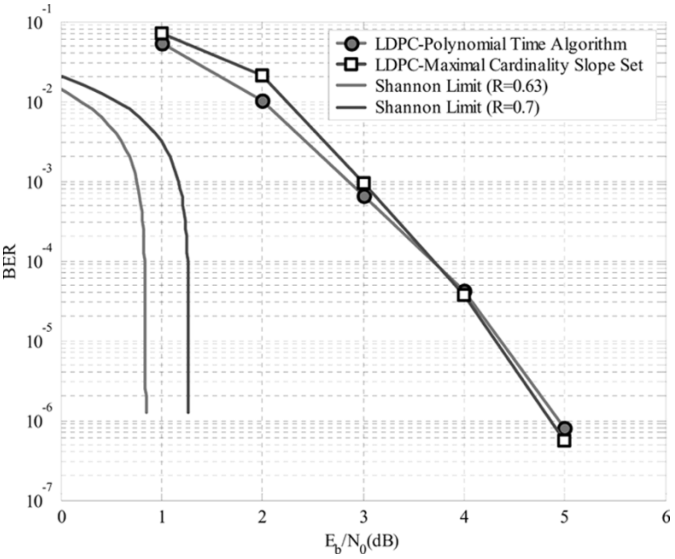

Fig. 2. Performance comparison of LDPC codes with maximal set slopes and the linear time method.

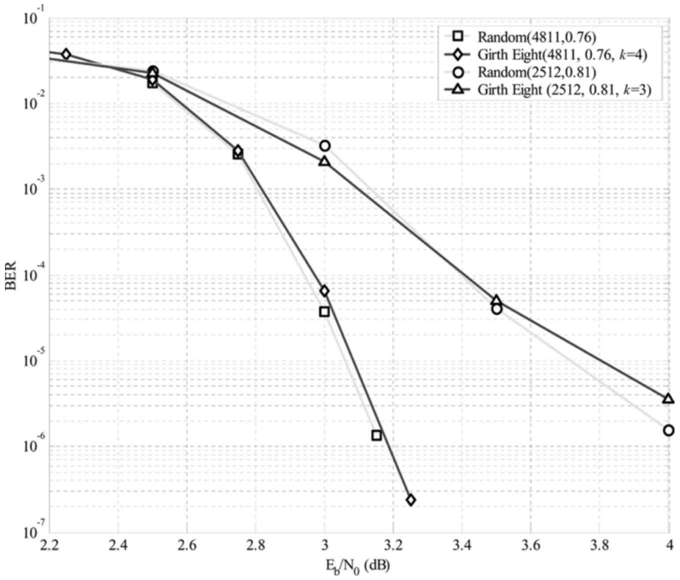

Fig. 3. Performance of girth-eight codes in an AWGN channel.

"greedy" when it comes to choosing the terms, for example: for the set $\{1, 2\}$, since 3 cannot be considered in the sequence, the sequence considers the first possible number, i.e., 4).

Theorem 3.1: For m arbitrary and $k = 3$, $S = \{a : a \in A \wedge a \leq m/2\}$ results in a girth-eight 1-configuration (V, B'), where A is the earliest sequence.

Proof: Given in the Appendix.

Theorem 3.1 is consequence of the fact that the sequence of the set of slopes obtained from the algorithm is greedy, and so is the earliest sequence. As we will show in the next section, the codes obtained by the proposed slope-selection algorithm or the above straightforward implication ($k = 3$), have performance slightly worse than codes with a slope set with maximum cardinality.

The lower bound on a minimum distance of a code with girth g, column weight k code is given by the formula shown at the bottom of the page [2]. The above bound can be aptly applied for the above girth-eight codes with $g = 8$.

IV. Simulation Results

The first experiment deals with the performance of codes obtained from the slope set generated using the above select-and-discard procedure. (Note that we do not consider high-rate codes, for the reason that we need to find a maximal slope set, which is tough to obtain for high-rate codes, as it involves large block length). For the specific case of $k = 3$ and $m = 53$, either with the proposed algorithm (or using *Theorem 3.1*), we obtain a slope set $S = \{0, 1, 3, 4, 9, 10, 12, 13\}$, resulting in a code rate of $R = 0.67$ (and $b = 424$). On the other hand, with an extensive computer search for a maximal slope set, we obtained $S_{\max} = \{7, 8, 14, 16, 19, 33, 35, 41, 42, 45\}$, resulting in a code rate of $R = 0.7$ (and $b = 530$). As we can see from Fig. 2, the code constructed from the maximal set of slopes is 2.8 dB away from its respective Shannon limit, while the code constructed using the polynomial time algorithm is 3.4 dB away from its respective Shannon limit, which is not bad for such short codes. In this particular case, the code constructed from the set with a maximal cardinality slope set has better performance. However, we do not have enough evidence to state this as a general conclusion.

