Spectral Techniques for Expander Codes

John D. Lafferty* Daniel N. Rockmore†

Abstract

This paper introduces methods based on generalized Fourier analysis for working with a class of error-correcting codes constructed in terms of Cayley graphs. Our work is motivated by the recent results of Sipser and Spielman [15] showing graph expansion to be essential for efficient decoding of certain low-density parity-check codes. They leave open the problem of sub-quadratic encoding for this class of codes, and it is this problem that we address. We show that when the codes are constructed in terms of Cayley graphs, the symmetry of the graphs can be exploited by using the representation theory of the underlying group to devise a sub-quadratic encoding algorithm that, in the case where the group is $\mathrm{PSL}_2(\mathbb{Z}/q\mathbb{Z})$*, requires* $O(n^{4/3})$ *operations, where* $n = O(q^3)$ *is the block length. Our results indicate that this new class of codes may combine many of the strengths of two of the most powerful and successful, but previously disparate areas of coding theory: the class of cyclic codes where the rich algebraic structure yields a large collection of techniques for finding and manipulating the codes, and the class of low-density parity-check codes which have simple and efficient decoding algorithms and good asymptotic properties.*

1 Introduction

This paper is concerned with a class of codes that can be viewed as generalized cyclic codes, in the sense that the code is defined to be invariant under a group of translations. Our investigations are motivated by the recent work of Sipser and Spielman [15] that revisits the low-density parity-check codes first introduced by Gallager [4] and the recursive codes investigated by Tanner [18], and shows that the expansion properties of the underlying graphs are essential for efficient decoding. Using explicit or random constructions of expanders, the results of [15] yield asymptotically good families of codes that can be decoded in linear time (in the *uniform cost model*; see [15]). The results of [16] go further and construct both linear time encodable and decodable codes by combining expander codes with encoding circuits based on superconcentrators; however the resulting codes have much weaker error correction properties.

While expander codes can be efficiently decoded, the only known encoding algorithm for them is the quadratic algorithm available for all linear block codes: reduce the parity-check matrix to a systematic form, and encode using matrix multiplication. Since these codes are attractive primarily for large block lengths, the quadratic encoding cost appears to make them impractical for many applications. The methods of [15], however, use only the expansion properties of the explicit constructions. These graphs have additional structure since they are Cayley graphs of certain nonabelian groups. We show how the symmetry of these graphs can be exploited by using the representation theory of the underlying group G to devise an encoding algorithm that requires $O(n^{3/2})$ operations in general, and $O(n^{4/3})$ operations when $G = PSL_2(\mathbb{Z}/q\mathbb{Z})$, where $n = O(|G|)$ is the block length.[1] Further reductions in complexity may be possible with continued improvements in algorithms for nonabelian FFTs.

This encoder is nonsystematic, however we also explain how a systematic encoder can be obtained using similar methods, but at the expense of an asymptotically vanishing loss in rate. In addition, we show that for $G = PSL_2(\mathbb{Z}/q\mathbb{Z})$, the constraints coming from certain representations of the group correspond to expander codes of smaller block length in the spectral domain. Using the tools of representation theory of finite groups,

*Department of Computer Science, Carnegie Mellon University. E-mail: lafferty@cs.cmu.edu. Supported in part by NSF grant IRI-9314969.

†Departments of Mathematics and Computer Science, Dartmouth College. E-mail: rockmore@cs.dartmouth.edu. Supported in part by NSF PFF award, grant DMS-9553134.

[1] Recall that $SL_2(\mathbb{Z}/q\mathbb{Z})$ is the *special linear group* of 2×2 matrices of determinant one having entries from the finite field $\mathbb{F}_q$ of q elements. The *projective special linear group* $PSL_2(\mathbb{Z}/q\mathbb{Z})$ is obtained by dividing $SL_2(\mathbb{Z}/q\mathbb{Z})$ by its center, $\{\pm I\}$ where I is the 2×2 identity matrix, and is a simple finite group of Lie type (for $q \geq 5$). The group $PSL_2(\mathbb{Z}/q\mathbb{Z})$ has been a part of coding theory for quite some time; in fact, it arises as the automorphism group of certain quadratic residue codes [10].

we are able to transform the parity-check conditions into a block-diagonal form, with each block corresponding to an irreducible representation. These spectral expander codes emerge after choosing suitable bases for the representations.

The group $PSL_2(\mathbb{Z}/q\mathbb{Z})$ is central to our work because explicit expander codes can be constructed using the explicit Ramanujan graphs that are known for this group, and our previous work [6] indicates that random Cayley graphs for this group are good expanders. The use of random Cayley graphs—that is, graphs constructed by choosing random generators for the group—removes some of the restrictions on block length and subcode size that the explicit codes impose. As we showed in [5], the expansion of a Cayley graph can be estimated efficiently by using Fourier analysis to calculate its spectrum.

The spectral methods that we present here for this new class of *low-density Cayley codes* can be seen as generalized versions of spectral techniques for classical cyclic codes. Our results, which make the first significant use of nonabelian Fourier analysis in coding, suggest that expander codes based on groups may combine many of the strengths of cyclic codes, for which the algebraic structure yields a powerful collection of techniques for finding and manipulating the codes, with those of the low-density parity-check codes, which are known to have simple and efficient decoding algorithms and good asymptotic properties.

2 Background

In this section we briefly review spectral techniques for classical codes, the essential elements of generalized Fourier analysis and the constructions of expander codes.

2.1 Classical spectral techniques

Many of the fundamental algorithms for classical cyclic codes have both "time domain" and "frequency domain" versions. These algorithms often have similar complexities, but Fourier analysis can sometimes be used to obtain more efficient algorithms, and the intuition developed in the frequency domain is often quite powerful. An instructive example is the proof of the BCH bound using Fourier analysis [3].

