Electronic Notes in Theoretical Computer Science 74 (2003)
URL: http://www.elsevier.nl/locate/entcs/volume74.html 8 pages

Weaknesses of Margulis and Ramanujan–Margulis Low-Density Parity-Check Codes

David J.C. MacKay [1] and Michael S. Postol [2]

Cavendish Laboratory,
Cambridge, CB3 0HE, United Kingdom.

Abstract

We report weaknesses in two algebraic constructions of low-density parity-check codes based on expander graphs. The Margulis construction gives a code with near-codewords, which cause problems for the sum-product decoder; The Ramanujan-Margulis construction gives a code with low-weight codewords, which produce an error-floor.

1 Introduction

A regular low-density parity-check code, or Gallager code (Gallager, 1962) has a parity-check matrix with uniform column weight j and uniform row weight k, both of which are very small compared to the blocklength. If the code has transmitted blocklength N and rate R then the parity-check matrix $\mathbf{H}$ has N columns and M rows, where $M \geq N(1-R)$. [Normally parity-check matrices have $M = N(1-R)$, but the matrices we construct may have redundant rows so that their rate could be higher than $1 - M/N$.] Randomly constructed low-density parity-check codes typically have excellent performance (MacKay and Neal, 1996; MacKay, 1999), especially if they are constrained to have large girth (Mao and Banihashemi, 2000).

Twenty years ago, Margulis (1982) proposed a Cayley graph construction of Gallager codes with rate 1/2 and with parameters $(j, k) = (3, 6)$. The performance of these codes was first investigated by Rosenthal and Vontobel (2000), who also proposed a similar 'Ramanujan-Margulis' code. Promising performance results were presented under message-passing decoding.

In this paper we investigate these codes and demonstrate that they have significant weaknesses.

[1] Email: mackay@mrao.cam.ac.uk
[2] Email: msposto@zombie.ncsc.mil

2 The Construction of Margulis

For each prime p, Let $SL_2(p)$ be the *Special Linear Group* whose elements consist of 2×2 matrices of determinant 1 over Z_p, the integers modulo p. The group has $M = (p^2-1)(p^2-p)/(p-1) = (p^2-1)p$ elements. For $p \geq 5$, Margulis defined a code of length $N = 2M = 2(p^2-1)p$ and rate 1/2. The rows of the parity-check matrix are indexed by the elements of $SL_2(p)$ and the columns are indexed by 2 copies of this group.

Let $SL_2(p)$ be generated by the matrices $A = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ and $B = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$. If $g \in SL_2(p)$ is the index of a row of the parity-check matrix, we place a one in the columns corresponding to gA^2, $gABA^{-1}$, and gB on the left hand side of the matrix and the columns corresponding to gA^{-2}, $gAB^{-1}A^{-1}$, and gB^{-1} on the right hand side of the matrix. This produces a low-density parity-check code with row weight $k = 6$ and column weight $j = 3$.

The code can also be described in terms of a graph. If G is a group and S is a subset of G, we define the *Cayley graph* of G with respect to S as the graph whose vertices are the elements of G and such that 2 elements g_1 and g_2 are adjacent if and only if $g_1^{-1}g_2 \in S$. To make the graph undirected, we choose S so that $S = S^{-1}$, i.e. $a \in S$ implies $a^{-1} \in S$.

We construct a slightly modified Cayley graph as follows: We let Y_p be the bipartite graph whose left vertices are elements of $G = SL_2(p)$, and the right vertices are elements of $G \times \{0, 1\}$. We join the element $g \in G$ to the 6 elements $(gA^2, 0)$, $(gABA^{-1}, 0)$, $(gB, 0)$, $(gA^{-2}, 1)$, $(gAB^{-1}A^{-1}, 1)$, and $(gB^{-1}, 1)$. Then Margulis's parity-check matrix is the *adjacency matrix* of this graph. Margulis has shown that the girth of the graph grows as $\log p$.

2.1 Results for $p = 11$

The code with $p = 11$ has length $N = 2640$ and girth 8. The parity-check matrix has full rank. The minimum distance of the code d is not known, but satisfies $d \leq 220$. (We found a row of this weight in a generator matrix.) This figure can be compared with the Gilbert distance for a (2640,1320) code, which is 290.

