Combinatorial Interleavers for Systematic Regular Repeat-Accumulate Codes

Sarah J. Johnson *Member IEEE* & Steven R. Weller *Member IEEE*

Abstract— **This paper proposes novel interleaver and accumulator structures for systematic, regular repeat-accumulate (RA) codes. It is well known that such codes are amenable to iterative (sum-product) decoding on the Tanner graph of the code, yet are as readily encodable as turbo codes. In this paper, interleavers for RA codes are designed using combinatorial techniques, as a basis for deterministic interleaver constructions, yielding RA codes whose Tanner graphs are free of 4-cycles. Further, a generalized RA code accumulator structure is proposed, leading to codes, termed w3RA codes, whose parity-check matrices have many fewer weight-2 columns than conventional RA codes. The w3RA codes retain the low-complexity encoding of conventional RA codes and exhibit improved error-floor performance.**

Index Terms— **Repeat-accumulate (RA) codes, Iterative decoding, Sum-product algorithm, Interleaver design, Low-density parity-check (LDPC) codes.**

I. INTRODUCTION

The introduction of turbo codes by Berrou, Glavieux and Thitimajshima [1] marked a fundamental departure from traditional approaches to code design. Through the ingenious use of parallel concatenation of two simple constituent convolutional codes and a pseudo-random block interleaver, Berrou et al. devised codes with error correction performance approaching fundamental capacity limits, yet which are easily encoded, and iteratively decodable with manageable complexity.

A recent addition to the family of "turbo-like" codes, repeat-accumulate (RA) codes, were first presented as a simple class of serially concatenated turbo codes [2]. The constituent codes of an RA code, a rate-$\frac{1}{q}$ repetition code and a rate-1 $\frac{1}{1+D}$ convolutional code called the accumulator (in some cases concatenated with with a rate-a combiner) were chosen to enable theoretical analysis. However, it was soon realized that, although simple, RA codes are powerful codes in their own right [2], [3].

Significantly, systematic RA codes, in which both the K original message bits and the M encoded parity-check bits are explicitly transmitted, can also be considered as a class of low density parity-check [4] (LDPC) codes (see e.g. [5], [6]). These RA codes can be decoded by sum-product decoding on the code's Tanner graph in exactly the same way as for LDPC codes.

The power of this interpretation of RA codes is that they can be encoded by a repetition operation followed by a simple convolutional encoder, but decoded using sum-product decoding on the code's Tanner graph, thus gaining both the

low encoding complexity of turbo codes and the decoding advantages of LDPC codes. As with LDPC codes, convergence to a valid codeword is easily detected, and so it is possible to both halt decoding once a valid codeword has been found, and to distinguish between detected and undetected errors.

Sum-product decoding performance is determined by the properties of the code's Tanner graph. Thus the crucial issue is to design RA code interleavers which have Tanner graph representations with the desired properties, such as avoiding short cycles. Randomly chosen interleavers can produce effective results, and indeed, most RA research to date has considered the performance of RA codes using pseudo-randomly chosen interleavers (see e.g. [2], [3], [5]). However, randomly constructed interleavers can pose implementation challenges, and the performance of RA codes with a randomly chosen interleaver cannot be determined in advance.

In this paper we present combinatorial constructions for RA code interleavers which guarantee RA Tanner graphs free of small cycles. Firstly, we show in Lemma 3, that for every possible Steiner 2-design there exists a row and column permutation that maps the incidence matrix of the design into an RA code interleaver and accumulator, thus producing high rate RA codes having 4-cycle free Tanner graphs.

We then expand our examination to RA codes with a wide range of rates by presenting codes constructed using the notion of resolvability of designs. Using Construction 2 we present regular RA codes for any a and q which have 4-cycle free Tanner graphs. For the case $q = 3$, we use the similarity of structure of the RA accumulator matrix to block circulant permutation matrices to prove the existence of a deterministic construction of an infinite class of RA codes in Construction 3.

We begin in Section II by determining minimum distance bounds for RA codes and proposing a new class of RA codes in Section III. In Section IV we present interleaver constructions using structures from combinatorics, before considering their performance on the additive white Gaussian noise (AWGN) channel. Section V concludes the paper.

II. THE MINIMUM DISTANCE OF RA CODES

For (j, r)-regular, 4-cycle free, LDPC codes there are j parity-check equations orthogonal on each bit and so it is easy to show that the minimum distance, $d_{\min}$, is $\geq j + 1$ [7]. For RA codes, however, some codeword bits (namely, the parity bits) are checked by just two parity-check equations, and this lower bounds the minimum distance to just 3 using the same method. However, we will show that 4-cycle free RA codes can in fact have a minimum distance advantage over the same rate, length, density and girth LDPC codes.

Lemma 1: For 4-cycle free RA codes with repetition q, the minimum distance satisfies $d_{\min} \geq q + 1$.

