Codes for Iterative Decoding From Partial Geometries

Sarah J. Johnson, *Member, IEEE,* and Steven R. Weller, *Member, IEEE*

***Abstract*—This paper develops codes suitable for iterative decoding using the sum-product algorithm. By considering a large class of combinatorial structures, known as partial geometries, we are able to define classes of low-density parity-check (LDPC) codes, which include several previously known families of codes as special cases. The existing range of algebraic LDPC codes is limited, so the new families of codes obtained by generalizing to partial geometries significantly increase the range of choice of available code lengths and rates. We derive bounds on minimum distance, rank, and girth for all the codes from partial geometries, and present constructions and performance results for the classes of partial geometries which have not previously been proposed for use with iterative decoding. We show that these new codes can achieve improved error-correction performance over randomly constructed LDPC codes and, in some cases, achieve this with a significant decrease in decoding complexity.**

***Index Terms*—Gallager codes, iterative decoding, low-density parity-check (LDPC) codes, partial geometries, sum-product decoding.**

I. Introduction

THE aim of this paper is to develop block codes suitable for iterative decoding using the sum-product algorithm. Block codes which are iteratively decoded were first presented by Gallager [1], and called low-density parity-check (LDPC) codes, as a sparse parity-check matrix is essential for the decoding. LDPC codes have been the focus of intense research interest in recent years, when rediscovered in the wake of turbo codes, and shown to perform remarkably close to the Shannon limit. When applied to LDPC codes, the sum-product algorithm has a decoding complexity linear in the blocklength which makes very long codes feasible. Further, the nature of the decoding makes graph-based code properties, such as girth, important for decoding performance, and the traditional properties of a good block code are not necessarily the most important properties of a good LDPC code.

For a good LDPC code, it is required that the parity-check matrix be sparse. The girth of the Tanner graph of the code is also important, particularly that the Tanner graph does not contain 4-cycles. Other properties considered are the rank over GF(2) of the parity-check matrix and the minimum distance of the code. The properties required of LDPC codes make the field of combinatorial designs a particularly promising source for algebraic code constructions. Certain balanced incomplete block designs (BIBDs) called *Steiner 2-designs*, in particular can be used to construct regular LDPC codes without 4-cycles [2]–[7]. However, while the codes from Steiner 2-designs avoid 4-cycles, they necessarily contain 6-cycles, and the girth of the codes from Steiner 2-designs is therefore restricted to six. Vontobel and Tanner [8] have recently presented algebraic LDPC codes from constructions called *generalized quadrangles* (GQs), which do not have their girth restricted in this way.

Steiner 2-designs and generalized quadrangles are both special cases of combinatorial constructions called *partial geometries*, which we consider in this paper. The benefits of considering partial geometries for LDPC codes are twofold. The first is that several new classes of codes are derived, and the second is that the structure of partial geometries can be used to derive expressions for the minimum distance, girth, and rank of both the existing codes from Steiner 2-designs and generalized quadrangles and the new codes presented in this paper.

We present the necessary background on partial geometries before describing some properties of codes from partial geometries in Section II. Constructions for two particular classes of codes from partial geometries are presented in Section III. The performance of LDPC codes from partial geometries is then shown in Section IV, and Section V concludes the paper.

A. Incidence, Graphs, and Designs

In this section, we introduce some notation before presenting partial geometries. Common to both designs and geometries is the notion of incidence, whether it be the incidence of points in lines or of elements in subsets. We define a block B as some subset of a set of points $\mathcal{P}$. An *incidence structure* $(\mathcal{P}, \mathcal{B}, \mathcal{I})$ consists of a finite nonempty set $\mathcal{P}$ of points and a finite nonempty 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.

The incidence of a design can be described by an incidence matrix N, which is a $|\mathcal{P}| \times |\mathcal{B}|$ matrix, with rows indexed by the points, columns indexed by the blocks of $\mathcal{D}$, and is defined by

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

Paper approved by M. Fossorier, the Editor for Coding and Communication Theory of the IEEE Communications Society. Manuscript received October 15, 2002; revised June 20, 2003. This work was supported in part by Commonwealth Scientific and Industrial Research Organization (CSIRO) through a Telecommunications and Industrial Physics postgraduate scholarship, in part by Bell Laboratories Australia, Lucent Technologies, and in part by the Australian Research Council under Linkage Project Grant LP0211210. This paper was presented in part at the IEEE International Symposium on Information Theory, Lausanne, Switzerland, June 30–July 5, 2002.

S. J. Johnson is with National ICT Australia, Sydney, NSW 2052, Australia (e-mail: sarah.johnson@nicta.com.au).

S. R. Weller is with the School of Electrical Engineering and Computer Science, University of Newcastle, Callaghan, NSW 2308, Australia (e-mail: steve@ee.newcastle.edu.au).

Digital Object Identifier 10.1109/TCOMM.2003.822737

The relationship between the points of a design is described in the *adjacency matrix* of $\mathcal{D}$ which is a $v \times v$ matrix A, indexed by the points of $\mathcal{D}$, and defined by

$$A_{i,j} = \begin{cases} 1, & \text{if } P_i, P_j \in B \text{ for any } B \in \mathcal{B},\ i \neq j \\ 0, & \text{otherwise.} \end{cases}$$

Graphical representations of designs are also a useful way to describe the relationship between points and blocks. The *incidence graph* of $\mathcal{D}$ has vertex set $\mathcal{P} \bigcup \mathcal{B}$ with two vertices, x and y, connected if and only if $(x, y) \in \mathcal{I}$ or $(y, x) \in \mathcal{I}$. A *cycle* in the incidence 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 the number of edges it contains, and the *girth* of a graph is the length of its shortest cycle. An incidence structure can also be described by a *point graph* $\mathcal{G}$, which has vertex set $\mathcal{V} = \mathcal{P}$ and $v = |\mathcal{V}|$ vertices. An edge connects two vertices if the corresponding points are incident with the same block $B \in \mathcal{B}$, and we say that the vertices (and corresponding points) are *connected*.

A graph $\mathcal{G}$ is said to be *regular* if each vertex is connected to exactly n_1 other vertices. Further, if any two connected vertices of $\mathcal{G}$ are both connected together to exactly p_1 other vertices, and any two unconnected vertices are both connected to exactly p_2 vertices together, the graph is *strongly regular* and specified by the parameters (v, n_1, p_1, p_2) [9].

The designs we consider in this paper, partial geometries $\mathrm{pg}(s, t, \alpha)$, were first presented in [10], and are designs specified by three parameters, s, t, and α, which must satisfy the following properties [11, p. 33].