Its performance on the Gaussian channel is good, but is marred by an error floor that appears at a block error probability of about $p_w = 10^{-6}$. This error floor, which was first noted by Rosenthal and Vontobel (2000), is not associated with low-weight codewords. Rather, it is caused by *near-codewords*.

We define a (w, v) *near-codeword* of a code with parity-check matrix $\mathbf{H}$ to be a vector $\mathbf{x}$ with weight w whose syndrome $\mathbf{z}(\mathbf{x}) \equiv \mathbf{Hx}$ has weight v. Near-codewords with both small v and relatively small w tend to be error states from which the sum-product decoding algorithm cannot escape. A small value of w corresponds to a quite-probable error pattern, while the small value of v indicates that only a few check-sums are affected by these error patterns.

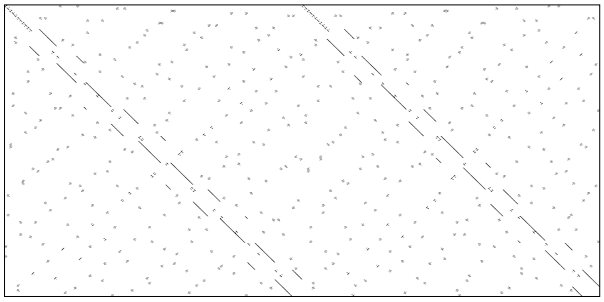

Fig. 1. The parity-check matrix of the $N = 2640$ Margulis code.

[Near-codewords are not identical to 'stopping sets' – collections of bits which will stop decoding if they are erased. A stopping set is a set S of bits such that all neighbours of S are connected to S at least twice. In a typical (w, v) near-codeword, there are v check nodes that are connected to the bits in the word only once.]

We simulated about seven million transmissions over a Gaussian channel and decodings using the sum-product algorithm, halting when the decoder reached a valid codeword, or when a maximum of 200 iterations was reached. By inspecting the final state of the decoding algorithm in every simulation, we found that the $N = 2640$ code has numerous (12,4) near-codewords and (14,4) near-codewords. These are the cause of the error floor, as can be seen in figure 2, which shows not only the block error probability but also the frequency with which the decoder failed by ending in a non-codeword state within a small distance of the true codeword.

To try to find a tighter bound on the minimum distance of the code, we took a near-codeword and formed the 1320 near-codewords given by multiplying it by the 1320 elements of $SL_2(11)$. We sought a linear combination of a few of them that formed a true codeword. We established that no eight of them form a codeword. There do exist collections of 24 of the near-codewords that make codewords, but this is an uninteresting result, since it only shows us that there is a word of weight 288, and we already know of one with weight 220.

3 Codes based on Ramanujan graphs

3.1 Construction

A *Ramanujan graph* is a graph such that any vertex has exactly k vertices adjacent to it and whose adjacency matrix has second largest eigenvalue no greater than $2\sqrt{k-1}$. It has been shown that these graphs have girths which surpass the lower bound of $\log_{k-1} n$ for randomly constructed graphs with n vertices each of which are adjacent to k neighbors.

Rosenthal and Vontobel (2000) gave the following construction for low-density parity-check codes based on these graphs.

Consider the group $GL_2(q)$ of 2×2 invertible matrices over $GF(q)$. In what follows we will let q be prime so that these are matrices over Z_q. The set D of nonzero 2×2 diagonal matrices form a normal subgroup of $GL_2(q)$ and the factor group $PGL_2(q) = GL_2(q)/D$ is called the *projective general linear group*. $PGL_2(q)$ has order $q^3 - q$ and its elements can be listed as follows:

(i) There are $q^2(q-1)$ matrices of the form

$$\begin{pmatrix} 1 & b \\ c & d \end{pmatrix}, \tag{1}$$

where b and c are arbitrary, and $d \neq bc$.

(ii) There are $q(q-1)$ matrices of the form

$$\begin{pmatrix} 0 & 1 \\ c & d \end{pmatrix}, \tag{2}$$

where d is arbitrary, and $c \neq 0$.