The proof of Lemma 1 can be seen by considering the Tanner graph subgraph induced by each codeword. This subgraph is the set of bit vertices corresponding to the non-zero codeword bits, the check vertices to which they are connected, and the edges between them. As there must be one non-zero message bit included in any non-zero codeword, we can consider each RA codeword subgraph as being centered on a degree-q bit vertex. Since the Tanner graph has girth at least 6 this subgraph graph is locally a tree to a depth of at least 2. The minimum possible size for the subgraph is then found by using counting arguments under the constraint that each check vertex must be connected to an even number of the subgraph bit vertices for the subgraph to represent a valid codeword.

If we compare (j, r)-regular LDPC codes to RA codes with $q = j$, both with girth 6 and rate R, the RA and LDPC codes will have the same lower bound on minimum distance, viz. $d_{\min} \geq j+1$. However, if we consider RA codes with the same parity-check matrix density as the LDPC codes, that is RA codes with $q = \frac{1}{R}(j - 2 + 2R)$, the minimum distance bound is then greater for RA codes when $R \leq 1/2$. For example, 4-cycle free, rate-1/4, $(3, 4)$-regular LDPC codes with minimum distance $d_{\min} \geq 4$ have the same parity-check matrix size and density as 4-cycle free, rate-1/4, $q = 6$, $a = 2$, regular RA codes with minimum distance $d_{\min} \geq 7$.

For codes with girth μ (i.e. with the smallest cycle size μ) we can consider the subgraph induced by each codeword as a local tree to a depth of $\mu/2 - 1$. For codes with all bit nodes of degree q there are $2^{\frac{\mu}{4}} q$ bit nodes at each level of the tree with $\frac{\mu}{2}$ even. However, the remainder of the non-zero codeword bits could be made up entirely of parity bits. The parity nodes of degree-2 reduce the expansion of the graph so that there may be as few as q bit nodes added at each level of the tree. The minimum number of codeword nodes in the tree of girth μ in this case is then

$$\begin{cases} \frac{\mu-2}{4}q + 1, & \frac{\mu}{2} \text{ odd}, \\ \frac{\mu-4}{4}q + 2, & \frac{\mu}{2} \text{ even}. \end{cases}$$

Further, by taking into account the possibility that the single degree-1 node, corresponding to the final parity-check bit, is introduced at the first level in the tree we have the following lower bound for the minimum distance of girth μ RA codes:

$$d_{\min} \geq \begin{cases} \frac{\mu-2}{4}(q-1) + 2, & \frac{\mu}{2} \text{ odd}, \\ \frac{\mu-4}{4}(q-1) + 3, & \frac{\mu}{2} \text{ even}. \end{cases}$$

However, for (j, r)-regular LDPC codes with girth μ a lower bound on minimum distance is [8]:

$$d_{\min} \geq \begin{cases} 1 + j + j(j-1) + j(j-1)^2 + \cdots \\ \quad + j(j-1)^{\frac{\mu-6}{4}} & \frac{\mu}{2} \text{odd} \\ 1 + j + j(j-1) + j(j-1)^2 + \cdots \\ \quad + j(j-1)^{\frac{\mu-8}{4}} & \frac{\mu}{2} \text{even} \end{cases} \tag{1}$$

Thus, when codes with larger girth are considered the weight two columns of the accumulator have the effect of reducing the minimum distance bound for RA codes, when compared to LDPC codes with the same girth. We thus propose an alternative RA code accumulator which produces columns of weight 3.

III. RA CODES WITH WEIGHT-3 ACCUMULATORS

Since the accumulator corresponds to weight two columns in the parity-check matrix of an RA code, the fraction $(1 - R)$ of the columns of H for a rate R code must be weight two. This results in a large proportion of weight two columns, particularly for low rate codes. Compared to the equivalent length (j, r)-regular LDPC codes, which have all columns weight j and rows weight r, any RA code with $q = j$ has a parity-check matrix with row weight $r - (j - 2)$. This has the advantage of a lower decoding complexity for the RA codes, since the number of decoding operations is proportional to the number of entries in H, but also results in reduced decoding performance.

To achieve codes which maintain the low encoding complexity of RA codes and retain a $q = 3$ repetition code, but which also have degree distributions, and performances, closer to those of LDPC codes, we present a modified column weight-3 accumulator for RA codes.

For a weight-3 accumulator we propose a rate-1

$$\frac{1}{1 + D + D^{g+1}}$$

convolutional code as the second constituent code. Here g is a design parameter of the new codes, which we call w3RA codes. This new accumulator was first presented in the conference version of this paper [9], and also generalized independently by Liva et al. in [10]. For w3RA codes the output of the accumulator, p_i, at time i is now

$$p_i = p_{i-1} \oplus p_{i-g-1} \oplus r_i, \qquad \text{for } i = g + 2, \ldots, M, \tag{2}$$

and the traditional $p_i = p_{i-1} \oplus r_i$ when $i < g + 2$. Here r_i is the bit output by the combiner at time i.

