A Family of Irregular LDPC Codes With Low Encoding Complexity

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

***Abstract*—We consider in this letter irregular quasi-cyclic low-density parity-check (LDPC) codes derived from difference families. The resulting codes can be encoded with low complexity and perform well when iteratively decoded with the sum-product algorithm.**

***Index Terms*—Difference families, low-density parity-check codes, quasi-cyclic codes.**

I. Introduction

LOW-DENSITY parity-check (LDPC) codes were first presented by Gallager [4] in 1962 and have created much interest recently when rediscovered and shown to perform remarkably close to the Shannon limit. Decoding is with the sum-product algorithm with complexity linear in the code length [8]. Decoding with the sum-product algorithm requires only that the parity-check matrix, H, be sparse. However, decoding performance can often be improved if the code is also free of 4-cycles, which occur if two code bits are both checked by the same pair of parity-check equations. Gallager described regular codes, defined by parity-check matrices with constant column and row weights, which were constructed pseudo-randomly to avoid 4-cycles [4].

Recently, Luby *et al*. extended Gallager's results to consider *irregular* codes, that is, codes with nonconstant row and column weights in H, and showed that these codes are capable of outperforming regular codes [6].The irregular codes are constructed via a pseudo-random process which usually involves discarding codes which contain 4-cycles.

While optimized irregular codes are capable of excellent performance with reasonable decoding complexity, one of the main hurdles in the implementation of LDPC codes is the computational complexity of the *encoding* algorithm. Encoding is, in general, performed by matrix multiplication and so complexity is quadratic in the code length.

One option for efficient encoding is to use algebraic code constructions and exploit the subsequent code structure. In the case of regular codes a number of algebraic constructions have been presented, such as in [7], [5], [12]. Less consideration however has been given to structured irregular codes. The aim of this letter is to determine if the gains achieved by irregular random codes over the regular random codes translate into similar gains for quasi-cyclic irregular codes. To this end we consider irregular quasi-cyclic codes free of 4-cycles constructed using difference families. The design of codes using difference structures is not a new idea; see for example the self-orthogonal quasi-cyclic codes of [11], or the difference-set cyclic codes [13], which give the powerful cyclic regular LDPC codes of [7]. In this work we are interested in the design of quasi-cyclic codes with irregular degree distributions selected to improve their performance with sum-product decoding.

Manuscript received September 4, 2002. The associate editor coordinating the review of this letter and approving it for publication was Prof. K. Narayanan. This work was supported by a CSIRO Telecommunications and Industrial Physics postgraduate scholarship and by Bell Laboratories Australia, Lucent Technologies, with the Australian Research Council under Linkage Project Grant LP0211210.

The authors are with the School of Electrical Engineering and Computer Science, The University of Newcastle, Callaghan, NSW 2308, Australia (email: sarah@ee.newcastle.edu.au; steve@ee.newcastle.edu.au).

Digital Object Identifier 10.1109/LCOMM.2002.808375

II. Quasi-Cyclic Codes

A code is quasi-cyclic if, for any cyclic shift of a codeword by l places, the resulting word is also a codeword [10]. A cyclic code is a quasi-cyclic code with $l = 1$. We consider binary quasi-cyclic codes described by a parity-check matrix

$$H = [A_1, A_2, \ldots, A_l] \tag{1}$$

where $A_1, \ldots, A_l$ are binary $v \times v$ circulant matrices. Provided that one of the circulant matrices is invertible (say A_l) the generator matrix for the code can be constructed in systematic form

$$G = \begin{bmatrix} & & (A_l^{-1}A_1)^T \\ & I_{v(l-1)} & (A_l^{-1}A_2)^T \\ & & \\ & & (A_l^{-1}A_{l-1})^T \end{bmatrix} \tag{2}$$

