Open access • Proceedings Article • DOI:10.1109/ITW.2001.955146

Regular low-density parity-check codes from combinatorial designs — Source link

Sarah J. Johnson, Steven R. Weller

Institutions: Newcastle University

Published on: 02 Sep 2001 - Information Theory Workshop

Topics: Block code, Low-density parity-check code, Linear code, Expander code and Turbo code

Regular low-density parity-check codes from combinatorial designs

Sarah J. Johnson[1]
Department of Electrical and Computer Engineering
University of Newcastle, NSW 2308, Australia
e-mail: sarah@ee.newcastle.edu.au

Steven R. Weller[2]
Department of Electrical and Computer Engineering
University of Newcastle, NSW 2308, Australia
e-mail: steve@ee.newcastle.edu.au

Abstract — **Analytically constructed LDPC codes comprise only a very small subset of possible codes and as a result LDPC codes are still, for the most part, constructed randomly. This paper extends the class of LDPC codes that can be systematically generated by presenting a construction method for regular LDPC codes based on combinatorial designs known as Kirkman triple systems. We construct $(3, \rho)$-regular codes whose Tanner graph is free of 4-cycles for any integer ρ, and examine girth and minimum distance properties of several classes of LDPC codes obtained from combinatorial designs.**

I. Introduction

Low-density parity-check (LDPC) codes were discovered by Gallager [1] in 1962 and have recently been rediscovered [2], [3]. LDPC codes are designed by specifying a parity-check matrix H to optimize the flow of information in the decoding process. In particular, H is chosen to be sparse so that the calculation of each check sum depends on few code word bits and the evaluation of code bit validity on few check sums. Using this property of LDPC codes Gallager presented iterative decoding algorithms whose complexity remains linear in the block length [1], with performance remarkably close to the Shannon limit [2], [4]. Recently it has been shown that the encoding complexity of LDPC codes can also be linear in the block length [5].

A Tanner graph displays the relationship between codeword bits and parity checks and is a useful way to describe LDPC codes [3]. Each of the n code bits, and m parity checks in H are represented by a vertex in the graph. A graph edge joins a code bit vertex to the vertices of the parity checks that include it. A *cycle* in a Tanner graph is a sequence of connected code bits and parity checks which start and end at the same vertex in the graph and contain no other vertices more than once. The length of the cycle is simply the number edges it contains and the *girth* of a Tanner graph is the size of its smallest cycle. It is known that the iterative sum-product decoding algorithm converges to the optimal solution provided that the Tanner graph of the code is free of cycles [6]. The shorter the cycles in the graph, the sooner the algorithm breaks down. To date, randomly constructed LDPC codes have largely relied on the sparsity of the parity-check matrix to avoid short cycles in the Tanner graph.

A key idea in this paper is that cycles of length less than 6 in the Tanner graph associated with an LDPC code can be systematically avoided by taking as parity-check matrices the incidence matrices of suitably chosen combinatorial designs. When the block lengths are small, good LDPC codes become more difficult to find using random construction methods [7]. So for small block lengths in particular, an analytic construction method that guarantees

1. small, uniform row and column weights; and
2. the absence of 4-cycles,

is expected to be particularly useful.

In this paper we present a construction based on Kirkman triple systems for a family of parity-check matrices having column weight 3, that satisfy both items 1 and 2. As our construction is based on combinatorial design theory, we present in Section II of this paper some background material on designs before describing some LDPC constructions.

II. LDPC Codes from combinatorial designs

A combinatorial design is an arrangement of a set $\mathcal{P}$ of v *points* into b subsets, called *blocks*, which satisfy certain conditions. In particular a *regular* design is one with a constant γ points per block and ρ blocks containing each point. It is *balanced* if there are exactly λ blocks containing each pair of points. A regular balanced design is often denoted as a $(v, b, \rho, \gamma, \lambda)$-design and satisfies $v \times \rho = b \times \gamma$.

