Proc. of 38th Allerton Conference on Communication, Control and Computing, pp. 248–257. Allerton House, Monticello, Illinois, October 4–October 6, 2000.

Constructions of LDPC Codes using Ramanujan Graphs and Ideas from Margulis*

Joachim Rosenthal
Department of Mathematics
University of Notre Dame
Notre Dame, Indiana 46556-5683, USA
e-mail: Rosenthal.1@nd.edu

Pascal O. Vontobel
Signal and Information Processing Laboratory
ETH Zürich
CH-8092 Zürich, Switzerland
e-mail: vontobel@isi.ee.ethz.ch

October 3, 2000

Abstract

Some twenty years ago G.A. Margulis [8] proposed an algebraic construction of LDPC codes. In this paper we analyze the performance of the codes proposed by Margulis. Mimicking the construction of Margulis we describe a new powerful regular LDPC code whose construction is based on a Ramanujan graph.

1 Introduction

Low-Density Parity-Check (LDPC) codes were introduced by Gallager [3] and they have been the focus of intense research in recent years. Roughly speaking, an LDPC code is a binary linear block code having an $m \times n$ parity-check matrix H whose nonzero entries are sparse. LDPC codes are typically described by a bipartite graph. The n left-vertices $\{v_1, \ldots, v_n\}$ represent the code symbols and the m right-vertices $\{c_1, \ldots, c_m\}$ represent the code constraints. There is an edge between vertex v_j on the left and vertex c_i on the right whenever the entry $h_{i,j}$ of the matrix H is 1. With this the matrix H represents the adjacency matrix of the bipartite graph.

We say that an LDPC code is a (λ, ρ)-*regular code* if the degree d_v of every vertex v on the left is equal to the integer λ and the degree d_c of every vertex c on the right is equal to the integer ρ. For a (λ, ρ)-regular code the equality $n\lambda = m\rho$ must necessarily hold. In terms of the parity-check matrix H, regularity simply means that every row contains ρ entries of 1 and every column contains λ entries of 1.

Consider now a sequence of randomly chosen (λ, ρ) regular codes whose block length n is increasing. It has already been shown by Gallager [3, 12] that there exist decoding algorithms whose complexity remains linear in the block length. Moreover, in the limit the codes can be decoded up to a certain *threshold* near capacity.

*This research is supported in part by NSF Grant No. DMS-00-72383 and by grant TH-16./99-3.

Since the work of Gallager several authors attempted to construct explicitly LDPC codes. Probably the first significant work was done by Margulis [8]. In the last year several papers have appeared and we would like to mention [1, 5, 7, 16].

In order that an LDPC code is good several things are desirable:

1. It is desirable that the bipartite graph G has no small cycles. Recall that the girth of a graph is the length of its smallest cycle. For a given block length n and given degrees (λ, ρ) it is desirable that the girth is as large as possible. This will guarantee that e.g. the sum-product algorithm (see e.g. [4]) performs best. For bipartite graphs the girth is always an even number.

2. The graph should be a "good expander" [14]. This means that if one starts from any subset S of left-vertices whose size satisfies $|S| \leq \frac{m}{2}$ then the set $\partial(S)$ of vertices on the right connected to the vertices of S should satisfy:

$$|\partial(S)| \geq \varepsilon |S|$$

   where ε is a 'large expansion factor'.

3. It is desirable that the code has a good minimum distance. This is particularly important if the code is used at a high signal-to-noise ratio.

4. It is desirable that the code can be compactly described and that the encoding complexity is low.

The listed items are of course somehow conflicting. Item 4. can be achieved if the block length is chosen small but this will not result in a large distance nor in a large girth. Upper bounds for the minimum distance in terms of the rate and block length are well known. The following lemma provides an upper bound for the girth:

Lemma 1 *Consider a (λ, ρ)-regular LDPC code having block length $n = m\rho/\lambda$. Let $\alpha = (\lambda - 1)(\rho - 1)$. If the girth $c \equiv 2 \bmod 4$ then one has necessarily the inequality:*

$$c \leq 4 \log_\alpha m + 2 \tag{1}$$

Proof: We start at a right vertex and count the number of right vertices reached after at most $\frac{c-2}{4}$ steps. This results in the inequality:

$$1 + \rho(\lambda - 1) + \rho(\lambda - 1)\alpha + \cdots + \rho(\lambda - 1)\alpha^{\frac{c-2}{4}-1} \leq m.$$

