Skoltech

Information and Coding Theory Project Report

# Margulis graph and LDPC codes


*Authors:*

Marina Dudina

Evgeny Marshakov

Leyla Mirvakhabova


Skoltech

Skolkovo Institute of Science and Technology

In collaboration with Massachusetts Institute of Technology

# Contents

# 1 Introduction

LDPC codes have many of their properties encoded in their Tanner graphs. Good expansion properties of a Tanner graph may guarantee good decoding. A bipartite graph with $n$ message nodes is called an $(\alpha, \beta)$-expander if for any subset $S$ of the message nodes of size at most $\alpha n$ the number of neighbors of $S$ is at least $\beta \cdot a_S \cdot |S|$, where $a_S$ is the average degree of the nodes in $S$.[5] The absence of short cycles (large girth) of a Tanner graph may increase the accuracy of belief propagation and bound the minimum distance for the code, as follows from the theorem by Tanner: **Theorem:** The minimum distance $d$ for an LDPC code with girth of the Tanner graph $g$ is bounded as:

$$d \geq \begin{cases} 1 + \frac{w}{w-2}\left(\left(w-1\right)^{\lfloor \frac{g-2}{4} \rfloor} - 1\right), \frac{g}{2} = 2m+1 \\ 1 + \frac{w}{w-2}\left(\left(w-1\right)^{\lfloor \frac{g-2}{4} \rfloor} - 1\right) + (w-1)^{\lfloor \frac{g-2}{4} \rfloor}, \frac{g}{2} = 2m \end{cases}$$

Hence it is desirable to construct a family of expander bipartite graph with large girth. In this project we study one of the constructions proposed by Margulis.

# 2 Margulis graphs

We aimed to implement the construction of bipartite expander graphs with high girth suggested by Margulis in [1]. Consider a group $G = SL2(F_q)$ of $2 \times 2$ matrices of determinant 1 over a finite field of $q$ element, for odd prime $q$. Consider the following set $S$

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

Take two copies of the group $G$, $\tilde{G}$ as left vertices of the constructed bipartite graph, and one more copy of G for the right vertices. An element $g \in G$ is connected to the right elements $gA^2, gABA^{-1}, gB$. An element $\tilde{g} \in \tilde{G}$ is getting connected to the right vertices $\tilde{g}A^{-2}, \tilde{g}AB^{-1}A^{-1}, \tilde{g}B^{-1}$

**Margulis theorem** Let $G = SL_2(\mathbb{F}_q)$. Then the Cayley graph $G_n(G, S)$ is a 4-regular graph with $n = q^3 - q$ vertices and girth

$$c \geq 2\log_\alpha(q/2) - 1, \text{ where } \alpha = 1 + \sqrt{2}.$$

# 3 Implementation

We developed a tool in SAGE to construct Margulis bipartite graphs. Given any odd prime $q$, the program returns an adjacency matrix of the graph, constructed according to the rules described above. We used $p = 7$ as an example, to study the performance of the related LDPC code. The obtained Bit Error Probability versus SNR curve is present in Figure 1.

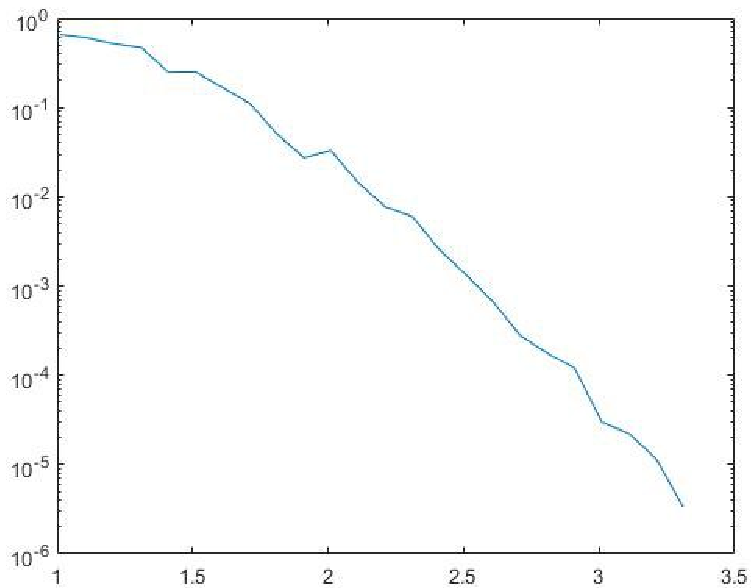


Figure 1: Margulis code with q=7 with parameters [672, 336]

## 3.1 Observations

In [3] the authors discovered that LDPC codes constructed with Margulis approach could have a error floor. The evidence for $q = 13$ is shown in Figure 2. As we found out on the course of our research, authors in [2] also simulated the code due to Margulis for $q = 7$. Their simulation curve, represented in Figure 3, correspond to ours.

