

Codes for Iterative Decoding from Partial Geometries

Sarah J. Johnson* and Steven R. Weller†

Department of Electrical and Computer Engineering
University of Newcastle, Callaghan, NSW 2308, Australia
{sarah, steve}@ee.newcastle.edu.au

Submitted to ISIT2002, October 21, 2001.

Technical Report EE01070

1 Introduction

The aim of this work is to develop codes suitable for iterative decoding using the sum-product algorithm. To this end, codes with sparse parity-check matrices, large girth and good minimum distance are sought. A sparse parity-check matrix is essential for workable decoding complexity, leading to so-called low-density parity-check (LDPC) codes. Large girth results in reduced dependence in the message passing and so to more efficient iterative decoding, while large minimum distance improves the error floor performance of the code. Further, regular codes, that is codes with parity-check matrix with fixed row and column weights, can simplify the implementation of LDPC codes. We consider in this paper regular LDPC codes, derived from partial geometries, which have girth at least 6 and sparse parity-check matrices. Partial geometries are a large class of combinatorial structures whose incidence matrices include several of the previously proposed algebraic constructions for LDPC codes as special cases. These include Steiner triple systems [12], Kirkman triple systems [7, 6], oval designs [19], generalized quadrangles [18], and some of the finite geometries from [11, 9]. We derive minimum distance bounds for codes from partial geometries, and present constructions and performance results for classes of partial geometries, namely transversal designs and the proper partial geometries, which have not previously been proposed for iterative decoding.

2 Incidence, graphs and designs

An *incidence structure* $(\mathcal{P}, \mathcal{B}, \mathcal{I})$ consists of a finite non-empty set \mathcal{P} of points and a finite non-empty set \mathcal{B} of blocks, together with an incidence relation $\mathcal{I} \subseteq \mathcal{P} \times \mathcal{B}$. A point p and block B are incident, denoted $p \in B$, if and only if $(p, B) \in \mathcal{I}$. A design \mathcal{D} is an incidence structure with a constant number of points per block and no repeated blocks. A t -design has the property that every set of t points occurs in a constant number of blocks together. The incidence matrix N of \mathcal{D} is a $|\mathcal{B}| \times |\mathcal{P}|$ matrix with rows indexed by the points and columns indexed by the blocks of \mathcal{D} and is defined by

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

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

†Work supported in part by the Centre for Integrated Dynamics and Control.

and $y \in \mathcal{B}$ or $x \in \mathcal{B}$ and $y \in \mathcal{P}$. The incidence graph of \mathcal{D} is bipartite as no point is connected to another point and no block to another block. A *cycle* in a graph is a sequence of connected vertices 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 graph is the size of its smallest cycle. The girth of an LDPC code C is defined by considering the parity-check matrix of C as the incidence matrix of a design \mathcal{D} . The girth of C is then the girth of the incidence graph of the design \mathcal{D} . As the incidence graph (also called a *Tanner graph* when considering parity-check matrices) is bipartite, the length of a cycle must be even and at least 4.

An incidence structure can also be described by a *point graph* \mathcal{G} which has vertex set $\mathcal{V} = \mathcal{P}$ with $v = |\mathcal{V}|$ vertices. An edge connects two vertices if the corresponding points are incident with the same block $B \in \mathcal{B}$. The *adjacency matrix* of \mathcal{G} is then a $v \times v$ matrix A , indexed by the vertices of \mathcal{G} , and defined by

$$A_{i,j} = \begin{cases} 1 & \text{if } i, j \text{ is an edge of } \mathcal{G} \\ 0 & \text{otherwise.} \end{cases}$$

A graph \mathcal{G} is said to be *regular* if each vertex is joined to n_1 other vertices, and not joined to n_2 vertices. If further, any two joined vertices of \mathcal{G} are both joined together to exactly p_1 other vertices, and any two unjoined vertices are both joined to exactly p_2 vertices together the graph is *strongly regular* [17]. In what follows we consider partial geometries, a class of 1-designs with strongly regular point graphs.