It will be useful to recall the basic spectral techniques, since our generalized methods parallel them. Let $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{F}_l$ be a function on the cyclic group of order n, taking values in the finite field $\mathbb{F}_l$ of l elements, where $n = l^m - 1$ for some m. Fixing a primitive element α of the finite field $\mathbb{F}_{l^m}$, the *Fourier transform* of f is the function $\widehat{f} : \mathbb{Z}/n\mathbb{Z} \to \mathbb{F}_{l^m}$ defined by

$$\widehat{f}(j) = \sum_{i=0}^{n-1} \alpha^{ij} f(i) ,$$

and the *Fourier inversion formula* then takes the form

$$f(i) = \frac{1}{n} \sum_{j=0}^{n-1} \alpha^{-ij} \widehat{f}(j) .$$

The duality between the frequency domain and time domain pictures is characterized by the *convolution theorem*, which shows that convolution in one domain is taken to a product in the other. That is, if

$$f \star g(i) = \sum_{j=0}^{n-1} f(j)\, g(i-j) ,$$

then

$$\widehat{f \star g}(j) = \widehat{f}(j)\, \widehat{g}(j) \quad j = 0, \ldots, n-1$$

and similarly, if we define $\widehat{h}(j)$ by

$$\widehat{h}(j) = \sum_{k=0}^{n-1} \widehat{f}(k)\, \widehat{g}(k-j) ,$$

then $h(i) = f(i)g(i)$ for $i = 0, \ldots n-1$. This fact is the basis for several spectral algorithms. In particular, one decoding algorithm for BCH codes computes the syndromes as spectral components, and applies the Berlekamp-Massey algorithm to the natural convolution equation in the frequency domain. On the level of groups, this takes advantage of the isomorphism between an abelian group and its dual, which is not available for nonabelian groups.

Fourier analysis is fundamental to the manipulation and study of cyclic codes. Multiplication in the ring $\mathbb{F}_l[x]/(x^n - 1)$ can be viewed as convolution of functions on $\mathbb{Z}/n\mathbb{Z}$, or equivalently, as multiplication in the group algebra $\mathbb{F}_l\mathbb{Z}/n\mathbb{Z}$. Thus, if $g(x)$ is the generator polynomial of the code, then a data polynomial $d(x)$ is encoded nonsystematically as

$$c(i) = \sum_{k=0}^{n-1} g(k)\, d(i-k) .$$

Taking Fourier transforms, this is expressed in the frequency domain as

$$\widehat{c}(j) = \widehat{g}(j)\, \widehat{d}(j), \quad j = 0, \ldots, n-1 .$$

Since any vector satisfying this expression is a codeword, and the spectrum of the data is arbitrary, the only constraints are that the spectrum of c must be zero at certain frequencies, provided that the inverse Fourier transform is an $\mathbb{F}_l$-valued function. In spectral terms, a t-error correcting BCH code is obtained by constraining $2t$ *consecutive* frequencies to zero, and a Reed-Solomon code is a BCH code for which the block length n is equal to $l-1$. The spectral encoding algorithm is particularly simple in this case. After setting the specified $2t$ frequencies of the code to zero, the data values (elements of $\mathbb{F}_l$) are placed in the remaining $n-2t$ frequencies, and we take an inverse Fourier transform to obtain a non-systematic codeword. For more general cyclic codes, conjugacy constraints must be imposed to ensure that the codeword lies in $\mathbb{F}_l^n$. These conditions will be generalized in Section 3.1.

2.2 Fourier analysis for finite groups

In this section we recall the necessary basics from representation theory. We will denote the group algebra of a finite group G over a field $\mathbb{F}$ as $\mathbb{F}G$. Recall that this is the vector space of formal $\mathbb{F}$-linear combinations $\sum_{x\in G} a_x x$ $(a_x \in \mathbb{F})$ with the multiplication given by extending the group multiplication. There is a natural 1:1 correspondence between $\mathbb{F}$-valued functions on the group and elements of $\mathbb{F}G$. The codes that we will consider can be viewed as left ideals in the group algebra.

Let $\overline{\mathbb{F}}$ be a finite extension of the base field $\mathbb{F}$. A representation η of G over $\overline{\mathbb{F}}$ is a map $\eta : G \longrightarrow GL_{d_\eta}(\overline{\mathbb{F}})$ such that $\eta(xy) = \eta(x)\,\eta(y)$ for all $x, y \in G$. Given a representation η of G and a function $f : G \longrightarrow \mathbb{F}$, the *Fourier transform of* f *at* η is the $d_\eta \times d_\eta$ matrix

$$\widehat{f}(\eta) = \sum_{x\in G} f(x)\,\eta(x).$$

The scalar sums $\widehat{f}(\eta_{ij}) = \sum_{x\in G} f(x)\,\eta_{ij}(x)$ are Fourier transforms of f at the *matrix coefficients* η_{ij}.

To simplify things we assume that we are working over an extension field $\overline{\mathbb{F}}$ of characteristic that does not divide the order of the group. The Fourier transforms at a complete set of inequivalent irreducible representations of G then accomplish a change of basis in the group algebra from the basis of delta functions to a basis of irreducible matrix coefficients, which we will denote as $\widehat{G}$. As a consequence, the dimensions of the irreducible representations satisfy $|G| = \sum_{\eta\in\widehat{G}} d_\eta^2$. The inverse map may be presented as the *Fourier inversion formula*

$$f(x) = \frac{1}{|G|}\sum_{\eta\in\widehat{G}} d_\eta\, trace\left(\widehat{f}(\eta)\,\eta(x^{-1})\right).$$