A w3RA code can be viewed as an LDPC code where the code parity-check matrix H has two parts; $H = [H_1, H_2]$. Here H_1 is a $Kq/a \times K$, column weight q, row weight a, matrix specified by the interleaver and H_2 is a $Kq/a \times Kq/a$ matrix which describes (2). Thus, the i-th column of H_2 will be non-zero in the i-th, $(i + 1)$-th and $(i + 1 + g)$-th rows, when the $(i + 1)$-th and $(i + 1 + g)$-th rows exist.

Thus g specifies the number of rows between the second and third non-zero entries in the columns of the accumulator as well as the number of weight two columns remaining in H. For example, Fig. 1 shows a length-10 w3RA code with $q = 3$, $a = 2$, a weight three accumulator specified by $g = 2$ and the interleaver $\Pi = [1, 7, 4, 10, 2, 5, 8, 11, 3, 9, 6, 12]$. Reducing g reduces the number of weight 2 columns in H but introduces cycles of size $2(g + 1)$ solely within H_2.

By using a column weight three accumulator we keep the extremely low encoding complexity of RA codes while obtaining greater flexibility in the design of H. Indeed, these new w3RA codes can be thought of either as RA codes modified to have parity-check matrices much closer to those of regular LDPC codes, or as LDPC codes designed to have very low encoding complexity.
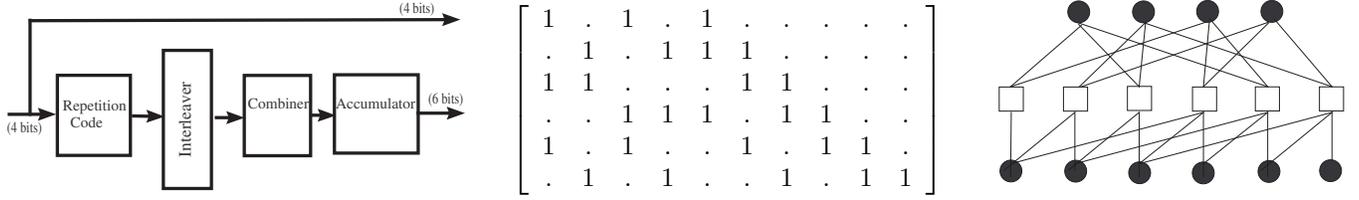
Fig. 1. The encoder, parity-check matrix and Tanner graph of a length-10 w3RA code with $q = 3$, $a = 2$, interleaver $\Pi = [1, 7, 4, 10, 2, 5, 8, 11, 3, 9, 6, 12]$, and the new accumulator with $g = 2$. In the Tanner graph filled circles represent bit nodes and unfilled squares represent check nodes.

IV. RA INTERLEAVERS FROM COMBINATORIAL DESIGNS

Short cycles in the Tanner graph of LDPC codes are known to adversely affect the decoding performance of the sum-product decoding algorithm [11]. For LDPC codes, combinatorial constructions have been successfully employed to construct a wide range of codes with excellent decoding performance, in part by guaranteeing Tanner graphs with a certain minimum cycle size [12], [13]. In this section we present combinatorial constructions for RA code interleavers which also guarantee RA Tanner graphs with no small cycles.

A (v, γ) Steiner 2-design is an arrangement of v *points* into $b = v(v-1)/\gamma(\gamma-1)$ subsets, called *blocks* such that [14]:

D1 there are exactly γ points in each block,
D2 there are exactly $\rho = (v-1)/(\gamma-1)$ blocks which contain each point, and
D3 every pair of points of the design appear in exactly one block together.

A Steiner 2-design can be described by a binary $v \times b$ incidence matrix $\mathcal{N}$, where each column in $\mathcal{N}$ represents a block B_j of the design and each row a point P_i:

$$\mathcal{N}_{i,j} = \begin{cases} 1 & \text{if } P_i \in B_j, \\ 0 & \text{otherwise.} \end{cases} \quad (3)$$

Lemma 2: Any row or column permutation of $\mathcal{N}$ is also the incidence matrix of a Steiner 2-design.

Proof: The properties of a Steiner 2-design (D1-D3) are independent of the ordering of points and blocks. ∎

By Property D3 we also have

$$\forall i \in \{1, \ldots, v-1\} \ \exists \ B_j \in \mathcal{N} \ : \ P_i, P_{i+1} \in B_j. \quad (4)$$

We denote by $B(i)$ the block containing both P_i and P_{i+1}. Then if

$$B(i) \neq B(j) \qquad \forall i, j \leq v-1, i \neq j, \quad (5)$$

the columns $B(1), \ldots, B(v-1)$ are distinct.

Lemma 3: For any $\mathcal{N}$ the incidence matrix of a Steiner 2-design with $\gamma \geq 3$, there exists a row permutation π so that (5) holds.