Partial geometries, first presented in [3], have the following properties:

1. Each point p is incident with $t + 1$ blocks and each block B incident with $s + 1$ points.
2. Any two blocks have at most one point in common.
3. For any non-incident point-block pair (p, B) the number of blocks incident with p and intersecting B equals some constant α .

The parameters of the point graph of a partial geometry $\text{pg}(s, t, \alpha)$ can be given terms of s, t and α [5, p. 33]:

$$\begin{aligned} n_1 &= s(t + 1), & p_1 &= t(\alpha - 1), & p_2 &= \alpha(t + 1), \\ |P| &= \frac{(s + 1)(st + \alpha)}{\alpha} & \text{and} & & |B| &= \frac{(t + 1)(st + \alpha)}{\alpha}. \end{aligned} \quad (1)$$

3 Codes from partial geometries

We can take the incidence matrix N of a partial geometry as the parity-check matrix H of an LDPC code which we denote by C^1 . The code C^1 has $m = |\mathcal{B}|$ parity-checks and length $n = |\mathcal{P}|$. The parity-check matrix is then regular with column weight $t + 1$, row weight $s + 1$ and the Tanner graph of C^1 has girth ≥ 6 . Alternatively, if we take $H = N^T$ we obtain a code C^2 with column weight $s + 1$, row weight $t + 1$, also with girth ≥ 6 .

In [15], Tanner presented the following bounds for the minimum distance d_{\min} of a code with a regular parity check matrix H provided the multiplicity of the largest eigenvalue μ_1 of HH^T is 1. Let w_{col} be the column weight of H , w_{row} the row weight of H and μ_2 the second largest distinct eigenvalue of HH^T . Then from [15, Theorem 3.1] we have the *bit-oriented bound*:

$$d_{\min} \geq \frac{N(2w_{\text{col}} - \mu_2)}{(\mu_1 - \mu_2)}, \quad (2)$$

$$d_{\min} \geq \frac{2N(2w_{\text{col}} + w_{\text{row}} - 2 - \mu_2)}{w_{\text{row}}(\mu_1 - \mu_2)}. \quad (3)$$

We can use the bit- and parity-oriented bounds, together with some properties of partial geometries, to give bounds on d_{\min} in terms of α , s and t for the codes C^1 and C^2 . We need first that the adjacency matrix of a strongly regular graph has three distinct real eigenvalues [5, p. 21]

$$n_2, \quad 0.5 \left[p_1 - p_2 \pm \sqrt{(p_1 - p_2)^2 + 4(n_2 - p_2)} \right]$$

with multiplicities

$$1, \quad 0.5 \left[n_1 - 1 \pm \frac{(n_1 - 1)(p_2 - p_1) - 2n_2}{\sqrt{(p_1 - p_2)^2 + 4(n_2 - p_2)}} \right].$$

For a partial geometry \mathcal{D} with incidence matrix N the adjacency matrix of the point graph of \mathcal{D} is [4, p. 386] $A = NN^T - (t+1)I$. It follows that if μ is an eigenvalue of A with multiplicity f then $\mu + (t+1)$ is an eigenvalue of NN^T with multiplicity f and so NN^T has eigenvalues

$$(s+1)(t+1), \quad s+t+1-\alpha, \quad 0$$

with corresponding multiplicities

$$1, \quad \frac{st(s+1)(t+1)}{\alpha(s+t+1-\alpha)}, \quad \frac{s(s+1-\alpha)(st+\alpha)}{\alpha(s+t+1-\alpha)}. \quad (4)$$

Lemma 1 *The minimum distance of a code C^1 is $d_{\min} \geq \max\{(s+1)(t+1-s+\alpha)/\alpha, 2(t+\alpha)/\alpha\}$*

Proof: With H the parity-check matrix of an LDPC code from a partial geometry, we use (4) to show that HH^T has a largest eigenvalue $(s+1)(t+1)$ with multiplicity 1 and second largest eigenvalue $s+t+1-\alpha$. Substituting into equations (2) and (3) the result follows. ■

Partial geometries can be divided into four (non-disjoint) classes. The minimum distance bounds for LDPC codes from each of these classes are given in Table 1.

