EUROPEAN TRANSACTIONS ON TELECOMMUNICATIONS
Euro. Trans. Telecomms. 2003; **14**:399–409 (DOI: 10.1002/ett.939)

Information Theory

Regular low-density parity-check codes from oval designs

Steven R. Weller[1]* and Sarah J. Johnson[2]

[1]*School of Electrical Engineering and Computer Science, University of Newcastle, Callaghan, NSW 2308, Australia*
[2]*Wireless Signal Processing Program, National ICT Australia (NICTA), University of New South Wales, Sydney 2052, Australia*

SUMMARY

This paper presents a construction of low-density parity-check (LDPC) codes based on the incidence matrices of oval designs. The new LDPC codes have regular parity-check matrices and Tanner graphs free of 4-cycles. Like the finite geometry codes, the codes from oval designs have parity-check matrices with a large proportion of linearly dependent rows and can achieve significantly better minimum distances than equivalent length and rate randomly constructed LDPC codes. Further, by exploiting the resolvability of oval designs, and also by employing column splitting, we are able to produce 4-cycle free LDPC codes for a wide range of code rates and lengths while maintaining code regularity. Copyright © 2003 AEI.

1. INTRODUCTION

Low-density parity-check (LDPC) codes were first presented by Gallager [1] in 1962 and have recently been rediscovered and extended [2, 3]. By specifying block codes with a sparse parity-check matrix, Gallager presented an iterative decoding algorithm with complexity linear in the block length and decoding performance remarkably close to the Shannon limit [1, 2, 4]. It is known that Gallager's iterative decoding algorithm, called sum-product decoding, converges to the optimal solution provided the Tanner graph of the code is free of cycles [5, 6]. The existence of short cycles in the Tanner graph prevents an exact error-probability analysis of iterative decoding procedures, and the shorter are the cycles in the graph, the sooner the analysis 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.

Small cycles 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 [7, 8]. In Reference [7], the incidence matrices of Steiner triple systems (STS) were proposed as parity-check matrices for LDPC codes and in References [8–10] the range of available LDPC code parameters from STS was expanded by using a subset of the resolution classes of the resolvable Kirkman triple systems. A second class of algebraic LDPC codes, from the incidence matrices of finite projective and Euclidean geometries, were presented in References [5, 11, 12]. Like the codes from STS, small cycles are avoided in the Tanner graph of the codes from finite geometries. Further, the finite geometry codes produce excellent error correction performances with iterative decoding, a performance attributed to the many linearly dependent rows in their parity-check matrices.

In this paper we present a new class of algebraic LDPC codes, taking as parity-check matrices the incidence matrices of combinatorial structures known as oval designs. The family of parity-check matrices so obtained have small, uniform row and column weights, and have Tanner graphs which are free of small cycles. Moreover,

* Correspondence to: Steven R. Weller, School of Electrical Engineering and Computer Science, University of Newcastle, Callaghan, NSW 2308, Australia. E-mail: steve@ee.newcastle.edu.au

Contract/grant sponsors: Bell Laboratories, Australia; Lucent Technologies.
Contract/grant sponsor: Australian Research Council; Contract/grant number: LP0211210.
Contract/grant sponsor: CSIRO Telecommunications & Industrial Physics.

the incidence matrices of oval designs have column weights which are no longer fixed, as for STS, but grow along with the number of parity-check equations. The properties of the oval codes are similar to those of the finite geometry codes, including a large proportion of linearly dependent rows in their parity-check matrices.

As our construction is based on combinatorial design theory, we present in Section 2 of this paper some background material on designs before describing oval designs in particular. Section 3 defines the codes from oval designs and Section 4 discusses the performance of oval codes with sum-product decoding. Section 5 concludes the paper.

2. COMBINATORIAL DESIGNS

Let $\mathcal{P}$ be a v-set and suppose $\mathcal{B}$ is a collection of k-subsets of $\mathcal{P}$ with the property that each t-subset of $\mathcal{P}$ is contained in exactly λ of the elements of $\mathcal{B}$. Then the ordered pair $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ is called a t-(v, k, λ) design, or simply a t-design. The elements of $\mathcal{P}$ are called points and the elements of $\mathcal{B}$ are blocks. A regular design is one with a constant k points per block and r blocks containing each point. Thus, a regular design has six parameters: t, v, b, r, k and λ where b is the number of blocks and is sometimes denoted as t-(v, b, r, k, λ) design. However, these parameters are not independent, as in any regular design, $bk = vr$.

A 2-design is also called a balanced incomplete block design (BIBD). If $t \geq 2$ and $\lambda = 1$, then a t-design is called a Steiner system or a Steiner t-design. A Steiner 2-design thus has the property that every pair of points in the design occur together in exactly one block of the design. A resolution of a design $\mathcal{D}$ is a partition of the blocks of $\mathcal{D}$ into classes such that each point of $\mathcal{D}$ is in precisely one block from each class; such a design is said to be resolvable.

Every design can be described by a $v \times b$ incidence matrix N where each column in N represents a block B_j of the design and each row a point P_i:

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

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 $x \in \mathcal{P}$ and $y \in \mathcal{B}$ or $x \in \mathcal{B}$ and $y \in \mathcal{P}$. 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 simply the number edges it contains and the girth of a graph is the length of its smallest cycle. As the incidence graph is bipartite, the length of a cycle must be even and at least four.

In the context of this work, we will henceforth follow the notation established by Kou *et al.* [11, 12] and denote by γ and ρ the column and row weights of N respectively. This avoids the unfortunate coincidence of the symbol k to denote both column weight of the incidence matrix of a design and the number of information symbols in an $[n, k, d]$ block code.

The oval designs we consider are constructed from projective planes, which have themselves been recently proposed for the algebraic construction of LDPC codes [11]. Background material on oval codes and projective planes is presented in the Appendix. Briefly, a projective plane of order q, $\mathrm{PG}_2(q)$, is a set of $q^2 + q + 1$ lines and $q^2 + q + 1$ points such that every line passes through exactly $q + 1$ points and every point is incident on exactly $q + 1$ lines with any pair of points in the plane incident together in exactly one line. An oval, $\mathcal{O}$, in a projective plane is a set of $q + 2$ points that meet each line of the plane in 0 or 2 points. The oval design is the incidence structure having, for points the lines of the plane exterior to $\mathcal{O}$ and for blocks the points of the plane not on the oval $\mathcal{O}$, called the retained points. Incidence is given by the incidence of the projective plane; that is, in an oval design, a point is considered to belong to a block if the corresponding point and line in $\mathrm{PG}_2(q)$ are incident. Oval designs are Steiner 2-$(q(q-1)/2, q/2, 1)$ designs with $q + 1$ blocks through each point and $q^2 - 1$ blocks (see e.g. Reference [13, Chapter 8]).