Proof: Take any column c of $\mathcal{N}$. There are

$$B_c = (v-2) \binom{\gamma}{3} 3!(v-3)! \quad (6)$$

permutations of the rows of $\mathcal{N}$ that will place three of the non-zero entries of column c into three consecutive rows. We call these the "bad" permutations for column c. There are $v(v-1)/\gamma(\gamma-1)$ columns in $\mathcal{N}$, so for any of the $v!$ row permutations to cause no bad columns, each permutation

which gives rise to a bad column must result in at least $\gamma - 2$ bad columns.

For each bad permutation, there are $3(\frac{v-1}{\gamma-1} - 1)$ columns in $\mathcal{N}$ which intersect column c at one of the three consecutive points, and the B_c permutations are bad for each of these columns a total of

$$B_I = 3! \binom{\gamma}{3} \left[3! \binom{\gamma-1}{3} (v-4)! + \frac{2}{3} \binom{\gamma-1}{2} 2!(v-4)! \right]$$

times. Further, the $b - 3(\frac{v-1}{\gamma-1} - 1) - 1$ remaining columns in $\mathcal{N}$, which do not intersect c at the three consecutive points, are each bad for a total of

$$B_N = 3! \binom{\gamma}{3} \left[2 \binom{v-4}{2} 3! \binom{\gamma}{3} (v-6)! \right] \quad (7)$$

of the B_c permutations. Thus the B_c permutations give rise to

$$B_T = B_c + 3 \left(\frac{v-1}{\gamma-1} - 1 \right) B_I + \left(b - 3\frac{v-1}{\gamma-1} + 2 \right) B_N$$

bad columns in total. Therefore the lemma is satisfied when

$$\frac{B_T}{B_c} = 1 + \frac{(\gamma-2)(v(v-8) - \gamma^2 + 8\gamma)}{(v-2)(v-3)} > \gamma - 2$$

which occurs provided

$$v > \frac{1}{2}(3\gamma - 1 + \sqrt{4\gamma^3 - 31\gamma^2 + 82\gamma - 71}). \quad (8)$$

Existence of a Steiner 2-design requires $v \geq \gamma^2 - \gamma + 1$. For $\gamma \geq 3$, equation (8) is satisfied for all such v and the proof follows. ∎

By Lemma 2, (4) holds for any permutation of the rows of $\mathcal{N}$, and by Lemma 3 we can always find a permutation of the rows of $\mathcal{N}$ such that (5) holds. Thus we have proven that, despite the constraints of the RA accumulator, a permutation always exists which maps the incidence matrix of a Steiner 2-design into the parity-check matrix of an RA code, using columns $B(1), \ldots, B(v-1)$ to form H_2 by removing the entries from $B(i)$ not in rows i or $i+1$. What is more, this code will always be 4-cycle free due to the properties of the original design.

Starting with the Skolem family of triple systems (see e.g. [15, Section 8.2]), we define a deterministic construction for such RA codes when $q = 3$:

Construction 1: Construct an RA code with $M = 6m+3$, $N = (6M+3)(6M+2)/6$ and $q = 3$ for any integer $m \geq 2$ as follows:

1 Arrange the numbers $1, 2, \ldots, 6m+2$ in three rows as

the array:

$$\begin{array}{cccccc} 0 & 1 & 2 & \ldots & 2m-1 & 2m \\ 2m+1 & 2m+2 & 2m+3 & \ldots & 4m & 4m+1 \\ 4m+2 & 4m+3 & 4m+4 & \ldots & 6m+1 & 6m+2 \end{array}$$

The i-th block of the design, for $i = 1, \ldots, 2m+1$, is given by the columns of this array i.e.

$$B_i = \{i, i+2m+1, i+4m+2\}.$$

2a For each pair $\{a,b\}$ in the first row find the entry c in the second row such that

$$2c \equiv a + b (\bmod\ 2m+1). \tag{9}$$

The triples $\{a,b,c\}$ in the order $j = 0, \ldots, 2m-1$, $k = j+1, \ldots, 2m$, $\{a,b\} = \{j,k\}$, give the next $\binom{2m+1}{2}$ blocks.

2b Repeat 2a) for each pair $\{a,b\}$ in the second row of the array, finding the entry c in the third row which satisfies (9). The triples $\{a,b,c\}$ taken in the order $j = 2m+1, \ldots, 4m$, $k = j+1, \ldots, 4m+1$, $\{a,b\} = \{j,k\}$, give the next $\binom{2m+1}{2}$ blocks.

2c Repeat 2a) for each pair $\{a,b\}$ in the third row of the array, finding the entry c in the first row which satisfies (9). The triples $\{a,b,c\}$ in the order $j = 4m+2, \ldots, 6m+1$, $k = j+1, \ldots, 6m+2$, $\{a,b\} = \{j,k\}$, give the final $\binom{2m+1}{2}$ blocks.