Every design can be described by an $b \times v$ incidence matrix I where each row in I represents a block B_i of the design and each column a point P_j:

$$I_{i,j} = \begin{cases} 1 & \text{if } P_j \in B_i, \\ 0 & \text{otherwise.} \end{cases}$$

The incidence matrix of a combinatorial design, or its transpose, can be used as the parity-check matrix of a binary LDPC code to give favorable properties to the code. Choosing a design with $\lambda = 1$ in particular, guarantees the absence of 4-cycles in the code. If $H = I^T$ the code will have v parity checks and block length equal to b. If the design is regular, H will have all its columns of weight γ and all rows of weight ρ and is described as (γ, ρ)-regular. As is the case for random constructions of parity-check matrices, the H constructed in this way are not necessarily full rank, in which case the number of message bits in the code is $k = n \quad \mathrm{rank}(H)$.

One class of combinatorial designs that have been proposed for generating LDPC codes are *Steiner triple systems* on v points, or $(v, b, \rho, 3, 1)$-designs [8], denoted simply as $\mathrm{STS}(v)$. These designs exist for all $v \equiv 1, 3 \pmod 6$, and the transpose of their incidence matrix produces binary codes which are regular, (with column weight 3, row weight $(v \quad 1)/2$) and free of 4-cycles. The resulting codes (STS-LDPC codes) have v parity checks, block length $n = v(v \quad 1)/6$, and are high rate.

If the restriction that $\lambda = 1$ is relaxed to allow $\lambda = 1$ or 0 for a given v, the block length and hence rate can be reduced. A simplistic approach is to remove some columns of H. However, this results in a parity-check matrix with variable row weights, in many cases as low as 1 or 0, which leads to performance penalties when iteratively decoded.

[1] Work supported in part by a CSIRO Telecommunications & Industrial Physics postgraduate scholarship

[2] Work supported by the Centre for Integrated Dynamics and Control

0-7803-7119-4/01/$10.00 ©2001 IEEE

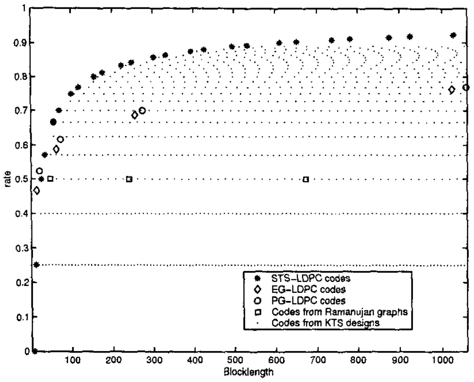

Fig. 1. Block length and rate of analytically constructed LDPC codes

The key idea presented in this paper is to use a class of designs called *Kirkman triple systems* (KTS) to derive regular LDPC codes. Kirkman triple systems are defined as the *resolvable* Steiner triple systems. That is, the blocks of a Kirkman triple system can be arranged into ρ groups such that the $\frac{v}{3}$ blocks of each group are disjoint, and each group contains every point precisely once.

To construct LDPC codes, we can take any KTS and use one or more of its groups to make up the columns of our parity-check matrix. The resulting H still has v parity-checks, column weight 3 and no 4-cycles(as there were no 4-cycles in the original H and removing columns cannot add any), but can have any desired row weight $\rho \in \{1, 2, \ldots, (v \quad 1)/2\}$ with $n = \frac{\rho v}{3}$. Of course for $\rho < 4$ the code would have an impractically small number of message bits and would not be useful. Kirkman triple systems exist for all $v \equiv 3 \pmod 6$. Construction methods for $v = 3q$ and $v = 2q + 1$, q a prime power are given in [9].