- A partial geometry with $\alpha = s+1$ is a *balanced incomplete block design* (BIBD) or 2 - $(v, s+1, 1)$ design.
- A partial geometry with $\alpha = t$ is called a *net* or, dually with $\alpha = s$, a *transversal design* (TD).
- A partial geometry with $\alpha = 1$ is called a *generalized quadrangle* (GQ).
- If $1 < \alpha < \min\{s, t\}$ the partial geometry is *proper*.

Designs from two classes of partial geometries, BIBDs and GQs, have been studied previously for use as LDPC codes. A number of different BIBDs have been proposed [12, 11, 9, 19], and Vontobel and Tanner recently presented some LDPC codes based on generalized quadrangles [18]. The minimum distance bounds in Table 1 for the generalized quadrangles were presented in [18]. In [9] the minimum distance for codes from two-dimensional projective geometries is given as $d_{\min} = 2^s + 2$, in the notation of partial geometries this is $d_{\min} = t + 2$ and we see that the bound given in Table 1 is tight for these BIBDs. The bit-oriented bound for BIBDs can be derived more simply by noting that for codes with girth at least 6 and constant column weight γ , at least $\gamma + 1$ columns of H are needed for a linear combination to sum to zero, and hence $d_{\min} \geq \gamma + 1$.

BIBD	$s + 1$	$d_{\min} \geq \max \left\{ t + 2, \frac{2(t+s+1)}{s+1} \right\}$
Net	t	$d_{\min} \geq \max \left\{ \frac{(s+1)(t+1)}{s}, \frac{2(s+t)}{s} \right\}$
Transversal design	s	$d_{\min} \geq \max \left\{ \frac{(s+1)(2t-s+1)}{t}, 4 \right\}$
Generalized quadrangle	1	$d_{\min} \geq \max \{ (s+1)(t+2-s), 2(t+1) \}$
Proper partial geometry	$1 < \alpha < \min\{s, t\}$	$d_{\min} \geq \max \left\{ \frac{(s+1)(t+1-s+\alpha)}{\alpha}, \frac{2(t+\alpha)}{\alpha} \right\}$

Table 1: Minimum distance bounds for LDPC codes from partial geometries

Two further constructions for LDPC codes are closely related to BIBDs. The codes in [7, 6] are derived from the resolution classes of a type of BIBD known as a Kirkman triple system (KTS) and so the bounds in Table 1 hold for these codes. The two-dimensional Euclidean (affine) geometry codes in [9] are derived from Euclidean geometry (EG) BIBDs with a point and all the blocks through that point removed. The removal of a point from the EG design means that the bounds in Table 1 do not necessarily hold. However, $d_{\min} \geq \gamma + 1$ still holds and this is met with equality in [9].

4 Constructions

Constructions for many BIBDs, including KTS designs and projective and Euclidean geometries are given in [1]. Alternatively, constructions are given in the relevant LDPC papers on the application of each design [6, 9]. Constructions for oval designs are given in [2, 8, 19]. We present here the construction methods used to generate the transversal designs and proper partial geometries employed in the following section.

The infinite family of partial geometries we construct is due to Thas [16]; see also [4, p. 443] and [17, p. 314]. For q a power of 2 and d a divisor of q , let $f(x, y) = \alpha x^2 + \beta xy + \gamma y^2$ be any irreducible quadratic over $\text{GF}(q)$, and let H be any subgroup, of order d , of the additive group of $\text{GF}(q)$. In the affine plane $\text{AG}(2, q)$, let