- P1. Each point P is incident with $t + 1$ blocks, and each block B is incident with $s + 1$ points.
- P2. Any two blocks have, at most, one point in common.
- P3. For any nonincident point-block pair (P, B), the number of blocks incident with P and intersecting B equals some constant α.

The properties required for partial geometries guarantee that their point graphs are always strongly regular. A point P of a partial geometry is incident in $t + 1$ blocks, and in each of these blocks connected to s other points. These $s(t + 1)$ points are unique, since the point P is in every block, and property P2 must hold, and so we have that each point is connected to $s(t + 1)$ others. Further, a pair of connected points (P_i, P_j) are both connected to the $s - 1$ other points on the same block in which they are connected, plus in each of the t other blocks incident on point P_i, there are $\alpha - 1$ points connected to point P_j, by property P3. Thus two connected points P_i and P_j are connected to $s - 1 + t(\alpha - 1)$ other points in common. Finally, consider an unconnected pair of points (P_i, P_j). The point P_i is incident with $t + 1$ blocks, each of which is not incident with the point P_j. Again by property P3, each of these blocks is incident with α points which are also connected to P_j, and so P_i and P_j are connected to $(t + 1)\alpha$ points in common. Thus the point graph of a partial geometry $\mathrm{pg}(s, t, \alpha)$ is strongly regular with parameters

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

II. Codes From Partial Geometries

We take the incidence matrix N of a partial geometry as the parity-check matrix H of a binary LDPC code C. These partial geometry LDPC codes have $m = |\mathcal{P}|$ parity checks, length $n = |\mathcal{B}|$, and parity-check matrices which are $(s + 1, t + 1)$-regular, that is, all columns are weight $s + 1$, and all rows are weight $t + 1$. The code C is defined as the set of all binary n-tuples, $\{c | cH^T = 0, c \in \mathrm{GF}(2)^n\}$, and the dimension of the code is $k = n - \mathrm{rank}_2(H)$. In the following, we use the properties P1–P3 of partial geometries and properties of strongly regular graphs to derive expressions for the minimum distance, rank, and girth of LDPC codes from partial geometries.

A. Minimum Distance

In [12], Tanner presented the following bounds for the minimum distance, $d_{\min}$, of a code with a regular parity-check matrix, H, provided that 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 [12, Th. 3.1], we have the *bit-oriented bound*

$$d_{\min} \geq \frac{n(2w_{\mathrm{col}} - \mu_2)}{(\mu_1 - \mu_2)} \tag{2}$$

and from [12, Th, 4.1], the *parity-oriented bound*

$$d_{\min} \geq \frac{2n(2w_{\mathrm{col}} + w_{\mathrm{row}} - 2 - \mu_2)}{w_{\mathrm{row}}(\mu_1 - \mu_2)}. \tag{3}$$

We shall use the bit- and parity-oriented bounds, together with the properties of strongly regular graphs, to derive, in a similar manner to [8], lower bounds on $d_{\min}$ in terms of α, s, and t for the codes obtained from partial geometries. For this, we need expressions for the values and multiplicities of the eigenvalues of NN^T, for which we shall use two known properties of strongly regular graphs presented in the following two lemmas.

Lemma 1 [11, p. 21]: The adjacency matrix, A, of a strongly regular graph has three distinct real eigenvalues

$$e_1, e_2 = \frac{(p_1 - p_2) \pm \sqrt{(p_1 - p_2)^2 + 4(n_1 - p_2)}}{2}$$

with multiplicities

$$f_1, f_2 = \frac{1}{2}\left[(v-1) \pm \frac{(v-1)(p_2 - p_1) - 2n_1}{\sqrt{(p_1 - p_2)^2 + 4(n_1 - p_2)}}\right].$$

From *Lemma 1*, the eigenvalues of A, written in the notation of partial geometries (1), are

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

with multiplicities

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

Lemma 2 [13, p. 386]: For a partial geometry $\mathcal{D}$ with incidence matrix N and adjacency matrix A, A and N are related by the expression $A = NN^T - (t + 1)I$.

TABLE I
MINIMUM DISTANCE BOUNDS FOR LDPC CODES FROM PARTIAL GEOMETRIES

Class of partial geometry	Code length	Minimum distance bounds for C
Steiner 2-design	$\frac{(t+1)(st+s+1)}{s+1}$	$d_{\min} \geq \max\left\{\frac{(t+1)(2s+2-t)}{s+1}, \frac{2(2s+1)}{s+1}\right\}$
Net	$(s+1)(t+1)$	$d_{\min} \geq \max\left\{\frac{(t+1)(s+1)}{t}, \frac{2(s+t)}{t}\right\}$
Transversal design	$(t+1)^2$	$d_{\min} \geq \max\left\{\frac{(t+1)(2s-t+1)}{s}, 4\right\}$
Generalized quadrangle	$(t+1)(st+1)$	$d_{\min} \geq \max\{(t+1)(s+2-t), 2(s+1)\}$
Proper partial geometry	$\frac{(t+1)(st+\alpha)}{\alpha}$	$d_{\min} \geq \max\left\{\frac{(t+1)(s+1-t+\alpha)}{\alpha}, \frac{2(s+\alpha)}{\alpha}\right\}$

From *Lemma 2*, it follows that if e is an eigenvalue of A with multiplicity f, then $e+(t+1)$ is an eigenvalue of NN^T with multiplicity f, and so for N, the incidence matrix of a partial geometry, NN^T has eigenvalues

$$(s+1)(t+1), \quad s+t+1-\alpha, \quad 0 \tag{5}$$

with multiplicities (4), and we can derive an expression for the minimum distance.

Lemma 3: The minimum distance of an LDPC code, C, from a partial geometry $\mathrm{pg}(s,t,\alpha)$, is

$$d_{\min} \geq \max\left\{\frac{(t+1)(s+1-t+\alpha)}{\alpha}, \frac{2(s+\alpha)}{\alpha}\right\}.$$

Proof: The parity-check matrix of a partial geometry LDPC code, H, defined as the incidence matrix of a partial geometry, $\mathrm{pg}(s,t,\alpha)$, has $w_{\mathrm{row}} = t+1$, $w_{\mathrm{col}} = s+1$, and $n = (t+1)(st+\alpha)/(\alpha)$. From *Lemma 1* and *Lemma 2*, HH^T has a largest eigenvalue $(s+1)(t+1)$ with multiplicity 1 and second largest eigenvalue $s+t+1-\alpha$. Substituting into (2) and (3) the result follows. ∎

There are four main classes of partial geometries:

- a partial geometry with $\alpha = s+1$ is a Steiner 2-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*.