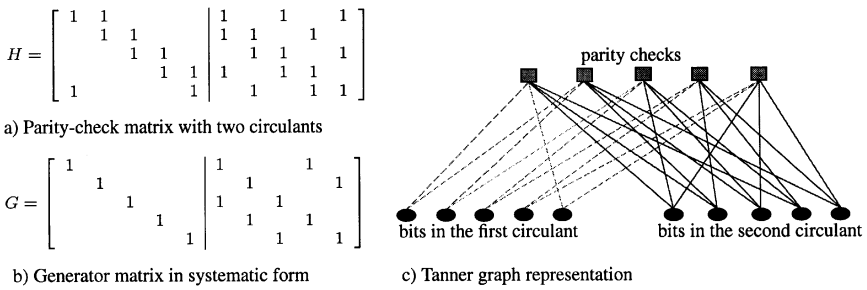
resulting in a quasi-cyclic code of length vl and dimension $v(l-1)$. Encoding can be achieved with linear complexity using a $v(l-1)$-stage shift register in much the same way as for cyclic codes [10].

The algebra of $(v \times v)$ binary circulant matrices is isomorphic to the algebra of polynomials modulo $x^v - 1$ over GF(2) [10]. A circulant matrix A is completely characterized by the polynomial $a(x) = a_0 + a_1 x + \cdots + a_{v-1}x^{v-1}$ with coefficients from its first row, and a code C with parity-check matrix of the form (1) is completely characterized by the polynomials $a_1(x), \ldots, a_l(x)$. Polynomial transpose is defined as

$$a(x)^T = \sum_{i=0}^{n-1} a_i x^{n-i}, \qquad x^n = 1.$$

For a binary $[n, k]$ code, length $n = vl$ and dimension $k = v(l-1)$, the k-bit message $[i_0, i_1, \ldots, i_{k-1}]$ is described by the polynomial $i(x) = i_0 + i_1 x + \cdots + i_{k-1}x^{k-1}$ and the codeword for this message is $c(x) = i(x), x^k p(x)$, where $p(x)$ is given by

$$p(x) = \sum_{j=1}^{l-1} i_j(x) * (a_l^{-1}(x) * a_j(x))^T \tag{3}$$



a) Parity-check matrix with two circulants

b) Generator matrix in systematic form

c) Tanner graph representation

Fig. 1. A rate-1/2 quasi-cyclic code from circulants, $a_1(x) = 1 + x$ and $a_2(x) = 1 + x^2 + x^4$.

$i_j(x)$ is the polynomial representation of the information bits $i_{v(j-1)}$ to i_{vj-1}

$$i_j(x) = i_{v(j-1)} + i_{v(j-1)+1}x + \cdots + i_{vj-1}x^{v-1}$$

and polynomial multiplication $(*)$ is mod $x^v - 1$.

As an example, consider a rate-1/2 quasi-cyclic code with $v = 5$, $l = 2$, first circulant described by $a_1(x) = 1 + x$, and second circulant described by $a_2(x) = 1 + x^2 + x^4$, which is invertible

$$a_2^{-1}(x) = x^2 + x^3 + x^4.$$

The generator matrix contains a 5×5 identity matrix and the 5×5 matrix described by the polynomial

$$(a_2^{-1}(x) * a_1(x))^T = (1 + x^2)^T = 1 + x^3.$$

Fig. 1 shows the parity-check matrix, generator matrix and Tanner graph of this code. For this example the code is not 4-cycle free. To construct a quasi-cyclic code for sum-product decoding we shall require that H is sparse and that the Tanner graph of the code is free of 4-cycles. In the following we present constructions for such codes using difference families.

III. Quasi-Cyclic Codes for Sum-Product Decoding

A difference family is an arrangement of a group of v elements, such as Z_v, into not necessarily disjoint subsets of equal size which meet certain difference requirements. More precisely:

Definition 1 [1]: The t γ-element subsets of the group Z_v, $D_1, \ldots, D_t$ with $D_i = \{d_{i,1}, d_{i,2}, \ldots, d_{i,\gamma}\}$ form a (v, γ, λ) *difference family* if the differences $d_{i,x} - d_{i,y}$, $(i = 1, \ldots t;\ x, y = 1, \ldots, \gamma, x \neq y)$ give each nonzero element of Z_v exactly λ times.