From this we deduce the inequality

$$1 + \alpha + \cdots + \alpha^{\frac{c-2}{4}} = \frac{\alpha^{\frac{c-2}{4}+1} - 1}{\alpha - 1} \leq m.$$

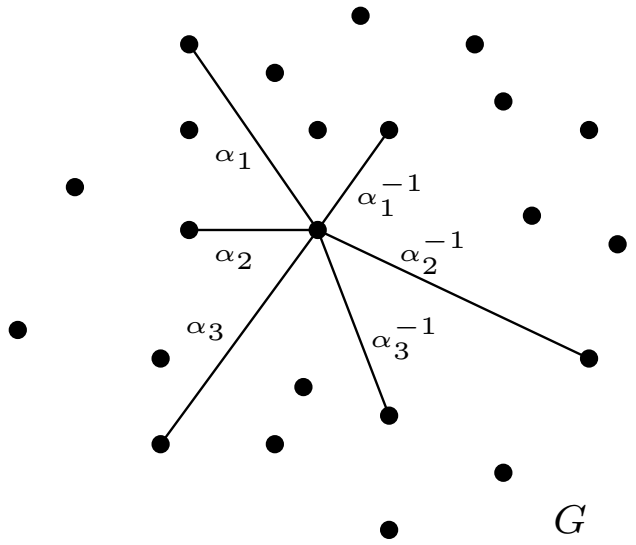
The result readily follows. □

In the next section we will study the performance of some LDPC codes introduced by Margulis [8]. In Section 3 we will use some known constructions of Ramanujan graphs [6, 9, 13] to design a remarkable $(3, 6)$-regular code, whose performance seems to be in a certain sense better than the performance of a randomly constructed code with the same design parameters. The code will have block length 4896 and almost optimal girth among all $(3, 6)$-regular codes. We have indications by simulations that the code has also a good minimum distance.

2 Cayley graphs and a construction of Margulis

One way of constructing k-regular graphs is by means of Cayley graphs. For this consider a finite group G. Let $\mathcal{A} \subset G$ be a subset of G satisfying $\mathcal{A} = \mathcal{A}^{-1}$. The Cayley graph $X(G, \mathcal{A})$ is the graph having as vertices the elements $g \in G$. The vertices $g, h \in G$ are connected by an edge whenever there is an $a \in \mathcal{A}$ such that $h = ga$. $X(G, \mathcal{A})$ is an undirected k-regular graph with $k = |\mathcal{A}|$.

Example 2 Assume the set $\mathcal{A}$ consists of $\mathcal{A} = \{\alpha_1, \alpha_1^{-1}, \alpha_2, \alpha_2^{-1}, \alpha_3, \alpha_3^{-1}\}$. Then one can think of the undirected graph as having the form:



Assume that the edges

$$(g_1, g_2), (g_2, g_3), \ldots, (g_{n-1}, g_n), (g_n, g_{n+1} = g_1)$$

form an n-cycle. By definition it follows that $g_1 = g_1 a_1 \cdots a_n$ or $a_1 \cdots a_n = e$, the identity element of the group G. This reasoning shows that a Cayley graph $X(G, \mathcal{A})$ has girth at least t if there are no non-trivial relations among the elements of $\mathcal{A}$ of length smaller than t.

One way of constructing a Cayley graph with good girth was given by Margulis [8]. For this let q be an odd prime. Let $\mathbb{F}_q$ be the finite field of q elements and consider the set $SL_2(\mathbb{F}_q)$ consisting of all 2×2 matrices $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ with entries in $\mathbb{F}_q$ and having determinant $ad - bc = 1$. One readily verifies that $SL_2(\mathbb{F}_q)$ is a group of order $q^3 - q$. Consider the subset

$$\mathcal{A} := \left\{ A = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}, A^{-1} = \begin{bmatrix} 1 & -2 \\ 0 & 1 \end{bmatrix}, B = \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}, B^{-1} = \begin{bmatrix} 1 & 0 \\ -2 & 1 \end{bmatrix} \right\}.$$