The minimum distance bounds for LDPC codes from each are given in Table I.

Designs from two classes of partial geometries, Steiner 2-designs and GQs, have been studied previously for use as LDPC codes. A number of different Steiner 2-designs have been considered, including Steiner triple systems [2], [14], Kirkman triple systems [5], [6], ovals [7] and projective geometries [3], [4], [15]. Vontobel and Tanner recently considered LDPC codes based on GQs [8], and the minimum distance bounds in Table I for the GQs were presented in that paper.

The minimum distance bounds from *Lemma 3* are weak for the Steiner 2-designs, nets and TDs; a better bound is provided by Massey [16], which for codes from partial geometries gives

$$d_{\min} \geq s+2.$$

However, for the GQ and proper partial geometry codes, the bounds from *Lemma 3* significantly improve on Massey's bound to give minimum distances up to twice the column weight of H.

B. Linearly Dependent Rows in H

The excellent performance of the projective geometry codes has been attributed to the highly redundant parity-check matrices of the codes [4], [8]. This has motivated the search for other designs in which the rank of H over GF(2), the 2-rank, is significantly less than the number of rows in H, such as the oval designs [7] and GQs [8]. In essence, the low 2-rank of H provides extra parity-check constraints without decreasing the code rate, at the cost of extra decoding computation. Consequently, expressions of the 2-rank of H for the partial geometry codes, as a function of the parameters of the partial geometry, are valuable, not only to determine the rate of a given code without needing to construct it, but also as a means to select those parameters which lead to highly redundant parity-check matrices.

A simple upper bound on the 2-rank of a code is $\mathrm{rank}(H)$, the number of nonzero eigenvalues of HH^T, which we know for partial geometry codes (4) to give

$$\mathrm{rank}_2(H) \leq \frac{st(s+1)(t+1)}{\alpha(t+s+1-\alpha)} + 1. \tag{6}$$

For a lower bound on the 2-rank of H, we use a result of Brouwer on the p-rank of the adjacency matrices of strongly regular graphs [17].

Lemma 4 [17]: If A is the adjacency matrix of a strongly regular graph with eigenvalues k, r, u, and multiplicities 1, f, and g, respectively, and the matrix M is defined as $M = A + bJ + cI$, for some b and c, then M has eigenvalues $\theta_0 = k + bv + c$, $\theta_1 = r + c$, $\theta_2 = u + c$, with multiplicities 1, f, and g, respectively. Further:

P1. if precisely one eigenvalue θ_i of M is $\equiv 0 \bmod p$ then $\mathrm{rank}_p(M) = v - m_i$, where m_i is the multiplicity of that eigenvalue;

P2. if $\theta_0 \equiv \theta_1 \equiv 0 \bmod p$ and $\theta_2 \not\equiv 0 \bmod p$, then $\mathrm{rank}_p(M) = g$ if $p|e$, and $\mathrm{rank}_p(M) = g+1$ otherwise. Similarly, if $\theta_0 \equiv \theta_2 \equiv 0 \bmod p$ and $\theta_1 \not\equiv 0 \bmod p$, then $\mathrm{rank}_p(M) = f$ if $p|e$, and $\mathrm{rank}_p(M) = f+1$ otherwise.

In the above, $e := \mu + b^2v + 2bk + b(\mu - \lambda)$, with $\lambda = r+u+\mu$ and $\mu = ru + k$.

For H, the incidence matrix of a partial geometry, we can define $M = HH^T = A + (t+1)I$, and thus $k = s(t+1)$, $r = s-\alpha$, $u = -(t+1)$, $\theta_0 = (s+1)(t+1)$, $\theta_1 = s+t+1-\alpha$,

TABLE II
KNOWN CONSTRUCTIONS FOR PROPER PARTIAL GEOMETRY DESIGNS

Construction	Parameter choice	(s,t,α)	Reference
Thas 1	$q=p^h$, p prime, $d<q$	$(q-d, q-\frac{q}{d}, q-\frac{q}{d}-d+1)$	[22]
Thas 2	$q=p^h$, p prime, $d<q$	$(q-1, (q+1)(d-1), d-1)$	[22]
De Clerk, Dye and Thas	$n\in\mathbb{Z}$	$(2^{2n-1}-1, 2^{2n-1}, 2^{2n-2})$	[29]
Mathon	$q=3^m$, $m\in\mathbb{Z}$	$(q-1, 0.5(q^2-1), 0.5(q-1))$	[30]
Sporadic	-	(26,27,18)	[31]
Sporadic	-	(5,5,2)	[32]
Sporadic	-	(4,17,2)	[33]

$\theta_2=0$, and $e=\alpha(t+1)$. Then Brouwer's results show that if $s+t+1-\alpha\equiv 1 \bmod 2$, the 2-rank of HH^T is

$$\operatorname{rank}_2(HH^T)=\frac{st(s+1)(t+1)}{\alpha(s+t+1-\alpha)}+1$$

when $(s+1)(t+1)\equiv 1 \bmod 2$ or $(t+1)\alpha\equiv 1 \bmod 2$, and

$$\operatorname{rank}_2(HH^T)=\frac{st(s+1)(t+1)}{\alpha(s+t+1-\alpha)}$$

otherwise. As $\operatorname{rank}_2(H)\geq\operatorname{rank}_2(HH^T)$, we now have a lower bound on the 2-rank of H for certain choices of s, t, and α, i.e., if $s+t+1-\alpha\equiv 1 \bmod 2$

$$\operatorname{rank}_2(H)\geq\frac{st(s+1)(t+1)}{\alpha(s+t+1-\alpha)}. \tag{7}$$

For Steiner 2-designs, we have $\alpha=s+1$, and the upper bound corresponds to a full rank H. For the projective geometries and the oval designs, a lower bound is not defined, however, exact expressions for rank have been determined based on the geometric properties of these designs, see [4] and [7], respectively. For the Steiner and Kirkman triple-system designs with $t\equiv 0 \bmod 2$, the upper bound is met with equality, and the parity-check matrices are always full rank, a result proved in [18].

The incidence matrix of TDs have, at least, s linearly dependent rows, and exactly that many for $t\equiv 0 \bmod 2$, while for any partial geometry design, we can choose s, t, and α to guarantee at least

$$\frac{s(s+1-\alpha)(st+\alpha)}{\alpha(s+t+1-\alpha)} \tag{8}$$

linearly dependent rows in the parity-check matrix. So all partial geometries with $\alpha<s+1$ produce codes with linearly dependent rows in their parity-check matrix. Only for the Steiner 2-designs can the incidence matrix be full 2-rank, although they are not necessarily so.

