Regular low-density parity-check codes from combinatorial designs

Sarah J. Johnson and Steven R. Weller
sarah@ee.newcastle.edu.au, steve@ee.newcastle.edu.au
Department of Electrical and Computer Engineering
University of Newcastle, Callaghan, NSW 2308, Australia

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 $(3, \rho)$-codes whose Tanner graph is free of 4-cycles for any value of ρ divisible by 3, 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 so that the relationship between code bits and parity-check sums can be adjusted 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]. Recently it has been shown that the encoding complexity of LDPC codes can also be linear in the block length [4]. When iteratively decoded using belief propagation, also known as sum-product decoding, [5], LDPC codes can perform remarkably close to the Shannon limit [2], [6].

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. It is known that the iterative sum-product decoding algorithm converges to the optimal solution provided that the Tanner graph of the code satisfies a structural constraint—namely, that it be free of *cycles* [7]. A cycle in a Tanner graph is a sequence of connected code bits and check sums 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. The shorter the cycles in the graph, the sooner the sum product decoding 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 4 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 [8]. 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 for a family of regular parity-check matrices having column weight 3, and 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 the constructions and their minimum distance and girth properties.

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

II. LDPC Codes from combinatorial designs

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

Every design can be described by an $m \times n$ incidence matrix I where each column in I represents a block B_j of the design and each row a point P_i:

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

The incidence matrix of a combinatorial design can be used as the parity-check matrix of a binary LDPC code to give favorable properties to the code. Choosing a design with $\lambda = 0$ or 1 in particular, guarantees the absence of 4-cycles in the code. 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 $n - \text{rank}(H)$.

One class of combinatorial designs that have been proposed for generating LDPC codes are *Steiner triple systems* on m points, or $(m, n, \rho, 3, 1)$-designs [8], denoted simply as STS(m). These designs exist for all $m \equiv 1, 3 \pmod 6$, are regular with column weight 3, row weight $(m-1)/2$, and are free of 4-cycles. However, the resulting codes (STS-LDPC codes) have codeword length $n = m(m-1)/6$, producing high rate codes.

If the restriction that $\lambda = 1$ is relaxed to allow $\lambda = 1$ or 0 this difficulty can be avoided. 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.

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

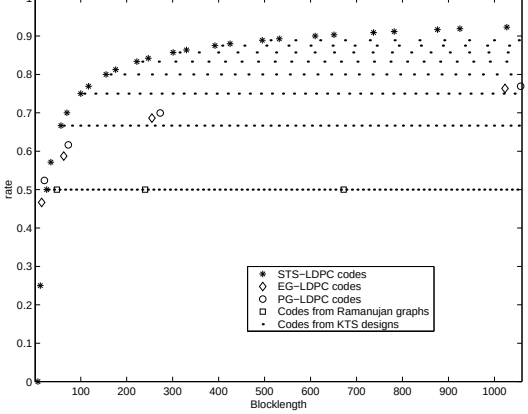

Fig. 1. Available block lengths and rates of analytically constructed LDPC codes

system (with row weight ρ), can be arranged into ρ groups such that the n/r blocks of each group are disjoint, each group contains every point precisely once and thus the weight of each row in a group is one. Consequently, if all blocks in a group are removed from H what remains is a parity-check matrix H_0 with row weight $\rho - 1$ containing $\frac{(\rho-1)n}{\rho}$ blocks. If we retain the blocks from just two groups, for example, the result is a $(3, 6)$-regular code without 4-cycles. (As there were no 4-cycles in the original H removing columns cannot add any).

In general, we can take any KTS and use one or more of its groups to make up our parity-check matrix. The resulting H has the same number of parity-checks as the original, still has column weight 3 and no 4-cycles, but can have any desired row weight $\rho \in \{1, 2, \ldots, (m-1)/2\}$. The choice of ρ determines the number of code bits n as the code is regular. Kirkman triple systems exist for all $m \equiv 3 \pmod 6$. Construction methods for $m = 3q$ and $m = 2q + 1$, q a prime power, are given in [9].

In addition to STS and KTS designs we examine:

- Codes from binary Euclidean geometries (EG-LDPC), which can be described as $(q^2 - 1, q^2 - 1, q, q, \{0, 1\})$-designs, and codes from binary projective geometries (PG-LDPC), which can be described as $(q^2+q+1, q^2+q+1, q+1, q+1, \{0, 1\})$-designs, q any prime, and have been investigated in [5].
- A construction for LDPC codes using Ramanujan graphs is presented in [10]. 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 $n = 2(q^3 - q)$ 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.

A. Girth

A simple lower bound on the block length of an LDPC code avoiding cycles of size c can be found by considering the associated Tanner graph. Our line of reasoning is similar to, though extends, Lemma 1 presented in [10] lower bounding the girth of LDPC codes for any girth $\equiv 2 \pmod 4$. Consider an arbitrary bit vertex n_1 which is connected to γ parity-check vertices. Each of these is in turn connected to $\rho - 1$ bit vertices other than n_1. If any of these $\gamma(\rho - 1)$ bit vertices are the same a 4-cycle results. Thus to avoid 4-cycles there must be at least

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

code word bits, so no two parity-checks on n_1 must share any.