Now define a homomorphism $\phi : PGL_2(q) \to \{-1, 1\}$ by

$$\phi(a) = \begin{cases} 1 & \text{if } \det(a) \text{ is a quadratic residue} \\ & \quad \text{(i.e. a perfect square) modulo } q \\ -1 & \text{otherwise,} \end{cases} \tag{3}$$

for $a \in PGL_2(q)$. We define the *projective special linear group* $PSL_2(q)$ to be $\phi^{-1}(1)$. $PSL_2(q)$ has order $(q^3 - q)/2$.

We now let p and q be primes both congruent to 1 modulo 4, with $p < q$ and such that p is a nonresidue modulo q. A theorem of Jacobi shows that the equation

$$p = a_0^2 + a_1^2 + a_2^2 + a_3^2 \tag{4}$$

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 be an element of Z_q such that $i^2 = -1$. For each of the $p + 1$ solutions define a matrix

$$\begin{pmatrix} a_0 + ia_1 & a_2 + ia_3 \\ -a_2 + ia_3 & a_0 - ia_1 \end{pmatrix} \tag{5}$$

and let X be the set of these matrices. Then $X = X^{-1}$ and every matrix in X has determinant p.

The Cayley graph of $PGL_2(q)$ with respect to X is then a Ramanujan graph with $q^3 - q$ vertices and girth at least

$$c \geq 4 \log_p q - \log_p 4. \tag{6}$$

We build an low-density parity-check code as follows: Let the columns of the parity-check matrix be indexed by 2 copies of $V = PSL_2(q)$. Since p is a nonresidue modulo q and $\det(A) = p$ for $A \in X$, the set VA for any matrix

$A \in X$ is a right coset of $V = PSL_2(q)$ in $PGL_2(q)$ and V and VA comprise all of the elements of $PGL_2(q)$. We index the rows of the parity-check matrix by the elements of VA.

For every column v, we put a one in the position of the rows $vA_1, vA_2, \cdots, vA_{(p+1)/2}$ for v in the left half of the matrix and we put a one in the position of the rows of $vA_1^{-1}, vA_2^{-1}, \cdots, vA_{(p+1)/2}^{-1}$ for v in the right half of the matrix, where X consists of the matrices $A_1, A_2, \cdots, A_{(p+1)/2}$ and their inverses. This forms a low-density parity-check code with length $q^3 - q$, rate 1/2, column weight $(p+1)/2$ and row weight $p+1$.

3.2 The 17,5 Ramanujan-Margulis code

Let $q = 17$ and $p = 5$. Then $N = 4896$, every column has weight 3, and every row has weight 6. Using $i = 4$, we have $i^2 = 16 = -1 \pmod{17}$. X consists of 6 matrices corresponding to the 6 solutions

$$(a_0, a_1, a_2, a_3) = (1, \pm 2, 0, 0), (1, 0, \pm 2, 0), (1, 0, 0, \pm 2) \tag{7}$$

They are

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

Note that $(A^+)^{-1} = A^-$ and the same holds for B and C, so we will drop the superscript "+".

Rosenthal and Vontobel (2000) presented promising performance results for the $q = 17$, $p = 5$ code with blocklength $N = 4896$. The performance at low signal-to-noise ratios is better than that of comparable random low-density parity-check codes because the parity-check matrix has several redundant rows, so the code has rate higher than 1/2 but decodes just as well as a random code of weight 1/2.

However, their simulation results only go down to the conventional bit error probability of 10^{-5}. The $q = 17$, $p = 5$ code with $N = 4896$ in fact has codewords of weight 24. These words were found by simulating the decoding of 16×10^6 words using the sum-product algorithm and watching for *undetected* errors. (An undetected error results when the decoder halts in a valid codeword that is not the transmitted codeword; a *detected* error is an error in which the decoder knows that it has not found a valid codeword and reports this failure.)

The reason for these codewords is as follows.