Notice that since the characteristic of $\mathbb{F}$ does not divide $|G|$, this formula makes sense. In general the relation between (matrix) Fourier transforms and convolution is given by

$$\widehat{f \star h}(\eta) = \widehat{f}(\eta)\cdot\widehat{h}(\eta)$$

where convolution over G is defined by

$$f \star h(x) = \sum_{s\in G} f(s)\,h(s^{-1}x).$$

When $G = \mathbb{Z}/n\mathbb{Z}$, this is all recognizable as the usual discrete Fourier transform and its inverse, and their relation to circular convolution. In this case the Cooley-Tukey FFT and its variants give fast algorithms for accomplishing the relevant computations. For arbitrary G, in many cases fast algorithms still exist, and in particular, for the projective special linear group $PSL_2(\mathbb{Z}/q\mathbb{Z})$, recent work shows that we can accomplish both forward and inverse Fourier transforms in $O(q^4)$ operations [12]. We use a standard computational model in which a single multiplication and addition over $\mathbb{F}$ has unit cost.

2.3 Expanders and Cayley codes

The construction of *expander codes* in [15] uses the same basic approach as [18], and results in a class of codes closely related to Gallager's low-density parity-check codes [4]. In order to obtain an easy lower bound on the rate of the code using only simple properties of the graph, this construction uses an unbalanced bipartite graph $\Gamma_{n,c,d}$ that is c-regular on one side and d-regular on the other, with $c < d$, and a subcode $\mathcal{S}_d$ of block length d over a finite field $\mathbb{F}$. (Sipser and Spielman use only the binary field, but the constructions and results easily generalize. Our results, however, do not depend on generalizations of their analysis of the decoding algorithms.) The code $\mathcal{C}(\Gamma_{n,c,d}, \mathcal{S}_d)$ is the collection of $\mathbb{F}$-valued functions on the c-regular vertices such that the neighbors of each of the d-regular vertices form a subcode word (with respect to a specified ordering of the neighbors). The following theorem is a simple consequence of the definition of expansion [15].

Theorem 1 *Let $\Gamma_{n,c,d}$ be a (c,d)-regular bipartite on n vertices, with $c < d$, and let $\mathcal{S}_d$ be an error-correcting code of block length d, with relative minimum distance ϵ and rate r. The rate of the graph code $\mathcal{C}(\Gamma_{n,c,d}, \mathcal{S}_d)$ is at least $c(r-1)+1$. If $\Gamma_{n,c,d}$ expands by a factor of $e \geq c/d\epsilon$ on all sets of vertices of size at most αn, then $\mathcal{C}(\Gamma_{n,c,d}, \mathcal{S}_d)$ has relative minimum distance at least α.*

Roughly speaking, Sipser and Spielman extend this result to prove that if the graph Γ is a sufficiently good expander and the subcode $\mathcal{S}$ is a sufficiently good code, then the code $\mathcal{C}(\Gamma, \mathcal{S})$ is good, and that a constant fraction of errors can be decoded in linear time. The decoding algorithm is very simple and natural, but we will not need to discuss it here.

2.4 Codes from Cayley graphs

When the underlying graph is a Cayley graph, the code has additional structure, as we now explain. Let G be a finite group and let $\mathcal{A} = \{s_1, s_2, \ldots, s_d\} \subset G$ be a symmetric set of ordered generators; thus, if $s \in \mathcal{A}$, then

$s^{-1} \in \mathcal{A}$. The *Cayley graph* $\Gamma(G, \mathcal{A})$ of G with respect to $\mathcal{A}$ is the d-regular graph having vertices indexed by G such that (g, h) is an edge if and only if $h = s^{-1}g$ for some $s \in \mathcal{A}$. This determines a canonical ordering on the neighbors of a vertex g: $x_i(g) = s_i^{-1}g$, for $i = 1, 2, \ldots, d$.

Definition 2 *Let $\mathcal{S}$ be an error-correcting code over $\mathbb{F}$ with block length d. The* ***Cayley vertex code*** *$\mathcal{C}_{\mathcal{V}}(G, \mathcal{A}, \mathcal{S})$ is the subspace of all functions $c : G \to \mathbb{F}$ such that for each $g \in G$,*

$$(c_1(g), c_2(g), \ldots, c_d(g)) \in \mathcal{S}\,, \tag{1}$$

where $c_i(g) = c(s_i^{-1}g)$. Similarly, the ***Cayley edge code*** *$\mathcal{C}_{\mathcal{E}}(G, \mathcal{A}, \mathcal{S})$ is the subspace of all edge functions $c : \mathcal{E}\Gamma(G, \mathcal{A}) \to \mathbb{F}$ that satisfy (1), but with $c_i(g) = c((g, s_i^{-1}g))$. This corresponds to a code $\mathcal{C}(\Gamma_{n,2,d}, \mathcal{S})$, where $\Gamma_{n,2,d}$ is the bipartite graph formed by inserting a new vertex on each edge. If $|\mathcal{A}|$ is small relative to G, then the parity check matrices of these codes are sparse. We will refer to such codes as* ***low-density Cayley codes****.*

Thus, a Cayley code is constructed using only the graph $\Gamma(G, \mathcal{A})$, but it inherits symmetries from the group. All of the classical cyclic codes are Cayley vertex codes, where the group G is $\mathbb{Z}/n\mathbb{Z}$, the subcode is a simple parity check, and the fundamental theorem of algebra can be used to design codes having various rates and distances. As will be evident, our methods apply to both vertex codes $\mathcal{C}_{\mathcal{V}}(G, \mathcal{A}, \mathcal{S})$ and edge codes $\mathcal{C}_{\mathcal{E}}(G, \mathcal{A}, \mathcal{S})$.

