Explicit Interleavers for a Repeat Accumulate Accumulate (RAA) code construction

Venkatesan Guruswami
Computer Science and Engineering
University of Washington
Seattle, WA 98195, USA
Email: venkat@cs.washington.edu

Widad Machmouchi
Computer Science and Engineering
University of Washington
Seattle, WA 98195, USA
Email: widad@cs.washington.edu

***Abstract*— Repeat Accumulate Accumulate (RAA) codes are turbo-like codes where the message is first repeated $k \geq 2$ times, passed through a first permutation (called interleaver), then an accumulator, then a second permutation, and finally a second accumulator. Bazzi, Mahdian, and Spielman (2003) prove that RAA codes are asymptotically good with high probability when the two permutations are chosen at random. RAA codes admit linear-time encoding algorithms, and are perhaps the simplest known family of linear-time encodable asymptotically good codes. An explicit construction of an asymptotically good RAA code is thus a very interesting goal. We focus on the case when $k = 2$ and we consider a variation of RAA codes where the inner repeat accumulate code is systematic. We give an explicit construction of the first permutation for which we show that the resulting code is asymptotically good with high probability when the second permutation is chosen at random. The explicit construction uses a cubic Hamiltonian graph with logarithmic girth.**

I. Introduction

Repeat Accumulate (RA) codes [DJM98] are turbo-like codes with the following encoding: the message is repeated k times, where k is called the *repetition factor* of the code, then the repeated message is passed through a first permutation π_1 and fed to an accumulator. An accumulator takes a binary string $a_1, a_2, \ldots, a_m$ and outputs the binary string $b_1, b_2, \ldots, b_m$ where $b_i = \bigoplus_{j=1}^{i} a_j$. In [BMS03], Bazzi, Mahdian and Spielman show that such a code is asymptotically bad, i.e. the minimum distance doesn't grow linearly with the bock length. Repeat Accumulate Accumulate (RAA) are extensions of RA codes studied, for example, in [BDMP98], [DJM98], [PS99], [BMS03]. To get RAA codes, the output bits from the RA code are passed through a second permutation π_2 and then fed to a second accumulator.

Definition 1: [BMS03] Let $k \geq 2$ and $n > 0$ be two integers and let $m = kn$. Let $r_k : \{0,1\}^n \to \{0,1\}^{kn}$ be the encoder of the repetition code with repetition factor k and let $A : \{0,1\}^m \to \{0,1\}^m$ be the encoder of the accumulator (code) given by: $A(a) = (\bigoplus_{j=1}^{i} a_j)_{i=1}^{m}$ where $a = a_1 a_2 \ldots a_m \in \{0,1\}^m$. Then the RAA code with repetition factor k and permutations π_1 and π_2 is the code whose encoder is

$$\begin{aligned} C_{k,\pi_1,\pi_2} : \{0,1\}^n &\to \{0,1\}^m \\ x &\mapsto A(\pi_2(A(\pi_1(r_k(x))))) \end{aligned}$$

In [BMS03], the authors prove that when π_1 and π_2 are chosen uniformly at random, C_{k,π_1,π_2} has, with high probability, a minimum distance linear in the block length.

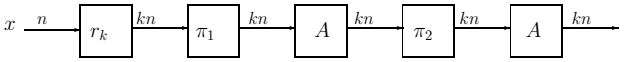

Fig. 1. Encoding scheme of C_{k,π_1,π_2}

Theorem 1 ([BMS03]): Let $k \geq 2$ and n be integers, and let π_1 and π_2 be two permutations of length kn chosen uniformly at random. Then for each constant $\delta > 0$, there exists a constant $\varepsilon > 0$, such that the RAA code encoded by C_{k,π_1,π_2} has minimum distance at least εn with probability at least $1-\delta$ for large enough n.