Let $\alpha = AB$, $\beta = BC$, $\gamma = CA$, where A, B, and C are as defined above. The following identities, each of which corresponds to a short cycle in the graph, hold:

$$(\alpha\beta^{-1})^3 = 1 \tag{9}$$

$$(\beta\gamma^{-1})^3 = 1 \tag{10}$$

$$(\gamma\alpha^{-1})^3 = 1 \tag{11}$$

$$(\alpha\beta^{-1}\alpha\gamma^{-1})^2 = 1 \tag{12}$$

Because of these identities, there exists a word of weight 24 that has 12 of its bits in each copy of V.

We also found a word of weight 36.

3.3 The 13,5 Ramanujan-Margulis code

The $q = 13$, $p = 5$ code is a low-density parity-check code with $j = 3$, $k = 6$, and $N = 2184$. In this case X also consists of 6 matrices, which we will again label as A, B, C, and their inverses. These matrices are different from the ones used for $q = 17$, since we use $i = 5$, because $5^2 = 25 = 12 \pmod{13} = -1 \pmod{13}$, and all our arithmetic is now done modulo 13. The 13,5 code's parity-check matrix does not have redundant rows.

The 13,5 code has codewords of weight 14. These codewords feature prominently in the performance curve and render the code useless for practical purposes. They are unrelated to the codewords of weight 24 in the 17,5 code. Each codeword, like the weight-24 codeword of the 17,5 code, has half its nonzero bits in each copy of V. The codeword depends on 8-cycles in the graph such as the following:

$$(CA)(CB)^{-1}(AB)(BC)^{-1} = 1$$
$$(AC)(AB)^{-1}(CA)(BC)^{-1} = 1$$

The codeword is constructed by including any element a on the left-hand copy of V and adding

aCA, aAB, aBC	on the right;
$aCA(BC)^{-1}, aAB(CA)^{-1}, aBC(AB)^{-1}$	on the left;
$aCA(BC)^{-1}CC, aAB(CA)^{-1}AA, aBC(AB)^{-1}BB$	on the right;
$aCA(BC)^{-1}CC(CA)^{-1}, aAB(CA)^{-1}AA(AB)^{-1},$ $aBC(AB)^{-1}BB(BC)^{-1}$	on the left; and
$aCA(BC)^{-1}CC(CA)^{-1}BC$	on the right.

We also found a word of weight 18 and one of weight 20.

4 Conclusions

The Margulis code would probably be a useful rate-1/2 code if accompanied by a post-processor to deal with the near-codewords (Fossorier, 2001). Since all errors caused by near-codewords are detectable, the post-processor would only be needed when an error is detected. As a result, the average decoding complexity would remain quite low.