The explicit expander codes of [15] are constructed using Cayley graphs of the projective special linear group. The graphs used are the explicit family of expander graphs (the so-called *Ramanujan graphs*) constructed by Lubotzky, Phillips, and Sarnak [8], and independently by Margulis [11]. These graphs are $(p+1)$-regular graphs, where is p is a prime that is not a quadratic residue modulo q. Since $|PSL_2(\mathbb{Z}/q\mathbb{Z})| = q(q^2-1)/2$, this results in codes with block length $n = (p+1)q(q^2-1)/4 = O(q^3)$ considering $p = O(1)$ as $q \to \infty$.

The significance of Fourier analysis lies in the following link. Let $\delta_{\mathcal{A}}$ be the characteristic function of the generating set $\mathcal{A}$. Then it immediately follows that the adjacency matrix of $\Gamma(G, \mathcal{A})$ is equal to the Fourier transform $\widehat{\delta_{\mathcal{A}}}(\rho_{reg})$, up to a reordering of the group elements, where ρ_{reg} denotes the right regular representation of G. Block diagonalization of the regular representation may be obtained using representation theory. Thus, if $\{\rho_1, \ldots, \rho_h\}$ is a complete set of inequivalent irreducible matrix representations of G, then there exists a change of basis such that

$$\widehat{\delta_{\mathcal{A}}}(\rho_{reg}) \sim \begin{pmatrix} B_1 & 0 & \cdots & 0 \\ 0 & B_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & B_h \end{pmatrix}$$

where

$$B_i = \begin{pmatrix} \widehat{\delta_{\mathcal{A}}}(\rho_i) & 0 & \cdots & 0 \\ 0 & \widehat{\delta_{\mathcal{A}}}(\rho_i) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \widehat{\delta_{\mathcal{A}}}(\rho_i) \end{pmatrix}$$

with d_{ρ_i} copies of $\widehat{\delta_{\mathcal{A}}}(\rho_i)$ on the diagonal. In particular,

$$\mathit{spectrum}\,(\Gamma(G, \mathcal{A})) = \bigcup_{i=1}^{h} \mathit{spectrum}\left(\widehat{\delta_{\mathcal{A}}}(\rho_i)\right)\,.$$

This is the basic fact that we used in [5, 6] to investigate expanders for this group, and it is also the key idea behind our use of spectral methods for codes.

If $h : G \to \mathbb{F}$ corresponds to a row of the parity-check matrix for the subcode $\mathcal{S}$, then $c \in \mathbb{F}G$ is a codeword of the vertex code if and only if for each $g \in G$,

$$h \star c(g) = \sum_{s \in G} h(s)\, c(s^{-1}g) = 0\,.$$

Taking Fourier transforms, this is cast in the spectral domain as

$$\widehat{h \star c}(\rho) = \widehat{h}(\rho) \cdot \widehat{c}(\rho) = 0_{d_\rho \times d_\rho}$$

for each $\rho \in \widehat{G}$. In other words, each column of $\widehat{c}(\rho)$ must be a spectral domain codeword for the parity-check matrix $\widehat{h}(\rho)$ over $\overline{\mathbb{F}}$.

3 Spectral Encoding

3.1 Conjugacy constraints

We first consider the issue of *conjugacy constraints* in a general group algebra. Suppose that we wish to specify an element of $\mathbb{F}_l G$ in terms of its spectrum. Because the Fourier transforms $\widehat{f}(\eta)$ take on values in an extension field $\overline{\mathbb{F}} \supset \mathbb{F}_l$, specifying these coefficients and then taking an inverse Fourier transform is not guaranteed to result in an element $f \in \mathbb{F}_l G \subset \overline{\mathbb{F}}G$. There are constraints on its spectrum analogous to those for Fourier transforms over the complex numbers.

Theorem 3 *Suppose that $\overline{\mathbb{F}}$ has characteristic π dividing l. Let $\{\widehat{f}(\eta_{ij}) \in \overline{\mathbb{F}}\}_{\eta \in \widehat{G}}$ be matrices of spectral coefficients. Then the inverse Fourier transform f is an element of $\mathbb{F}_l G$ if and only if for each $\eta \in \widehat{G}$,*

$$\widehat{f}^{\,l}(\eta_{ij}) = \widehat{f}(\eta_{ij}^{(l)}) \tag{2}$$

where $\eta^{(l)}$ is the representation defined by $\eta^{(l)}(x) = \eta(x)^l$.

Proof: First notice that the matrix coefficients given by $\eta_{ij}^{(l)}(x) = \eta_{ij}^l(x)$ define a representation $\eta^{(l)}$ precisely because $\overline{\mathbb{F}}$ has characteristic π dividing l. This l^{th} power map is also called the Frobenius automorphism of $\overline{\mathbb{F}}$, and the cyclic group it generates thereby acts upon the $\overline{\mathbb{F}}$-valued irreducible representations of G, breaking them up into orbits. Following the standard coding theory terminology we call these orbits the *chords* of G, and denote them $\widehat{G}_i$. Thus, $\widehat{G} = \coprod_i \widehat{G}_i$, where

$$\widehat{G}_i = \left\{\eta_i, \eta_i^{(l)}, \eta_i^{(l^2)}, \ldots, \eta_i^{(l^{m_i})}\right\} \tag{3}$$

for some m_i depending on i.