For example, the subsets $D_1 = \{1, 2, 5\}$, $D_2 = \{1, 3, 9\}$ of Z_{13} form a (13,3,1) difference family with differences

$$\begin{aligned} \text{From } D_1 &: 2-1=1,\ 1-2=12,\ 5-1=4, \\ &\quad 1-5=9,\ 5-2=3,\ 2-5=10 \\ \text{From } D_2 &: 3-1=2,\ 1-3=11,\ 9-1=8, \\ &\quad 1-9=5,\ 9-3=6,\ 3-9=7. \end{aligned}$$

In this work we are interested in difference families with $\lambda = 1$ which, as we will see in the following, allows the design of codes free of 4-cycles. The existence of $(v, 3, 1)$ difference families has long been established for all $v \equiv 1 \bmod 6$, v a prime power [1]. Recently, existence results for $(v, 4, 1)$ and $(v, 5, 1)$ difference families, $v \equiv 1 \bmod 12$ and $v \equiv 1 \bmod 20$, respectively, have been proven for all v a prime power [3]. In the following we describe the construction we propose for irregular quasi-cyclic codes using these difference families. For an irregular quasi-cyclic code we define the column weight distribution of a length vl rate $l-1/l$ code as the vector $W = [w_1, w_2, \ldots, w_l]$, where w_j is the column weight of the columns in the jth circulant. We denote by $w_{\max}$ the maximum column weight of H

$$w_{\max} = \max\{w_1, w_2, \ldots, w_l\}.$$

Construction 1: To construct a length vl rate $(l-1)/l$ irregular quasi-cyclic code, $H = [a_1(x), a_2(x), \ldots, a_l(x)]$, with weight distribution $W = [w_1, w_2, \ldots, w_l]$, take l sets $D_1, \ldots, D_l$ of a $(v, \gamma, 1)$ difference family with $\gamma \geq w_{\max}$, such that $a_j(x)$ is defined, using w_j of the elements of D_j, as

$$a_j(x) = x^{d_{j,1}} + x^{d_{j,2}} + \cdots + x^{d_{j,w_j}}.$$

To ensure invertibility at least one $a_j(x)$ must divide $x^v - 1$.

For a regular code all of the elements in each set are included in each circulant, while for an irregular code the choice of which elements in the set to use is arbitrary, and in fact a single set can be used to construct two circulants provided that different elements are chosen for each. The row weight, ρ, of the parity-check matrix is constant, and given by

$$\rho = \sum_{i=1}^{l} w_i. \tag{4}$$

To demonstrate that the quasi-cyclic codes are free of 4-cycles we need a well known result of difference families:

Lemma 1 [1]: A pair of elements from Z_v occur together exactly λ times in the set of translates of every set in a (v, γ, λ) difference family.

Lemma 2: The codes of Construction 1 have Tanner graphs free of 4-cycles.

Proof: Follows from the choice of $\lambda = 1$. First consider the regular case. Each column of $H = [a_1(x), a_2(x), \ldots, a_l(x)]$ is a translate of one of the sets D_j in the difference family. To show that there can be no 4-cycles in H we need to show that no two columns of H can have a nonzero entry in the same two rows, which is equivalent to requiring that two elements of Z_v can occur together in at most one of all the translates of the sets in the difference family. Since two elements occur together in exactly λ translates, we need only choose $\lambda = 1$ to avoid 4-cycles. The argument follows naturally to the irregular construction. By considering only w_j of the elements in a given set of

