High-Rate LDPC Codes from Unital Designs

S. J. Johnson and S. R. Weller
School of Electrical Engineering and Computer Science
The University of Newcastle
Callaghan, NSW 2308, Australia.
e-mail:{sarah,steve}@ee.newcastle.edu.au

***Abstract*— This paper presents a construction of very high-rate low-density parity-check (LDPC) codes based on the incidence matrices of unital designs. Like the projective geometry and oval designs, unital designs exist with incidence matrices which are significantly rank deficient. Thus high-rate LDPC codes with a large number of linearly dependent parity-check equations can be constructed. The LDPC codes from unitals have Tanner graphs free of 4-cycles and perform well with iterative decoding, offering new LDPC codes at rates and lengths not available with existing algebraic LDPC codes.**

I. Introduction

Low-density parity-check (LDPC) codes were first presented by Gallager [1] in 1962 and have recently been rediscovered and extended [2], [3]. LDPC codes are obtained by specifying a sparse parity-check matrix H, so that the calculation of each checksum depends on few code word bits, and the evaluation of code bit validity depends on few checksums. Using this property of LDPC codes Gallager presented an iterative decoding algorithm whose complexity remains linear in the block length with performance remarkably close to the Shannon limit [1], [2], [4].

A Tanner graph displays the relationship between codeword bits and parity checks and provides a useful representation of LDPC codes [3]. Each of the code bits and parity checks in H are represented by a vertex in the graph. A graph edge joins a code bit vertex to the vertices of the parity checks that include it. It is known that the iterative sum-product decoding algorithm [5] converges to the optimal solution provided that the Tanner graph of the code is free of *cycles*. A cycle in a Tanner graph is a sequence of connected code bits and check sums which start and end at the same vertex in the graph, and which contain other vertices no more than once. The length of the cycle is simply the number of edges it contains.

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.

This work was supported by a CSIRO Telecommunications and Industrial Physics postgraduate scholarship and Bell Laboratories Australia, Lucent Technologies, with the Australian Research Council under Linkage Project Grant LP0211210.

Cycles of length less than 6 in the Tanner graph associated with an LDPC code can be systematically avoided by taking as parity-check matrices the incidence matrices of suitably chosen combinatorial designs called Steiner 2-designs [6], [7], [8], [9]. A Steiner 2-design, denoted 2-$(v, b, r, \gamma, 1)$ or simply 2-$(v, \gamma, 1)$, is an arrangement of a set of v *points* into b subsets, called *blocks*, such that the number of points in each block, and the number of blocks which contain each point, designated γ and r respectively, are the same for every point and block in the design and that every pair of points appears together in exactly one block.

Besides the Steiner 2-designs with constant column weight, the Steiner 2-designs of interest benefit from rank deficient incidence matrices and can be derived from projective geometries. These are the projective geometry (PG) designs themselves, which are 2-$(m^2 + m + 1, m + 1, 1)$ designs, the 2-$(m(m-1)/2, m/2, 1)$ oval designs and unital designs which are 2-$(m^3 + 1, m + 1, 1)$ designs. The majority logic decodable codes constructed in [10], [11] which were derived from projective geometries have recently been shown to also make excellent LDPC codes in [7] and along with Euclidean geometries (EG) in [8]. Motivated by the excellent performance of these codes, oval designs were used to construct new LDPC codes in [12].

In this paper we construct the parity-check matrices of LDPC codes using the incidence matrices of unital designs. The family of parity-check matrices so obtained have uniform row and column weights, and have Tanner graphs which are free of 4-cycles. The parameters of the family of unital designs were presented in [13, Table II] where it was assumed that the code rates would be $(b-v)/b$ if codes were constructed from the incidence matrices of unital designs on $v = m^3+1$ points. However, for odd m the corresponding incidence matrices are significantly rank deficient for small m and conjectured to be so for larger m [14]. Consequently, LDPC codes from unital designs with odd m benefit from both higher rates and the decoding advantages attributed to a large number of linearly dependent rows in the parity-check matrix [8], [15]. Thus we consider in this paper the properties and performance of LDPC codes derived from unital designs. Further, column splitting is applied to the codes from unital designs to construct even higher-rate LDPC codes free of 4-cycles.