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

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

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 size c, and the parity-check and code-word bit degrees, γ and ρ, respectively: $\alpha = (\gamma - 1)(\rho - 1)$.

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

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

The inequalities in (1)–(2), and in particular the restriction on n to avoid 6-cycles, 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 equations (1)–(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 $\lambda = 0$ or 1 and the result follows. ■

No such bounds can be placed on the regular codes derived from Kirkman triple systems, or the regular 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 go to infinity 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 [11, Theorem 1] showed that the minimum distance is at most 10. While this upper bound on minimum distance is so small as to preclude the use of Steiner triple system LDPCs for all but the shortest block lengths, it is possible to systematically construct STS LDPCs having minimum distance at least 6 for all m for which STS(m) exist except for $m = 7$ or 13, where the minimum distance is 4.

To show that the minimum distance is at least 6, we use the existence of Steiner triple systems that lack collections of 4 blocks employing just 6 points. In the combinatorial design literature this is called a *Pasch configuration*, or *quadrilateral*. The term *anti-Pasch* is used to describe a Steiner triple systems that lacks a Pasch configuration. For the case $m \equiv 3 \pmod 6$, an anti-Pasch STS(m) has long been known to exist and the case in which $m \equiv 1 \pmod 6$ has recently been solved [12], [13]. We therefore have the following result.

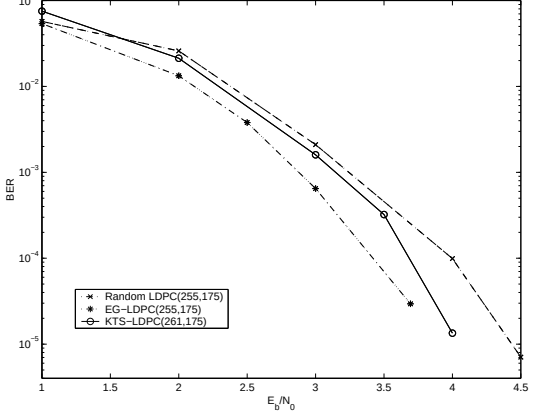

Fig. 2. BER vs. E_b/N_0 for rate $2/3$ LDPC codes, max iterations = 50

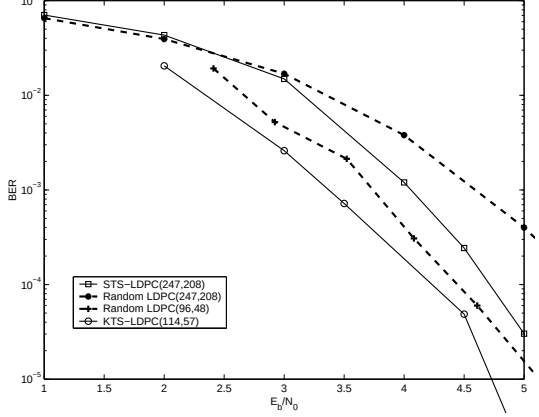

Fig. 3. BER vs. E_b/N_0 for KTS, STS and random LDPC codes

Lemma 2: For all $m \equiv 1, 3 \pmod 6$ except for $m = 7, 13$, there exist regular LDPC codes of length $m(m-1)/6$, having parity check matrices with uniform column weight 3, uniform row weight $(m-1)/2$ and minimum distance at least 6.

C. Simulation results using iterative decoding

We employed belief propagation decoding, also known as sum-product decoding, as presented in [5]. A number of randomly generated LDPC codes have been used, and where possible we have used codes already published [14]. However, where there are none available we have used the best random construction we could generate using the construction method from [2].

Fig. 2 shows the performance of rate-$2/3$ KTS, EG and randomly generated LDPC codes. The 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 four 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.

Fig. 3 shows the performance of KTS, STS and randomly generated LDPC codes. The two length $n = 247$ codes have the same rate (0.84) and density of H and a maximum of 200 decoding iterations have been used, while the two smaller length codes are both rate-$1/2$, have equal density parity-check matrices and a maximum of 500 decoding iterations have been used. 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 our 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 improve upon their good girth properties.

III. 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 $\rho \in \{1, 2, \ldots, (m-1)/2\}$. The construction is particularly useful for small block lengths, and for high rate codes which random construction methods have difficulty removing 4-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] T. Richardson and R. Urbanke, "Efficient encoding of low-density parity-check codes", *IEEE Trans. Inform. Theory*, vol. 47, no. 2, pp. 638–656, February 2001.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

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

[10] 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.

[11] 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⟩.

[12] 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.

[13] A. C. H. Ling, C. J. Colbourn, M. J. Grannell, and T. S. Griggs, "Construction techniques for anti-Pasch Steiner triple systems", *J. Lond. Math. Soc.*, vol. 61, no. 3, pp. 641–657, June 2000.

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