In addition to STS and KTS designs we examine:

- Codes from binary Euclidean geometries (EG-LDPC), $(q^2 \quad 1, q^2 \quad 1, q, q, 1)$-designs, and codes from binary projective geometries (PG-LDPC), $(q^2+q+1, q^2+q+1, q+1, q+1, 1)$-designs, $q = 2^s$, s any integer, have been investigated in [10]. PG and EG designs produce square incidence matrices, however previous results have established a combinatorial expression for the rank of H and hence the rate of these codes [11].
- A construction for LDPC codes using Ramanujan graphs is presented in [12]. The advantage of this method of construction is that it produces $(3, 6)$-regular codes. However these codes can only be constructed for block lengths $n = 2(q^3 \quad q)$ where q is prime.

As can be seen in Fig. 1, one advantage of using Kirkman triple systems to construct $(3, \rho)$-regular LDPC codes is the wealth of code rates and block lengths that are available. Note that Fig. 1 does not include any of the LDPC codes that could be created via column or row splitting [10].

A. Girth

A simple lower bound on the girth of an LDPC code can be found by considering the associated Tanner graph. Our line of reasoning is similar to, though extends, Lemma 1 presented in [12] relating the girth of codes from Ramanujan graphs to block length for any girth $\equiv 2 \pmod 4$.

Consider a parity check matrix $H = I^T$ where I is the incidence matrix of a regular combinatorial design. Take an arbitrary bit vertex n_1 which is connected to γ parity-check vertices. Each of these is in turn connected to $\rho \quad 1$ bit vertices other than n_1. If any of these $\gamma(\rho \quad 1)$ bit vertices are the same a 4-cycle results. Thus to avoid 4-cycles there must be

$$n \geq \gamma(\rho \quad 1) + 1$$

codeword bits, as no two parity-checks on n_1 can share any.

Now consider the $\gamma(\rho \quad 1)$ bit vertices above; each is connected to a further $\gamma \quad 1$ parity-check vertices. To avoid both 4- and 6-cycles these $\gamma(\rho \quad 1)(\gamma \quad 1)$ vertices and the γ other parity-check vertices already connected to n_1 must be distinct. Thus to avoid 6-cycles

$$m \geq \gamma(\rho \quad 1)(\gamma \quad 1) + \gamma.$$

Similarly we can start with an arbitrary parity-check vertex p_1, and the reasoning can be extended to any cycle size c to obtain the following relationship between the block length n needed to avoid a cycle of size c, and the parity-check and codeword bit degrees, γ and ρ, respectively:

$$\begin{aligned} n &\geq 1 + \gamma(\rho \quad 1) + \cdots + \gamma(\rho \quad 1)\alpha^{\frac{c}{4} \quad 1}, \\ & \qquad c \equiv 0 \pmod 4 \qquad (1) \\ n &\geq \rho + \rho\alpha + \cdots + \rho\alpha^{\frac{2c}{4}}, \\ & \qquad c \equiv 2 \pmod 4), \qquad (2) \end{aligned}$$

where $\alpha = (\gamma \quad 1)(\rho \quad 1)$.

The inequality in (2), can be used to prove the following.

Lemma 1: The girth of any STS-LDPC, EG-LDPC, or PG-LDPC code is 6.

Proof: In each case, we use the appropriate design parameters and substitute into equation (2) for $c = 6$ to show that the inequality can not be met and 6-cycles must exist. Further, the existence of cycles smaller than 6 are excluded by the restriction that $\lambda = 1$ in each of these designs and the result follows. ■

No such upper bound on girth can be placed on the codes derived from Kirkman triple systems, or the codes derived from Ramanujan graphs. These codes have constant row and column weight as n increases and so their density decreases allowing the girth to increase with n.