Oval designs are also resolvable, with $q - 1$ blocks per resolution class and $q + 1$ classes in each design [13, Chapter 7]. Figure 1 shows an incidence matrix for the oval on six points constructed in the Appendix with columns partitioned into resolution classes. Zero entries are indicated by dots.

3. CONSTRUCTIONS OF LOW-DENSITY PARITY-CHECK CODES FROM OVAL DESIGNS

In this section, we employ the incidence matrices of the oval designs described in the previous section as

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

Figure 1. The incidence matrix of the 2-(6, 2, 1) oval design constructed in Appendix.

parity-check matrices of LDPC codes; we shall refer to the codes so obtained as oval codes. Further, we will employ two methods to increase the range of available LDPC codes derived from oval designs. Firstly, the resolvability of the oval designs will be used to produce lower rate codes, which we call R-oval codes and secondly, column splitting will be used to produce even higher rate codes, which we call S-oval codes. In both the cases, the codes obtained will also be regular and free of 4-cycles.

3.1. *LDPC codes from oval designs*

The incidence matrix of an oval design is used as the parity-check matrix of a binary LDPC code to give favourable properties to the code. In particular, the girth of the Tanner graph of an oval LDPC code corresponds to the girth of the incidence graph of the oval design. The incidence graph of an oval has girth at least 6 since no two points can be in the same two blocks together. Thus choosing an oval design to construct an LDPC code guarantees the absence of 4-cycles in the code. As $H = N$ the code will have v parity checks and block length $n = b$. Oval designs are regular and so all columns of H have constant weight γ and all rows constant weight ρ; such a code is said to be (γ, ρ)-regular.

The incidence matrix of a design is not necessarily full rank and so the the code dimension is $k = n - \text{rank}_2(N)$. For instance, the Euclidean and projective geometry codes have a significant proportion of linearly dependent rows in their incidence matrix and so give quite high rate codes despite N being square [12]. Oval designs also have a significant portion of linearly dependent rows which give the codes extra parity-check equations and subsequently improved decoding performances with sum-product decoding. Oval designs are the same length as the Euclidean geometry (EG) designs but produce higher rate LDPC codes.

We define oval codes as binary LDPC codes with parity-check matrix, H, whose rows are the the incidence vectors of the lines of $\text{PG}(2, 2^m)$ exterior to a regular oval $\mathcal{O}$. The columns of H correspond to points of the plane not on $\mathcal{O}$. Thus H has $2^{2m} - 1$ columns and $2^m(2^m - 1)/2$ rows. Since there are $2^m + 1$ ones per row of H and 2^{m-1} ones per column, H is regular and has a density of

$$\frac{2^m + 1}{2^{2m} - 1} \tag{1}$$

The 2-rank of the incidence matrix of a regular oval design is known to be given by Reference [14]

$$\text{rank}_2(W(\Pi, \mathcal{O})) = 3^m - 2^m \tag{2}$$

which yields both the number of code message bits

$$k = (2^m)^2 + 2^m - 3^m - 1 \tag{3}$$

and number of linearly dependent rows in H:

$$2^{2m-1} - 2^{m-1} - 3^m + 2^m \tag{4}$$

Avoiding 4-cycles guarantees a minimum distance of at least $2^{m-1} + 1$ via Massey's bound [15], as each bit in the code is checked by $\gamma = 2^{m-1}$ orthogonal parity-check equations. Thus the minimum distance of the oval codes increases with the length of the code as

$$d \geq \frac{1}{2}(\sqrt{n+1} + 1)$$

However, this also means that the density of the parity-check matrix decreases only with the square root of the code length as opposed to proportionally to the code length as is the case for codes defined with constant column weight.

For example, the oval design in Figure 1 has a 6×15 incidence matrix with column weight 2 and row weight 5. Thus, the oval LDPC code from this design is (2,5)-regular with length 15. The 2-rank of the incidence matrix is 5 (the last row is linearly dependent on the previous five) and so the oval LDPC code will have dimension $k = 15 - 5 = 10$. The minimum distance of the code is at least 3 by Massey's bound. Further, by observation we see that columns 1, 6 and 9 sum to zero modulo 2 so there is a code word of weight 3 with non-zero entries in bit positions 1, 6 and 9 and so the code minimum distance is exactly 3.

Table 1 shows the parameters of the oval designs and their corresponding oval codes for $m = 2, \ldots, 6$. For the two shortest codes, the minimum distance has been obtained by exhaustive computation. For the longer codes, corresponding to $m \geq 4$ in Table 1, the range of minimum distances has been obtained using Magma [16] for an upper bound and Massey's lower bound applied to oval LDPC codes.

The girth of the oval codes is always 6, as the requirement that $\lambda = 1$ and $t = 2$ guarantees the existence of 6-cycles as well as the absence of 4-cycles. Further, the structure associated with the Steiner 2-designs allows

Table 1. Parameters of codes from oval designs.

m	$H(v, b, \rho, \gamma)$	$\text{rank}_2(H)$	$[n, k, d]$
2	(6, 15, 5, 2)	5	[15, 10, 3]
3	(28, 63, 9, 4)	19	[63, 44, 5]
4	(120, 255, 17, 8)	65	[255, 190, 9–10]
5	(496, 1023, 33, 16)	211	[1023, 812, 17–36]
6	(2016, 4095, 65, 32)	665	[4095, 3430, 33–78]

the use of counting arguments to show that there are exactly

$$\frac{n}{3}\binom{\gamma}{2}(\rho-1)(\gamma-1) = 2^m\binom{2^{m-1}}{2}\frac{(2^{m-1}-1)(2^{2m}-1)}{3},$$

6-cycles in an oval code.