C. Code Girth

A further parameter important in the performance of LDPC codes with sum-product decoding is the girth of the code. The girth of an LDPC code C is defined as the girth of the incidence graph corresponding to the parity-check matrix of C. 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 four.

From property P2 of partial geometries, an LDPC code cannot contain a 4-cycle, so the girth is at least six. For any $\alpha>1$, property P3 guarantees the existence of a 6-cycle, so all partial geometries other than the GQs have a girth of six. What may also be interesting is the number of 6-cycles in the code (N_6) which, due to the structure of a partial geometry, can be enumerated exactly.

Lemma 5: The exact number of 6-cycles in the Tanner graph of a code from a partial geometry, $\operatorname{pg}(s,t,\alpha)$, is

$$N_6=\frac{nt(\alpha-1)}{3}\binom{s+1}{2}.$$

Proof: The number of 6-cycles in H can be counted using only the properties P1–P3 of the partial geometries. If we take a line l of the partial geometry, there are $\binom{s+1}{2}$ different pairings of the points in l. Now, take one pair (P_1,P_2) of points in l. The point P_1 is incident in t lines other than line l, none of which contain the point P_2. However, the point P_2 is connected to α of the points in each of these lines, and thus the points P_1 and P_2 are connected in a cycle of size six through each of the t lines containing P_1 for each of the $\alpha-1$ lines intersecting them. So, each pair of points (P_1, P_2) is involved in $t(\alpha-1)$ 6-cycles together. Given that there are $\binom{s+1}{2}$ pairs of points in a line l, there are $t(\alpha-1)\binom{s+1}{2}$ 6-cycles containing the points in l. There are n lines in total, and given a single 6-cycle, includes three pairs of points, the result follows. ■

III. CONSTRUCTIONS

Constructions for many Steiner 2-designs, including Steiner and Kirkman triple systems and projective geometries, are given in [19]. Alternatively, constructions are given in the relevant LDPC papers on the application of each design [4], [6]. Constructions for oval designs are given in [7], [20], and [21]. We present here the construction methods used to generate the TDs and proper partial geometries.

A. Proper Partial Geometries

The known constructions for proper partial geometries are given in Table II. We present the construction for the first class in the table which are due to Thas [22] and derived from maximal arcs.

A Steiner 2-design with q^2+q+1 points and $s=t=q$ for some integer $q\geq 2$, is called a *finite projective plane of order q* and denoted $\operatorname{PG}(2,q)$ [19]. An (m,γ)-arc in a projective plane of order q is a set of m points, no γ of which are collinear. The

arc is perfect if $m = (q+1)(\gamma-1)+1$. To construct an (m, γ)-arc in $\mathrm{PG}(2,q)$, choose an irreducible quadratic over $\mathrm{GF}(q)$

$$f(y,z) = ay^2 + byz + cz^2$$

with $a, b, c \in \mathrm{GF}(q)$, and let H be any subgroup of the additive group of $\mathrm{GF}(q)$ with order γ. Then in the affine plane, $\mathrm{AG}(2,q)$, embedded in $\mathrm{PG}(2,q)$, the arc is defined as the points

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

Any affine line meets A in 0 or γ points, and A is a perfect (m, γ)-arc.

To construct a partial geometry $\mathrm{pg}(s,t,\alpha)$ with parameters

$$s = q-d, \quad t = q(d-1), \quad \alpha = \frac{(q-1)(d-1)}{d}$$

requires an $((q+1)(d-1)+1, d)$-arc defined in a projective plane of order q. Such an arc exists for all $q = 2^h$, $d = 2^m$, for h, m, any integers so long as $h > m$. The points of the partial geometry are the points of $\mathrm{PG}(2,q)$ that are not contained in the arc, and the lines of the partial geometry are the lines of $\mathrm{PG}(2,q)$ that are incident with k points of the arc, where the incidence of is that of $\mathrm{PG}(2,q)$.

For example, the finite projective plane $\mathrm{PG}(2,2^2)$, has elements from the field $\mathrm{GF}(2^2)$, which can be thought of as the set $\{0, 1, \alpha, \alpha+1\}$, where $\alpha^2 = \alpha + 1$. Writing β in place of $\alpha+1$, so that $\alpha\beta = \alpha(\alpha+1) = \alpha^2 + \alpha = 1$ and $\beta^2 = (\alpha+1)^2 = \alpha^2 + 1 = \alpha$, and omitting brackets and commas, the 21 points of $\mathrm{PG}(2,2^2)$ can be written as

$$\begin{array}{lllllll} 100, & 010, & 001, & 1\alpha\alpha, & 1\beta 0, & 01\beta, & 1\alpha 1, \\ 101, & 10\alpha, & 1\beta\alpha, & 1\beta 1, & 10\beta, & 11\alpha, & 1\beta\beta, \\ 110, & 011, & 1\alpha 0, & 01\alpha, & 1\alpha\beta, & 11\beta, & 111. \end{array}$$

Note that there are 21 points, and not $4^3 - 1 = 63$, since we identify points that differ only by a scalar multiple. Thus, for example, 01β and $0\alpha 1$ define the same point, since $\alpha(0,1,\beta) = (0,\alpha,1)$. The 21 lines in $\mathrm{PG}(2,2^2)$ are defined as the set of all points such that $\alpha_0 x + \alpha_1 y + \alpha_2 z = 0$ for $\alpha = (\alpha_0, \alpha_1, \alpha_2)$, a triple of elements of $\mathrm{GF}(q)$, not all zero. For example, the five points identified as lying on the line $[1\alpha\beta]$ are, by definition, those points (x,y,z) which satisfy the equation $x + \alpha y + \beta z = 0$

$$[1\alpha\beta] : 1\beta 0 \quad 01\beta \quad 10\alpha \quad 1\alpha\beta \quad 111.$$