B. Minimum distance

For regular LDPC codes whose parity-check matrix is the incidence matrix of a Steiner triple system, MacKay and Davey [8, Theorem 1] showed that the minimum distance is at most 10. Recall that the minimum distance of a code is equal to the minimum nonzero number of columns in the parity-check matrix for which a nontrivial linear combination sums to zero [13, p. 84] and it is easy to see that designs with column weight 3 and $\lambda \leq 1$ have a minimum distance of at least 4. Further it is possible to systematically construct STS-LDPC codes having minimum distance at least 6. These STS designs are termed anti-Pasch, as they lack collections of 4 blocks employing just 6 points called a *Pasch configuration*, or *quadrilateral*. Anti-Pasch STS designs have recently been shown to exist for all v for which STS(v) exist except for $v = 7$ or 13 [14].

The minimum distance of the $(3, \rho)$-regular codes described above can only be the same or better than that of the resolvable STS codes from which they are constructed (removing

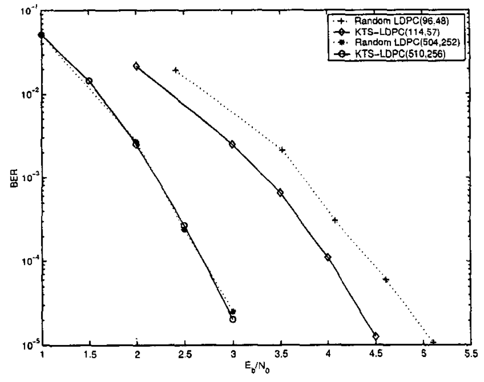

Fig. 2. BER vs. E_b/N_0 for rate $1/2$ LDPC codes, max iterations = 500

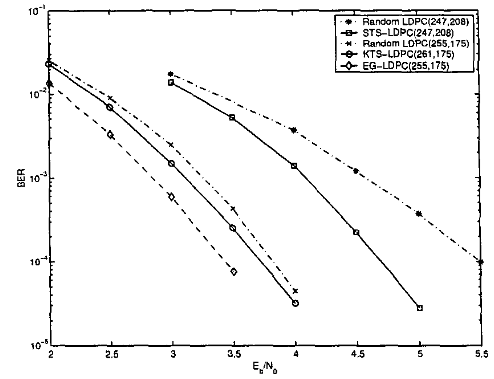

Fig. 3. BER vs. E_b/N_0 for LDPC codes, max iterations = 50

columns cannot reduce, but can increase, the size of the linear combination of columns that sum to zero). However, as yet we have no explicit determination of the minimum distance of the $(3, \rho)$-regular codes presented here. It is worth noting that resolvable $(v, b, \rho, \gamma, 1)$ designs exist for $\gamma = \{4, 5, ...\}$ and that these designs would result in codes with minimum distance $d = \{5, 6, ...\}$. The authors are currently investigating these designs for use as LDPC codes.

III. Simulation results using iterative decoding

We employed belief propagation decoding, also known as sum-product decoding, as presented in [10]. A number of randomly generated LDPC codes have been used, and where possible we have used codes already published [15]. However, where there are none available we have used the best code we could generate using the construction method from [2].

Fig. 2 shows the performance of rate $1/2$ KTS and randomly generated LDPC codes. All codes have parity-check matrices of approximately the same density and a maximum of 500 decoding iterations have been used.

Fig. 3 shows the performance of higher rate KTS, STS, EG and randomly generated LDPC codes. The rate-2/3 LDPC code generated from Kirkman triple systems is a $(3, 9)$-regular code, the EG code is $(16, 16)$-regular, and the randomly generated LDPC has row weights between 7 and 12, and constant column weight 3. While all three codes have similar block lengths and rates, the EG code has more than five times as many non zero entries in its parity-check matrix, resulting in a significant increase in computational complexity for the same number of decoding iterations. The two length $n = 247$ codes have the same rate (0.84) and density of H. Using the random construction method we were unable to eliminate 4-cycles from the high rate $n = 247$ code. This is perhaps the primary advantage of analytically constructed codes over random constructions and the reason we attribute to their improved performance.