Theorem 3 (Margulis [8]) *Let $G = SL_2(\mathbb{F}_q)$ and let $\mathcal{A}$ be as above. Then the Cayley graph $X(G, \mathcal{A})$ is a 4-regular graph with $q^3 - q$ vertices and girth*

$$c \geq 2 \log_\alpha(q/2) - 1, \quad \textit{where } \alpha = 1 + \sqrt{2} = 2.4142\ldots$$

In [8] Margulis showed how it is possible to construct from the graph $X(G, \mathcal{A})$ a $(3, 6)$-regular LDPC code whose girth is at least as large as half the girth of the original graph. In the sequel we describe this construction and we investigate thereafter the performance of these codes for certain parameters.

As left vertices we will take two copies of G, say G and $\tilde{G}$. The right vertices of the bipartite graph will consist of the set G. An element $g \in G$ on the left will be connected with the right vertices

$$gA^2, gABA^{-1}, gB.$$

An element $\tilde{g} \in \tilde{G}$ on the left will be connected with the right vertices

$$\tilde{g}A^{-2}, \tilde{g}AB^{-1}A^{-1}, \tilde{g}B^{-1}.$$

If the smallest non-trivial relation among the elements $\{A, A^{-1}, B, B^{-1}\}$ has length c then one verifies that the elements

$$\{A^2, A^{-2}, ABA^{-1}, AB^{-1}A^{-1}, B, B^{-1}\}$$

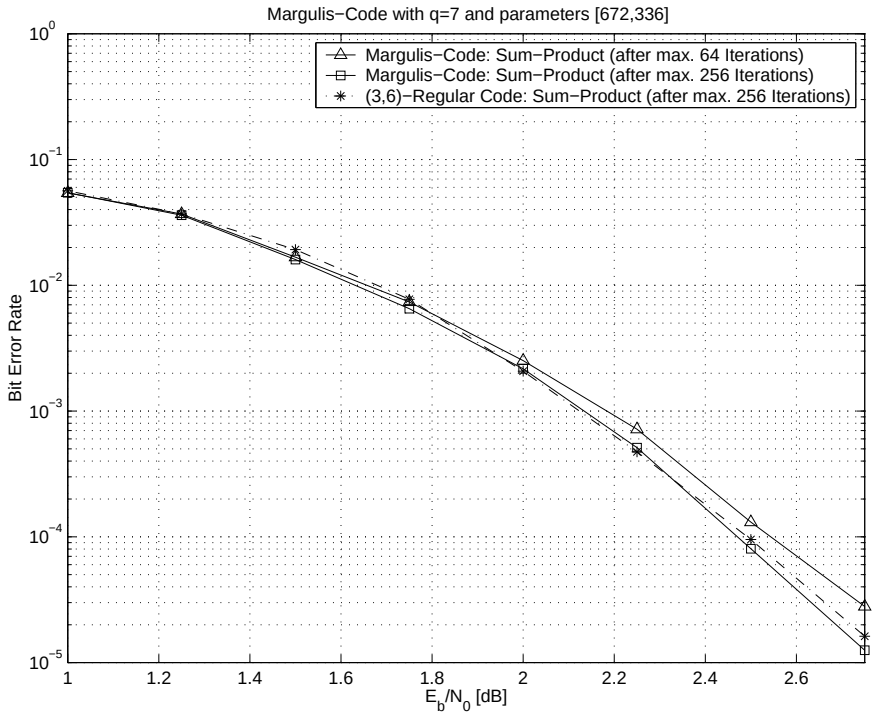
have no nontrivial relations of length smaller than $c/2 - 1$. It therefore follows:

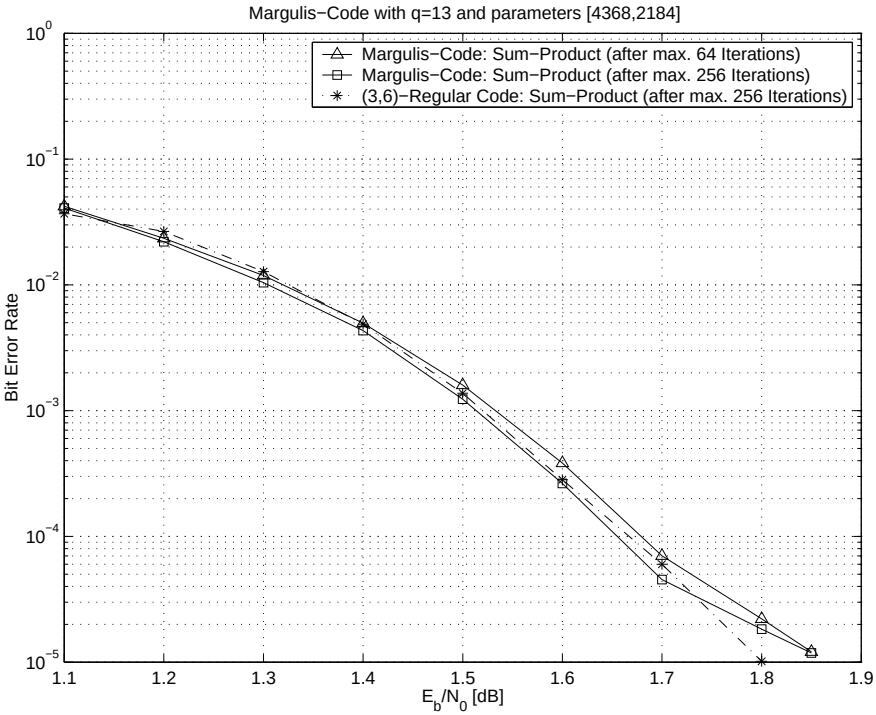
Lemma 4 *The bipartite graph described above describes a* $(3, 6)$*-regular LDPC code of block length* $2(q^3 - q)$ *and girth*

$$c \geq \log_\alpha(q/2) - 1, \quad \textit{where } \alpha = 1 + \sqrt{2} = 2.4142\ldots$$

For small numbers of q the lower bound of the girth is of course not very impressive. Important is however the fact that the lower bound increases linearly in terms of $\log_\alpha n$, where n is the block length of the code. This is the best one can expect.

We found it interesting to simulate the performance of these codes for different parameters. We did simulations in the case when $q = 7$ and $q = 13$. When $q = 7$ we deal with a $(3, 6)$ code of length $n = 672$ and dimension 336. When $q = 13$ we deal with a $(3, 6)$ code of length $n = 4368$ and dimension 2184. We did perform the simulations using the sum-product algorithm (see e.g. [4])).





In the simulations the decoding process is terminated if the syndrome of the decoded codeword is zero or if the maximum number of iterations is reached.

3 A rate-1/2 code constructed from a Ramanujan graph

Ramanujan graphs are k-regular graphs which are in a certain sense optimal in their expansion behavior. Formally, a Ramanujan graph is defined through the property that the second largest eigenvalue of the adjacency matrix is not larger than $2\sqrt{k-1}$. Note that in the limit the second largest eigenvalue is always at least $2\sqrt{k-1}$.

Lubotzky, Phillips, and Sarnak [6] and independently Margulis [9] constructed an infinite family of k-regular Ramanujan graphs. These graphs have not only an exceptional expansion rate but their girth surpasses also the asymptotic Erdős–Sachs bound [2] which states that a randomly generated k-regular graph with n vertices has girth at least $c \geq \log_{k-1} n$ with probability approaching 1 as $n \to \infty$.

In the sequel we will describe the construction in [6] and then we will show how these k-regular graphs give rise to excellent regular LDPC codes.

Consider the group $GL_2(\mathbb{F}_q)$ of 2×2 invertible matrices over the Galois field of q elements. The set of diagonal matrices

$$\mathcal{D} = \left\{ \left[\begin{array}{cc} x & 0 \\ 0 & x \end{array} \right] \middle| \, x \in \mathbb{F}_q^* \right\}$$

forms a normal subgroup of $GL_2(\mathbb{F}_q)$. The factor group

$$PGL_2(\mathbb{F}_q) := GL_2(\mathbb{F}_q)/\mathcal{D}$$

is called the *projective general linear group*. Since $GL_2(\mathbb{F}_q)$ has $(q^2-1)(q^2-q)$ elements and since $\mathcal{D}$ has $q-1$ elements it follows that $PGL_2(\mathbb{F}_q)$ is a group of order q^3-q.