Now, if $f \in \mathbb{F}_l G$, then

$$\begin{aligned} \widehat{f}^{\,l}(\eta_{ij}) &= \left(\sum_x f(x)\,\eta_{ij}(x)\right)^l \\ &= \sum_x f(x)\,\eta_{ij}(x)^l \\ &= \widehat{f}(\eta_{ij}^{(l)})\,. \end{aligned}$$

Conversely, if $\widehat{f}$ is constant on each chord $\widehat{G}_i$, then applying the Fourier inversion formula,

$$\begin{aligned} f(x)^l &= \frac{1}{|G|}\sum_{\eta\in\widehat{G}} d_\eta\, trace^l\left(\eta(x^{-1})\,\widehat{f}(\eta)\right) \\ &= \frac{1}{|G|}\sum_{\eta\in\widehat{G}} d_\eta\, trace\left(\eta^{(l)}(x^{-1})\,\widehat{f}(\eta^{(l)})\right) \\ &= f(x)\,, \end{aligned}$$

so that $f \in \mathbb{F}_l G$. $\square$

The usual situation in classical coding theory is that $G = \mathbb{Z}/n\mathbb{Z}$, so the irreducible representations are the characters α_j. In this case we have $\alpha_j^{(l)}(x^k) = \alpha^{ljk}$, with α a primitive element of $\mathbb{F}_{l^m}^*$, so that $\alpha_j^{(l)} = \alpha_{lj}$. The chords are then of the form $\widehat{G}_j = \{\alpha_j, \alpha_{lj}, \ldots, \alpha_{l^{n_j}j}\}$ for some n_j and the conjugacy constraints on a codeword $c(x)$ become $\widehat{c}(j) = \widehat{c}(lj) = \cdots = \widehat{c}(l^{r-1}j)$. Notice that $\widehat{G}_j$ and $\widehat{G}_{-j}$ are in 1:1 correspondence. Thus, if we restrict ourselves to indices j with $0 \le j \le (n-1)/2$, then we have chords $\widehat{G}_0, \widehat{G}_1, ..., \widehat{G}_\ell, \widehat{G}_{-1}, ..., \widehat{G}_{-\ell}$ for some ℓ.

3.2 The algorithm

We will now describe the encoding algorithm in some detail for Cayley edge codes since the results of [15] are obtained for this class. We fix a Cayley graph $\Gamma = \Gamma(G, \mathcal{A})$. For an edge function $f \in \mathcal{E}\Gamma(\mathbb{F})$, we will let $f^{(i)} : G \to \mathbb{F}$ denote the function $f^{(i)}(g) = f((g, s_i^{-1}g))$. In this notation, an edge function $c \in \mathcal{E}\Gamma(\mathbb{F})$ is a codeword of $\mathcal{C}(G, \mathcal{A}, \mathcal{S})$ if and only if

$$\left(c^{(1)}(g), c^{(2)}(g), \ldots, c^{(d)}(g)\right) \in \mathcal{S} \quad \text{for each } g \in G\,. \tag{4}$$

There are relations on the functions $c^{(i)}$ because the edges are unoriented. The following lemma shows how these relations are expressed in the spectral domain. Its proof entails a simple calculation using the homomorphism property of ρ and the Fourier inversion formula.

Lemma 4 *An element $c \in \mathcal{E}\Gamma(\mathbb{F})$ is a codeword of $\mathcal{C}(G, \mathcal{A}, \mathcal{S})$ if and only if for each $\rho \in \widehat{G}$, $1 \le i, j \le d_\rho$, and $1 \le k \le d$,*

(a) $\left(\widehat{c^{(1)}}(\rho_{ij}), \widehat{c^{(2)}}(\rho_{ij}), \ldots, \widehat{c^{(d)}}(\rho_{ij})\right) \in \overline{\mathcal{S}}$

(b) $\widehat{c^{(k)}}(\rho) = \rho(s_l^{-1})\,\widehat{c^{(l)}}(\rho)$ *where* $s_l = s_k^{-1}$

(c) $\widehat{c^{(k)}}^{\,l}(\rho_{ij}) = \widehat{c^{(k)}}(\rho_{ij}^{(l)})$

where $\overline{\mathcal{S}}$ is the code over $\overline{\mathbb{F}}$ obtained using the parity-check matrix of $\mathcal{S}$.

Proof: If $H = (h_{lm})$ is the parity-check matrix for the subcode $\mathcal{S}$, then taking Fourier transforms of the parity checks

$$\sum_{m=1}^{c} h_{lm} c^{(m)}(g) = 0 \quad g \in G$$

for each $l = 1, \ldots, (1-r)c$ yields equations (a) in the spectral domain. Now suppose that the c_a are defined from an edge function. Then for any representation ρ,

$$\begin{aligned} \widehat{c_{a^{-1}}}(\rho) &= \sum_{g\in G} c_{a^{-1}}(g)\,\rho(g) \\ &= \sum_{g\in G} c_a(a^{-1}g)\,\rho(g) \\ &= \rho(a)\sum_{g\in G} c_a(a^{-1}g)\,\rho(a^{-1}g) \\ &= \rho(a)\,\widehat{c_a}(\rho) \end{aligned}$$

using the homomorphism property of ρ. Conversely, if equations (b) and (c) hold, then by the Fourier inversion formula,

$$\begin{aligned} c_{a^{-1}}(g) &= \frac{1}{|G|}\sum_{\rho\in\widehat{G}} d_\rho trace\left(\rho(g^{-1})\,\widehat{c_{a^{-1}}}(\rho)\right) \\ &= \frac{1}{|G|}\sum_{\rho\in\widehat{G}} d_\rho trace\left(\rho(g^{-1})\,\rho(a)\,\widehat{c_a}(\rho)\right) \\ &= \frac{1}{|G|}\sum_{\rho\in\widehat{G}} d_\rho trace\left(\rho\left((a^{-1}g)^{-1}\right)\,\widehat{c_a}(\rho)\right) \\ &= c_a(a^{-1}g) \end{aligned}$$

so that $c(g, ag) = c_a(g) \in \mathbb{F}$ is well-defined. Equations (c) are the conjugacy constraints of Theorem 3. $\square$

We will refer to (a) as the *spectral subcode constraints*, (b) as the *edge constraints*, and (c) as the *conjugacy constraints*. For a fixed representation ρ, the edge and spectral subcode constraints of Lemma 4 form a linear system over $\overline{\mathbb{F}}$ that can be represented by a $(2-r)dd_\rho \times dd_\rho$ spectral-parity check matrix which we will denote as $\widehat{H}(\rho)$. (A total of $(1-r)dd_\rho$ constraints come from the subcode $\mathcal{S}$.)