$$\mathcal{A} := \{(x, y) : f(x, y) \in H\}.$$

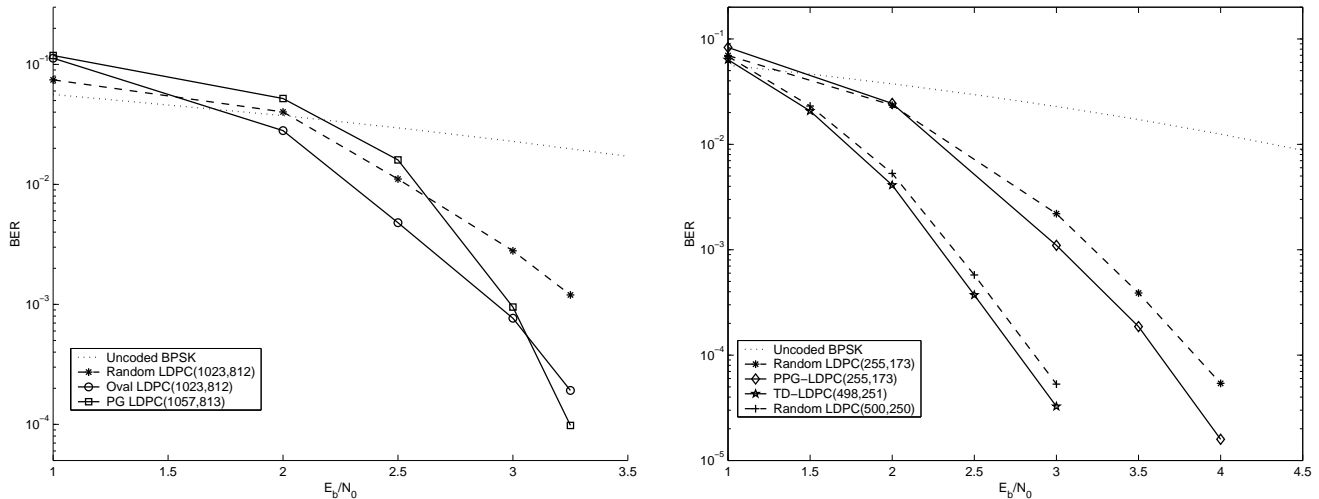
When the affine plane is embedded in a projective geometry, $\text{PG}(2, q)$, \mathcal{A} is a maximal arc of degree d . Using \mathcal{A} , an incidence structure $\mathcal{S}(\mathcal{A})$ can be defined. The points of $\mathcal{S}(\mathcal{A})$ are the points of $\text{PG}(2, q)$ that are not contained in \mathcal{A} . The blocks of $\mathcal{S}(\mathcal{A})$ are the blocks of $\text{PG}(2, q)$ that are incident with d points of \mathcal{A} . The incidence is the one of $\text{PG}(2, q)$. Then $\mathcal{S}(\mathcal{A})$ is a partial geometry with parameters $t = q - q/d$, $s = q - d$, and $\alpha = q - q/d - d + 1$.

To construct transversal designs we follow the method from [1, p. 121]. We start with an orthogonal array $\text{OA}(s+1, t+1)$ on $(t+1)$ symbols which is an $(s+1) \times (t+1)^2$ array such that any two rows give, in their vertical pairs, each ordered pair of symbols exactly once. An $\text{OA}(s+1, t+1)$ exists for any $(t+1)$ a prime power and $s \leq t+1$ and can be constructed using $s-1$ mutually orthogonal latin squares of order $(t+1)$. Given an orthogonal array on elements $1, \dots, (t+1)$ add $(i-1)(t+1)$ to each entry on the i -th row to obtain a $\text{TD}(s, t)$.

Transversal designs have the important property of resolvability which requires that the blocks of a design can be partitioned into subsets of disjoint blocks containing each point in the design exactly once in each subset. The resolvability of EG and KTS designs was applied in [10] and [7] respectively, to

5 Simulation results using iterative decoding

We employed sum-product decoding, also known as belief propagation decoding, as presented in [11]. For all simulations we used the termination rule: stop if the syndrome of the decoded codeword is the zero vector or if 50 iterations is reached. In the simulation results that follow, we compare LDPC codes from partial geometries with randomly constructed codes. For the randomly constructed codes we have used the construction method from [13] (source code from [14]) and have chosen only parity-check matrices which are free of 4-cycles.



(a) BER vs. E_b/N_0 for rate ≈ 0.79 LDPC codes in an AWGN channel, maximum of 50 iterations.

(b) BER vs. E_b/N_0 for LDPC codes in an AWGN channel, maximum of 50 iterations.