3 Set $u = v/3$ then define $\zeta_1 = u+1$, $\zeta_u = 3u-3$, $\zeta_{u+1} = (m+1)u+1$, $\zeta_{2u} = (m+3)u-3$, $\zeta_{2u+1} = (2m+1)u+1$, and $\zeta_{3u} = \frac{u}{2}(3u-1)-1$. Then, for $j = 0, \ldots, 2$, $k = 1, \ldots, u-2$,

$$\zeta_{ju+k+1} = \zeta_{ju+k} + u - k. \tag{10}$$

4 Construct the design incidence matrix $\mathcal{N}$ as per (3). The columns $\zeta_1, \ldots, \zeta_i, \ldots, \zeta_v$ of $\mathcal{N}$ form H_2 and the remaining columns of $\mathcal{N}$ are kept in their existing order to form H_1. Finally, for $i = 1, \ldots, v$, replace the '1' entry of the i-th column of H_2 which is not in the i-th and $(i+1)$-th rows with '0'. $\square$

Step 1 of Construction 1 mirrors the construction method defined for Skolem triple systems. The modifications required to construct an RA code are the constraint on the ordering of the blocks in Step 2, and the definition of the required column permutation in (10).

Steiner 2-designs produce very high rate codes, since the original incidence matrices contain the maximum number of columns possible without adding 4-cycles. Thus codes from these constructions are likely to be useful in applications such as magnetic recording or long haul optical transmission. To produce codes with lower rates, for applications such as wireless communications, we propose in the following section a construction modification employing resolvable designs.

A. RA interleavers from resolvable designs

A design is *resolvable* if the blocks of the design can be arranged into r groups, called *resolution classes*, such that the v/γ blocks of each resolution class are disjoint, and each class contains every point precisely once [14]. If the columns of the incidence matrix of a resolvable design are arranged into its

resolution classes, each set of v/γ columns in $\mathcal{N}$ will contain a '1' entry in every row. Constructions for resolvable Steiner 2-designs on v points exist for all $v \equiv 3 \pmod 6$ for $\gamma = 3$ and $v \equiv 4 \pmod{12}$ for $\gamma = 4$ [14]. For larger γ, existence results are incomplete, although constructions exist for many v (see e.g. [14], [15]).

To construct RA and w3RA codes from resolvable designs, we use only a subset of the resolution classes of the design to construct H. RA and w3RA codes with parameters a and q are constructed using $a + 3 \leq (v-1)/(q-1)$ of the resolution classes of a (v,q) Steiner 2-design with three of these classes used to construct the accumulator. Since the columns of $\mathcal{N}$ need to be maintained in their resolution classes, we cannot permute $\mathcal{N}$ to construct H_1 in the same way as in Lemma 3. Instead, a pseudo-random construction is proposed; minimizing the number of column permutations which occur outside of the three resolution classes designated for H_2.

Construction 2: Construct a length N, rate $R = a/(a+3)$, w3RA code with gap g (or RA code by setting $g = M-1$) with repetition $q = 3$ using the incidence matrix $\mathcal{N}$ of a resolvable $(v = (1-R)N, 3)$ Steiner 2-design as follows:

For $i = 1, \ldots, v-1$,

1 Find the minimum $l \geq i$ such that the l-th column of $\mathcal{N}$ contains a '1' in row i. If $l \leq v$ and $i \leq g$, and there exists a '1' in the j-th row of column l such that either $j \geq i+1+g$, or $i+1 \leq j \leq g+1$, swap the l-th and i-th columns of $\mathcal{N}$ and swap the j-th and $(i+1)$-th rows of $\mathcal{N}$. Otherwise, find the column $B(i)$ in $\mathcal{N}$ and swap this column with the i-th column of A. In the second case the resolution class which contained $B(i)$ must now be excluded from use in H_1 as it is no longer regular.

2 If the third non-zero entry of column i is in row $i+3$, randomly swap this row with some other row r satisfying $r > i+3$. If either $g+2 \leq i+3 \leq i+g+1$ or $g+2 \leq r \leq i+g+1$, the accumulator entries that have been moved by this permutation must now be manually replaced and the columns which also contain the newly created pairs must be excluded from use in H_1.

3 If $i \geq v - g$, replace the third non-zero entry in column i with '0'. Otherwise, for $i < v - g$: if the third entry of the new i-th column is in row $j \geq i+g$, switch the j-th and $(i+g+1)$-th rows of $\mathcal{N}$, otherwise place a zero in entry $\mathcal{N}(j,i)$ and a one in entry $\mathcal{N}(i+g+1,i)$. In the latter case, the two columns with the pairs $\{i, i+g+1\}$ and $\{i+1, i+g+1\}$, respectively, must now be excluded from H_1 in order to avoid 4-cycles.