Extensions of RAA codes are studied also in [CKZ07] where the authors prove that the gap to Gilbert-Varshamov bound can be made arbitrarily small by serially concatenating RAA codes with multiple accumulators and random permutations.
In this paper, we will consider a different version of these RAA codes. We use the inner-systematic RAA code, C^s_{k,π_1,π_2}, given by the following map:

$$\begin{aligned} C^s_{k,\pi_1,\pi_2} : \{0,1\}^n &\to \{0,1\}^{(k+1)n} \\ x &\mapsto A(\pi_2(x, A(\pi_1(r_k(x))))) \end{aligned}$$

Note that, although the repetition factor is still k, the block length and the length of π_2 are $(k+1)n$. We use systematic RA codes for technical convenience.

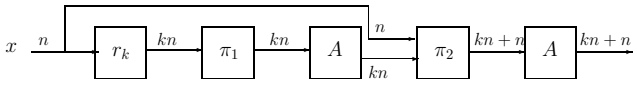

Fig. 2. Encoding scheme of C^s_{k,π_1,π_2}

A. Problem motivation and context

RA codes have the advantage of a simple structure and extremely simple linear time encoding algorithm. However, it is known that their structure is too simple to yield asymptotically good codes. Indeed, a direct application of Theorem 2 in [BMS03] on RA codes (the convolutional encoder described in the theorem is now an accumulator) with repetition factor k and message length n gives a minimum distance $d =$

$O(n^{1-2/k}\log n)$, which is not linear in the block length kn. Namely, for $k=2$, the distance is bounded by $d=O(\log n)$. One of the motivations behind studying RAA codes was to determine whether, unlike RA codes, they could include asymptotically good codes, i.e., whether their minimum distance could grow linearly with the block length for a suitable choice of the interleavers. By Theorem 1, RAA codes can be asymptotically good, which raise the following interesting question problem that was the motivation for our work:

> Can one find two **explicit** permutations π_1 and π_2 such that the resulting code C_{k,π_1,π_2} has a minimum distance linear in the block length?

Finding such permutations would give us an explicit asymptotically good code with linear time encoding. So far, the construction of Spielman [Spi96] (based on a cascade of expander graphs) is the only known explicit construction of linear-time encodable codes that are asymptotically good. Our hope is to investigate if RAA codes, which have admit linear time encoding by design, can be made explicit, while also being asymptotically good.

B. Summary of results

We focus on the case $k=2$. We construct an explicit permutation π_1 for which we show that a random permutation π_2 gives, with high probability, a linear minimum distance for the inner-systematic RAA code C^s_{2,π_1,π_2}. We divide the result into two main parts. In the first part, we derive properties of a binary linear code C such that the code C' that maps $x\in\{0,1\}^n$ to $A(\pi_2(C(x)))$ has, with high probability, a good minimum distance. Specifically, we prove:

Lemma 1: Let n be a positive integer and $c>1$, d and l be positive constants. Let π_2 be a permutation chosen uniformly at random and A the encoder of the accumulator code. Let C be a binary linear code with message length n and block length cn. Let C' be the code with the following encoder: $C':\{0,1\}^n\rightarrow\{0,1\}^{cn}, x\mapsto A(\pi_2(C(x)))$.
If C satisfies the following properties:

1) minimum distance property: C has minimum distance at least $\log dn$
2) exponential weight distribution property: The number of codewords in C of weight w is at most l^w

Then, for every constant $\delta>0$, there exists a constant $\varepsilon>0$ dependent only on δ, c, d and l, such that for all large enough n, the code C' has minimum distance at least εn with probability $1-\delta$, where the probability is taken over the uniform random choice of π_2.

The next result gives an explicit construction of a code C satisfying both properties. We use an RA code with repetition factor 2, where the permutation π_1 is constructed from a cubic Hamiltonian graph with logarithmic girth g. Proving that such systematic RA codes satisfy the conditions relies on the fact that $k=2$. We set C to be the systematic version of C_{2,π_1}, where we append the original message to the output of the code. We prove that the number of codewords of weight w is at most exponential in w. Moreover, using techniques from [BMS03] and [FK04], we prove that the minimum distance of the systematic version is g. In particular, we show that:

Lemma 2: let n be a positive integer and let C_{2,π_1} be an RA code with permutation π_1. Let C be the block length-$3n$ code whose encoder maps $x\in\{0,1\}^n$ to $(C_{2,\pi_1}(x),x)$. Then, for infinitely many values of n, there exist an explicit construction of π_1 from a cubic Hamiltonian graph with logarithmic girth such that:

1) C has minimum distance at least $\log 2n$
2) The number of codewords in C of weight w is at most 16^w

Combining the two lemmas above and setting c to 3, d to 2 and l to 16 in Lemma 1, we get the main theorem of this work:

Theorem 2: Let n be a positive integer and π_2 a permutation on $3n$ elements chosen uniformly at random. Let C^s_{2,π_1,π_2} be the inner-systematic RAA code with $k=2$, first permutation π_1 constructed from a cubic Hamiltonian graph with logarithmic girth, as explained in Section III, and second permutation π_2 . Then for every constant $\delta>0$, there exists a constant $\varepsilon>0$, such that, for infinitely many n, C^s_{2,π_1,π_2} has minimum distance at least εn with probability $1-\delta$, where the probability is taken over the random choice of π_2.

C. Organization of rest of the paper

In Section II, we prove Lemma 1 using the probabilistic method and properties of the accumulator code. In Section III, we give an explicit description of the code C by constructing the permutation π_1 of the RA code from a cubic Hamiltonian graph with logarithmic girth.

II. Serially concatenating a weak code with an accumulator

In this section, we prove Lemma 1. We assume the existence of the code C with the required properties. Now, we will permute the bits of the codewords of C and feed them to an accumulator. We want to find a permutation π_2 so that the minimum distance at the output of the accumulator, i.e. the minimum distance of C', is linear in the block length. We will show that such permutation exists by the probabilistic method. We follow the same technique used in [BMS03] to prove that RAA codes have good minimum distance when both permutations are chosen at random.
Let C' be the code described in Lemma 1:

$$C':\{0,1\}^n \quad\rightarrow\quad \{0,1\}^{cn}, x\mapsto A(\pi_2(C(x)))$$

We will calculate the probability that C' has minimum distance less than εn. By Markov's inequality, the probability that there exists a nonzero codeword of weight less than εn is bounded from above by the expected number of codewords of weight less than εn. We will denote this latter expectation by $E_{\varepsilon n}$. Let $\alpha_{w,h}$ denote the probability that a random cn bit input string of weight w leads to Hamming weight weight h at the

accumulator's output. By linearity of expectation, we clearly have

$$E_{\varepsilon n} = \sum_{h=1}^{\varepsilon n} \sum_{w=\log dn}^{2\varepsilon n} X_w \alpha_{w,h} \ .$$

where X_w denotes the number of codewords with input weight w. Note that the upper bound of w is set to $2\varepsilon n$: for a binary string x of weight w at the input of an accumulator, the output $A(x)$ will have weight at least $\lceil \frac{w}{2} \rceil$. Hence we get a codeword of weight $h \leq \varepsilon n$ only if the input weight of the codeword is at most $2\varepsilon n$.

In [DJM98], the authors calculate the number of codewords of an accumulator code of input weight w and output weight h, denoted $A_{w,h}$. If N is the block length of the accumulator, then $A_{w,h}^{(N)} = \binom{N-h}{\lfloor \frac{w}{2} \rfloor} \binom{h-1}{\lceil \frac{w}{2} \rceil - 1}$.

Back to $\alpha_{w,h}$, we get:

$$\alpha_{w,h} = \frac{A_{w,h}^{(cn)}}{\binom{cn}{w}} = \frac{\binom{cn-h}{\lfloor \frac{w}{2} \rfloor}\binom{h-1}{\lceil \frac{w}{2} \rceil - 1}}{\binom{cn}{w}} < \frac{\binom{cn}{\lfloor \frac{w}{2} \rfloor}\binom{h}{\lceil \frac{w}{2} \rceil - 1}}{\binom{cn}{w}}$$