The next simulation result gives the BER performance of girth-eight codes obtained from rectangular integer lattices in an AWGN channel. Fig. 3 shows the comparison of girth-eight codes with randomly constructed codes with column weights three and four, respectively. Girth-eight LDPC code with column weight three ($k = 3$), code rate $R = 0.81$, with set of slopes $S = \{0, 1, 3, 4, 9, 10, 12, 13, 27, 28, 30, 31, 36, 37, 39, 40\}$ and girth-eight code with parameters $k = 4$ and $R = 0.76$ are used. The result shows that girth-eight codes constructed using the above algorithm perform quite close to random codes. Random codes are generated such that cycles of length four are omitted.

V. Conclusion

We have given a simple construction of girth-eight codes using integer lattices. The construction is based on a judicious selection of sets of parallel lines in the lattice subgeometry. The construction gives a set of codes with a wide range of lengths and rates. The algorithm used to create girth-eight codes can be readily generalized to higher girths. In $k = 3$, we have an explicit construction using arithmetic sequences.

$$d_{\min} \geq \begin{cases} 1 + \frac{k}{k-2} \cdot ((k-1)^{\lfloor (g-2)/4 \rfloor} - 1), & \text{if } \frac{g}{2} \text{ is odd} \\ 1 + \frac{k}{k-2} \cdot ((k-1)^{\lfloor (g-2)/4 \rfloor} - 1) + (k-1)^{\lfloor (g-2)/4 \rfloor}, & \text{if } \frac{g}{2} \text{ is even.} \end{cases}$$

APPENDIX
PROOF OF *THEOREM 3.1*

Proof

Fan [23] derived the condition for occurrence of a cycle in a particular class of Tanner graphs whose parity-check matrix H has the structure defined in *Remark 3.1*. For the specific case of eliminating cycles of length six with $k = 3$, the condition in [23] reduces to the following triangle condition:

$$\alpha(s_1 - s_2) + \beta(s_3 - s_1) \neq 0(\bmod m) \qquad (1)$$

where $\alpha = i_1 - i_3$ and $\beta = i_2 - i_3$ (the indexes i_h are associated with the submatrices H_{i_h, j_h}) such that

$$\alpha \neq 0, \beta \neq 0 \text{ and } \alpha \neq \beta. \qquad (2)$$

For $k = 3$, since $i_h \in \{1, 2, 3\}$, we have the obvious inequality

$$-3 < \alpha, \beta < 3. \qquad (3)$$

Thus, the set of slopes S must be a subset of the earliest sequence A defined above. An arithmetic progression, where, for example, $s_2 = (s_1 + s_3)/2$, corresponds to the case $\alpha = 2$, $\beta = 1$.

Now we shall prove that S cannot contain values bigger that $m/2$.

Let s_3 be the potential slope considered to be included in S. s_1 and s_2 are two elements already in S.

We can add to $d = m - 2s_3$ a number s_1 made out of zeros and ones as digits, in the way that sum is a number that is made out of zeros and ones. We do that simply by taking a digit of s_1 to be one when a corresponding digit of d is two. Note that $-m/2 \leq d \leq 0$. If d does not have any two as a digit, we take s_1 to be zero. This result can be seen as a negative of a number that has only ones and zeros as digits, and is smaller then $m/2$. We constructed s_2, thus eliminating s_3. This construction corresponds to $\alpha = 1, \beta = 2$.

REFERENCES

[1] L. M. Batten, *Combinatorics of Finite Geometries*. London, U.K.: Cambridge Univ. Press, 1997.

[2] R. G. Gallager, *Low-Density Parity-Check Codes*. Cambridge, MA: MIT Press, 1963.

[3] 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. Inform. Theory*, vol. 47, pp. 2711–2736, Nov. 2001.