To see this, consider that every pair of points is incident together in exactly one block of the design. So if we choose an arbitrary pair of points (P_1, P_2) in a block B together, P_1 is incident in $\rho-1$ blocks other than B, say $\{D_1, \ldots, D_{\rho-1}\}$, (which cannot contain P_2). Likewise P_2 is incident in $\rho-1$ blocks other than B, say $\{E_1, \ldots, E_{\rho-1}\}$, (which cannot contain P_1). Since every pair of points must be incident in a block together, all the $(\rho-1)(\gamma-1)$ points other than P_1 incident in the blocks $\{D_1, \ldots, D_{\rho-1}\}$ must be incident in the blocks $\{E_1, \ldots, E_{\rho-1}\}$ so that each point is incident with both P_1 and P_2. In fact the only points not in the sets $\{D_1, \ldots, D_{\rho-1}\}$ and $\{E_1, \ldots, E_{\rho-1}\}$ are the points incident with P_1 and P_2 in B. We can then connect a 6-cycle from P_1 to a point in D_i and through the same point in E_j, back to P_2 to form a 6-cycle. This can be done $(\rho-1)(\gamma-1)$ times for each pair of points (P_1, P_2). There are $\binom{\gamma}{2}$ pairs of points in a block and n blocks in the design. A 6-cycle involves a pairs of points in three different blocks and the result follows.

LDPC codes from oval designs have lower column weight and fewer parity-checks than the equivalent length EG codes but more than the equivalent length STS LDPC codes. They therefore represent a middle ground in the tradeoff between minimum distance and decoding performance. However, as for the codes from finite geometries and STS, as the length of the oval code increases so too does the rate and so the longer oval LDPC codes are very high rate codes. The solution, which is to consider the resolution classes of oval designs to obtain low rate codes, is presented in the following section.

3.2. *Lower rate LDPC codes from resolvable oval designs*

The advantage of the resolvability of oval designs, for use as LDPC codes, occurs when only a subset of their resolution classes are employed to construct H. By removing from H all the columns in a resolution class the weight of every row in the parity-check matrix is decreased by exactly 1 and the matrix is still regular. As the columns of the incidence matrices of oval designs can be divided into $\gamma n/v$ resolution classes with v/γ columns per class we can generate a regular code with any block length

$$\frac{v}{\gamma} \times l \quad \text{for} \quad l \in \left\{1, 2, \ldots, \gamma\frac{n}{v}\right\}$$

So by using a fraction of the resolution classes of an oval design to define the LDPC codes, we can achieve codes with low rates and a wider range of code lengths.

An R-oval code formed from the resolution classes of an oval on $v = 2^m(2^m-1)$ points will have at least $2^{2m-1} - 2^{m-1} - 3^m + 2^m$ linearly dependent rows in its parity-check matrix and a minimum distance lower bounded by $2^{m-1}+1$. This is because removing columns from the incidence matrix can not increase its rank and nor can it decrease the number of orthogonal parity-check equations on each bit.

For example, the resolution classes of the oval on 120 points can be used to construct regular codes free of 4-cycles with the following parameters.

[240, 175, 9], [225, 160, 9], [210, 145, 9],
[195, 130, 9], [180, 115, 9], [165, 100, 9],
[150, 85, 9], [135, 70, 9], [120, 55, 9],
[105, 44, 9], [90, 33, 9], [75, 22, 9], [60, 11, 9].

(Note that the number of linearly dependent parity-checks in each code is $120 - k + n$.)

The decoding performance of the length 210 code is shown in the following section. A different selection of resolution classes can result in codes with the same length but with variations in rate depending on how many of the existing linearly dependent parity-checks are made linearly independent by removing columns of N.

3.3. *Higher rate LDPC codes from oval designs using column splitting*

One feature of both the oval and S-oval LDPC codes is their very high column weight. This is good for the code minimum distance, however minimum distance alone does not determine the decoding performance with sum-product decoding. The larger column weight which gives rise to this increase in decoding performance also increases the density of H, and we will see in the following section that a decoding performance degradation can result.

This motivates the third method of generating LDPC codes from oval designs, column splitting, a technique also employed in Reference [12]. The large column weight of oval designs allows us to split the non-zero entries of one column into s lower weight columns. The resulting matrix will have s times as many columns as the original, the same number of rows and row weight and most importantly will still be free of 4-cycles. This is in effect a pseudo-random construction of LDPC codes initialized with the oval design. Starting with an oval design allows very high rate LDPC codes to be derived which are both regular and free of 4-cycles. The minimum distance of the codes is still lower bounded by $\gamma + 1$, where γ is now defined as the weight of the smallest weight column in the parity-check matrix.

For example, each column in the incidence matrix of the 2-(496, 1023, 33, 16) oval design can be split into four weight 4 columns to produce a (4,33)-regular $[4092, 3596, \geq 5]$ LDPC code without 4-cycles. Table 2 shows the parameters of some of the LDPC codes we have obtained using this method.

We can also obtain codes which are irregular by using uneven column splitting. The oval design on 496 points for example can provide an S-oval code of length 4092 with half the columns of weight 4 and a quarter of the columns of each weight 3 and 5. The row weights of the code will still be 33 and the corresponding Tanner graph will still be free of 4-cycles.

4. SIMULATION RESULTS USING SUM-PRODUCT DECODING

In this section, we show the performance of LDPC codes derived from oval designs when decoded using the sum-product decoding algorithm [4] on an additive white Gaussian noise (AWGN) channel. In each simulation, a maximum number of iterations has been set and the standard stopping criterion for LDPC codes, $zH' = 0$, is applied to terminate the decoding early if the hard decision of the bit probabilities, z, is a valid codeword.

Table 2. Parameters of some S-oval codes from the oval designs in Table 1.

m	s	H	$[n, k, d]$
4	2	(4,17)-regular	[500, 380, ≥ 5]
5	4	(4,33)-regular	[4092, 3596, ≥ 5]
5	2	(8,33)-regular	[2046, 1550, ≥ 9]
6	8	(4,65)-regular	[32760, 30744, ≥ 5]
6	4	(8,65)-regular	[16380, 14364, ≥ 9]
6	2	(16,65)-regular	[8190, 6174, ≥ 17]

The LDPC codes from ovals are compared to randomly constructed LDPC codes and existing algebraic LDPC codes from STS codes [7] and EG codes [11, 12]. For the random LDPC codes we have used the following construction method [2, 4] using source code from Reference [17]:

- γ ones are placed in each column of H with an attempt made to keep the number of ones in each row approximately the same,
- extra ones are randomly added so that the weight of each row is greater than one,
- to remove 4-cycles, ones are moved randomly within columns involved in the cycle.