Using $\binom{x}{\lfloor \frac{y}{2} \rfloor} \leq \left(\frac{4ex}{y}\right)^{y/2}$, $\binom{x}{\lceil \frac{y}{2} \rceil - 1} \leq \left(\frac{4ex}{y}\right)^{y/2}$ and $\binom{x}{y} \geq \left(\frac{x}{y}\right)^{y}$, we get

$$\alpha_{w,h} < \frac{\left(\frac{4cen}{w}\right)^{w/2}\left(\frac{4eh}{w}\right)^{w/2}}{\left(\frac{cn}{w}\right)^{w}} = \left(\frac{4e\sqrt{h}}{\sqrt{cn}}\right)^{w}$$

Then

$$\begin{aligned} E_{\varepsilon n} &< \sum_{h=1}^{\varepsilon n} \sum_{w=\log dn}^{2\varepsilon n} X_w \left(\frac{4e\sqrt{h}}{\sqrt{cn}}\right)^{w} \\ &= \sum_{w=\log dn}^{2\varepsilon n} X_w \left(\frac{4e}{\sqrt{cn}}\right)^{w} \sum_{h=1}^{\varepsilon n} h^{w/2} \\ &\leq \sum_{w=\log dn}^{2\varepsilon n} X_w \left(\frac{4e}{\sqrt{cn}}\right)^{w} \varepsilon n \ (\varepsilon n)^{w/2} \\ &= \varepsilon n \sum_{w=\log dn}^{2\varepsilon n} X_w \left(\frac{4e\sqrt{\varepsilon}}{\sqrt{c}}\right)^{w} \ . \end{aligned}$$

Using the exponential weight property of the code C: $X_w \leq l^w$, we get

$$E_{\varepsilon n} < \varepsilon n \sum_{w=\log dn}^{2\varepsilon n} \left(\frac{4le\sqrt{\varepsilon}}{\sqrt{c}}\right)^{w} .$$

For $\frac{4le\sqrt{\varepsilon}}{\sqrt{c}} < \frac{1}{2}$, i.e. $\varepsilon < \frac{c}{4^3 e^2 l^2}$, we get

$$E_{\varepsilon n} < \varepsilon n \sum_{w=\log dn}^{2\varepsilon n} 2^{-w} < \varepsilon n 2^{-\log dn + 4} = \frac{16\varepsilon}{d} \ .$$

To sum up, for $\varepsilon < \frac{c}{4^3 e^2 l^2}$, we have shown that the probability that the minimum distance of $C' \geq \varepsilon n$ is at least $1 - \frac{16\varepsilon}{d}$. Thus by picking $\varepsilon < \min\{\frac{c}{4^3 e^2 l^2}, \frac{\delta d}{16}\}$, we can conclude that C' has minimum distance at least εn with probability at least $1 - \delta$, as desired. ■

In the above proof, we assumed the existence of the code C with the minimum distance and the exponential weight distribution properties. In the following section, we construct such codes from systematic RA codes with repetition factor 2, and Lemma 1 will apply by setting $c = 3$, $d = 2$ and $l = 16$.

III. Systematic RA codes from cubic Hamiltonian graphs

In this section, we construct codes satisfying the properties needed in the serial concatenation scheme used in section 2. These codes are systematic RA codes whose permutation π_1 is constructed from cubic Hamiltonian graphs with logarithmic girth. The repetition factor k is set to 2. The construction and proof heavily use the fact that $k = 2$. We will show that the systematic RA code, C^s_{2,π_1}, has the requisite minimum distance and exponential weight distribution properties:

1) C^s_{2,π_1} has minimum distance at least $\log 2n$.

2) Let X_w is the number of codewords in C^s_{2,π_1} of weight w. Then $X_w \leq 16^w$, for all w.

If n is the message length of the systematic RA code, the block length is $3n$: $2n$ from the output of the accumulator and n from the appended message. The construction of the permutation π_1 is based on the construction presented in [BMS03] and adapted in [FK04] for RA codes.

A. Construction

The construction uses a cubic Hamiltonian (undirected) graph $G = (V, E)$ with logarithmic girth. Constructions of such graphs were proposed by Erdös and Sächs [Big98] based on a greedy algorithm.