Figure 1: Bit-error rate plots for iteratively decoded low-density parity-check codes

Fig. 1(a) shows the performance of some LDPC codes derived from BIBDs. The BER performance over an AWGN channel of the oval-(1023, 812) code is compared with the PG-(1057, 813) projective geometry code [9] and a randomly generated LDPC code. The oval code is (16, 33)-regular, the PG code is (33, 33)-regular, and the randomly generated LDPC code has a column weight of 3 and row weights between 11 and 19.

Fig. 1(b) shows the performance of a (3, 6)-regular LDPC code derived from a TD(2, 82) compared with a randomly constructed code of the same rate, length and density. Also shown is the performance of a (15, 9)-regular LDPC code derived from a proper pg(8, 14, 7) compared with a randomly constructed code of the same rate and length.

References

- [1] I. Anderson. *Combinatorial Designs: Construction Methods*. Mathematics and its Applications. Ellis Horwood, Chichester, 1990.
- [2] E. F. Assmus, Jr. and J. D. Key. *Designs and their Codes*, volume 103 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, U.K., 1993.

- [3] *Math.*, 13:389–419, 1963.
- [4] F. Buekenhout. *Handbook of Incidence Geometry*. North-Holland, Amsterdam, The Netherlands, 1995.
- [5] P. J. Cameron and J. H. van Lint. *Graphs, Codes and Designs*. London Mathematical Society Lecture Note Series, No. 43. Cambridge University Press, Cambridge, 1980.
- [6] S. J. Johnson and S. R. Weller. Construction of low-density parity-check codes from Kirkman triple systems. In *Proc. IEEE Globecom Conf.*, San Antonio, TX, November 2001. To appear.
- [7] S. J. Johnson and S. R. Weller. Regular low-density parity-check codes from combinatorial designs. In *Proc. IEEE Information Theory Workshop*, pages 90–92, Cairns, Australia, September 2001.
- [8] J. D. Key. Some applications of Magma in designs and codes: Oval designs, Hermitian unitals and generalized Reed–Muller codes. *J. Symbolic Computation*, 31(1/2):37–53, January/February 2001.
- [9] Y. Kou, S. Lin, and M. Fossorier. Low density parity check codes based on finite geometries: A rediscovery and more. *IEEE Trans. Inform. Theory*, to appear.
- [10] S. Lin, H. Tang, Y. Kou, J. Xu, and K. Abdel-Ghaffar. Codes on finite geometries. In *Proc. IEEE Information Theory Workshop*, pages 14–16, Cairns, Australia, September 2001.
- [11] 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.*, 48(6):931–937, June 2000.
- [12] D. J. C. MacKay and M. C. Davey. Evaluation of Gallager codes for short block length and high rate applications. In B. Marcus and J. Rosenthal, editors, *Codes, Systems and Graphical Models; volume 123 of IMA Volumes in Mathematics and its Applications*;, pages 113–130. Springer-Verlag, New York, 2000. available from (<http://wol.ra.phy.cam.ac.uk/mackay/CodesRegular.html>).
- [13] D. J. C. MacKay and R. M. Neal. Near Shannon limit performance of low density parity check codes. *Electronics Letters*, 32(18):1645–1646, March 1997.
- [14] R. M. Neal. (<http://www.cs.toronto.edu/radford/homepage.html>).
- [15] R. M. Tanner. Minimum distance bounds by graph analysis. *IEEE Trans. Inform. Theory*, 47(2):808–821, February 2001.
- [16] J. A. Thas. Construction of partial geometries. *Simon Stevin*, 46:95–98, 1973.
- [17] J. H. van Lint and R. M. Wilson. *A Course in Combinatorics*. Cambridge University Press, Cambridge, 1992.
- [18] P. O. Vontobel and R. M. Tanner. Construction of codes based on finite generalized quadrangles for iterative decoding. In *Proc. International Symposium on Information Theory.*, Washington, DC, June 24–29 2001.
- [19] S. R. Weller and S. J. Johnson. Iterative decoding of codes from oval designs. *Defense Applications of Signal Proc. (DASP)* 2001. To appear; available at (<http://www.ee.newcastle.edu.au/users/staff/steve/>).