Regular randomly constructed codes perform best with column weight 3 [4], and so we have constructed random LDPC codes with this column weight. Further, in an attempt to get the best random LDPC codes, we have generated random LDPC codes with as few 4-cycles as possible where this produces a better code. However, there is a tradeoff between removing code cycles and obtaining code regularity as the process of removing 4-cycles causes the row weight to be more variable.

The more parity checks per bit there are in H, the more calculations that are required to perform an iteration of the sum-product decoding algorithm. The effect this has on decoding complexity at various signal-to-noise ratios (SNR) is also shown in this section. The average number of multiplication floating point operations (flops) required to decode a codeword can be calculated by estimating the number of flops for one iteration of the sum-product algorithm as $6n\gamma$ [4] and counting the number of iterations required to decode each codeword. There are other measurements of decoding complexity such as Reference [18] which include operations other than multiplication. Our values are only an estimation, used solely to give a comparison between the decoding complexity of LDPC codes with different column weights.

4.1. The decoding performance of oval codes

Figure 2 shows the performance of the oval [63, 44, 5] code compared to that of a randomly generated length 63 rate-0.7 LDPC code in an AWGN channel. The oval code is (4,9)-regular and the randomly generated LDPC code has a column weights of 3 and row weights between of 9 and 10. Also shown in an STS LDPC code from a 2-(21, 3, 1) design. The STS LDPC code is the same rate as the oval code but is (3,10)-regular and slightly longer. The

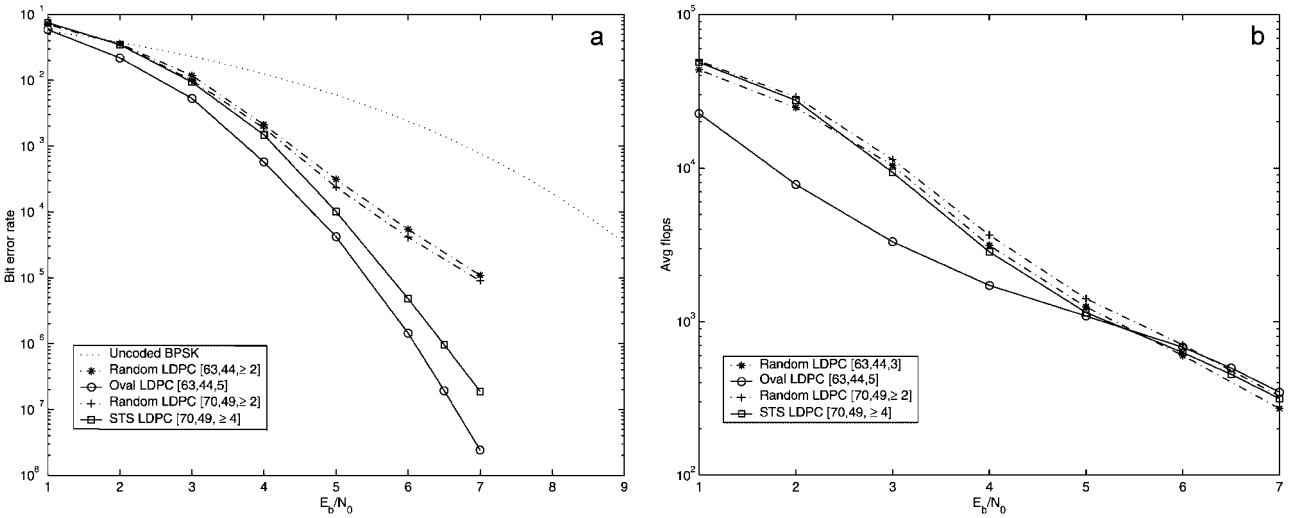

Figure 2. The decoding performance of the length 63 oval LDPC code in an AWGN channel using sum-product decoding with a maximum of 50 iterations. (a) Simulated error correction performance; (b) Average number of floating point multiply operations to decode a codeword.

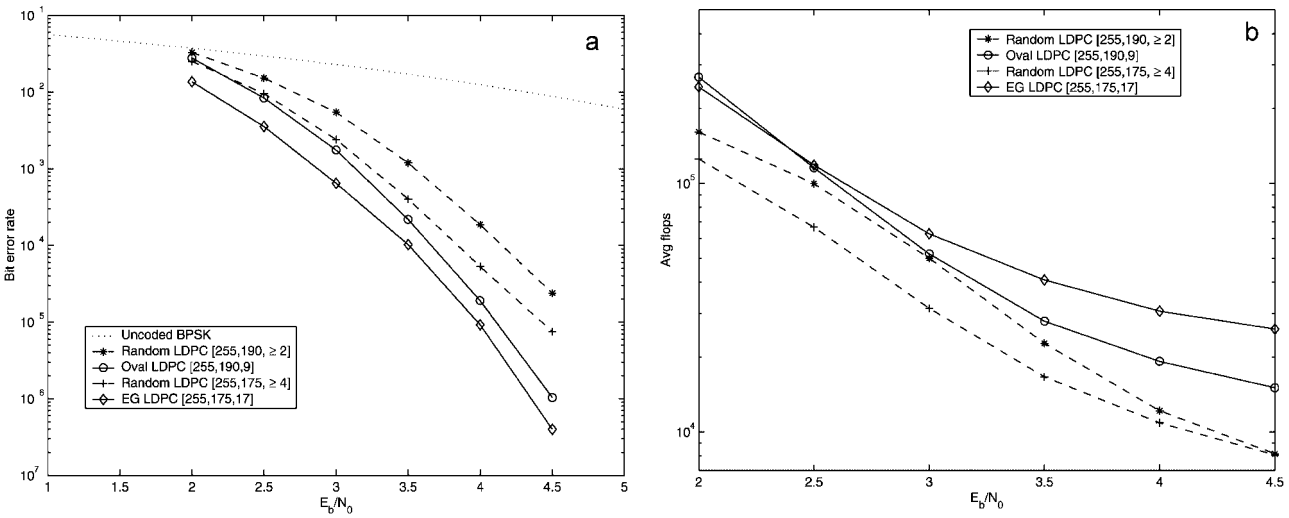

Figure 3. The decoding performance of the length 255 oval LDPC code in an AWGN channel using sum-product decoding with a maximum of 50 iterations. (a) Simulated error correction performance; (b) Average number of floating point multiply operations to decode a codeword.

better performance of the oval code despite its shorter length is attributed to the many extra parity-check equations in the oval code caused by the low rank of the oval incidence matrix.