We present unital designs in some detail in Section II before describing the LDPC codes constructed using unital designs

in Section III. Section IV details the performance of unital LDPC codes when decoded using the sum-product algorithm and Section V concludes the paper.

II. Unital designs

Unital designs are constructed from projective geometries and we present some background material on both projective geometries and unitals in this Section. Further details on projective planes and their close connections with error-correcting codes can be found in [16], [17]. Our treatment of projective geometries follows Anderson [17], while the material on unital designs is essentially the presentation of Assmus and Key [16], [14].

Consider the set S of triples $\mathbf{x} = (x, y, z)$ 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 $\mathbf{x}$ and $\mathbf{y}$ if $\mathbf{x} = \lambda\mathbf{y}$ for some non-zero element $\lambda \in$ GF(q), and say that $\mathbf{x}$ and $\mathbf{y}$ are equivalent. Denote the equivalence class of $\mathbf{x}$ by $[\mathbf{x}]$. 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 $[\mathbf{x}]$, 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 $[\alpha]$ to be the set of all points $[\mathbf{x}]$ 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 $[\alpha]$ 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 $[\mathbf{x}]$ is on $[\alpha]$, 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 $[\mathbf{x}]$ on $[\alpha]$.

As an example, we construct the finite projective plane PG$(2, 2^2)$. 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

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

$$11\alpha, 11\beta, 1\alpha0, 1\alpha1, 1\alpha\alpha, 1\alpha\beta, 1\beta0, 1\beta1, 1\beta\alpha, 1\beta\beta.$$

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, 01α and $0a\beta$ define the same point since $(0, \alpha, \beta) = \alpha(0, 1, \alpha)$.

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

$$[100] : 001 \quad 010 \quad 011 \quad 01\alpha \quad 01\beta,$$

$$[011] : 100 \quad 011 \quad 111 \quad 1\alpha\alpha \quad 1\beta\beta,$$

$$[1\alpha\beta] : 01\beta \quad 10\alpha \quad 111 \quad 1\alpha\beta \quad 1\beta0.$$

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

Fig. 1. The incidence matrix of the 2-$(9, 3, 1)$ unital design from the unitary polarity on the plane PG$(2, 2^2)$.

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 *unitary polarity* in a projective plane of even order $q = m^2$ is a set of points of the plane with cardinality $m^3 + 1$ having the property that every line of the plane meets the set in 1 or $m + 1$ points. For example, the hermitian unital in PG$(2, m^2)$ is the set of points (x, y, z) satisfying [14]

$$f(x, y, z) = x^{m+1} + y^{m+1} + z^{m+1} = 0.$$

For the plane PG$(2, 2^2)$ presented above, the set of points

$$110, 011, 1\alpha0, 01\alpha, 1\beta0, 01\beta, 101, 10\alpha, 10\beta$$

form the unitary polarity described by $x^3 + y^3 + z^3 = 0$. The lines

$$[11\beta], [010], [1\beta1], [\beta\alpha1], [1\alpha1], [111],$$

$$[001], [\alpha11], [100], [\beta11], [11\alpha], [1\alpha\beta],$$

all contain 3 of the points in the unitary polarity and all other lines contain one of these points.

A *unital design* or *unital* has as points the point set of a unitary polarity and for blocks those lines in the projective plane that meet the point set of the unitary polarity in $m + 1$ points [16]. The points and blocks of the design retain the incidence of the points and lines of the geometry. Thus a unital design is a *Steiner* 2*-design* with parameters 2-$(m^3 + 1, m + 1, 1)$. That is, a unital design consists of $b = m^2(m^3 + 1)/(m + 1)$ subsets, called blocks, of a set of $v = m^3 + 1$ points with the property that every point is contained in $r = m^2$ blocks, every block contains $\gamma = m + 1$ points and every pair of points is contained in exactly one block together.

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

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

The unitary polarity defined above on the plane GF(2^2) produces a 2-$(9, 3, 1)$ unital design with incidence matrix shown in Fig. 1.

The unitals described above are *Hermitian unitals*, which are the set of points and lines of a unitary polarity on a desarguesian plane of order m^2 [16]. These unitals exist for all m a prime power. However other unital 2-$(m^3 + 1, m + 1, 1)$ designs exist, for m not necessarily a prime power, which are

not defined on a desarguesian plane [16]. The codes presented in this paper are derived from Hermitian unitals constructed using the method of [14].