Algorithm 5 *(Spectral Encoding)*

Initial Data:

1. *Low-density Cayley code $\mathcal{C}(G, \mathcal{A}, \mathcal{S})$.*
2. *Complete set $\widehat{G}$ of irreducible representations of G.*

Initialization:

1. *Compute the chords $\widehat{G} = \coprod_i \widehat{G}_i$.*
2. *Choose one representation $\rho_i \in \widehat{G}_i$ in each chord, and reduce $\widehat{H}(\rho_i)$ to a systematic form, computing the rank $\widehat{r}_{\rho_i}$ over $\overline{\mathbb{F}}$. The dimension of $\mathcal{C}(G, \mathcal{A}, \mathcal{S})$ is*
$$k = n - [\overline{\mathbb{F}} : \mathbb{F}] \sum_{chords\ i} d_{\rho_i} \widehat{r}_{\rho_i} \,. \tag{5}$$

To encode a vector $x \in \mathbb{F}^k$ as $e(x) \in \mathbb{F}^n$:

1. *For each distinguished $\rho_i \in \widehat{G}_i$, use matrix multiplication by the systematic form of $\widehat{H}(\rho_i)$ to encode the appropriate piece of x as the matrices $\widehat{c^{(1)}}(\rho_i), \ldots, \widehat{c^{(d)}}(\rho_i)$ to satisfy equations (1) and (2) of Lemma 4.*
2. *Copy the matrices $\widehat{c^{(l)}}(\rho)$ to the other elements of the chord.*
3. *Take inverse Fourier transforms to obtain $e(x)$.*

Theorem 6 *Let $e : \mathbb{F}^k \to \mathbb{F}^n$ be the encoding function for the Cayley code $\mathcal{C}(G, \mathcal{A}, \mathbb{F}) \subset \mathbb{F}^n$ given by Algorithm 5, where k is the dimension computed in (5). Then $e(x)$ can be computed in $O(n \max_{\rho \in \widehat{G}} d_\rho) = O(n^{3/2})$ operations. The initialization stage of the algorithm to compute the dimension k of the code and the spectral parity-check matrices $\widehat{H}(\rho)$ requires $O(n^{3/2})$ operations and $O(n)$ space. For the group $\mathrm{PSL}_2(\mathbb{Z}/q\mathbb{Z})$, $e(x)$ can be computed in $O(n^{4/3})$ operations.*

Sketch of proof: The matrix $\widehat{H}(\rho)$ can be reduced to a systematic form in $O(d_\rho^3)$ operations, and multiplying a column of $(\widehat{c^{(1)}}(\rho), \ldots, \widehat{c^{(d)}}(\rho))$ by the resulting matrix requires $O(d_\rho^2)$ operations. Thus, the total cost of encoding in the spectral domain is no more than

$$\sum_{chords\ i} d_{\rho_i}^3 \leq \max_{\rho \in \widehat{G}} d_\rho \sum_{\rho \in \widehat{G}} d_\rho^2 = \max_{\rho \in \widehat{G}} d_\rho \, |G| \leq |G|^{3/2} \ , \tag{6}$$

and we obtain the rough bound stated because the same general bound holds for Fourier inversion. The analysis for the initialization stage is similar.

For the group $PSL_2(\mathbb{Z}/q\mathbb{Z})$, the irreducible representations occur as $O(q)$ matrices of size $O(q)$; see [5]. Thus, the encoding of $\widehat{e}(\rho)$ takes $O(q^4)$ operations, and using the results of [12], we have the same complexity for Fourier inversion. $\square$

This gives a coarse estimate of the complexity of this algorithm for an arbitrary finite group, and an estimate for $PSL_2(\mathbb{Z}/q\mathbb{Z})$ using the latest results for Fourier analysis on this group. Further improvements in FFT algorithms for $PSL_2(\mathbb{Z}/q\mathbb{Z})$ may well lead to a reduced complexity for this algorithm.

3.3 Systematic encoding

The encoding algorithm we have outlined above for Cayley codes is nonsystematic. When used together with the time domain decoding procedure developed in [15], this means that although the codeword $c \in \mathcal{E}\Gamma(\mathbb{F})$ may be decoded from the received vector in $O(n)$ operations (or $O(n \log n)$ in the logarithmic cost model), the original information symbols can be recovered only after then taking a Fourier transform of c and reading off the data in the frequency domain.

Recall that a systematic encoder for cyclic codes can be obtained using the Euclidean algorithm. If $\mathcal{C}$ is an (n, k) cyclic code and $d(x)$ is a data polynomial of degree $k-1$, this encoder first shifts the data up by multiplying by x^{n-k}, and then divides by the generating polynomial $g(x)$. Thus, the systematic codeword is obtained as

$$c(x) = x^{n-k} d(x) - R_g \left[x^{n-k} d(x) \right]$$

where R_g is the remainder upon dividing by g.

There does not appear to be a direct analogue of this algorithm in a general group algebra. One approach for devising a systematic encoder is instead to exploit the subgroup structure of the group. For the group $PSL_2(\mathbb{Z}/q\mathbb{Z})$, the subgroups are completely known. In particular, the proper subgroups include dihedral groups of order $2z$ where $z \mid (q \pm 1)/2$ and noncommutative subgroups of the image (under projection from $SL_2(\mathbb{Z}/q\mathbb{Z})$) of the upper triangular subgroup $B = \left\{ \left(\begin{smallmatrix} \alpha & b \\ 0 & \alpha^{-1} \end{smallmatrix} \right) \right\}$ and its conjugates.