Figure 3 shows the performance of the oval [255, 190, 9] code compared to that of a randomly generated LDPC code in the AWGN channel. The oval code is a (8,17)-regular code and the randomly generated LDPC code has column weight 3 and row weights between 7 and 18. The oval code has a higher column weight than the random code and so has a higher decoding complexity per iteration. However, in some cases the faster convergence of the oval code gives the two codes a similar decoding complexity overall.

Figure 4 shows the decoding performance over an AWGN channel of the oval [1023, 812, 17] code compared with a randomly generated LDPC code. Also shown is the [1023,781,33] EG code [11, 12]. The oval code is (16,33)-regular, the EG code is (32,32)-regular and the randomly generated LDPC codes have a column weight of 3 and row weights between 11 and 19. Again, the number of

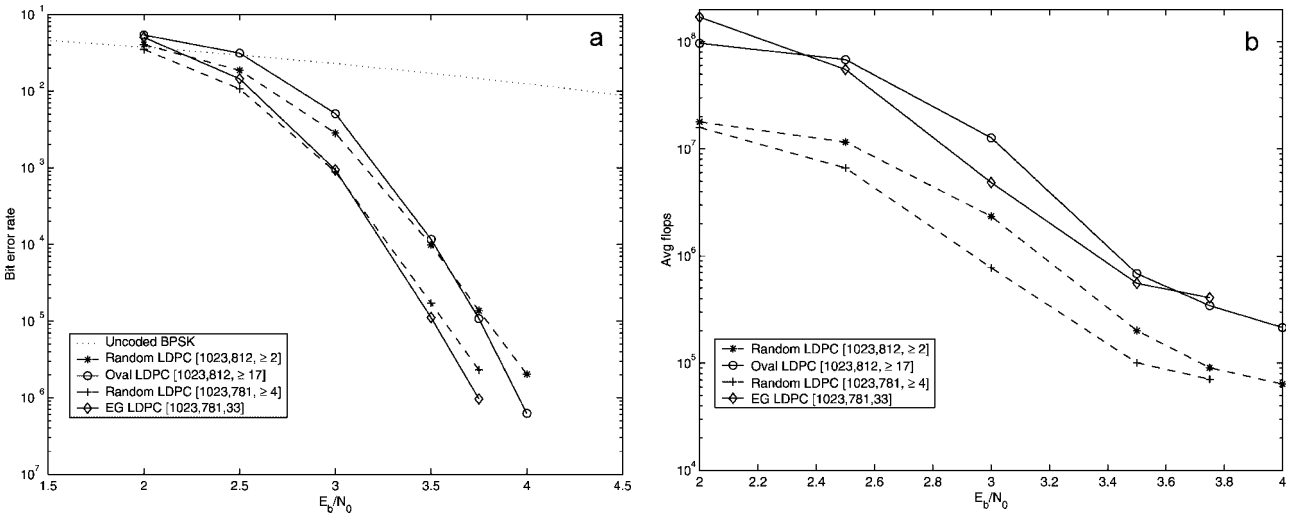

Figure 4. The decoding performance of the length 1023 oval LDPC code in an AWGN channel using sum-product decoding with a maximum of 1000 iterations. (a) Simulated error correction performance; (b) Average number of floating point multiply operations to decode a codeword.

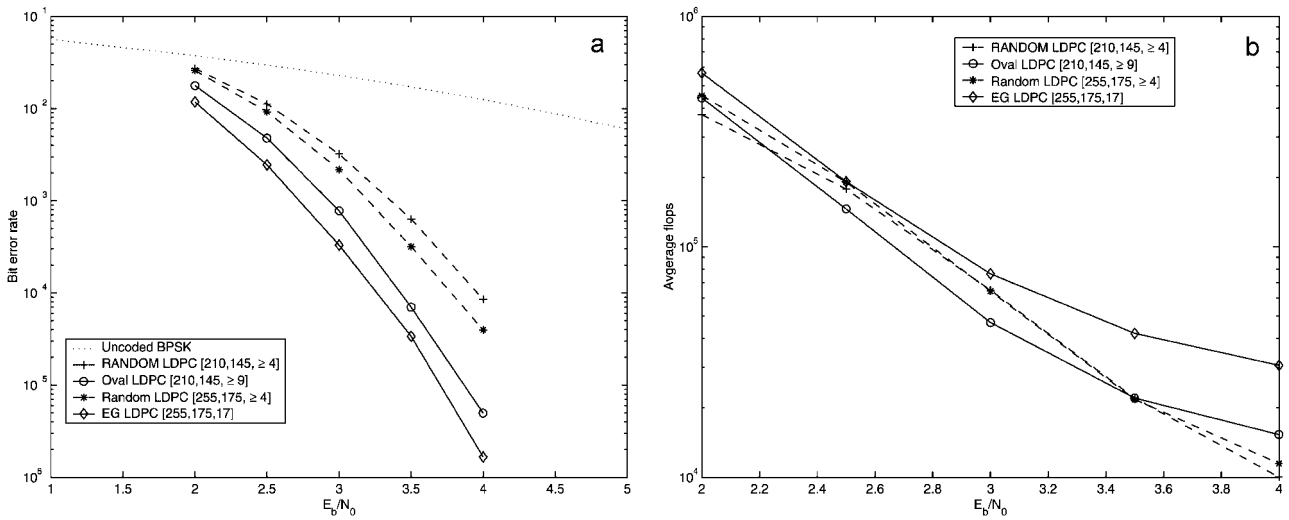

Figure 5. The decoding performance of rate 0.7 LDPC codes in an AWGN channel using sum-product decoding with a maximum of 200 iterations. (a) Simulated error correction performance; (b) Average number of floating point multiply operations to decode a codeword.

parity checks in H has a significant effect on decoding complexity as shown in Figure 4b. Like the EG code, the oval code outperforms the equivalent length and rate randomly constructed code only at the higher SNR.