III. LDPC CODES FROM UNITAL DESIGNS

We will construct LDPC codes from unital designs in two ways. We define type-A codes, also called unital codes, by taking the incidence matrix of the unital design as the parity-check matrix of the code. A unital LDPC code will thus have v parity checks and block length equal to b. All columns of H will have constant weight γ and all rows constant weight r; the codes are thus said to be (γ, r)-regular. The density of the parity-check matrix of a unital code is

$$\frac{m+1}{m^3+1},$$

which decreases as the code length increases.

The unital designs have the property that every pair of points in the design occur together in exactly one block. Thus a pair of points cannot occur together in two blocks and cycles of size 4 are avoided in the Tanner graph of unital codes. However cycles of size 6 always occur in codes from Steiner 2-designs [9], and there are exactly

$$N_6(m) = \binom{m+1}{2} \frac{m^3(m^3+1)(m-1)}{3}$$

6-cycles in a unital code from the unital design on m^3+1 points.

Since no pair of points can occur together in two blocks the unital codes have an orthogonal check set and Massey's minimum distance bound can be applied to unital codes. Unital codes thus have a lower bound on the minimum distance of one plus the column weight and we have

$$d \geq m+2. \tag{1}$$

The parity-check matrices constructed from incidence matrices of unitals are not necessarily full 2-rank and so the number of message bits in the code is $k = n - \text{rank}_2(H)$. While an explicit formula for the 2-ranks of the incidence matrices of unital designs is not yet available, it is known that the 2-rank can only be less than m^2 if $2|m+1$ [16, Theorem 8.3.1]. For the unitals presented in Table I the 2-ranks of the incidence matrices have been calculated in [14] where it is conjectured that the 2-rank of those unitals where $2|m+1$ is

$$m(m^2-m+1).$$

Table I shows the parameters of the unital designs obtained for values of $m = 2, \ldots, 9$, m a prime power. Also shown are the parameters of the associated linear block code. The notation $[n, k, d]$ specifies the length, dimension and minimum distance of the code respectively. The range of possible values for the minimum distance of the unital codes has been shortened via exhaustive search using Magma [18]. We see that the small unital codes have minimum distances better than the lower bound.

TABLE I
PARAMETERS OF TYPE-A CODES FROM UNITAL DESIGNS

m	$(v, b, \gamma, \rho, \lambda)$	$\text{rank}_2(H)$	$[n, k, d]$
2	$(9, 12, 3, 4, 1)$	9	$[12, 3, 6]$
3	$(28, 63, 4, 9, 1)$	21	$[63, 42, 6]$
4	$(65, 208, 5, 16, 1)$	65	$[208, 143, 6\text{–}10]$
5	$(126, 525, 6, 25, 1)$	105	$[525, 420, 7\text{–}9]$
7	$(344, 2107, 8, 49, 1)$	301	$[2107, 1806, 9\text{–}12]$
8	$(513, 3648, 9, 64, 1)$	513	$[3648, 3135, \geq 10]$
9	$(730, 5913, 10, 81, 1)$	657	$[5913, 5256, \geq 11]$

TABLE II
PARAMETERS OF TYPE-B CODES FROM UNITAL DESIGNS

m	s	H	$[n, k, d]$
4	2	$\gamma = 2$ and 3, $r = 16$	$[416, 351, \geq 3]$
5	2	$(3, 25)$-regular	$[1050, 924, \geq 4]$
7	2	$\gamma = 3$ and 5, $r = 49$	$[4214, 3870, \geq 4]$
8	2	$\gamma = 3$ and 6, $r = 64$	$[7296, 6783, \geq 4]$
8	3	$(3, 64)$-regular	$[10944, 10431, \geq 4]$
9	3	$\gamma = 3$ and 4, $r = 81$	$[11826, 11096, \geq 4]$

The Type-A unital codes provide a deterministic construction, guaranteed girth, and regularity. The benefit of a deterministic construction is that the storage requirements necessary to completely describe the code are reduced. If storage is a significant issue it is possible to specify only the required m and the entire code can be constructed on-line with some expenditure in terms of computational complexity. Alternatively, where the hard-wiring of the codes Tanner graph is employed [19] the exact regularity of the unital codes translates directly into regularity in the layout of an ASIC. Unital codes are thus very promising LDPC codes for moderate to high signal-to-noise ratio channels.