MacKay and Davey rejected Steiner triple systems as LDPC codes due to their poor minimum distance properties [8]. While they do have poor minimum distances our results suggest that their good girth properties for small n compensate for this when belief propagation decoding is used. Even more promising is that the $(3, \rho)$-regular codes derived from Kirkman triple systems do not have the minimum distance constraints of the STS codes and have the additional advantage that they can improve upon their good girth properties.

IV. Conclusion

We have presented a construction method for LDPC codes that produces parity-check matrices having constant column and row weight and girth at least 6. These $(3, \rho)$-regular codes can be constructed for any number of parity-check sums $m \equiv 3 \pmod 6$, and for all row weights $\rho \in \{1, 2, \ldots, (m \quad 1)/2\}$. The construction is particularly useful for codes with small block lengths, and high rates, for which random construction methods have difficulty removing4-cycles.

References

[1] R. G. Gallager, "Low-density parity-check codes," *IRE Trans. Information Theory*, vol. IT-8, no. 1, pp. 21–28, January 1962.

[2] D. J. C. MacKay and R. M. Neal, "Near Shannon limit performance of low density parity check codes," *Electronics Letters*, vol. 32, no. 18, pp. 1645–1646, March 1997.

[3] R. M. Tanner, "A recursive approach to low complexity codes," *IEEE Trans. Inform. Theory*, vol. IT-27, no. 5, pp. 533–547, September 1981.

[4] D. J. C. MacKay, "Good error-correcting codes based on very sparse matrices," *IEEE Trans. Inform. Theory*, vol. 45, no. 2, pp. 399–431, March 1999.

[5] T. Richardson and R. Urbanke, "Efficient encoding of low-density parity-check codes," *IEEE Transactions on Information Theory*, vol. 47, no. 2, pp. 638–656, February 2001.

[6] R. J. McEliece, D. J. C. MacKay, and J.-F. Cheng, "Turbo decoding as an instance of Pearl's "belief propagation" algorithm," *IEEE J. Selected Areas Commun.*, vol. 16, no. 2, pp. 140–152, February 1998.

[7] D. J. MacKay and M. C. Davey, "Evaluation of Gallager codes for short block length and high rate applications," *Proceedings of the IMA Workshop on Codes, Systems and Graphical Models*, 1999.

[8] D. J. C. MacKay and M. C. Davey, "Evaluation of Gallager codes for short block length and high rate applications," in *Codes, Systems and Graphical Models; volume 123 of IMA Volumes in Mathematics and its Applications;*, B. Marcus and J. Rosenthal, Eds., pp. 113–130. Springer-Verlag, New York, 2000, available from ⟨http://wol.ra.phy.cam.ac.uk/mackay/CodesRegular.html⟩.

[9] I. Anderson, *Combinatorial Designs: Construction Methods*, Mathematics and its Applications. Ellis Horwood, Chichester, 1990.

[10] R. Lucas, M. P. C. Fossorier, Y. Kou, and S. Lin, "Iterative decoding of one-step majority logic decodable codes based on belief propagation," *IEEE Trans. Commun.*, vol. 48, no. 6, pp. 931–937, June 2000.

[11] S. Lin, "On the number of information symbols in polynomial codes," *IEEE Trans. Inform. Theory*, vol. IEEE Trans. Inform. Theory, no. IT-18, pp. 785–794, November 1972.

[12] J. Rosenthal and P. O. Vontobel, "Constructions of LDPC codes using Ramanujan graphs and ideas from Margulis," *Proceedings of 38th Allerton Conference on Communications, Control and Computing.*, October 2000.

[13] S. B. Wicker, *Error Control Systems for Digital Communication and Storage*, Prentice-Hall, Upper Saddle River, NJ 07458, 1995.

[14] M. J. Grannell, T. S. Griggs, and C. A. Whitehead, "The resolution of the anti-Pasch conjecture," *J. Combin. Designs*, vol. 8, no. 4, pp. 300–309, July 2000.

[15] D. J. MacKay, ," http://wol.ra.phy.cam.ac.uk/mackay/.