Constructions of Regular and Irregular LDPC Codes Using Ramanujan Graphs and Ideas from Margulis

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

Pascal O. Vontobel[2]
Lab. for Signal and Inform. Proc.
EE Deptartment, ETH Zurich
Sternwartstr. 7, CH-8092 Zurich
e-mail: vontobel@isi.ee.ethz.ch

Abstract — **Some twenty years ago Margulis [1] proposed an algebraic construction of LDPC codes. In this paper we mimick the construction of Margulis and we describe a method for algebraically constructing regular and irregular LDPC codes.**

I. Introduction

For the construction of Tanner graphs of codes which are decoded iteratively there are several rules of thumb for getting good decoding performance. One of them is that the girth should be large (or that the graph has a good local-girth distribution) so as to assure the independence of the messages as long as possible. Furthermore, the graphs should have irregular degrees as proposed in [2].

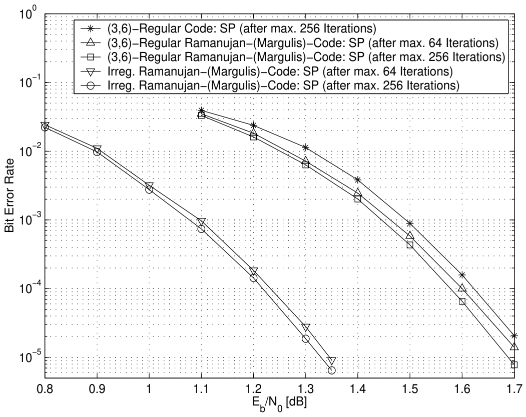
II. Cayley and Expander Graphs

Lubotzky, Phillips and Sarnak [3] found a special class of expander graphs which have several execeptional properties, among others they have high girth. Based on other principles, Margulis [4] independently found nearly the same class of graphs.

First we describe directed Cayley graphs which are defined by specifying a group $\mathcal{G}$ and a subset $\mathcal{S} \subseteq \mathcal{G}$ of generators. A directed graph is then built in the following way: there are $|\mathcal{G}|$ vertices and to each vertex we associate a group element g_i; there is a directed edge from vertex g_i to vertex g_j if and only if there is an $s \in \mathcal{S}$ such that $g_j = g_i \cdot s$. Let $\mathrm{GL}_2(q)$ be the general linear group of all invertible 2×2-matrices with elements from $\mathrm{GF}(q)$. The projective general linear group $\mathrm{PGL}_2(q)$ is $\mathrm{GL}_2(q)$ modulo non-zero multiples of the identity matrix. For odd q's the projective special linear group $\mathrm{PSL}_2(q)$ finally is an index-2 subgroup of $\mathrm{PGL}_2(q)$. The class of graphs defined by LPS/Margulis are Cayley graphs parametrized by q and p which must be primes and equal 1 modulo 4. If p is a quadratic non-residue modulo q then the underlying group is $\mathrm{PGL}_2(q)$ and the number of vertices is $q(q^2-1)$, otherwise it is $\mathrm{PSL}_2(q)$ and the number of vertices is $q(q^2-1)/2$. In both cases, the set $\mathcal{S}$ consists of $p+1$ generators. The resulting graphs are called Ramanujan graphs because the second largest of the eigenvalues (in absolute value) of the adjacency matrix is below a certain bound. Among other special properties, the girth of the corresponding undirected Cayley graph is lower bounded by $4\log_p(q) - \log_p(4)$ (which is above the Erdős-Sachs bound) in the first case and by $2\log_p(q)$ in the second case.

III. Construction of Codes

Inspired by a code construction of Margulis [1], we now discuss the construction of a binary rate-1/2 code of length $q(q^2-1)$ with irregular degrees. To this end, let p be a quadratic residue in $\mathrm{GF}(q)$, so the underlying group is $\mathrm{PSL}_2(q)$. We build a Tanner graph in the following way: the check vertices are a copy of $\mathrm{PSL}_2(q)$ and the bits are two copies of $\mathrm{PSL}_2(q)$. To each bit g_i node we associate a set $\mathcal{S}_{g_i} \subseteq \mathcal{S}$ of generators which specify to which check node the bit is connected. The sizes of the sets $\mathcal{S}_{g_i}$ were chosen so as to finally match approximately the bit and check degree percentages as given in [2]. With the additional constraint that the subsets $\mathcal{S}_{g_i}$'s of the first copy must contain different elements than the subsets $\mathcal{S}_{g_i}$'s in the second copy, the girth cannot be smaller than the girth in the original (undirected) Cayley graph. A possibility to specify the subsets $\mathcal{S}_{g_i}$ of generators is to subdivide the elements of $\mathrm{PSL}_2(q)$ in $q+1$ classes. For this we view the first row of a matrix in $\mathrm{PSL}_2(q)$ as a point in $\mathbb{P}^1_{\mathrm{GF}(q)}$. Apart from this, it was taken care that the degree-two bit nodes did not form a loop. Similar constructions can be done if p is a quadratic nonresidue in $\mathrm{GF}(q)$ or if one desires different rates. The figure shows bit error rates for the following codes, which are all of length 4896 and have designed rate 1/2: a randomly generated $(3,6)$-regular code, a $(3,6)$-regular code (with 26 redudant rows in the parity-check matrix) as presented in [5] and an irregular code with maximal bit degree 11.



References

[1] G. A. Margulis, "Explicit Constructions of Graphs Without Short Cycles and Low Density Codes," *Combinatorica*, vol. 2, no. 1, pp. 71–78, 1982.

[2] T. Richardson, A. Shokrollahi, and R. Urbanke, "Design of Capacity-Approaching Irregular Low-Density Parity-Check Codes," *IEEE Trans. Inform. Theory*, vol 47, no. 2, pp. 619–639, 2001.

[3] A. Lubotzky, R. Phillips, and P. Sarnak, "Ramanujan Graphs," *Combinatorica*, vol. 8, no. 3, pp. 261–277, 1988.

[4] G. A. Margulis, "Explicit Group-Theoretic Constructions of Combinatorial Schemes and Their Applications in the Construction of Expanders and Concentrators," *Problemy Peredachi Informatsii*, vol. 24, no. 1, pp. 51–60, 1988.

[5] J. Rosenthal and P. O. Vontobel, "Constructions of LDPC Codes Using Ramanujan graphs and Ideas from Margulis," in *Proc. of the 38-th Allerton Conference on Communication, Control, and Computing*, pp. 248–257, 2000.

[1]This work was supported by NSF Grant No. DMS-00-72383.
[2]This work was supported by Grant TH-16./99-3.