We can list the elements of $PGL_2(\mathbb{F}_q)$ in the following simple way:

1. There are $q^2(q-1)$ matrices having the form
$$\begin{bmatrix} 1 & b \\ c & d \end{bmatrix}, \text{ where } b, c \text{ arbitrary and } d \neq bc.$$
2. There are $q(q-1)$ matrices having the form
$$\begin{bmatrix} 0 & 1 \\ c & d \end{bmatrix}, \text{ where } d \text{ arbitrary and } c \neq 0.$$

These $(q^2+q)(q-1) = q^3-q$ matrices describe the group $PGL_2(\mathbb{F}_q)$ exactly.

For the rest of the paper we will assume that q is a prime. If $x \in \mathbb{F}_q^*$ is any nonzero element we define the Legendre symbol $\left(\frac{x}{q}\right)$ to be equal to 1 if x is a quadratic residue modulo q and as -1 if x is a quadratic non-residue.

Example 5 If $q = 17$ the quadratic residues of $\mathbb{F}_q^*$ are:
$$1, 4, 9, 16, 8, 2, 15, 13.$$
The quadratic non-residues are:
$$3, 5, 6, 7, 10, 11, 12, 14.$$

If $x, y \in \mathbb{F}_q^*$ then it is well known that $\left(\frac{x}{q}\right)\left(\frac{y}{q}\right) = \left(\frac{xy}{q}\right)$. As a consequence it follows that $\left(\frac{\det(xA)}{q}\right) = \left(\frac{x^2\det(A)}{q}\right) = \left(\frac{\det(A)}{q}\right)$ for every $A \in GL_2(\mathbb{F}_q)$ and $x \in \mathbb{F}_q^*$. It follows that
$$\varphi : PGL_2(\mathbb{F}_q) \longrightarrow \{-1, 1\}, \quad A \longmapsto \left(\frac{\det(A)}{q}\right)$$
is a well-defined group homomorphism.

Definition 6 $PSL_2(\mathbb{F}_q) := \varphi^{-1}(1)$ is called the *projective special linear group* over the field $\mathbb{F}_q$.

One readily verifies that $PSL_2(\mathbb{F}_q)$ has order $(q^3-q)/2$. The construction in [6] builds a Cayley graph whose vertices are the elements of $PGL_2(\mathbb{F}_q)$ respectively $PSL_2(\mathbb{F}_q)$.

For this, let p, q be two unequal primes both congruent to 1 modulo 4. By a theorem of Jacobi one knows that the equation
$$p = a_0^2 + a_1^2 + a_2^2 + a_3^2 \tag{2}$$
has exactly $p+1$ integer solutions with a_0 odd and greater than zero and a_j even for $j = 1, 2, 3$. Let $i \in \mathbb{F}_q^*$ be an element satisfying $i^2 = -1$. For each of the $p+1$ solutions of (2) define a matrix
$$\begin{bmatrix} a_0 + ia_1 & a_2 + ia_3 \\ -a_2 + ia_3 & a_0 - ia_1 \end{bmatrix}$$
and denote by $\mathcal{A}$ the set of these $p+1$ matrices. Note that $\mathcal{A} = \mathcal{A}^{-1}$ and for every $A \in \mathcal{A}$ one has $\det(A) = p$. Let $X^{p,q}$ be the Cayley graph $X(PGL_2(\mathbb{F}_q), \mathcal{A})$.

Theorem 7 ([6, 9]) *Let p, q be unequal primes congruent to 1 modulo 4 and satisfying $\left(\frac{p}{q}\right) = -1$. Note that $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ in our situation. Then $X^{p,q}$ represents a bipartite graph having $q^3 - q$ vertices and girth at least*

$$c \geq 4 \log_p q - \log_p 4.$$

The graph $X^{p,q}$ is bipartite since we can take as left vertices the elements of $PSL_2(\mathbb{F}_q)$ and as right vertices the remaining group elements inside $PGL_2(\mathbb{F}_q)$. The homomorphism φ introduced above decides if an element belongs to left or to the right. Since the determinant of every element in $\mathcal{A}$ is a quadratic non-residue modulo q it follows that vertices on the left side are only connected to vertices on the right.