4 The first v columns of $\mathcal{N}$ now give H_2. Take the columns from a of the unused resolution classes in $\mathcal{N}$ to make up the columns of H_1. $\square$

In Construction 2 an attempt is made to use only the first three resolution classes of the design, corresponding to the first v columns of $\mathcal{N}$, to construct the accumulator. Where this is not possible, columns from resolution classes outside of the first three are then used. In this case the resolution class from which the additional column is taken is thus incomplete and cannot be used to construct a regular H_1. In practice, however, very few columns outside of the first v are needed to form H_2, and so it is possible to construct completely regular RA and

w3RA codes for most values of a. Again, because we start with $\mathcal{N}$ the incidence matrix of a Steiner 2-design, we have codes with Tanner graphs free of 4-cycles.

Construction 2 is not deterministic. However, by using the deterministic nature of the design, deterministic constructions for some RA codes can be given by starting with the Ray-Chaudhuri and Wilson construction for resolvable $\gamma = 3$ designs [16] as follows.

Firstly, we consider a traditional $M \times M$ accumulator matrix, H_2, with the addition of a single '1' entry in the last position of the first row. Applying the permutation

$$\Pi = [1, 4, 7, 10, \ldots, \frac{M}{3} - 2, 2, 5, 8, \ldots, \frac{M}{3} - 1, 3, 6, 9, \ldots, \frac{M}{3} - 1] \quad (11)$$

to both the rows and columns of H_2, gives the matrix

$$\widehat{H_2} = \begin{bmatrix} I^0 & 0 & I^1 \\ I^0 & I^0 & 0 \\ 0 & I^0 & I^0 \end{bmatrix},$$

where I^i is a cyclic shift by i places of the $M/3 \times M/3$ identity matrix and 0 is the $M/3 \times M/3$ all zeros matrix.

Given any circulant permutation matrix

$$C = \begin{bmatrix} I^a & 0 & I^f \\ I^b & I^c & 0 \\ 0 & I^d & I^e \end{bmatrix},$$

row and column permutations exist to permute C into the form $\widehat{H_2}$, and hence H_2, when

$$f - (e - d) - (c - b) \pmod{M/3} \equiv a + 1 \pmod{M/3}. \quad (12)$$

The condition in (12), together with the relationship between C and H_2, is used to construct RA codes in Construction 3.

Construction 3: Let $\varphi = 6m + 1$ be a prime power, m any integer. Then construct an RA code with $q = 3$, $M = 3\varphi$, $N = (a + 3)\varphi$ and $R = \frac{a}{a+3}$, for any $a = 1, \ldots, (M-1)/3$ as follows:

1   Let $\varphi = 6m + 1$ be a prime power, m an integer and take θ a primitive element of $GF(\varphi)$, where $GF(\varphi)$ is the Galois field of order φ, so that $\theta^{6m} = 1$, $\theta^{3m} = -1$, and $\theta^{2m} + 1 = \theta^m$. Consider the point set $\mathcal{P} = GF(\varphi) \times Z_3$. Then $\mathcal{P}$ consists of 3φ elements, these being 3 copies of each element of $GF(\varphi)$. An element $(a, i) \in \mathcal{P}$ represents the i-th copy of the element a in $GF(\varphi)$.
Construct the blocks:

$$\begin{array}{llll} A & = & \{0_1, 0_2, 0_3\}, & \\ B_{i,j} & = & \{\theta_j^i, \theta_j^{i+2m}, \theta_j^{i+4m}\}, & 1 \le i \le m, \\ C_{i,j} & = & \{\theta_j^{i+m}, \theta_{j+1}^{i+3m}, \theta_{j+2}^{i+5m}\}, & 1 \le i \le m, \\ D_{i,j} & = & \{\theta_j^i, \theta_{j+1}^{i+2m}, \theta_{j+2}^{i+4m}\}, & 1 \le i \le m, \end{array}$$

for $1 \le j \le 3 \pmod 3$, where $\theta_j^i = (\theta^i, j) \in \mathcal{P}$.

2a From the set of m blocks $\mathcal{D} = \bigcup D_{i,1}$ for $i = 1, \ldots, m$, choose the block $D_{i',1}$ which contains the two elements (θ^{x_1}, y_1) and (θ^{x_2}, y_2) such that θ^{x_2} plus $2m$ copies of the additive identity of $GF(\varphi)$ gives θ^{x_1}. Such a block must exist since each block $D_{i,1}$ contains 6 differences, none of which can repeat due to the properties of the design, giving all $6m$ elements in $GF(\varphi)$ (other than the additive identity) in the differences from the blocks in $\mathcal{D}$.

