Spectral Techniques for Expander Codes and Generalized Cyclic Codes

John D. Lafferty[1]
School of Computer Science
Carnegie Mellon University
Pittsburgh, PA 15213 USA

Daniel N. Rockmore[2]
Department of Mathematics
Dartmouth College
Hanover, NH 03755 USA

Abstract — **We show that spectral techniques can be used to encode the explicit expander codes recently constructed by Sipser and Spielman. These codes can be viewed as generalized cyclic codes for certain nonabelian groups. Many of the classical spectral techniques for cyclic codes extend to this general setting.**

I. Introduction

This paper shows how generalized Fourier analysis can be used for working with a class of error-correcting codes constructed in terms of Cayley graphs. Our investigations are motivated by recent work [4] that revisits the low-density parity-check codes first studied by Gallager and the recursive codes investigated by Tanner, and shows that the expansion properties of the underlying graphs are essential for efficient decoding. Using explicit or random constructions of expanders, this work yields asymptotically good families of codes that can be decoded in linear time. While expander codes can be efficiently decoded, the only previously known encoding algorithm for them was the quadratic algorithm available for all linear codes. Since the codes are attractive primarily for large block lengths, the quadratic encoding cost appears to make them impractical for applications. However, the methods of [4] only use the expansion properties of the explicit constructions. These graphs have additional structure since they are Cayley graphs of certain nonabelian groups. We show that the symmetry of these graphs can be exploited by using the representation theory of the underlying group to devise an encoding algorithm that requires $O(n^{4/3})$ operations, where n is the block length.

II. Generalized Cyclic Codes

A cyclic code of block length n over a finite field $\mathbf{F}$ is a linear subspace $\mathcal{C} \subset \mathbf{F}^n$ that is closed under cyclic shift. Replacing the cyclic group $\mathbf{Z}/n\mathbf{Z}$ with an arbitrary finite group G, and assuming that the characteristic of $\mathbf{F}$ does not divide the order of the group, the natural definition of a *generalized cyclic code* $\mathcal{C}$ is a collection of G-invariant functions $c : G \to \mathbf{F}$. Thus, if $c \in \mathcal{C}$ then $g \cdot c \in \mathcal{C}$ for each $g \in G$, where $g \cdot c\,(h) \equiv c(g^{-1}h)$. If we require that $\mathcal{C}$ forms a linear subspace, then the generalized cyclic codes for G are just the left ideals in the group algebra $\mathbf{F}G$.

The idea that it might be profitable to consider codes that are defined to be invariant under a group of symmetries other than $\mathbf{Z}/n\mathbf{Z}$ is an old one. MacWilliams [2] refers to a suggestion of Gleason that such codes be considered, and proceeds to make the basic definitions and consider the example of the dihedral group. Tanner [5] shows that transform methods similar to those for cyclic codes can be applied to groups more general than $\mathbf{Z}/n\mathbf{Z}$, but strong restrictions are made to ensure that BCH decoding algorithms can be used. In this paper we show how basic spectral techniques apply to certain expander codes in a manner that is parallel to the use of the fast Fourier transform for the cyclic group.

Given a representation η of a finite group G and a function $f : G \longrightarrow \mathbf{F}$, the *Fourier transform of f at η* is the $d_\eta \times d_\eta$ matrix $\hat{f}(\eta) = \sum_{x \in G} f(x)\eta(x)$. The Fourier transforms at a complete set of inequivalent irreducible representations determine f via the *Fourier inversion formula*; see [3]. When the parity-check conditions of a code are given by convolution $c \star h = 0$, these equations can be solved as matrix equations $\hat{c}(\eta)\hat{h}(\eta) = \mathbf{0}$ in the spectral domain, and the (nonsystematic) codeword is then obtained after taking an inverse Fourier transform. The conjugacy constraints on the spectrum that force the codeword to lie in the base field $\mathbf{F}$ parallel those for the cyclic group. Similarly, the fact that classical cyclic codes are generated by idempotent polynomials generalizes naturally for nonabelian groups; a generalized cyclic code is generated by a group algebra element with Fourier transforms given by idempotent matrices.

III. Codes on $PSL_2(q)$

The explicit expander codes of [4] are constructed using Cayley graphs of the projective special linear group $PSL_2(q)$ of 2×2 matrices (mod $\pm I$) with determinant one over the finite field $\mathbf{F}_q$. In order to obtain a lower bound on the rate of the code, the codewords are constructed as $\mathbf{F}$-valued functions on the edges, rather than the vertices, but a minor variation on the spectral encoding procedure suggested above applies. The paper [1] presents an algorithm for performing Fourier analysis on $PSL_2(q)$ using at most $O(n^{4/3}\log n)$ operations, for $n = |PSL_2(q)| = O(q^3)$. This is reduced to $O(n^{4/3})$ operations in [3]. The calculations of [1] indicate that random Cayley graphs for this group have good expansion properties. Furthermore, the expansion can be evaluated in time $O(n^{4/3})$ using Fourier analysis. The use of random Cayley graphs for this group relaxes the constraints on block length and subcode length imposed by the explicit constructions.

References

[1] J. Lafferty and D. Rockmore. Fast Fourier analysis for SL_2 over a finite field and related numerical experiments. *Experimental Mathematics*, Vol. 1, No. 2, 1992, pp. 115–139.

[2] F.J. MacWilliams. Codes and ideals in group algebras. In R.C. Bose and T.A. Dowling, editors, *Combinatorial Mathematics and its Applications*, pages 317–328. University of North Carolina Press, Chapel Hill, 1969.

[3] D. Maslen and D. Rockmore. Separation of variables and the computation of Fourier transforms on finite groups, I. *J. of the Amer. Math. Soc.*, **10**, No. 1, 1997, pp. 169–214.

[4] M. Sipser and D. Spielman. Expander codes. *IEEE Trans. on Information Theory*, Vol. 42, No. 6, November 1996, pp. 1710–1722.

[5] R. M. Tanner. A transform theory for a class of group-invariant codes. *IEEE Trans. on Information Theory*, Vo. 34, No. 4, July, 1988, pp. 752–775.

[1] Supported in part by NSF grant IRI-9314969.
[2] Supported in part by NSF PFF award, grant DMS-9553134.