Theorem 7 *Let $\mathcal{C}(G, \mathcal{A}, \mathcal{S})$ be a low-density Cayley code on $\mathrm{PSL}_2(\mathbb{Z}/q\mathbb{Z})$ with block length n and rate r. Then $\mathcal{C}$ can be encoded systematically up to rate $r' = r - O(n^{-1/3})$ in $O(n^{4/3})$ operations.*

Sketch of proof: For a general group G, let H be a subgroup and $\{s_1, \ldots, s_m\}$ a set of coset representatives for $H\backslash G$. If ρ is any representation and $f \in \mathbb{F}G$, then

$$\begin{aligned}\widehat{f}(\rho) &= \sum_i \left(\sum_{h \in H} f(h\, s_i)\, \rho(h) \right) \rho(s_i) \\ &= \sum_i \widehat{f}_i(\rho \downarrow H)\, \rho(s_i)\end{aligned}$$

where $\rho \downarrow H$ is the representation ρ restricted to H, and $f_i(h) = f(hs_i)$. This recurrence is the basis for certain fast Fourier analysis algorithms; see [13]. Let $m' = \lfloor r\,|G|\,/\,|H| \rfloor$. For the purposes of spectral encoding, suppose that we can choose a subset of coset representatives $\{s_{i_1}, \ldots, s_{i_{m'}}\}$ such that whenever

$$f_{i_1}, \ldots, f_{i_{m'}} \in \mathbb{F}H$$

are given, we can choose (not necessarily uniquely),

$$f_{i_{m'+1}}, \ldots, f_{i_m} \in \mathbb{F}H$$

in such a way that the element of $\mathbb{F}G$ this defines is a codeword. A systematic encoder is then obtained by placing the data symbols on the cosets $s_{i_1}H, \ldots, s_{i_{m'}}H$ and solving for $f_{i_{m'+1}}, \ldots, f_{i_m}$. This encoding results in a loss of rate proportional to $|H|\,/\,|G|$.

To solve the required equations in the spectral domain, we may use the fact that H-*adapted* bases can always be chosen so that for each irreducible representation ρ, the restricted representation is block diagonal,

$$\rho \downarrow H \sim \eta_1 \oplus \cdots \oplus \eta_r\,,$$

where η_i is an irreducible representation of H.

For the group $PSL_2(\mathbb{Z}/q\mathbb{Z})$, we can work with the image of the subgroup $B \subset SL_2(\mathbb{Z}/q\mathbb{Z})$, with $|B| = O(q^2) = O(|G|^{2/3})$. In this case, the desired cosets can be found and the equations solved in $O(q^4)$ operations. The resulting encoding leads to a loss of rate of order $O(1/q)$. □

3.4 Spectral expander codes

If c is a codeword of a Cayley code $\mathcal{C}(G, \mathcal{A}, \mathcal{S})$, we have seen that for each irreducible representation ρ, each column of $\widehat{c}(\rho)$ is a spectral domain codeword of some code $\widehat{\mathcal{C}}_\rho(G, \mathcal{A}, \overline{\mathcal{S}})$ over $\overline{\mathbb{F}}$ of block length d_ρ. We now show that if $G = PSL_2(\mathbb{Z}/q\mathbb{Z})$ and $\mathcal{C}(G, \mathcal{A}, \mathcal{S})$ is an expander code, then for certain representations these spectral domain codes are also expander codes.

Let $\mathbb{P}^1(\mathbb{F}_q) = \{0, 1, \ldots, q-1, \infty\}$ denote the projective line over $\mathbb{F}_q$. Then $PSL_2(\mathbb{Z}/q\mathbb{Z})$ acts on $\mathbb{P}^1(\mathbb{F}_q)$ by fractional linear transformations:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \omega = \frac{a\,\omega + b}{c\,\omega + d}\,.$$

The following theorem shows the relevance of this fact to Fourier analysis and expander codes.

Theorem 8 *Let $\mathcal{C}(\mathrm{PSL}_2(\mathbb{Z}/q\mathbb{Z}), \mathcal{A}, \mathcal{S})$ be an expander code, with symbols on either the edges or the vertices. Then for each induced representation ρ_ψ, $\psi \in \widehat{\mathbb{F}_q^\times}$, there is a collection of subcodes $\overline{\mathcal{S}}_\psi$ over $\overline{\mathbb{F}}$ such that $c \in \mathcal{C}$ only if each column of $\widehat{c}(\rho_\psi)$ is an element of the expander code $\mathcal{C}(\mathbb{P}^1(\mathbb{F}_q), \mathcal{A}, \overline{\mathcal{S}}_\psi)$.*

Sketch of proof: Let the matrices

$$s_u = \begin{pmatrix} 0 & 1 \\ -1 & -u \end{pmatrix},\ u = 0, \ldots, q-1\ s_\infty = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

be a fixed set of coset representatives of $B\backslash SL_2(\mathbb{Z}/q\mathbb{Z})$, which we identify with $\mathbb{P}^1(\mathbb{F}_q)$. In [5] we constructed the principal series representations of $SL_2(\mathbb{Z}/q\mathbb{Z})$ by inducing characters from B, and expressing these matrices in terms of their action on $\{s_u\}$. In particular, if $\psi : \mathbb{F}_q^\times \to \overline{\mathbb{F}}$ is a modular character of B, then

$$\rho_\psi(g) s_u = \psi(f(u, g)) s_{g \cdot s_u} \tag{7}$$

for some function $f(u, s) \in \mathbb{F}_q^\times$, where $g \cdot s_u$ is the action of fractional linear transformation. Thus, $\widehat{\delta_{\mathcal{A}}}(\rho_\psi)$ has non-zero entries precisely where the adjacency matrix of $\Gamma(\mathbb{P}^1(\mathbb{F}_q), \mathcal{A})$ is non-zero; we refer to [5] for details. If $\Gamma(PSL_2(\mathbb{Z}/q\mathbb{Z}), \mathcal{A})$ is a good expander, then $\Gamma(\mathbb{P}^1(\mathbb{F}_q), \mathcal{A})$ is also a good expander since its spectral gap is at least as large. In particular, the explicit Ramanujan graphs for $PSL_2(\mathbb{Z}/q\mathbb{Z})$ restrict to give Ramanujan graphs on $\mathbb{P}^1(\mathbb{F}_q)$; see [14]. Thus, the relations (7) define a spectral domain expander code, where the subcode may vary with each constraint. □