The three blocks $D_{i',1}, D_{i',2}, D_{i',3}$ each contain one copy of each θ^{x_1}, θ^{x_2} and a third element θ^{x_3}. Order the blocks $D_{i',1}, D_{i',2}, D_{i',3}$ so that the block containing $(\theta^{x_1}, 1)$, is designated d_1. If d_1 contains $(\theta^{x_2}, 2)$ define as d_2 the block containing $(\theta^{x_1}, 2)$ and define $\varpi_1 = 2$, $\varpi_2 = 3$, otherwise, d_1 contains $(\theta^{x_2}, 3)$, and the block holding $(\theta^{x_1}, 3)$ is now designated d_2 with $\varpi_1 = 3$, $\varpi_2 = 2$. The remaining block is then designated d_3. Each block d_1, d_2, and d_3, with its translates, make up one of the three resolution classes that will be used to construct the accumulator. (The φ translates of a block d are the blocks

$$d + g := \{(e \circ g, i) : (e, i) \in d\}$$

for all $g \in GF(\varphi)$, where $\circ$ is the additive operator defined for $GF(\varphi)$).

2b Construct the 3φ blocks in the order, d_1 and its translates, d_2 and its translates, and d_3 and its translates, where the translates are taken in the order $g = \{0, 1, 1 \circ 1, 1 \circ 1 \circ 1, \ldots\}$, where 0 is the additive identity and 1 is the multiplicative identity of $GF(\varphi)$. Then, taking the 3φ points in the order

$$\begin{aligned} \{&(0, 1), (1, 1), (1 \circ 1, 1), (1 \circ 1 \circ 1, 1), \ldots, \\ &(0, \varpi_1), (1, \varpi_1), (1 \circ 1, \varpi_1), (1 \circ 1 \circ 1, \varpi_1), \ldots, \\ &(0, \varpi_2), (1, \varpi_2), (1 \circ 1, \varpi_2), (1 \circ 1 \circ 1, \varpi_2)\}, \quad (13) \end{aligned}$$

the incidence matrix of these blocks gives H_2.

3a Each of the remaining $3m - 3$ blocks in D, other than d_1, d_2 and d_3, gives, with its set of translates, a resolution class. These classes provide the first $\varphi(3m - 3)$ blocks which can be used to construct H_1.

3b The blocks in A, B and C together make up the blocks of one resolution class. Each translate of this set of blocks gives a further resolution class. These φ^2 blocks make up the remaining φ resolution classes which can be used to construct H_1.

3c Select any a of these $9m - 2$ resolution classes and form H_1 by constructing the incidence matrix of the selected blocks, using the same point set ordering as for H_2.

4 Each block in D contains one element from each copy of $GF(\varphi)$ and thus the incidence matrix of the translates of these blocks produce a column of three $\varphi \times \varphi$ circulant permutation matrices. By Step 2, the three columns of circulant matrices corresponding to d_1, d_2, and d_3:

$$H_2 = \begin{bmatrix} I^a & I^d & I^g \\ I^b & I^e & I^h \\ I^c & I^f & I^i \end{bmatrix}$$

have $a = e = i$, $b = f = g$, and $a - b = 2m$. Thus

$$\begin{aligned} & g - (i - f) - (e - b) \pmod{6m + 1} \\ = \; & a - 2m - (2m) - (2m) \pmod{6m + 1} \\ = \; & a + 1 \pmod{6m + 1}. \end{aligned}$$

So for this circulant permutation submatrix, (12) is satisfied and $H = [H_1, H_2]$ can be transformed into the form required by replacing the circulants I^c, I^d, I^h with the $\varphi \times \varphi$ all zero matrix, replacing the '1' entry in
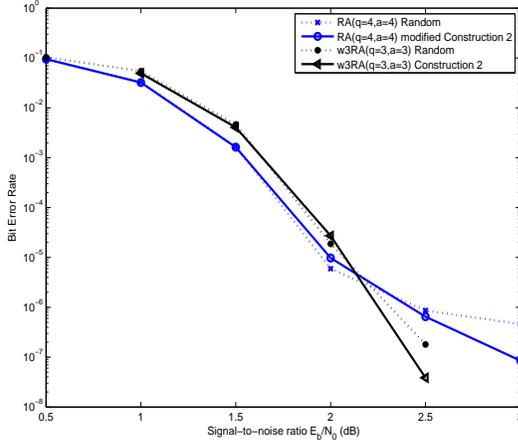
Fig. 2. The error correction performance on an AWGN channel of rate-1/2 length-2022 RA and w3RA codes, using sum-product decoding with a maximum of 1000 decoder iterations.
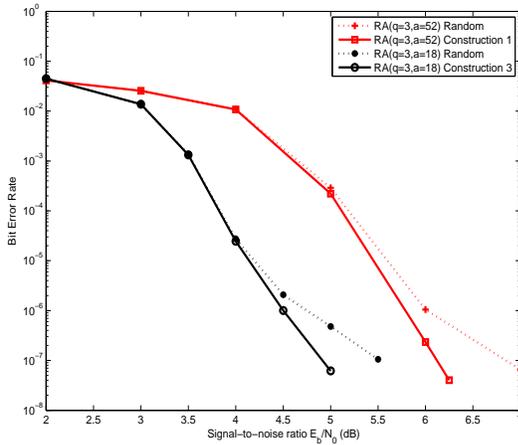

Fig. 3. The error correction performance on an AWGN channel of length-2035, rate-0.945 ($a = 52$), and length-2037, rate-0.857 ($a = 18$), RA codes using sum-product decoding with a maximum of 1000 decoder iterations.

the last column of I^g with '0', and applying the inverse permutation of (11) to the rows of H and the columns of H_2. □

Step 1 of Construction 3 is the Ray-Chaudhuri and Wilson construction for resolvable $\gamma = 3$ designs. (The design construction is completed by forming the translates of the blocks in A, B, C and D.) Steps 2 to 4 in Construction 3 are new, and are required to transform the blocks of the design into the incidence matrix of an RA code.