For even longer oval codes, this trend continues and the performance of the oval codes relative to the standard random codes grows significantly worse at low SNR due to the increasing density of their parity-check matrices. The longer oval codes have significantly better minimum distances than are possible with a randomly constructed codes and so their disappointing performance is direct evidence of the limitations of comparing LDPC codes by minimum distance alone. The increase in column weight which provides this minimum distance gain also serves to greatly increase the density of H causing the poorer decoding performances. Only at very high SNR do the long oval codes outperform randomly constructed codes.

4.2. The decoding performance of R-oval codes

A (8,14)-regular rate-0.7 code R-oval [210, 145, 9] has been designed by taking 14 of the resolution classes of the 2-(120, 8, 1) oval. Figure 5 shows the decoding

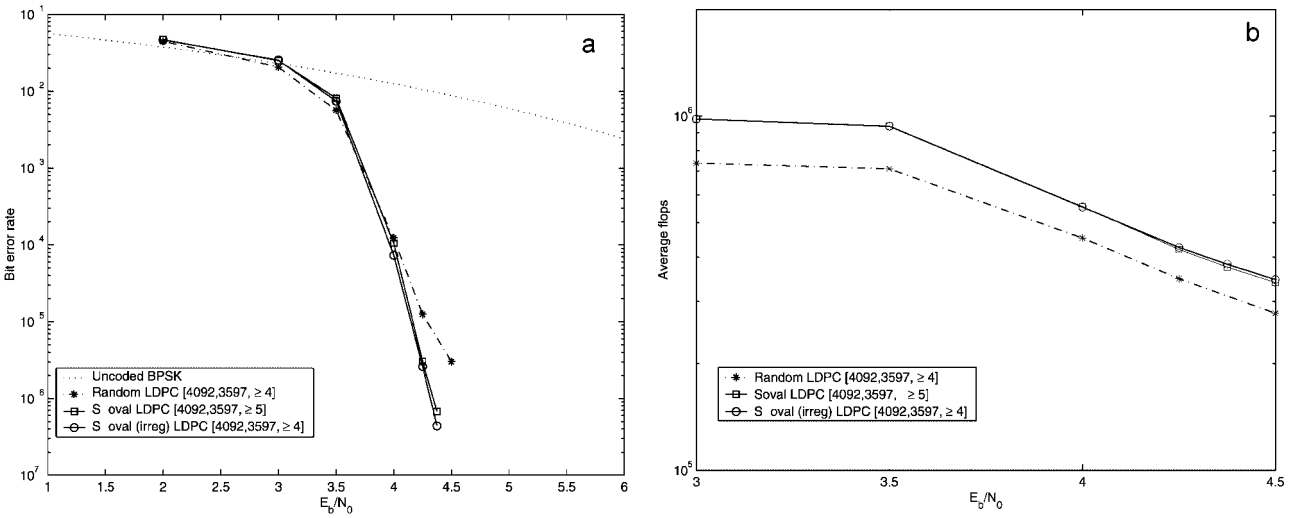

Figure 6. The decoding performance of length 4092, rate 0.88, LDPC codes in an AWGN channel using sum-product decoding with a maximum of 10 iterations. (a) Simulated error correction performance; (b) Average number of floating point multiply operations to decode a codeword.

performance of this code in an AWGN channel compared to a randomly generated LDPC code with the same rate and codeword length. Also shown is the length 255 EG code which also has the rate 0.7 compared to a randomly generated LDPC code with the same rate and codeword length. The EG code performs better than the R-oval code but the performance gain is only slightly more than would be expected due to its longer length.

Removing the columns of the oval design does not change its density or minimum distance or reduce the number of linearly dependent parity-check constraints and so we will see the same trend in performance for the R-oval codes as for the codes from the whole oval design. That is, improved error correction performance at all SNR, compared to the random LDPC codes, for short codes and worse error correction performances at low SNR, compared to random LDPC codes, as the code length and hence column weight is increased.

4.3. The decoding performance of S-oval codes

Figure 6 shows the performance of two LDPC codes constructed using column splitting, one regular and one irregular. Both have been constructed by randomly splitting each of the columns of the 2-(496, 1023, 33, 16) oval incidence matrix into four. Both the regular and irregular codes from the oval design have the same row weight, 33, and the same average column weight, 4, however by considering an irregular code, with column weights between 3 and 5, there is a small performance gain achieved.

5. CONCLUSIONS

In this paper, low-density parity-check codes based on combinatorial structures known as oval designs have been presented. Oval designs provide a deterministic construction for regular LDPC codes whose Tanner graphs are free of 4-cycles. Furthermore, codes with a significant portion of linearly dependent rows in their parity-check matrices are produced. Simulation results with the iterative sum-product decoding algorithm demonstrate that the LDPC codes from oval designs provide a good tradeoff between error correction performance and decoding complexity when compared to existing algebraic and randomly constructed LDPC codes.

The number of blocks in an oval design increases with the square of the number of points and so the rate of the oval-LDPC codes increases with their length. However, lower rate LDPC codes are obtained by using only a subset of the resolution classes of the oval designs to construct R-oval codes with properties similar to the oval codes but with a large range of rates.

The oval and R-oval LDPC codes seem particularly promising codes with sparse matrices, good minimum distances and many linearly dependent rows in their parity-check matrices. For short lengths, codes from oval designs significantly outperform the randomly constructed codes on an AWGN channel when decoded with the sum-product algorithm. The linearly dependent rows in the incidence matrices of the oval designs improve the performance of the shorter oval and R-oval codes at all SNR.

For the longer oval and R-oval LDPC codes, the large column weight negatively affects code performance due to the increased density of the parity-check matrix. For these codes, a decoding performance improvement over randomly constructed LDPC codes is only achieved at very high SNR. However, by using column splitting, new codes called S-oval codes are produced with low column weights, no 4-cycles and decoding performances similar to randomly constructed codes. By using column splitting, very high rate LDPC codes which are free of 4-cycles can be produced, a task that is difficult with traditional random code constructions.