The asymptotic Erdős–Sachs bound [2] for a $(p+1)$-regular graph with $n = q^3 - q$ elements predicts that the girth of a randomly constructed graph will asymptotically satisfy $c \geq 3 \log_p q$. The girth of the graphs $X^{p,q}$ surpass the Erdős–Sachs bound for every pair p, q satisfying the assumption of the theorem. It was pointed out by Margulis [9] that the Erdős–Sachs bound has a flavor similar to the Gilbert–Varshamov bound as there exist also codes with a minimum distance which beats the average of randomly generated ones.

In the rest of the paper we show how the graphs $X^{p,q}$ give rise to interesting LDPC codes. We restrict ourselves to one example. During the preparation of this paper we learned that Lafferty and Rockmore [5] constructed also some LDPC codes starting from the Ramanujan graphs $X^{p,q}$. The construction approach taken by Lafferty and Rockmore differs however from the one presented next.

Let $p = 5$ and $q = 17$. Note that 5 is a quadratic non-residue in $\mathbb{F}_{17}$, i.e. $\left(\frac{5}{17}\right) = -1$. The graph $X^{p,q}$ consists in this case of $n = q^3 - q = 4896$ vertices.

Let $i := 4$ have the property that $i^2 = -1$ in $\mathbb{F}_{17}$. There are exactly $p+1 = 6$ solutions (a_0, a_1, a_2, a_3) having the property that

$$a_0^2 + a_1^2 + a_2^2 + a_3^2 = p = 5$$

with a_0 odd and positive and the others even, namely:

$$(1, \pm 2, 0, 0),\ (1, 0, \pm 2, 0),\ \text{and } (1, 0, 0, \pm 2).$$

This results in 6 matrices:

$$A^{\pm 1} := \begin{bmatrix} 1 \pm 8 & 0 \\ 0 & 1 \mp 8 \end{bmatrix},\ B^{\pm 1} := \begin{bmatrix} 1 & \pm 2 \\ \mp 2 & 1 \end{bmatrix},\ C^{\pm 1} := \begin{bmatrix} 1 & \pm 8 \\ \pm 8 & 1 \end{bmatrix}$$

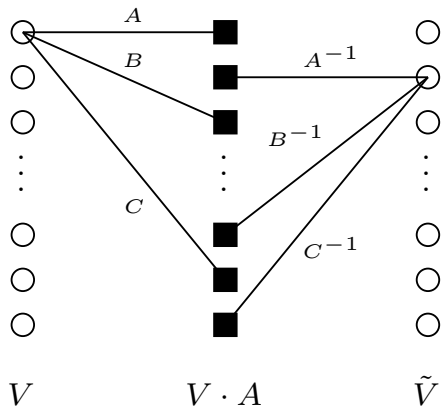
forming the set $\mathcal{A}$ of the Cayley graph. Note that the determinant is each time 5 modulo 17.

The graph $X^{p,q}$ has in a natural way a bipartite structure. The left node consist of $PSL_2(\mathbb{F}_{17})$, these are all elements whose determinant is a quadratic residue modulo 17. As right nodes take the elements whose determinant is a quadratic non-residue modulo 17. Note that a quadratic residue modulo 17 multiplied by 5 results in a quadratic non-residue modulo 17.

In order to build an LDPC code we take as left vertices two copies of $PSL_2(\mathbb{F}_{17})$, say V and $\tilde{V}$. As right vertices we take the right coset $VA \subset PGL_2(\mathbb{F}_{17})$ of $PSL_2(\mathbb{F}_{17})$.

As in the Margulis construction described in the last section we connect every element $v \in V$ on the left with the vertices vA, vB, vC on the right. An element $\tilde{v} \in \tilde{V}$ on the left will be connected with the vertices $\tilde{v}A^{-1}, \tilde{v}B^{-1}, \tilde{v}C^{-1}$ on the right.

The following diagram depicts the situation. The set VA describes the right coset of $PSL_2(\mathbb{F}_{17})$ in $PGL_2(\mathbb{F}_{17})$. The code bits are represented by the sets V and $\tilde{V}$. Note that for convenience the set $\tilde{V}$ has been drawn on the far right.