We demonstrate in Figs. 2-3 the performance of the new RA and w3RA codes compared to pseudo-randomly constructed codes. The RA codes with combinatorial interleavers are capable of outperforming RA codes with randomly constructed interleavers, particularly for higher rate codes where the combinatorial interleavers give a significant error floor advantage.

We are aware of one other structured construction for regular RA codes in the π-rotation LDPC code from [6], noting that the π-rotation LDPC codes are actually RA codes with $q = 4$. Our rate-1/2 construction for RA codes with $q = 4$ performs equivalently to the π-rotation code with length-2000 in [6]. More importantly, our combinatorial w3RA codes perform as well as combinatorial LDPC codes with the

same length, rate and density (i.e. column weight 3 LDPC codes). Thus we have achieved repeat-accumulate codes with equivalent performances to LDPC codes while maintaining the advantage of a simple encoding circuit.

V. CONCLUSION

In this paper we have considered the design and implementation of repeat-accumulate codes. Firstly, we proposed a new accumulator design to improve the error floor performance of RA codes. These w3RA codes generalize repeat-accumulate codes, thereby giving rise to RA codes with parity-check matrices closer to those of LDPC codes. We then showed in Lemma 3 that for every possible Steiner 2-design there exists a row and column permutation mapping the incidence matrix of the design into an RA code interleaver and accumulator, thus producing RA codes with Tanner graphs of girth 6. Lastly, we expanded our examination to codes constructed using the notion of design resolvability, to present regular RA and w3RA codes which have Tanner graphs free of 4-cycles.

REFERENCES

[1] C. Berrou, A. Glavieux, and P. Thitimajshima, "Near Shannon limit error-correcting coding and decoding: Turbo-codes," in *Proc. IEEE Int. Conf. on Communications (ICC'93)*, Geneva, Switzerland, May 1993, pp. 1064–1070.

[2] D. Divsalar, H. Jin, and R. J. McEliece, "Coding theorems for "turbo-like" codes," in *Proc. 36th Allerton Conf. on Communications, Control, and Computing*, Allerton, Illinois, September 1998, pp. 201–210.

[3] A. Roumy, S. Guemghar, G. Caire, and S. Verdú, "Design methods for irregular repeat-accumulate codes," *IEEE Trans. Inform. Theory*, vol. 50, no. 8, pp. 1711–1727, August 2004.

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

[5] M. Yang, W. E. Ryan, and Y. Li, "Design of efficiently encodable moderate-length high-rate irregular LDPC codes," *IEEE Trans. Comms.*, vol. 52, no. 4, pp. 564–571, April 2004.

[6] R. Echard and S.-C. Chang, "The π-rotation low-density parity-check codes," in *Global Telecommunications Conference, San Antonio, TX, 2001*, November 2001, pp. 980–984.

[7] J. L. Massey, *Threshold Decoding*. Cambridge, Massachusetts: M.I.T. Press, 1963.

[8] A. Orlitsky, R. L. Urbanke, K. Viswanathan, and J. Zhang, "Stopping sets and the girth of Tanner graphs," in *Proc. International Symposium on Information Theory (ISIT'2002)*, Lausanne, Switzerland, June 30–July 5 2002, p. 2.

[9] S. J. Johnson and S. R. Weller, "Interleaver and accumulator design for systematic repeat-accumulate codes," in *Proc. 6th Australian Communications Theory Workshop (AusCTW'05)*, Brisbane, Australia, 2-4 February 2005.

[10] G. Liva, E. Paolini, and M. Chiani, "Simple reconfigurable low-density parity-check codes," *IEEE Commun. Letters*, vol. 9, no. 3, pp. 258–260, March 2005.

[11] 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.

[12] 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.

[13] S. J. Johnson and S. R. Weller, "Resolvable 2-designs for regular low-density parity-check codes," *IEEE Trans. Commun.*, vol. 51, no. 9, pp. 1413–1419, September 2003.

[14] C. J. Colbourn and J. Dinitz (Eds.), *The CRC Handbook of Combinatorial Designs*. Boca Raton: CRC Press, 1996.

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

[16] D. K. Ray-Chaudhuri and R. M. Wilson, "Solution of Kirkmans schoolgirl problem," *Proc. Symp. Math.*, vol. 19, pp. 187–203, 1971.