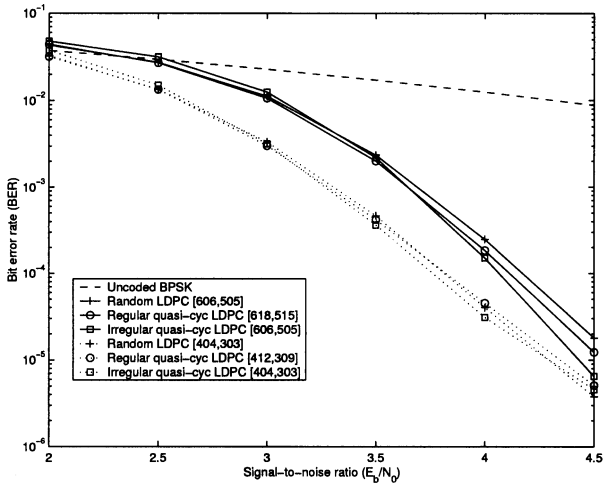


Fig. 2. Error correction performance of LDPC codes on an AWGN channel using sum-product decoding with max.iterations $= 50$. The rate-3/4, [404, 303] irregular quasi-cyclic code with $W = [5, 5, 3, 2]$, and the rate-5/6, [606, 505] irregular quasi-cyclic code with $W = [5, 5, 5, 3, 3, 2]$ are compared to randomly constructed codes with the same rate and length and to similar length regular quasi-cyclic codes.

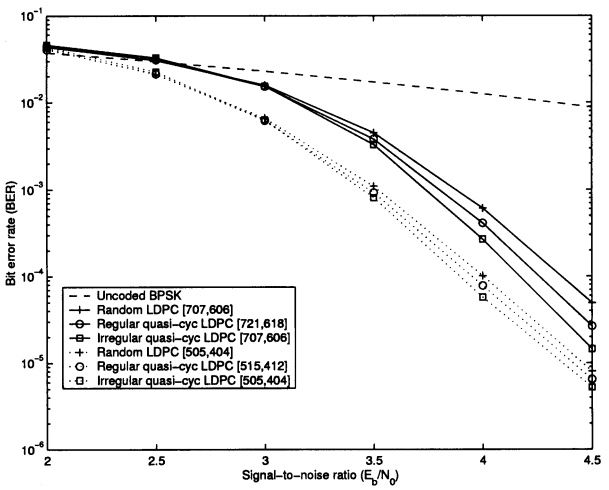


Fig. 3. Error correction performance of LDPC codes on an AWGN channel using sum-product decoding with max.iterations $= 50$. The rate-4/5, [505, 404] irregular quasi-cyclic code with $W = [5, 5, 3, 3, 2]$, and the rate-6/7, [707, 606] irregular quasi-cyclic code with $W = [5, 5, 5, 3, 3, 2, 2]$ are compared to randomly constructed codes with the same rate and length and to similar length regular quasi-cyclic codes.

the difference family we are in effect removing elements from the set of translates and 4-cycles cannot be added by removing entries from H. ■

IV. Simulation Results

Using the (101,5,1) difference family from [2],

$$D_1 = \{0, 14, 42, 47, 55\},\ D_2 = \{0, 95, 83, 52, 63\}$$
$$D_3 = \{0, 17, 51, 21, 74\},\ D_4 = \{0, 36, 7, 92, 26\}$$
$$D_5 = \{0, 100, 98, 76, 61\},$$

four quasi-cyclic irregular LDPC codes have been constructed:

- a rate-3/4, [404, 303] code with $a_1 = x^{D_2}$, $a_2 = x^{D_5}$, $a_3 = 1 + x^{51} + x^{74}$, $a_4 = x^{17} + x^{21}$;
- a rate-4/5, [505, 404] code with $a_1 = x^{D_1}$, $a_2 = x^{D_2}$, $a_3 = 1 + x^7 + x^{26}$, $a_4 = 1 + x^{98} + x^{61}$, $a_5 = x^{17} + x^{21}$;
- a rate-5/6, [606, 505] code with $a_1 = x^{D_2}$, $a_2 = x^{D_3}$, $a_3 = x^{D_4}$, $a_4 = 1 + x^{42} + x^{55}$, $a_5 = 1 + x^{98} + x^{61}$, $a_6 = x^{100} + x^{76}$;
- a rate-6/7, [707, 606] code with $a_1 = x^{D_1}$, $a_2 = x^{D_2}$, $a_3 = x^{D_3}$, $a_4 = 1 + x^7 + x^{26}$, $a_5 = 1 + x^{98} + x^{61}$, $a_6 = x^{100} + x^{76}$, $a_7 = x^{36} + x^{92}$;