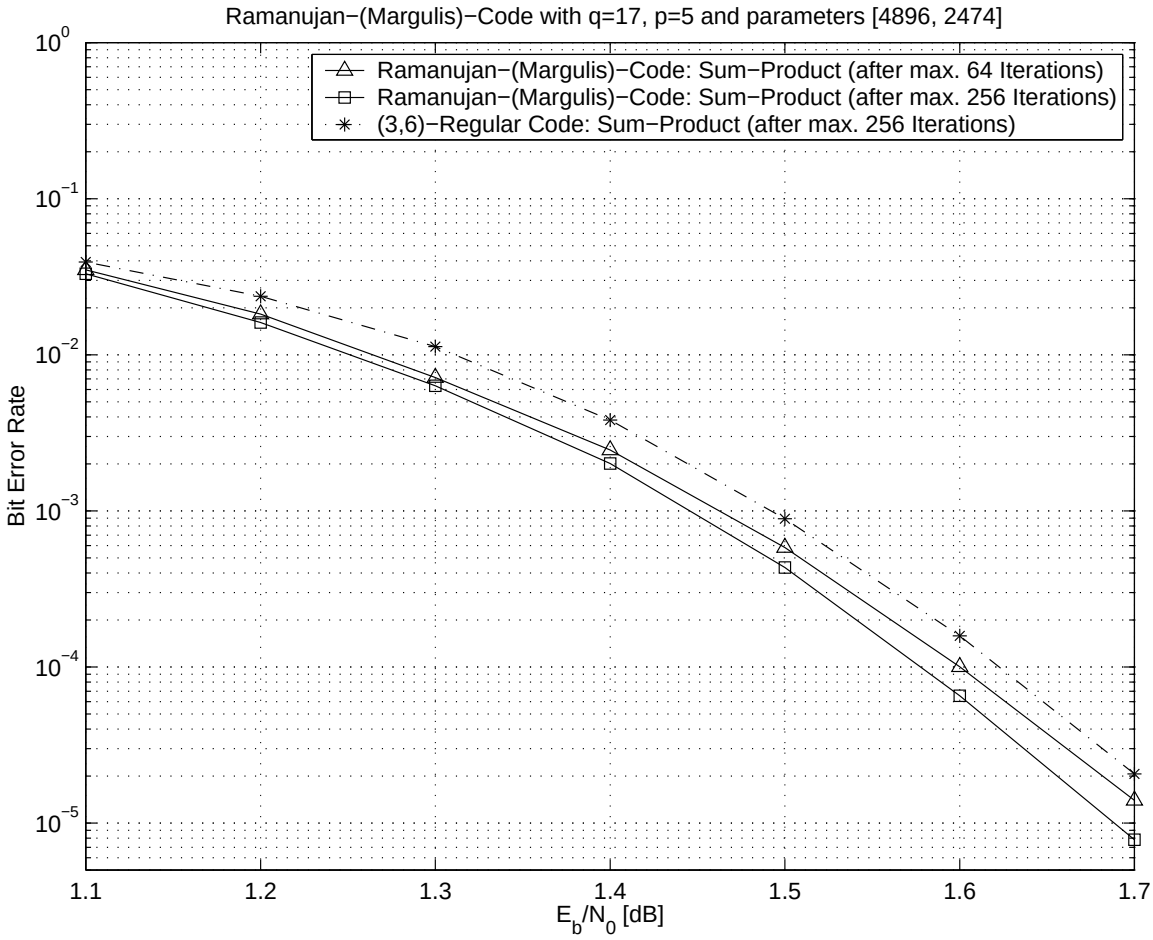


The construction results in a $(3, 6)$-regular LDPC code having block length $n = 4896$ and $m = 2448$ parity-check equations. There are few things we readily can say from some theoretical considerations. First the girth can be at most 14. Indeed if it were 16 we could start at a right vertex. All the vertices reached after 7 steps would have to be different. In this way we could predict that there are 6+60+600+6000 different left vertices when there are actually only 4896. So the girth cannot be more than 14 for these parameters. We computed the actual girth as 12 using MATLAB.

Similarly one can make a counting argument for the minimum distance. An active parity check on the right is connected with two nonzero bits on the left. In two further steps these two bits are connected to 4 more nonzero bits. Completing this argument it follows that the minimum distance is at least 14. Actually we believe that the distance is much higher. Indeed during all our simulations, a large number of errors with large Hamming weight could be corrected.