The large column weight of the unital codes motivates the second type of codes from unital designs, type-B codes, which we construct using column splitting, a technique employed in [8]. The large column weight of unital designs allows us to split the non zero entries of one column into two or more (designated s) lower weight columns. The resulting matrix will have s times as many columns as the original, the same number of rows, and most importantly will still be free of 4-cycles. By increasing the length of the code without increasing the number of parity-check equations we can derive very high rate LDPC codes without 4-cycles.

For example each column in the incidence matrix of the 2-$(126, 525, 6, 25, 1)$ unital design can be split into two weight 3 columns to produce a $(3, 25)$-regular $[1050, 924, \geq 4]$ LDPC code without 4-cycles. Splitting columns in this way produces sparser parity-check matrices and codes with still higher rates. The minimum distance of the type B codes is still lower bounded by (1) where γ is now defined as the weight of the smallest weight column in the parity-check matrix.

Table II shows the codes we have obtained using this method.

IV. SIMULATION RESULTS

The performance of unital LDPC codes on the additive white gaussian noise (AWGN) channel, when decoded us-

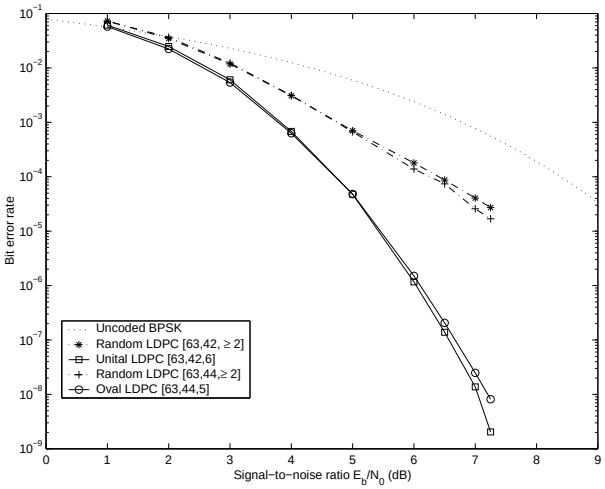

Fig. 2. The decoding performance of length 63 LDPC codes on an AWGN channel using sum-product decoding with a maximum of 10 iterations.

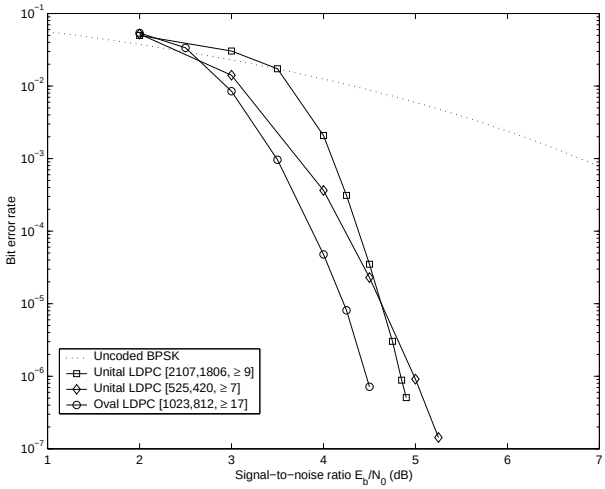

Fig. 3. The decoding performance of unital and oval LDPC codes on an AWGN channel using sum-product decoding with a maximum of 10 iterations.

ing the sum-product decoding algorithm [4], [2], have been compared to that of randomly generated codes of the same rate and length and existing algebraic LDPC codes from oval designs. 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 on the bit probabilities, z, is a valid codeword.

For the random LDPC codes we have used the construction method from [4], [2] using source code from [20]. At the signal-to-noise ratios we consider the regular randomly constructed LDPC codes perform best with column weight 3 and so we have constructed random LDPC codes with this column weight rather than constructing random codes with the column weight of the unital codes. Further, in an attempt to get the best random LDPC codes we have generated random LDPC codes with as few 4-cycles as possible in the cases where the removal of 4-cycles produces a better performing LDPC 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.