Next, we find the affine geometry $\mathrm{AG}(2,2^2)$ embedded in the $\mathrm{PG}(2,2^2)$, by removing one line from $\mathrm{PG}(2,2^2)$ and all the points through it. By omitting all points on the line $x = 0$ from $\mathrm{PG}(2,2^2)$, we see that all remaining points have $x = 1$, and so we can represent the points of $\mathrm{AG}(2,2^2)$ by the shortened (y, z). Thus $\mathrm{AG}(2,2^2)$ contains the points

$$\begin{array}{llllllll} 00, & \alpha\alpha, & \beta 0, & \alpha 1, & 01, & 0\alpha, & \beta\alpha, & \beta 1, \\ 0\beta, & 1\alpha, & \beta\beta, & 10, & \alpha 0, & \alpha\beta, & 1\beta, & 11 \end{array}$$

and has lines which are all the lines of $\mathrm{PG}(2,2^2)$ except [100]. For example, the line $[1\alpha\beta]$ from $\mathrm{PG}(2,2^2)$ is

$$[1\alpha\beta] : \beta 0 \quad 0\alpha \quad \alpha\beta \quad 11$$

$$\begin{bmatrix} 1 & . & . & . & 1 & . & 1 & . & . & . & . & . & . & . & . \\ . & 1 & . & 1 & . & . & . & . & 1 & . & . & . & . & . & . \\ . & 1 & . & . & 1 & . & . & . & . & . & 1 & . & . & . & . \\ . & . & . & . & . & 1 & . & . & . & 1 & . & 1 & . & . & . \\ . & . & . & 1 & . & 1 & 1 & . & . & . & . & . & . & . & . \\ 1 & . & . & . & . & . & . & . & 1 & . & . & . & 1 & . & . \\ 1 & . & . & . & . & . & . & . & . & 1 & . & . & . & 1 & . \\ . & . & . & . & . & . & . & 1 & 1 & . & . & 1 & . & . & . \\ . & . & 1 & . & 1 & . & . & . & . & . & . & 1 & . & . & . \\ . & 1 & . & . & . & . & . & . & . & 1 & . & . & . & . & 1 \\ . & . & 1 & . & . & . & . & . & . & . & . & . & 1 & . & 1 \\ . & . & . & . & . & . & . & 1 & . & . & 1 & . & . & 1 & . \\ . & . & . & . & . & . & 1 & 1 & . & . & . & . & . & . & 1 \\ . & . & . & . & . & 1 & . & . & . & . & 1 & . & 1 & . & . \\ . & . & 1 & 1 & . & . & . & . & . & . & . & . & . & 1 & . \end{bmatrix}$$

Fig. 1. Incidence matrix of the pg(2, 2, 1) design.

in $\mathrm{AG}(2,2^2)$. Next, we choose $H = \{0,1\}$, and find those points (y, z) in $\mathrm{AG}(2,2^2)$ for which

$$f(y,z) = \alpha y^2 + yz + z^2 = 0 \text{ or } 1$$

which are the points in the set $A := \{00, \alpha\alpha, 01, \beta\alpha, \beta 1, \alpha 0\}$. Finally, the points of the partial geometry are all the points in $\mathrm{PG}(2,2^2)$ other than those in A

$$\begin{array}{llllllll} 010, & 001, & 1\beta 0, & 01\beta, & 1\alpha 1, & 10\alpha, & 10\beta, & \\ 11\alpha, & 1\beta\beta, & 110, & 011, & 01\alpha, & \alpha\beta, & 11\beta, & 111 \end{array}$$

and the lines of the partial geometry are the lines of the $\mathrm{PG}(2,2^2)$, which contain two points of A

$$\begin{array}{llllllll} [010], & [001], & [011], & [101], & [1\alpha 1], & [01\alpha], & [1\beta 0], & \\ [01\beta], & [10\beta], & [11\alpha], & [1\alpha 1], & [1\beta 1], & & & \\ [\alpha 11], & [1\beta\alpha], & [111] & & & & & \end{array}$$

and we have a pg(2, 2, 1) with incidence matrix shown in Fig. 1. Note that the partial geometry produced by this method is only a GQ for this case, for all other h and m, a proper partial geometry is produced.

B. TDs

A TD of order q, blocksize γ, and index λ, denoted $\mathrm{TD}_\lambda(\gamma, q)$ is a triple $(\mathcal{V}, \mathcal{G}, \mathcal{B})$, where:

- $\mathcal{V}$ is a set of γq elements;
- $\mathcal{G}$ is a partition of $\mathcal{V}$ into γ classes (called groups) each of size q;
- $\mathcal{B}$ is a collection of q^2 γ subsets of $\mathcal{V}$ (called blocks);
- every unordered pair of elements from $\mathcal{V}$ is either contained in exactly one group, or is contained in exactly λ blocks, but not both.

The existence of a $\mathrm{TD}_1(\gamma, q)$, written $\mathrm{TD}(\gamma, q)$, is equivalent to the existence of $\gamma - 2$ mutually orthogonal Latin squares (MOLS) of order q. The exact number of mutually orthogonal squares that exist for a given order q has not yet been resolved, however, constructions exist for γ MOLS of order q, for q, a prime power, and $\gamma \leq q+1$ [23]. Let $GF(q) = \{\phi_1, \phi_2, \ldots, \phi_{q-1}, \phi_q\}$, and define $q-1$ MOLS by

the $q \times q$ matrices $A_1, \ldots, A_{q-1}$, taking the (i,j)th entry of A_l to be

$$A_l(i,j) = \phi_i \phi_l + \phi_j.$$

To construct a TD (γ, q) [19], take a set of $\gamma - 2$ mutually orthogonal squares of order q and construct a $\gamma \times q^2$ array M with one column for each of the positions $(i,\ j)$ in the Latin squares. The first two rows of M label positions in the Latin squares, the first row giving the row number, and the second the column number. In the third row are placed the corresponding entries of the first Latin square and so on, so that the lth row of M contains the entries of the $(l-2)$th Latin square. The result is that any two rows of M give, in their vertical pairs, each ordered pair of points exactly once. Now add $(l-1) * q$ to each entry on the lth row of M and the columns of M are the blocks of the TD.

For TDs with $\lambda = 1$, the blocks of a TD are exactly the blocks of a partial geometry on $q\gamma$ points with parameters $(s = \gamma - 1,\ t = q - 1,\ \alpha = \gamma - 1)$. TDs produce LDPC codes with the following parameters:

Length :	$n = \frac{(t+1)(st+s)}{s}$
Number of parity bits :	$n - k \leq \frac{(s+1)(st+1)-1}{s}$
Minimum distance :	$d_{\min} \geq s + 2$
Row weight of the parity-check matrix :	$t + 1$
Column weight of the parity-check matrix :	$s + 1$

TDs also 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 Euclidean geometry (EG) and Steiner triple system (STS) designs was applied in [15] and [5], respectively, to derive regular codes with a large range of rates, dimensions, and lengths, and the same principle can be applied to TDs.

Interestingly, the code parameters obtained by codes from TDs are exactly those obtained if the class of maximum distance separable (MDS) array codes from [24, Sec. 4] are viewed as binary codes. This is not surprising if we consider that the TDs and the MDS codes both require the existence of orthogonal arrays (see [25, p. 328] for a discussion on the relationship between MDS codes and orthogonal arrays).