Note that the resulting parity-check matrix has a significant number of dependent rows so that the dimension is 2474. (A difference of about 1% to the designed one). In our simulations we compare this with a randomly constructed $(3, 6)$-regular code with parameters $[4896, 2448]$ which has the same decoding complexity per iteration.

The following diagram provides some simulation results.



The simulations suggest that the obtained algebraically constructed code performs superior over a randomly constructed $(3, 6)$-regular code.

4 Conclusion

In this paper we studied the performance of some algebraically constructed LDPC codes proposed by Margulis [8]. We adapted the construction using some Ramanujan graphs. It seems that these codes perform better than the randomly constructed codes of equal size and equal degrees.

References

[1] J. Bond, S. Hui, and H. Schmidt. Linear-congruence construction of low-density check codes. In B. Marcus and J. Rosenthal, editors, *Codes, Systems and Graphical Models*, IMA Vol. 123, pages 83–100. Springer-Verlag, 2000.

[2] P. Erdős and H. Sachs. Reguläre Graphen gegebener Taillenweite mit minimaler Knotenzahl. *Wiss. Z. Martin-Luther-Univ. Halle-Wittenberg Math.-Natur. Reihe*, 12:251–257, 1963.

[3] R.G. Gallager. *Low-Density Parity Check Codes.* M.I.T. Press, Cambridge, MA, 1963. Number 21 in Research monograph series.

[4] F. R. Kschischang, B. J. Frey, and H.-A. Loeliger. Factor graphs and the sum-product algorithm. Submitted to IEEE Trans. Inform. Theory, available at http://www.comm.utoronto.ca/frank/factor/, 2000.

[5] J. Lafferty and D. Rockmore. Codes and iterative decoding on algebraic expander graphs. To appear in the Proceedings of ISITA 2000, Honolulu, Hawaii, available at http://www.cs.cmu.edu/afs/cs.cmu.edu/user/lafferty/www/, November 2000.

[6] A. Lubotzky, R. Phillips, and P. Sarnak. Ramanujan graphs. *Combinatorica*, 8(3):261–277, 1988.

[7] D. J. C. MacKay and M. C. Davey. Two small Gallager codes. In B. Marcus and J. Rosenthal, editors, *Codes, Systems and Graphical Models*, IMA Vol. 123, pages 131–134. Springer-Verlag, 2000.

[8] G. A. Margulis. Explicit constructions of graphs without short cycles and low density codes. *Combinatorica*, 2(1):71–78, 1982.

[9] G. A. Margulis. Explicit group-theoretic constructions of combinatorial schemes and their applications in the construction of expanders and concentrators. *Problems Inform. Transmission*, 24(1):39–46, 1988. Translation from Problemy Peredachi Informatsii.

[10] M. Morgenstern. Existence and explicit constructions of $q + 1$ regular Ramanujan graphs for every prime power q. *J. Combin. Theory Ser. B*, 62(1):44–62, 1994.

[11] T. Richardson, A. Shokrollahi, and R. Urbanke. Design of provably good low-density parity check codes. Submitted to IEEE Trans. Inform. Theory, 1999.

[12] T. Richardson and R. Urbanke. An introduction to the analysis of iterative coding systems. In B. Marcus and J. Rosenthal, editors, *Codes, Systems and Graphical Models*, IMA Vol. 123, pages 1–37. Springer-Verlag, 2000.

[13] P. Sarnak. *Some Applications of Modular Forms.* Cambridge University Press, Cambridge, 1990.

[14] M. Sipser and D. A. Spielman. Expander codes. *IEEE Trans. Inform. Theory*, 42(6, part 1):1710–1722, 1996.

[15] R. M. Tanner. A recursive approach to low complexity codes. *IEEE Trans. Inform. Theory*, 27(5):533–547, 1983.

[16] R.M. Tanner. Transforming quasi-cyclic codes with sparse graphs. Preprint, January 2000.

[17] J.-P. Tillich and G. Zémor. Optimal cycle codes constructed from Ramanujan graphs. *SIAM J. Discrete Math.*, 10(3):447–459, 1997.