Fig. 2 shows the performance of the unital $[63, 42, 6]$ code compared to a randomly generated LDPC code on the AWGN channel. The unital code is a $(4, 9)$-regular code and the randomly generated LDPC code is $(3, 9)$-regular. Also shown is the performance of the equivalent length but slightly higher rate oval LDPC code which is also $(4, 9)$-regular. Probably due to its better minimum distance, the unital code outperforms the oval code at very high signal-to-noise ratios.

Fig. 3 shows the performance over an AWGN channel of the unital $[525, 420, \geq 7]$ and $[2107, 1806, \geq 9]$ codes. The 2-dimensional PG and EG LDPC codes with the closest rate are length 4161 and 4095 respectively while the closest rate oval LDPC code is length 1023. The performance of the $[1023, 812, \geq 17]$ oval code is also shown in Fig. 3. In a Similar manner to the oval, EG and PG codes, as the size of the unital increases so too does the column weight of the unital code. This provides a good minimum distance for the code, and hence excellent decoding performance at high signal-to-noise ratios, but also degrades the decoding performance at low signal-to-noise ratios. The length 525 unital code out-performs randomly constructed codes for bit error rates lower than 10^{-4}, while the length 2107 unital code out-performs randomly constructed codes for bit error rates lower than 10^{-6}.

The column weight of the LDPC codes from unital designs can be reduced, to improve their performance at low signal-to-noise ratios, by employing column splitting. Such codes are no longer completely deterministic but they can still be regular and do retain the guaranteed girth. Using column splitting very high rate LDPC codes can be achieved which is beneficial for applications such as magnetic recording channels. Figs. 4–5 show the performance of type-B LDPC codes constructed using column splitting. For these codes the column weights are keep small and high rate LDPC codes free of 4-cycles are constructed.

Fig. 4 shows the BER performance over an AWGN channel of the $[416, 351, \geq 3]$ code from the unital on 65 points compared with a randomly generated LDPC code. The unital code is nearly regular with half the columns weight 3 and the other half weight 2, with all rows weight 16. The randomly generated LDPC code has column weights of 3 and row weights between 8 and 63. Also shown is the BER performance over an AWGN channel of the $[4214, 3870, \geq 3]$ code from the unital on 344 points compared with a randomly generated LDPC code. The unital code has half the columns weight 2 and the other half weight 3 with each row weight 49 while the randomly generated LDPC code has all columns weight 3 and row weights between 28 and 48. The length 4214 unital code performs similarly to the slightly longer but equivalent rate $[4599, 4227, \geq 9]$ type-II EG-LDPC code [8]

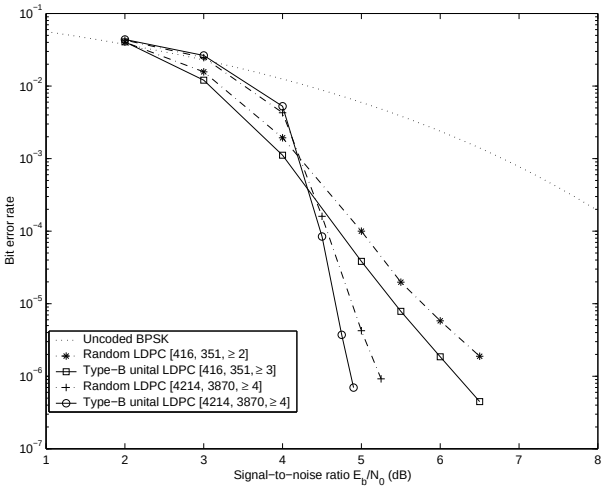

Fig. 4. The decoding performance of LDPC codes on an AWGN channel using sum-product decoding with a maximum of 10 iterations.

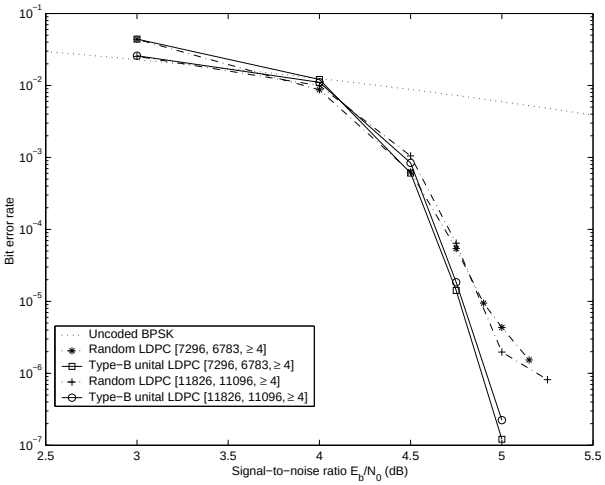

Fig. 5. The decoding performance of LDPC codes on an AWGN channel using sum-product decoding with a maximum of 10 iterations.

which is $(8, 72)$-regular.