IV. Simulation Results

In the simulation results that follow, we compare the performance of LDPC codes from partial geometries with that of randomly constructed codes on the additive white Gaussian noise (AWGN) channel, using the sum-product decoding algorithm from [26]. For each figure, the LDPC codes are labeled with their type and parameters, $[n,\ k]$. For the randomly constructed codes, we have used the construction method from [26] (source code from [27]) to produce codes with as few 4-cycles as possible. The number of floating-point multiplications (flops) required to decode a code word are calculated based on approximately $6nt$ flops per iteration [26], [28], with the number of iterations used for each simulation counted.

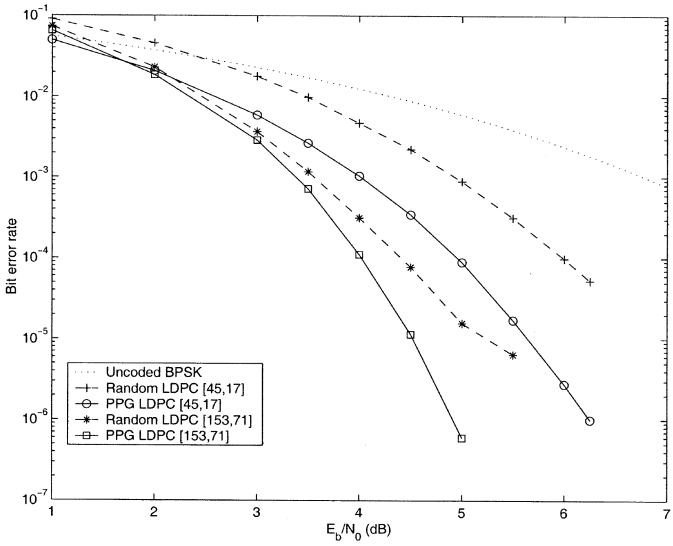


Fig. 2. Performance of LDPC codes in an AWGN channel using sum-product decoding. A (7, 5)-regular LDPC code from a pg(6, 4, 3) design is compared with a column weight 3, randomly constructed code with the same rate and length, both using a maximum of 10 iterations. A (15, 9)-regular LDPC code from a pg(14, 8, 7) design is compared with a column weight 3, randomly constructed code with the same rate and length, both using a maximum of 10 iterations.

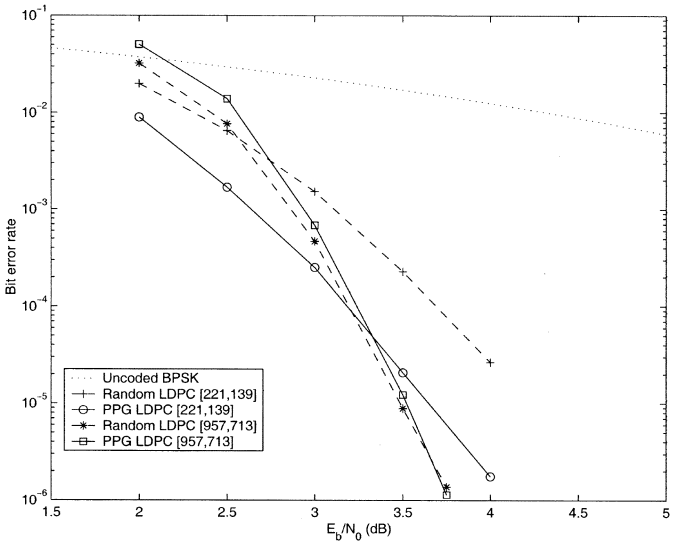


Fig. 3. Performance of LDPC codes in an AWGN channel using sum-product decoding. A (13, 13)-regular LDPC code from a pg(12, 12, 9) design is compared with a column weight 3, randomly constructed code with the same rate and length, both using a maximum of 200 iterations. A (25, 29)-regular LDPC code from a pg(24, 28, 21) design is compared with a column weight 3, randomly constructed code with the same rate and length, both using a maximum of 1000 iterations.

Fig. 2 shows the performance of two LDPC codes derived from the proper partial geometries pg(6, 4, 3) and pg(8, 14, 7), compared with that of randomly constructed LDPC codes with the same rate and length, but with column weight 3. Fig. 3 shows the performance of two LDPC codes derived from the proper partial geometries pg(12, 12, 9) and pg(24, 28, 21), compared with that of randomly constructed LDPC codes with the same rate and length, but with column weight 3. We see that for the

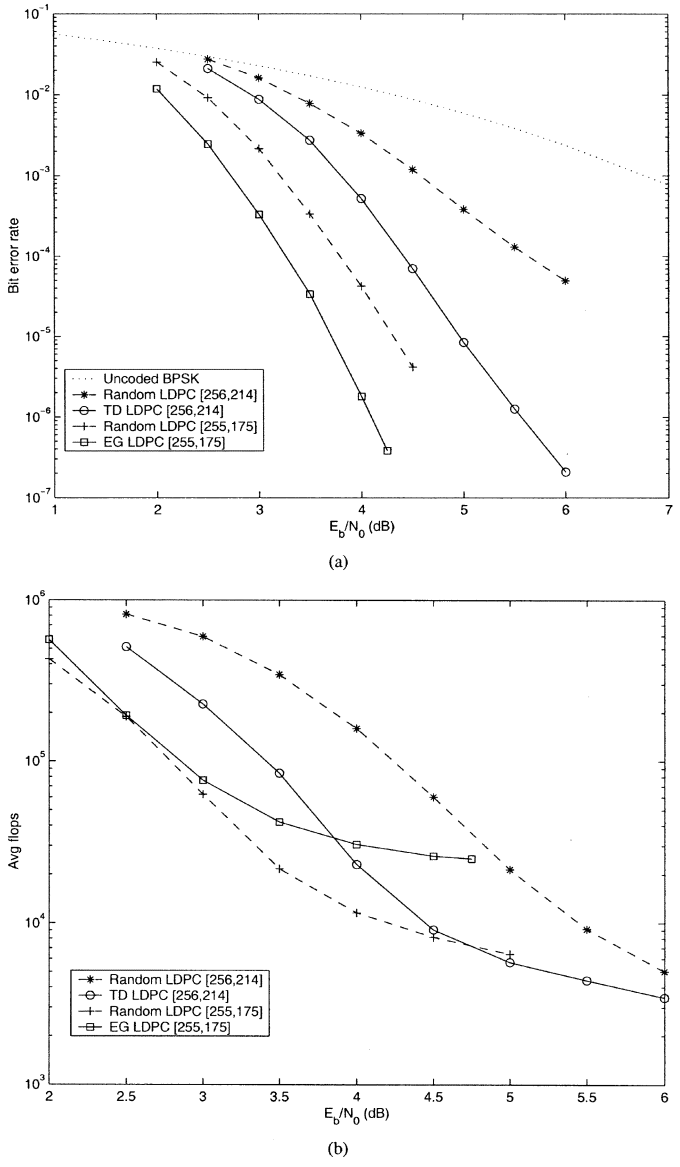


Fig. 4. Performance of LDPC codes in an AWGN channel, using sum-product decoding with a maximum of 200 iterations. A (3, 16)-regular LDPC code from a pg(2, 15, 2) is compared with a randomly constructed, column weight 3, LDPC code with the same rate and length. A similar length but lower rate (16, 16)-regular EG LDPC code is also compared with a randomly constructed, column weight 3, LDPC code with the same rate and length. (a) Bit-error rate. (b) Average number of flops to decode a codeword.