[4] D. MacKay and M. Davey. Evaluation of Gallager codes for short block length and high rate applications. [Online]. Available: http://www.cs.toronto.edu/~mackay/CodesRegular.html.

[5] J. Pearl, *Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference*. San Mateo, CA: Morgan Kaufmann, 1988.

[6] R. M. Tanner, “A recursive approach to low complexity codes,” *IEEE Trans. Inform. Theory*, vol. IT-27, pp. 533–547, Sept. 1981.

[7] B. Vasic, “Combinatorial constructions of structured low-density parity-check codes for iterative decoding,” in *Proc. IEEE Information Theory Workshop*, 2001, p. 134.

[8] R. A. Beezer, “The girth of a design,” *J. Combinatorial Math. Combinatorial Comput.*, to be published.

[9] F. R. Kschischang and B. J. Frey, “Iterative decoding of compound codes by probability propagation in graphical models,” *IEEE J. Select. Areas Commun.*, vol. 16, pp. 219–230, Feb. 1998.

[10] F. R. Kschischang, B. J. Frey, and H.-A. Loeliger, “Factor graphs and the sum-product algorithm,” *IEEE Trans. Inform. Theory*, vol. 47, pp. 498–519, Feb. 2001.

[11] G. D. Forney, Jr., “Codes on graphs: Normal realizations,” *IEEE Trans. Inform. Theory*, vol. 47, pp. 520–548, Feb. 2001.

[12] N. Wiberg, H.-A. Loeliger, and R. Kötter, “Codes and iterative decoding on general graphs,” *Eur. Trans. Telecommun.*, vol. 6, pp. 513–525, Sept./Oct. 1995.

[13] D. J. C. MacKay, “Good error-correcting codes based on very sparse matrices,” *IEEE Trans. Inform. Theory*, vol. 45, pp. 399–431, Mar. 1999.

[14] D. J. C. MacKay and R. M. Neal, “Good codes based on very sparse matrices,” in *Proc. IMA Conf. Cryptography, Coding*, vol. 1025, Lecture Notes Comput. Sci., C. Boyd, Ed., 1995, pp. 110–111.

[15] R. Lucas, M. Fossorier, Y. Kou, and S. Lin, “Iterative decoding of one-step majority logic decodable codes based on belief propagation,” *IEEE Trans. Commun.*, vol. 48, pp. 931–937, June 2000.

[16] T. H. Cormen, C. E. Leiserdon, and R. L. Rivest, *Introduction to Algorithms*. New York: McGraw-Hill, 1989.

[17] J.-L. Kim, U. N. Peled, I. Perepelitsa, and V. Pless, “Explicit construction of families of LDPC codes with girth at least six,” in *Proc. 40th Annu. Allerton Conf. Communications, Control, Computing*, Oct. 2002, pp. 1024–1031.

[18] I. J. Rosenthal and P. O. Vontobel, “Construction of LDPC codes using Ramanujan graphs and ideas from Margulis,” in *Proc. IEEE Int. Symp. Information Theory*, 2001, p. 4.

[19] F. Lazebnik and V. A. Ustimenko, “Explicit construction of graphs with arbitrary large girth and of large size,” *Discr. Appl. Math.*, vol. 60, pp. 275–284, 1997.

[20] B. Vasic, “Combinatorial construction of low-density parity-check codes,” in *Proc. IEEE Int. Symp. Information Theory*, Lausanne, Switzerland, June–July 2002, p. 312.

[21] S. Litsyn and V. Shevelev, “On ensembles of low-density parity-check codes: Asymptotic distance distributions,” *IEEE Trans. Inform. Theory*, vol. 48, pp. 887–908, Apr. 2002.

[22] M. Odlyzko and R. P. Stanley, “Some curious sequences constructed with the greedy algorithm,”, Bell Labs Internal Memo., 1978.

[23] J. L. Fan, “Array codes as low-density parity-check codes,” in *Proc. 2nd Int. Symp. Turbo Codes and Related Topics* , Brest, France, Sept. 2000, pp. 543–546.

[24] M. A. Margulis, “Explicit group-theoretic constructions for combinatorial designs with applications to expanders and concentrators,” *Problemy Peredachi Informatsii*, vol. 24, no. 1, pp. 51–60, 1988.