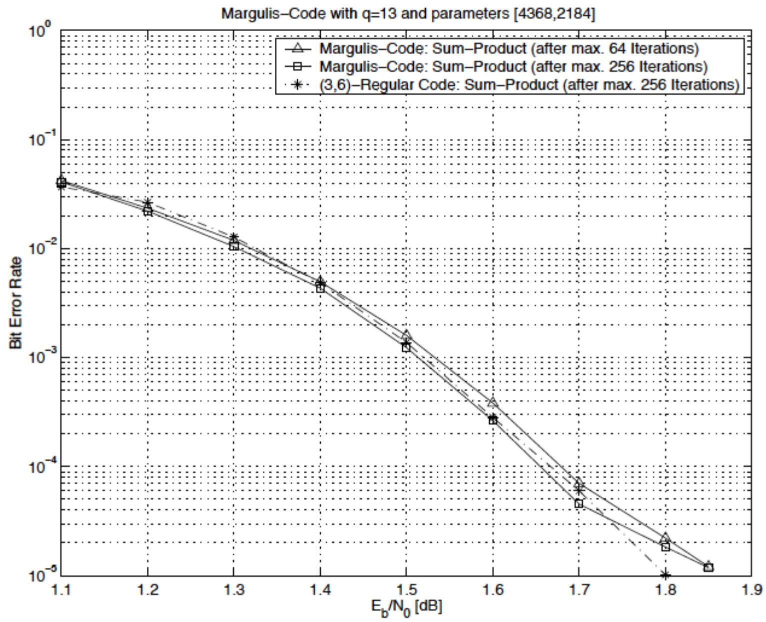


Figure 2: Margulis code with q=13 with parameters [4368, 2184]

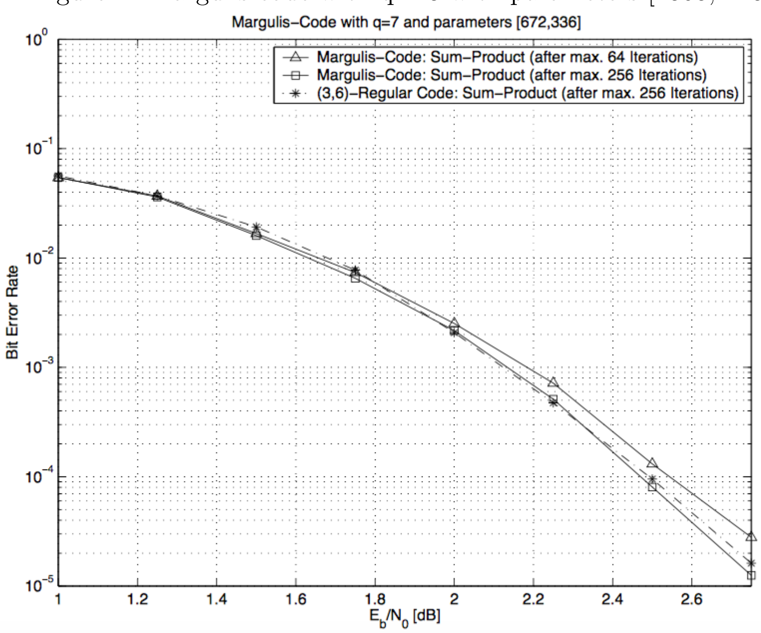


Figure 3: Margulis code with q=7 with parameters [672, 336]

## 3.2 Further analysis

We also implemented a slightly modified version of Margulis construction: we observed the fenerating matrices $A$, $B$ were of order 7 in $SL_2(F_7)$. We chose different generator $\tilde{A}$ of order 4 instead of $A$, and the order of the other generator was preserved to be 7. Clearly the girth of the Cayley graph of $SL_2(F_7)$ is at most 4, hence the girth of Margulis Tanner graph is also at most 4.

The simulation for the modified construction is shown in Figure 4.Clearly, the algorithm performs worse, as the girth decreases, as it is theoretically predicted. However, that is interesting to notice, that though cycles of length 4 are known to have trapping sets for the decoding algorithm, in this case the achieved error rate with waterfall curve is big. In [4] a group of codes that have cycles of length 4 and perform well under iterative decoding are discussed. That would be interesting to see if our code could be also presented as cyclic or quasi-cyclic.

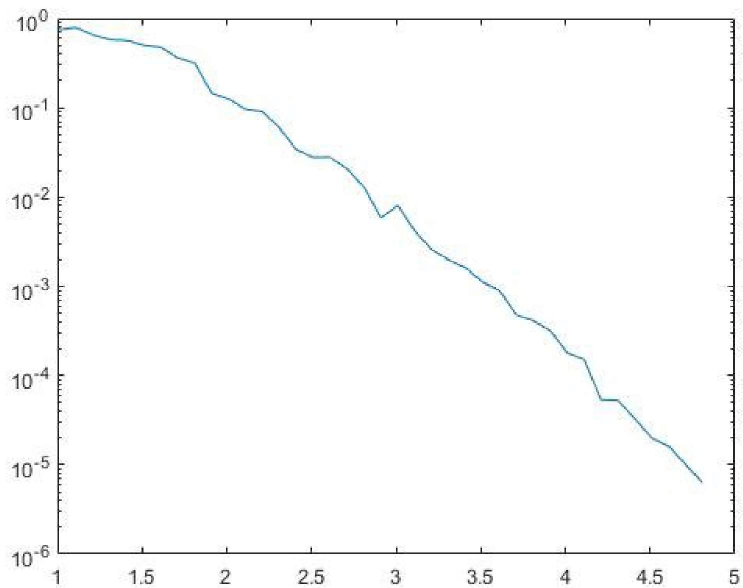


Figure 4: Margulis code with q=7 with parameters [672, 336], generators of order 4,7

# References

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

[2] P. O. Vontobel J. Rosenthal, *Constructions of regular and irregular LDPC codes using Ramanujan graphs and ideas from Margulis*, Proceedings IEEE International Symposium on Information Theory (IEEE Cat. No.01CH37252) **1** (2001).

[3] Michael S. Postol David J.C. MacKay, *Weaknesses of Margulis and Ramanujan-Margulis Low-Density Parity-Check Codes*, Electronic Notes in Theoretical Computer Science **74** (2003).

[4] Jun Xu Heng Tang S. Lin and K. A. S. Abdel-Ghaffar, *Codes on finite geometries*, IEEE Transactions on Information Theory **51** (2005).

[5] Amin Shokrollahi, *LDPC Codes: An Introduction*, 2003.