ACKNOWLEDGEMENTS

We thank the reviewers for their careful reading of this paper and Prof. Radford M. Neal for his on-line repository of LDPC-related software. Helpful discussions with Prof. S. Lin are also gratefully acknowledged.

APPENDIX

Construction of oval designs

For completeness, we present here an overview of the construction of oval designs from ovals on projective planes so that the LDPC codes presented in this paper can be readily constructed by the reader. Oval designs and projective planes are well known; further details can be found in References [13, 19]. Our treatment of projective planes follows Anderson [19], while the material on oval designs is essentially Bose and Shrikhande's original presentation [20], using the terminology of Assmus and Key [13, 21].

A 2-$(q^2+q+1,\ q+1,\ 1)$ design, for some integer $q \geq 2$, is called a finite projective plane of order q. Consider the set S of triples $\mathrm{x} = (x, y, z)$ of elements of the finite field GF(q), where (x, y, z) are not all zero. S has q^3-1 members, but we identify triples x and y if $\mathrm{x} = \lambda \mathrm{y}$ for some non-zero element $\lambda \in \mathrm{GF}(q)$, and say that x and y are equivalent. Denote the equivalence class of x by [x]. Each equivalence class has $q-1$ members, corresponding to the $q-1$ possible non-zero values of λ, and so there are $(q^3-1)/(q-1) = q^2+q+1$ different classes [x] which we take as the points of PG(2, q).

Next, define the blocks (or *lines*) as follows: If $\alpha = (\alpha_0, \alpha_1, \alpha_2)$ is a triple of elements of GF(q), not all zero, define the line [α] to be the set of all points such that $\alpha_0 x + \alpha_1 y + \alpha_2 z = 0$. By an argument similar to the one for points, there are q^2+q+1 blocks. To see that there are $q+1$ points on each line, consider the line [α] where $\alpha = (\alpha_0, \alpha_1, \alpha_2)$. Not all the α_i are zero, so suppose for example that $\alpha_1 \neq 0$. Then, if [x] is on [α], x_1 is uniquely determined by x_0 and x_2, where x_0 and x_2 cannot both be zero. There are q^2-1 choices of x_0 and x_2, so there are q^2-1 vectors $x \neq 0$ satisfying $\alpha_0 x + \alpha_1 y + \alpha_2 z = 0$, and hence there are $(q^2-1)/(q-1) = q+1$ distinct points [x] on [α].

As an example, we construct the finite projective plane PG(2, 2^2), which is a 2-(21, 5, 1) design. Here we use GF(2^2), which can be thought of as $\{0, 1, \alpha, \alpha+1\}$, 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 can be written as

$$100,\ 010,\ 001,\ 1\alpha\alpha,\ 1\beta 0,\ 01\beta,\ 1\alpha 1,\ 101,\ 10\alpha,\ 1\beta\alpha,\ 1\beta 1,$$
$$10\beta,\ 11\alpha,\ 1\beta\beta,\ 110,\ 011,\ 1\alpha 0,\ 01\alpha,\ 1\alpha\beta,\ 11\beta,\ 111$$

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 $\alpha(0, 1, \beta) = (0, \alpha, 1)$.

There are 21 lines in PG(2, 2^2), a representative selection being as follows:

$$[100] : 010 \quad 001 \quad 01\beta \quad 011 \quad 01\alpha$$
$$[1\alpha\beta] : 1\beta 0 \quad 01\beta \quad 10\alpha \quad 1\alpha\beta \quad 111$$

In the above, the five points identified as lying on the line $[1\alpha\beta]$ are, by definition, those points (x, y, z) which satisfy the equation $x + \alpha y + \beta z = 0$.

An oval in a projective plane of even order q is a set of $q+2$ points that meet each line of the plane in 0 or 2 points; ovals of $q+2$ points are often called *hyperovals* in the literature. To construct such a set of points, consider the projective plane PG$(2, 2^m)$, and take a non-degenerate conic C on this plane, for example, the conic

$$xz = y^2.$$

There are $s+1$ points $P_1, P_2, \ldots, P_{s+1}$ on this conic, where $s = 2^m$. Through any point $P_i = (x', y', z')$ on the conic, there pass $s+1$ lines, S of which meet the conic in the other s points on the conic, and the remaining line $z'x + x'z = 0$ meets the conic in the single point P_i, and is therefore tangent to C. The $s+1$ tangents to the conic all pass through the point $P_0 = (0, 1, 0)$ which is called the nucleus (also *pole* or *knot*) of the conic. The s^2+s+1 lines of the plane may be divided into three classes:

(a) the $s(s+1)/2$ secants, each of which meets the conic in 2 points, neither of which is P_0;
(b) the $s+1$ tangents, each of which meets the conic in one point and passes through P_0; and
(c) the $s(s-1)/2$ exterior lines which do not meet the conic and hence do not pass through P_0.

A regular oval $\mathcal{O}$ in the projective plane PG(2, 2^m) is now formed by taking the $s+1$ points $P_1, P_2, \ldots, P_{s+1}$ on the conic, together with the nucleus P_0. The s^2-1 points of the plane other than P_0 and the points of the conic are called retained points.

Oval designs can now be defined: let Π be a projective plane of even order q and let $\mathcal{O}$ be an oval of Π. The oval design $W(\Pi, \mathcal{O})$ is the incidence structure having for points the lines of Π exterior to $\mathcal{O}$, and for blocks the points of Π not on the oval $\mathcal{O}$, namely the retained points. Incidence is given by the incidence in Π that is, in an oval design, a point is considered to belong to a block if the corresponding line and point in PG(2, 2^m) are incident. It is easy to show that oval designs are Steiner systems with parameters $2-(q(q-1)/2, q/2, 1)$; see Reference [13, Chapter 8]. Oval designs are resolvable with a distinct resolution defined by each point p on $\mathcal{O}$: the $s-1$ blocks corresponding to the retained points on a secant or tangent through p form a single parallel class and the full set of $s+1$ parallel classes forms the resolution [21]. The family of oval designs constructed in this way have the following parameters:

$$\upsilon = \frac{s(s-1)}{2}, \quad b = s^2-1, \quad \rho = s+1, \quad \gamma = \frac{s}{2}, \quad \lambda = 1,$$

where $s = 2^m$.