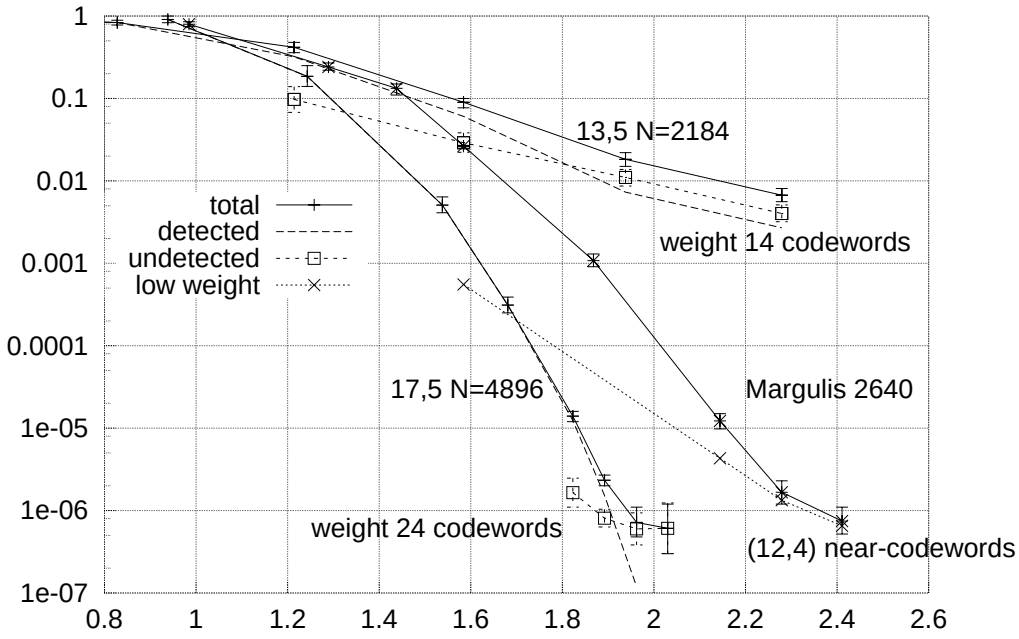

Fig. 2. Performance of all three codes on the Gaussian channel. Horizontal axis: E_b/N_0; vertical axis: *block* error probability. For each Ramanujan-Margulis code, the three curves show the total block error probability, the *undetected* error probability, and the *detected* error probability. For the Margulis code, the total block error probability and the probability of low-weight detected errors are shown. The Margulis code made no undetected errors.

The low-weight codeword in the 17,5 code carries with it the following morals:

(i) The widespread practice of plotting error probability without distinguishing *detected* from *undetected* errors would not have spotted this code weakness.

(ii) The widespread practice of simulating performance only down to a *bit error probability* of 10^{-5} is not adequate for revealing a code's practical properties. It is essential to simulate down to a *block* error probability of 10^{-5} or 10^{-6}.

What can we say about algebraic constructions for low-density parity-check codes? If a construction came accompanied by an impressive distance property, there would be a strong case for using it in place of a random construction; but for large N, while a random LDPC code can be constructed for any value of N and K, only a handful of algebraically constructed LDPC codes with a relatively good distance is known. Yes, random code-constructions carry with them an uncertainty about the properties of any one chosen code. But non-random constructions also carry a risk: the risk that the structure in the construction produces low-weight codewords or near-codewords. A compensating advantage of some systematic constructions is that their parity-check

matrices have redundancies, which allow the sum-product algorithm to perform better than a comparable random code, as illustrated by the 17,5 code (at least in its high SNR regime), and by difference set cyclic codes (Lucas *et al.*, 2000). Algebraic constructions clearly deserve further study.

As we finalised this paper, we learnt of the constructions of Lafferty and Rockmore (2000); their codes are based on Cayley graphs but the constraints used are based on Hamming codes rather than simple parity checks.

Acknowledgements

We thank John Lafferty, Michael Tanner, and Pascal Vontobel for helpful discussions.

DJCM's group is supported by the Gatsby Foundation and by a partnership award from IBM Zürich Research Laboratory.

References

Fossorier, M. (2001) Iterative reliability-based decoding of low-density parity check codes. *IEEE Journal on Selected Areas in Communications* **JSAC-19**: 908–917.

Gallager, R. G. (1962) Low density parity check codes. *IRE Trans. Info. Theory* **IT-8**: 21–28.

Lafferty, J., and Rockmore, D. (2000) Codes and iterative decoding on algebraic expander graphs. In *International Symposium on Information Theory and its Applications*.

Lucas, R., Fossorier, M., Kou, Y., and Lin, S. (2000) Iterative decoding of one-step majority logic decodable codes based on belief propagation. *IEEE Transactions on Communications* **48**: 931–937.

MacKay, D. J. C. (1999) Good error correcting codes based on very sparse matrices. *IEEE Transactions on Information Theory* **45** (2): 399–431.

MacKay, D. J. C., and Neal, R. M. (1996) Near Shannon limit performance of low density parity check codes. *Electronics Letters* **32** (18): 1645–1646. Reprinted *Electronics Letters*, **33**(6):457–458, March 1997.

Mao, Y., and Banihashemi, A. (2000) Design of good LDPC codes using girth distribution. In *IEEE International Symposium on Information Theory, Italy, June, 2000*.

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

Rosenthal, J., and Vontobel, P. O. (2000) Constructions of LDPC codes using Ramanujan graphs and ideas from Margulis. In *Proceedings of the 38th Annual Allerton Conference on Communication, Control, and Computing*, pp. 248–257.