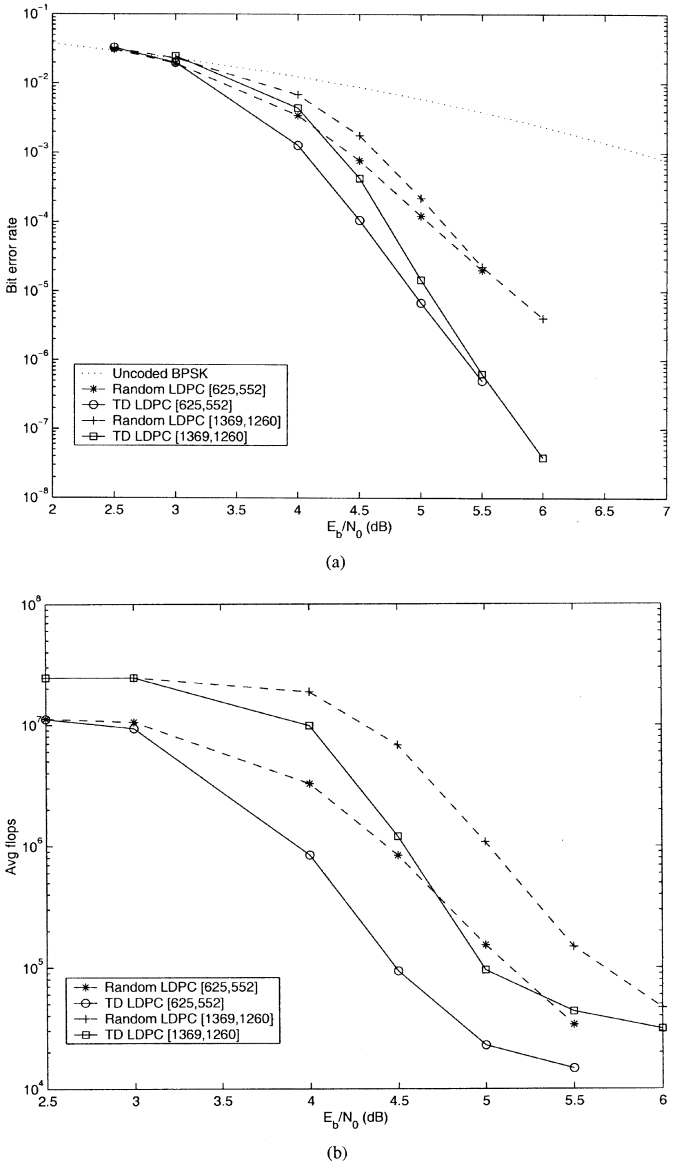


Fig. 5. Performance of LDPC codes in an AWGN channel, using sum-product decoding with a maximum of 1000 iterations. A (3, 25)-regular LDPC code from a pg(2, 24, 2) design and a (3, 37)-regular LDPC code from a pg(2, 36, 2) design are each compared with a randomly constructed, column weight 3, LDPC code with the same rate and length. (a) Bit-error rate. (b) Average number of flops to decode a codeword.

short codes, the many linearly dependent rows in H do contribute to a significantly improved decoding performance. However, for longer partial geometry codes, this does not appear to be the case. A possible reason for this is the increased density of H for the proper partial geometry pg(24, 28, 21) code, 25/957 as compared with 3/957 for the random code, which gives a greater concentration of short cycles in the code, outweighing the positive effects of the extra linearly dependent rows.

We wish to consider then partial geometry codes with small column weights which still involve linearly dependent rows in H, and thus consider TDs with $s = 2$. Fig. 4 shows the performance of a (3, 16)-regular LDPC code from the TD pg(2, 15, 2), compared with a randomly constructed code of the same rate and length. Also shown is the same length EG code compared with an equivalent-rate random LDPC code. We can see that as for the EG LDPC code, the LDPC code from the TD offers a significant decoding performance improvement over the same rate random code, but unlike the EG code, does this with a decrease rather than an increase in decoding complexity over the random code. The pg(2, 15, 2) LDPC code has a higher rate than the EG LDPC code of the same length, and a significantly lower decoding complexity at larger signal-to-noise ratios.

Fig. 5 shows the performance of two regular LDPC codes derived from the pg(2, 24, 2) and pg(2, 36, 2) designs, compared with randomly constructed codes of the same rate and length. We see that with TDs, we can achieve high-rate codes which significantly outperform randomly constructed LDPC codes, while at the same time providing a reduction in decoding complexity.

V. Conclusion

In this paper, a class of LDPC codes derived from partial geometries is presented. We have determined expressions, or bounds, for the key properties of codes defined from partial geometries, namely minimum distance, girth, and dimension. The codes from partial geometries offer improved error-correction performance over randomly constructed LDPC codes, and, in the case of the TDs, achieve this with a significant decrease in decoding complexity.

Acknowledgment

The authors wish to thank the reviewers of both the conference and paper versions of this manuscript, whose constructive comments and suggestions improved the presentation of this paper, and Prof. R. M. Neal for his on-line repository of LDPC-related software. Helpful discussions with Prof. S. Lin and Dr. P. Vontobel are also gratefully acknowledged.

References

[1] R. G. Gallager, "Low-density parity-check codes," *IRE Trans. Inform. Theory*, vol. IT-8, pp. 21–28, Jan. 1962.

[2] 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*, B. Marcus and J. Rosenthal, Eds. New York: Springer-Verlag, 2000, vol. 123, IMA Volumes in Mathematics and Its Applications, pp. 113–130.

[3] 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, pp. 931–937, June 2000.

[4] 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.