To complete the example above, we take the conic $xz = y^2$ defined on points (x, y, z) of the projective plane PG$(2, 2^2)$. There are $s+1=5$ points $P_1, P_2, \ldots, P_5$ on this conic:

$$100,\ 001,\ 1\alpha\beta, 1\beta\alpha, 111$$

and these points, together with the nucleus $P_0 = 010$, form an oval $\mathcal{O}$. The $s^2+s+1=21$ lines of the plane are divided into three classes:

(a) the $s(s+1)/2 = 10$ secants:

$$[01\alpha],\ [010],\ [1\alpha\beta],\ [111],\ [1\beta 0],\ [01\beta],\ [1\beta\alpha],\ [110],\ [011],\ [1\alpha 0]$$

Table 1A. Construction of the resolution classes of an oval design.

Secant/tangent	Retained points on secant/tangent		
$[01\alpha]$	01β	$1\alpha 1$	11β
[010]	101	10α	10β
$[01\beta]$	$1\beta 1$	11α	01α
[011]	$1\alpha\alpha$	$1\beta\beta$	011
[001]	$1\beta 0$	110	$1\alpha 0$

(b) the $s+1=5$ tangents:

$$[100],\ [10\beta],\ [001],\ [101],\ [10\alpha]$$

(c) the $s(s-1)/2 = 6$ exterior lines:

$$[11\alpha],\ [1\beta\beta],\ [1\alpha\alpha],\ [1\alpha 1],\ [11\beta],\ [1\beta 1].$$

Choosing point $P = 100$ on $\mathcal{O}$ leads to a resolvable oval design as follows: $s+1=5$ members of the set of secants and tangents listed above intersect point P and each such line contains $s-1=3$ retained points. The set of secant/tangent lines and their corresponding retained points are shown in Table 1A.

We now take as points of the oval design the 6 exterior lines and as blocks the set of $s^2+s+1-(s+2) = (s+1)(s-1) = 15$ retained points, taken from Table 1A in the natural (left-to-right, top-to-bottom) order. Each row of Table 1A therefore constitutes a resolution class of the design, and we obtain the incidence matrix of the 2-(6, 2, 1) oval design given in Figure 1.

The first column, for example, reflects that the retained point 01β is incident with the two lines $[11\alpha], [1\beta 1]$ exterior to the oval.

REFERENCES

1. Gallager RG. Low-density parity-check codes. *IRE Transctions on Information Theory* 1962; **IT-8**(1): 21–28.
2. MacKay DJC, Neal RM. Near Shannon limit performance of low density parity check codes. *Electronic Letters* 1996; **32**(18): 1645–1646, Reprinted *Electronic Letters* 1997; **33**(6): 457–458.
3. Tanner RM. A recursive approach to low complexity codes. *IEEE Transactions on Information Theory* 1981; **IT-27**(5): 533–547.
4. MacKay DJC. Good error-correcting codes based on very sparse matrices. *IEEE Transactions on Information Theory* 1999; **45**(2): 399–431.
5. Lucas R, Fossorier MPC, Kou Y, Lin S. Iterative decoding of one-step majority logic decodable codes based on belief propagation. *IEEE Transactions on Communications* 2000; **48**(6): 931–937.

6. McEliece RJ, MacKay DJC, Cheng J-F. Turbo decoding as an instance of Pearl's 'belief propagation' algorithm. *IEEE Journal on Selected Areas in Communications* 1998; **16**(2): 140–152.
7. MacKay DJC, Davey MC. 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. Marcus B, Rosenthal J (eds). Springer-Verlag: New York, 2000; pp. 113–130. Available at http://wol.ra.phy.cam.ac.uk/mackay/CodesRegular.html
8. Johnson SJ, Weller SR. Regular low-density parity-check codes from combinatorial designs. In *Proceedings of IEEE Information Theory Workshop*, Cairns, Australia, September 2001, pp. 90–92.
9. Johnson SJ, Weller SR. Construction of low-density parity-check codes from Kirkman triple systems. In *Proceedings of IEEE Globecom Conference*, San Antonio, TX, November 2001, pp. 970–974.
10. Johnson SJ, Weller SR. Resolvable 2-designs for regular low-density parity-check codes. *IEEE Transactions on Communication*, 2003; **51**(9): 1413–1419.
11. Kou Y, Lin S, Fossorier MPC. Low-density parity-check codes: Construction based on finite geometries. In *Proceedings of IEEE Globecom Conference*, San Francisco, CA, November 2000, pp. 825–829.
12. Kou Y, Lin S, Fossorier MPC. Low-density parity-check codes based on finite geometries: a rediscovery and new results. *IEEE Transactions on Information Theory* 2001; **47**(7): 2711–2736.
13. Assmus EF, Jr., Key JD. *Designs and Their Codes*. Vol. 103 of Cambridge Tracts in Mathematics. Cambridge University Press: Cambridge, 1993.
14. Carpenter LL. Oval designs in desarguesian projective planes. *Designs, Codes and Cryptography* 1996; **9**(1): 51–59.
15. Massey JL. *Threshold Decoding*. M.I.T. Press: Cambridge, Massachusetts, 1963.
16. Bosma W, Cannon J, Playoust C. The Magma algebra system I: The user language. *Journal of Symbolic Computation* 1997; **24**(3/4): 235–265.
17. Neal RM. www.cs.toronto.edu/radford/homepage.html December 2001.
18. Fossorier MPC. Iterative reliability-based decoding of low-density parity check codes. *IEEE Journal on Selected Areas in Communications* 2001; **19**(5): 908–917.
19. Anderson I. *Combinatorial Designs: Construction Methods*, Mathematics and its Applications. Ellis Horwood, Chichester, 1990.
20. Bose RC, Shrikhande SS. On the construction of sets of mutually orthogonal Latin squares and the falsity of a conjecture of Euler. *Transactions of American Mathematical Society* 1960; **95**: 191–209.
21. Key JD. Some applications of Magma in designs and codes: oval designs, Hermitian unitals and generalized Reed–Muller codes. *Journal of Symbolic Computation* 2001; **31**(1/2): 37–53.