For a message length n, G has $2n$ vertices and $3n$ edges. We remove the edge (v_1, v_{2n}) for technical convenience that we explain later. The nodes represent the bits of the message after repetition. Let $v_1, \ldots, v_{2n}$ be the nodes of G and let $x = x_1, \ldots, x_{2n}$ be the repeated permuted version of a message $m \in \{0,1\}^n$, then v_i is associated with the bit x_i. Let y be the output of the accumulator when applied to x, i.e $y = C_{2,\pi_1}(m) = A(x)$.

All the edges along the broken Hamiltonian cycle will be referred to as *line edges*. The remaining edges are referred to as *matching edges*. The nodes at the endpoints of a matching edge are repeated nodes, so if (v_i, v_j) is a matching edge, then $x_i = x_j$. The matching edges are ordered from 1 to n so that each matching edge corresponds to one of the n bits of the original message m. To encode, we set to 1 the nodes of each matching edge corresponding to 1 in the input message and to 0 the remaining nodes in the graph. The bits are then entered in the nodes' order to the accumulator.

Figure 3 shows the graph G and how the nodes and edges correspond to the bits of the message and the codeword. To summarize, we have the following:

- $m \in \{0,1\}^n$ is the original message, $x = \pi_1(r_2(m)) \in \{0,1\}^{2n}$, $y = A(x) \in \{0,1\}^{2n}$ and $C^s_{2,\pi_1}(m) = (y, m) \in \{0,1\}^{3n}$.
- $G = (V, E)$ is the graph where $|V| = 2n$ and $|E| = 3n$. If $v_i, v_{i+1}, v_j \in V$ $(i < j)$ and $(v_i, v_{i+1}), (v_i, v_j) \in E$,

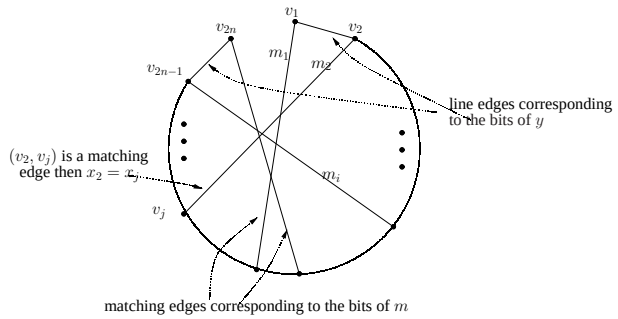

Fig. 3. Graph G

then v_i is associated with x_i, the (line) edge (v_i, v_{i+1}) is associated with y_i and the (matching) edge (v_i, v_j) is associated with m_l, for some $l \in \{1, \cdots, n\}$.

B. Minimum Distance

To calculate the minimum distance of C^s_{2,π_1}, we will show the equivalence between a codeword and a union of disjoint simple cycles: the weight of a codeword corresponds to the total length of the cycles. This correspondence is a variation of that in [BMS03] and [FK04] adapted to RA codes.

For each nonzero codeword (y, m), construct the graph G_y as follows: If $m_i = 1$, add the matching edge corresponding to m_i to G_y. If $y_j = 1$, add the line edge (v_j, v_{j+1}) to G_y.

Note that the line edge (v_1, v_{2n}) is never picked since $y_{2n} = x_1 \oplus x_2 \oplus \ldots \oplus x_{2n} = 0$.

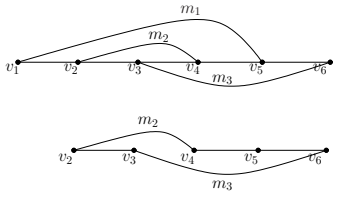

Fig. 4. An example showing how to construct G_y for $(y, m) = (010110, 011)$. The top graph is G and the bottom one G_y.

We will prove that G_y is a union of disjoint cycles and then deduce the minimum distance from the equivalence of codewords and unions of disjoint cycles.