where $x^{D_j} = x^{d_{j,1}} + \cdots + x^{d_{j,\gamma}}$.

These new codes are compared to randomly constructed codes [8], [9], and regular column weight three quasi-cyclic codes with similar parameters. The quasi-cyclic codes can be encoded with a shift register circuit of size equal to the code dimension while encoding of the random codes is via matrix multiplication. For example, encoding of the quasi-cyclic codes requires $(n - k)\alpha$ binary operations, α is one less than the row weight of G, while matrix multiplication requires $(n - k)(2k - 1)$ binary operations.

The decoding performance of the quasi-cyclic codes, shown in Figs. 2 and 3, demonstrates that there is a modest performance gain to be made over the regular quasi-cyclic codes by using irregular quasi-cyclic codes. Further, for reasonably short lengths and high rates, the quasi-cyclic LDPC codes show an improved decoding performance over the standard randomly constructed LDPC codes. Although it is not expected that the codes presented will outperform randomly constructed optimized irregular codes they have the advantage of a reduced encoding complexity.

References

[1] I. Anderson, "Combinatorial designs: Construction methods," in *Mathematics and its Applications*. Chichester, U.K.: Ellis Horwood, 1990.
[2] M. Buratti, "Constructions of (q, k, 1) difference familes with q a prime power and $k = 4, 5$," *Discrete Math.*, vol. 138, no. 1–3, pp. 169–175, 1995.
[3] K. Chen and L. Zhu, "Existence of (q, k, 1) difference families with q a prime power and $k = 4, 5$," *J. Comb. Designs*, vol. 7, no. 1, pp. 21–30, 1999.
[4] R. G. Gallager, *Low-Density Parity-Check Codes*. Cambridge, MA: MIT Press, 1963.
[5] S. J. Johnson and S. R. Weller, "Construction of low-density parity-check codes from Kirkman triple systems," *Proc. IEEE Globecom Conf.*, pp. 970–974, Nov. 2001.
[6] M. G. Luby, M. Mitzenmacher, M. A. Shokrollahi, and D. A. Spielman, "Efficient erasure correcting codes," *IEEE Trans. Inform. Theory*, vol. 47, pp. 569–584, Feb. 2001.
[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, pp. 931–937, June 2000.
[8] D. J. C. MacKay, "Good error-correcting codes based on very sparse matrices," *IEEE Trans. Inform. Theory*, vol. 45, pp. 399–431, Mar. 1999.
[9] R. M. Neal. (2002, June) Software for low density parity check (LDPC) codes. [Online]. Available: http://www.cs.toronto.edu/~radford/ldpc.software.html
[10] W. W. Peterson and E. J. Weldon, *Error-Correcting Codes*, 2nd ed. Cambridge, MA: MIT Press, 1972.
[11] R. L. Townsend and E. J. Weldon, "Self-orthogonal quasicyclic codes," *IEEE Trans. Inform. Theory*, vol. IT-13, pp. 183–195, Apr. 1967.
[12] B. Vasic, "Structured iteratively decodable codes based on Steiner systems and their application in magnetic recording," *Proc. IEEE Globecom Conf.*, pp. 2954–2960, Nov. 2001.
[13] E. J. Weldon, "Difference-set cyclic codes," *Bell Syst. Tech. J.*, vol. 7, pp. 1045–1055, Sept. 1966.