Fig. 5 shows the BER performance over an AWGN channel of the $[7296, 6783, \geq 4]$ code from the unital on 344 points compared with a randomly generated LDPC code. The unital code has half the columns weight 2 and the other half weight 3 with each row weight 49 while the randomly generated LDPC code has all columns weight 3 and row weights between 34 and 52. Fig. 5 also shows the BER performance over an AWGN channel of the $[11826, 11096, \geq 4]$ code from the unital on 730 points compared with a randomly generated LDPC code. The unital code has columns weight 3 and 4 and row weights between 44 and 67 while the randomly generated LDPC code has all columns weight 3 and row weights between 39 and 56.

V. Conclusions

In this paper low-density parity-check codes, based on combinatorial structures known as unital designs, have been presented. We have constructed high-rate LDPC codes with Tanner graphs free of 4-cycles, and in some cases with a large number of linearly dependent parity checks as well. Simulation results with the sum-product decoding algorithm demonstrate that the codes from unital designs provide excellent decoding performances.

References

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

[2] D. J. C. MacKay and R. M. Neal, "Near Shannon limit performance of low density parity check codes," *Electron. Lett.*, vol. 32, no. 18, pp. 1645–1646, March 1996, reprinted *Electron. Lett*, vol. 33(6), pp. 457–458, March 1997.

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

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

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

[6] D. J. C. MacKay and M. C. Davey, "Evaluation of Gallager codes for short block length and high rate applications," in *Codes, Systems and Graphical Models; volume 123 of IMA Volumes in Mathematics and its Applications;*, B. Marcus and J. Rosenthal, Eds. New York: Springer-Verlag, 2000, pp. 113–130.

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

[8] 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, no. 7, pp. 2711–2736, November 2001.

[9] S. J. Johnson and S. R. Weller, "Resolvable 2-designs for regular low-density parity-check codes," *IEEE Trans. Commun.*, 2003, in press.

[10] L. D. Rudolph, "A class of majority logic decodable codes," *IEEE Trans. Inform. Theory*, vol. IT-13, no. 2, pp. 305–307, April 1967.

[11] E. J. Weldon, "Difference-set cyclic codes," *Bell Sys. Tech. J.*, vol. 7, pp. 1045–1055, September 1966.

[12] S. R. Weller and S. J. Johnson, "Regular low-density parity-check codes from oval designs," *Eur. Trans. Telecommun.*, in press.

[13] B. Vasic, "High-rate low-density parity check codes based on anti-Pasch affine geometries," *Proc. IEEE Int. Conf. on Communications (ICC'2002)*, vol. 3, pp. 1332–1336, April 28 – May 2 2002.

[14] J. D. Key, "Some applications of Magma in designs and codes: Oval designs, Hermitian unitals and generalized Reed–Muller codes," *J. Symbolic Computation*, vol. 31, no. 1/2, pp. 37–53, January/February 2001.

[15] 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, p. 223.

[16] E. F. Assmus, Jr. and J. D. Key, *Designs and their Codes*, ser. Cambridge Tracts in Mathematics. Cambridge, U.K.: Cambridge University Press, 1993, vol. 103.

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

[18] W. Bosma, J. Cannon, and C. Playoust, "The Magma algebra system I: The user language," *J. Symbolic Computation*, vol. 24, no. 3/4, pp. 235–265, September 1997.

[19] A. J. Blanksby and C. J. Howland, "A 690-mW 1-Gb/s 1024-b, rate-$1/2$ low-density parity-check code decoder," *IEEE J. Solid-State Circuits*, vol. 37, no. 3, pp. 404–412, March 2002.

[20] R. M. Neal, ⟨www.cs.toronto.edu/radford/homepage.html⟩.