Remark 8 The existence of an analogous basis for the discrete series representations would show that the time domain decoding algorithm for expander codes studied in [15] can be carried out in the frequency domain, independently for each representation.

Remark 9 We can carry out fast Fourier analysis on $\mathbb{P}^1(\mathbb{F}_q)$ by working with B-invariant functions on $PSL_2(\mathbb{Z}/q\mathbb{Z})$ and choosing special bases for the principal series representation induced from the identity character. This enables the Fourier transform of a function on $\mathbb{P}^1(\mathbb{F}_q)$ to be carried out in $O(q \log q)$ operations. It does not, however, lead to a fast convolution algorithm and thus an efficient encoding algorithm for expander codes on the projective line. The difficulty is that convolution needs to be carried out in the full group, and the "parity check" function h by which we convolve is not B-invariant.

4 Related Work

One of the first references that we know of for nonabelian codes using the perspective of group algebras is MacWilliams' article [9]. In this paper the difficulties of working in the time domain, even for the simplest example of the dihedral group, are apparent. Representation theory is not proposed as an essential tool. The article of Beth [2] is one of the first to consider efficient Fourier transform algorithms for nonabelian groups, and the paper also suggests the connection with coding. Much is now known about the complexities of various groups, and understanding of the relevant algorithms is just now beginning to mature. We refer to [13] for a summary of this recent work. The article of Ward [19] discusses aspects of the general framework for codes as ideals in the group algebra, representation theory, and various results related to codes with automorphism group $PSL_2(\mathbb{Z}/q\mathbb{Z})$ (quadratic residue codes), the Mathieu groups, and others. There is a fairly large literature on various group-algebraic aspects of cyclic codes or codes invariant under affine groups, for example [7]. One reference closely related in spirit is the paper of Tanner [17], which shows that algebraic methods analogous to those for cyclic codes can be applied to groups more general than $\mathbb{Z}/n\mathbb{Z}$, although strong restrictions are made to ensure that BCH decoding algorithms can be used. The applicability of representation theory is not fully recognized, and in particular, the hybrid polynomial/abelian Fourier transform method that is adopted in this paper does not seem to extend readily to more general groups. Alon *et al.* [1] use the explicit Ramanujan graphs of $PSL_2(\mathbb{Z}/q\mathbb{Z})$ to construct low rate codes that are not directly related to the Cayley codes we use here.

References

[1] N. Alon, J. Bruck, J. Naor, M. Naor, and R.M. Roth. Construction of asymptotically good low-rate error-correcting codes through pseudo-random graphs. *IEEE Trans. on Information Theory*, Vol. 38, No. 2, pp. 509–516, March, 1992.

[2] T. Beth. Generalizing the discrete Fourier transform. *Discrete Mathematics*, 56:95–100, 1985.

[3] R.E. Blahut. *Theory and Practice of Error-Control Codes*. Addison-Wesley, 1983.

[4] R. G. Gallager. Low-density parity-check codes. *IRE Trans. Inform. Theory*, Vol. 8, pp. 21–28, January, 1962.

[5] 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, pp. 115–139, 1992.

[6] J. Lafferty and D. Rockmore. Numerical investigation of the spectrum of certain families of Cayley graphs. In J. Friedman, editor, *Expanding Graphs. DIMACS Series in Discrete Math. and Theoretical Computer Science*, Vol. 10, pp. 63–73, Amer. Math. Soc., Providence, RI, 1993.

[7] P. Landrock and O. Manz. Classical codes as ideals in group algebras. *Designs, Codes and Crypt.*, Vol. 2, pp. 273–285, 1992.

[8] A. Lubotzky, R. Phillips, and P. Sarnak. Ramanujan conjectures and explicit construction of expanders. In *Proceedings of the ACM Symposium on the Theory of Computing*, pp. 240–246, 1986.

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

[10] F.J. MacWilliams and N.J.A. Sloane. *The Theory of Error-Correcting Codes.* North-Holland, Amsterdam, 1977.

[11] G.A. Margulis. Explicit group theoretical constructions of combinatorial schemes and their application to the design of expanders and concentrators. *Problems of Information and Transmission*, Vol. 24, No. 1, pp. 39–46, July, 1988.

[12] 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.

[13] D. Maslen and D. Rockmore. Generalized FFTs: A survey of some recent results. In L. Finkelstein and W. Kantor, editors, *Proc. 1995 DIMACS Workshop in Groups and Computation*, to appear.

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

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

[16] D. Spielman. Linear time encodable and decodable error-correcting codes. *IEEE Trans. on Information Theory*, Vol. 42, No. 6, November 1996, pp. 1723–1731.

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

[18] R. Michael Tanner. A recursive approach to low complexity codes. *IEEE Trans. on Information Theory*, Vol. 27, No. 5, pp. 533–547, September, 1981.

[19] H.N. Ward. Coding theory and representation theory. In *The Arcata Conference on Representations of Finite Groups. Proc. Sympos. Pure Math.*, Vol. 47, pp. 339–348, Amer. Math. Soc., Providence, RI, 1987.