Lemma 3: Let (y, m) be a codeword in C^s_{2,π_1} and let G_y be the subgraph of G corresponding to (y, m) as explained above. Then

1) G_y is a union of disjoint cycles of length equal to the Hamming weight of (y, m), denoted $\mathrm{wt}((y, m))$.

2) Each union of disjoint cycles in G correspond to a codeword of C^s_{2,π_1}.

Proof:

1) By the construction of G_y, the number of edges in G_y equals $\mathrm{wt}(y) + \mathrm{wt}(m) = \mathrm{wt}((y, m))$.

Let $v_i \in G_y$. v_i is connected to 3 edges in G: the two line edges (v_{i-1}, v_i) and (v_i, v_{i+1}) and the matching edge (v_i, v_j). Let m_l be the bit in m corresponding to the matching edge (v_i, v_j). Note that $x_i = x_j = m_l$.

We have two cases for m_l:

- If $m_l = 1$, then $x_i = 1$ and the matching edge (v_i, v_j) is in G_y. Note that $y_{i-1} \neq y_i$ since $y_i = y_{i-1} \oplus x_i = y_{i-1} \oplus 1$. Hence only one of the two line edges (v_{i-1}, v_i) and (v_i, v_{i+1}) appears in G_y. Therefore v_i is connected to exactly two edges in G_y.
- If $m_l = 0$, then $x_i = 0$ and the matching edge (v_i, v_j) is **not** in G_y. $y_{i-1} = y_i$ since $y_i = y_{i-1} \oplus x_i = y_{i-1} \oplus 0$. Hence both edges (v_{i-1}, v_i) and (v_i, v_{i+1}) appear in G_y since $v_i \in G_y$. Therefore v_i is only connected to the two line edges in G_y.

Thus all nodes in G_y have degree 2. This implies that G_y has is a disjoint union of cycles.

2) Each cycle in the union should have at least one matching edge since the line edge (v_1, v_{2n}) is removed. Setting to 1 the bits corresponding to the endpoints of each matching edge and to 0 the remaining bits gives us a binary string x, where $x = \pi_1(r_2(m))$ for some codeword (y, m) in C^s_{2,π_1}: the matching edges correspond to the 1-bits in the message m and the endpoints of the matching edges will correspond to the 1-bits in x. These bits come in pair (repetition factor 2) since both bits corresponding to the endpoints are set simultaneously. Hence, the codeword (y, m) will correspond to the union of cycles considered by the construction of G_y explained above.

Note that if we did not remove the edge (v_1, v_{2n}) from G, a cycle may contain (v_1, v_{2n}). This would imply that $y_{2n} = 1$, which is not true, and hence the equivalence between codewords and union of disjoint simple cycles breaks. ■

Combining all the above, we get the following variation of the codewords-cycles correspondence in [BMS03], [FK04], adapted to systematic RA codes:

Corollary 1: Let G be a cubic Hamiltonian graph with girth g and let C^s_{2,π_1} be the systematic RA code whose permutation π_1 is constructed from G as explained above. Then C^s_{2,π_1} has minimum distance equal to the girth g of G.

C. Number of codewords of each weight

We now show that C^s_{2,π_1} has the exponential weight distribution property. By the equivalence of codewords and cycles, we prove that the number of unions of disjoint cycles in the cubic Hamiltonian graph is at most exponential in the total length of these cycles. In particular, we show that:

Lemma 4: $X_w \leq 16^w$, for all w, where X_w is the number of codewords in C^s_{2,π_1} of weight w.

Proof: Let G be the cubic Hamiltonian graph used as the permutation π_1. G has $2n$ vertices and a girth $g = \log 2n$. Our goal is to bound X_w. Since C^s_{2,π_1} has minimum distance $\log 2n$, $X_w = 0$ for all $w < \log 2n$. Recall from Lemma 3 that X_w is equal to the number of unions of disjoint simple cycles of total length w. To simplify counting, we will consider cycles

with ordered nodes and not necessarily simple and disjoint cycles.