[5] S. J. Johnson and S. R. Weller, "Regular low-density parity-check codes from combinatorial designs," in *Proc. IEEE Information Theory Workshop (1TW2002)*, Cairns, Australia, Sept. 2001, pp. 90–92.

[6] ——, "Resolvable 2-designs for regular low-density parity-check codes," *IEEE Trans. Commun.*, vol. 51, pp. 1413–1419, Sept. 2003.

[7] S. R. Weller and S. J. Johnson, "Regular low-density parity-check codes from oval designs," *Eur. Trans. Telecommun.*, vol. 14 (5), pp. 399–409, Oct. 2003.

[8] P. O. Vontobel and R. M. Tanner, "Construction of codes based on finite generalized quadrangles for iterative decoding," in *Proc. Int. Symp. Information Theory (ISIT'200J)*, Washington, DC, June 24–29, 2001, p. 223.

[9] J. H. van Lint and R. M. Wilson, *A Course in Combinatorics*. Cambridge, U.K.: Cambridge Univ. Press, 1992.

[10] R. C. Bose, "Strongly regular graphs, partial geometries and partially balanced designs," *Pacific J. Math.*, vol. 13, pp. 389–419, 1963.

[11] P. J. Cameron and J. H. van Lint, *Graphs, Codes and Designs*, ser. London Math. Soc. Lecture Note Series, no. 43. Cambridge, U.K.: Cambridge Univ. Press, 1980.

[12] R. M. Tanner, "Minimum-distance bounds by graph analysis," *IEEE Trans. Inform. Theory*, vol. 47, pp. 808–821, Feb. 2001.

[13] F. Buekenhout, *Handbook of Incidence Geometry*. Amsterdam, The Netherlands: North-Holland, 1995.

[14] B. Vasic, "Structured iteratively decodable codes based on Steiner systems and their application in magnetic recording," in *Proc. IEEE GLOBECOM Conf.*, San Antonio, TX, Nov. 2001, pp. 2954–2960.

[15] S. Lin, H. Tang, Y. Kou, J. Xu, and K. Abdel-Ghaffar, "Codes on finite geometries," in *Proc. IEEE Information Theory Workshop (1TW2002)*, Cairns, Australia, Sept. 2001, pp. 14–16.

[16] J. L. Massey, *Threshold Decoding*. Cambridge, MA: MIT Press, 1963.

[17] A. E. Brouwer and C. A. van Eijl, "On the p-rank of strongly regular graphs," *Algebra and Combinatorics*, vol. 1, pp. 72–82, Apr. 1992.

[18] J. Doyen, X. Hubaut, and M. Vandensavel, "Ranks of incidence matrices of Steiner triple systems," *Math. Z.*, vol. 163, pp. 251–259, 1978.

[19] I. Anderson, *Combinatorial Designs: Construction Methods, Mathematics and Its Applications*. Chichester, U.K.: Ellis Horwood, 1990.

[20] E. F. Assmus, Jr. and J. D. Key, *Designs and Their Codes*. Cambridge, U.K.: Cambridge Univ. Press, 1993, vol. 103, Cambridge Tracts in Math.

[21] J. D. Key, "Some applications of Magma in designs and codes: Oval designs, Hermitian unitals and generalized Reed-Muller codes," *J. Symbolic Computat.*, vol. 31, pp. 37–53, Jan./Feb. 2001.

[22] J. A. Thas, "Construction of partial geometries," *Simon Stevin*, vol. 46, pp. 95–98, 1973.

[23] R. C. Bose, "On the application of the properties of Galois fields to the construction of hyper-Graeco-Latin squares," *Sankhya*, vol. 3, pp. 323–338, 1938.

[24] M. Blaum, P. Farrell, and H. van Tilborg, "Array codes," in *Handbook of Coding Theory*, W. C. Huffman, Ed. Amsterdam, The Netherlands: Elsevier, 1998, pp. 1855–1909.

[25] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North-Holland, 1977.

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

[27] R. M. Neal.. [Online]. Available: www.cs.toronto.edu/radford/homepage.html

[28] M. P. C. Fossorier, "Iterative reliability-based decoding of low-density parity check codes," *IEEE J. Select. Areas Commun.*, vol. 19, pp. 908–917, May 2001.

[29] F. De Clerk, R. H. Dye, and J. A. Thas, "An infinite class of partial geometries associated with the hyperbolic quadratic in $\mathrm{PG}(4n-1,2)$," *Euro. J. Combin.*, vol. 1, pp. 323–326, 1980.

[30] R. A. Mathon, "A new family of partial geometries," *Geometriae Dedicata*, vol. 73, pp. 11–19, 1998.

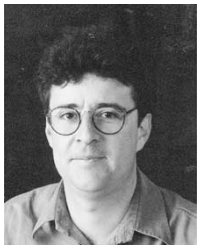
[31] J. A. Thas, "Some results on quadratics and a new class of partial geometries," *Simon Stevin*, vol. 55, pp. 129–139, 1981.

[32] J. H. van Lint and A. Schrijver, "Construction of strongly regular graphs, two weight codes and partial geometries by finite fields," *Combinatorica*, vol. 1, pp. 63–73, 1981.

[33] W. H. Haemers, "A new partial geometry constructed form the Hoffman-Singleton graph," in *Finite Geometries and Designs*. ser. London Math. Soc. Lecture Note Series, P. J. Cameron, J. W. P. Hirschfeld, and D. R. Hughes, Eds. Cambridge, U.K.: Cambridge Univ. Press, 1981, vol. 49, pp. 119–127.

Sarah J. Johnson (M'03) was born in Napier, New Zealand, in 1977. She received the B.E. degree (Hons I) in 2000 from the University of Newcastle, Callaghan, Australia, where she is currently working toward the Ph.D. degree in electrical engineering.

Since September 2003, she has been with National ICT Australia (NICTA), Sydney, Australia. Her research interests include low-density parity-check codes and iterative decoding.



Steven R. Weller (S'88–M'90) was born in Sydney, Australia, in 1965. He received the B.E. degree (Hons I) in computer engineering in 1988, the M.E. degree in electrical engineering in 1992, and the Ph.D. degree in electrical engineering in 1994, all from the University of Newcastle, Callaghan, Australia.

From 1994 to 1997, he was a Lecturer in the Department of Electrical and Electronic Engineering, University of Melbourne, Melbourne, Australia, and was a member of the Centre for Sensor Signal and Information Processing. Since 1997, he has been with the University of Newcastle, where he is currently a Senior Lecturer in the School of Electrical Engineering and Computer Science. His research interests include low-density parity-check codes, iterative decoding algorithms, space–time coded communications, and combinatorics.