For $w \geq \log 2n$, let Z_w be the number of unions of ordered cycles (not necessarily simple and disjoint) with ordered nodes of total length w. Thus, $X_w \leq Z_w$. We will bound Z_w by induction on w. Let C_w be the number of single cycles (not necessarily simple) with ordered nodes of length w. For $w = g = \log 2n, C_w = Z_w$ since a union of cycles of length equal to the girth should contain one cycle only.

1) Bound on C_w: For a cycle of length w, we have at most $2n$ choices for the first vertex, which has 3 choices for its neighbor. The last vertex has one choice only, the first vertex. The remaining $w-2$ vertices each has 2 choices. We get:

$$C_w \leq 2n \cdot \left(3 \cdot 2^{w-2}\right) = 6n \cdot 2^{w-2} \leq 4^w$$

($\frac{\log 6n-2}{w} \leq 1$ since $w \geq g = \log 2n$)

2) Bound on Z_w: We will show by induction on w that $Z_w \leq 4^{2w}$. The base case is when $w = g$ and $Z_g = C_g = 4^g \leq 4^{2g}$. Assume the hypothesis is true for all $l,\ g \leq l \leq i$, we will prove it true for $i+1$.

$$\begin{aligned} Z_i &\leq \sum_{l=g}^{i} C_l Z_{i-l} \leq \sum_{l=g}^{i} 4^l\ 4^{2(i-l)} = 4^{2i} \sum_{l=g}^{i} 4^{-l} \\ &\leq 4^{2i} \frac{4^{-g}}{1-\frac{1}{4}} = 4^{2i} \frac{\frac{1}{4}}{1-\frac{1}{4}} \times 4^{-g+1} \leq 4^{2i} \end{aligned}$$

since $4^{-g+1} \leq 1$, $\forall g \geq 1$.

Finally, we get $X_w \leq Z_w \leq 16^w$ for all w. ■

Note that the logarithmic girth becomes an essential condition in proving the upper bound on C_w.

IV. Conclusions

We gave an explicit construction of a permutation π_1 such that the inner-systematic RAA code with first permutation π_1 is, with high probability, asymptotically good, where the probability is taken over the random choice of the second permutation π_2. This leads to the following questions:

1) Can the properties of the cubic Hamiltonian graph help construct an explicit permutation π_2, so that the resulting inner-systematic RAA code has good minimum distance?
2) Can other constructions of cubic Hamiltonian graphs, eg., algebraic constructions, give more insight on the construction of π_2 to achieve a good minimum distance?

References

[BMS03] L. Bazzi, M. Mahdian, and D. Spielman. The Minimum Distance of Turbo-Like Codes, preprint, 2003. To appear in *IEEE Transactions on Information theory*.

[BDMP98] S. Benedetto, D. Divsalar, G. Montorsi, and F. Pollara. Analysis, design, and iterative decoding of double serially concatenated codes with interleavers, *IEEE Journal on Selected Areas In Communications*, Vol. 16, No. 2, February 1998.

[Big98] N.Biggs. Construction of Cubic Graphs with Large Girth. *Electronic Journal of Combinatorics*, 5(A1), 1998.

[CKZ07] D. J. Costello, Jr, J. Kliewer , and K. S. Zigangirov. New results on the minimum distance of repeat multiple accumulate codes.*Proceedings of the Annual Allerton Conference on Communication, Control, and Computing*, September 2007.

[DJM98] D. Divsalar, H. Jin, and R. McEliece. Coding Theorems for "Turbo-Like"Codes. *Proceedings of the Annual Allerton Conference on Communication, Control, and Computing*, pp. 201-210, 1998.

[FK04] J. Feldman, and D. Karger. Decoding Turbo-Like Codes with Linear Programming. *Journal of Computer and System Sciences*, Volume 68, Issue 4, June 2004.

[PS99] H. Pfister, and P. H. Siegel. On the serial concatenation of rate-one codes through uniform random interleavers.*37th Allerton Conference on Communication, Control, and Computing*, September 1999.

[Spi96] D. Spielman. Linear-time encodable and decodable error-correcting codes. *IEEE Transactions on Information Theory* Volume 42, No 6, pp. 1723-1732, 1996.