SOME GRAPHS WITH SMALL SECOND EIGENVALUE

Joel Friedman

CS-TR-230-89

October 1989

Some Graphs with Small Second Eigenvalue

Joel Friedman*
Department of Computer Science
Princeton University
Princeton, NJ 08544

October 11, 1989

1 Introduction

In this article we discuss several very simple graphs which have fairly small eigenvalues. Perhaps the most important result is that one of the graphs is a Cayley graph whose corresponding Cayley hypergraphs has a second eigenvalue which is essentially as small as a Cayley hypergraph can have. Also these graphs are very simple to write down, and the eigenvalue calculation is based on well known results about exponential sums. This could be interesting for two reasons. First, it is hoped that such simple graphs may be better analyzed with respect to their expansion properies; in particular, good expanders are known to exist with much better expansion properties than can be guarenteed by eigenvalue estimates. Secondly, for a certain class of applications it is required that the number of vertices (and the degree) be exponential in n, where n is the parameter of the problem, and we'd like to carry out the calculations quickly. For some of the constructions, e.g. that of [LPS86] and [Mar87], it is not clear how to do this quickly. For Chung's sum graphs in [Chu] the calculations can be done fairly quickly, and the eigenvalue estimate is essentially the same; our graphs are somewhat simpler, and the eigenvalue calculation is based on somewhat more basic facts.

*The author wishes to acknowledge the National Science Foundation for supporting this research in part under Grant CCR–8858788, and the Office of Naval Research under Grant N00014–87–K–0467.

Given an undirected graph, $G = (V, E)$, which is d-regular in the sense that each vertex has degree d, it is easy to see that d is an eigenvalue of G's adjacency matrix, A, in fact the largest eigenvalue in absolute value. By the second largest eigenvalue, λ_2, of G, we mean the second largest eigenvalue in absolute value. For directed graphs, G, we define d-regularity by requiring that both the indegree and outdegree of each vertex be d. We can define the second eigenvalue as before, though it is somewhat more natural to define it as being the square root of the second largest eigenvalue of AA^T (see, for example, [FW]). All directed graphs in this paper are Cayley graphs, where the two notions are equivalent (see [FW]).

In this paper we will consider the following graphs and some variants and generalizations of them to be described in later sections.

For a prime p, let SUMPROD(p) denote the graph with vertex set $(\mathbf{Z}/p\mathbf{Z})\times(\mathbf{Z}/p\mathbf{Z})^*$, with each vertex (x, y) having a directed edge to $(x+a, ya)$ for each $a = 1, 2, \ldots, p-1$. Thus SUMPROD(p) is a directed graph with $p(p-1)$ vertices, with each vertex having indegree and outdegree $p-1$.

For an integer $k \geq 2$, let POWER(p, k) be the graph with edge vertex set $(\mathbf{Z}/p\mathbf{Z})^k$, with each vertex

$$(x_1, \ldots, x_k)$$

having a directed edge to each of

$$(x_1 + a, x_2 + a^2, \ldots, x_k + a^k)$$

for $a = 0, 1, \ldots, p-1$. Thus POWER(p, k) is a directed graph with p^k vertices and vertex has indegree and outdegree p.

For a group, G, and a subset, $H \subset G$, the *Cayley graph on G with generators H* to be the directed graph with vertex set G and directed edges

$$\{(g, gh) \mid g \in G,\ h \in H\}.$$

Unlike the classical definition, we do not require H to be a set of generators. Also, if $H^{-1} = H$ then we can view the graph as undirected in the obvious way.

Finally, let AFFINE(p) denote the group of affine linear transformations of $\mathbf{Z}/p\mathbf{Z}$,

$$\{ax + b \mid a \in (\mathbf{Z}/p\mathbf{Z})^*,\ b \in \mathbf{Z}/p\mathbf{Z}\}$$

with the usual group law

$$(ax + b) \circ (cx + d) = (ac)x + (b + ad).$$

Assume that p is a prime $\equiv 3 (\mathrm{mod}\ 4)$, and let SQRT($p$) be the Cayley graph on AFFINE(p) with generators

$$H = \{r^2x + r,\ -r^2x + r \mid r \in (\mathbf{Z}/p\mathbf{Z})^*\}.$$

Since $H^{-1} = H$ it follows that SQRT(p) is an *undirected* graph with $p(p-1)$ vertices and degree $2(p-1)$.

For the above graphs we will prove:

Theorem 1.1 *The graph SUMPROD(p) has second eigenvalue of absolute value* $\leq \sqrt{p}$.

Theorem 1.2 *The graph POWER(p, k) has second eigenvalue of absolute value* $\leq (k-1)\sqrt{p}$.

Theorem 1.3 *The graph SQRT(p) has second eigenvalue of absolute value* $\leq 2\sqrt{p}$. *The associated t-uniform Cayley hypergraph has second eigenvalue* $\leq 2p^{(t-1)/2}$.

For the first two graphs one can easily write down the eigenvectors and eigenvalues. One can estimate their eigenvalues with standard facts and tricks known for exponential sums; the proofs for SUMPROD(p) and POWER($p, 2$) are particularly simple (the latter's eigenvalues are Gauss sums). Bounding the eigenvalues of SQRT(p) involves the trace method and is slightly more complicated, but it is important since its corresponding Cayley hypergraph has small eigenvalues.

The first two graphs, which are not undirected graphs, have variants which are undirected graphs of the same degree, with the same eigenvalue bound holding. This is true of any Cayley graph of a commutative group (of which the first two graphs are examples), a fact that is implicit in [Chu]. Also, for the directed versions of the graphs, the second eigenvalue is also the "second eigenvalue" in the stronger sense of, say, [FW]; in this case the second eigenvalue of a directed, d-regular graph with adjacency matrix A is the same as the (classical) second eigenvalue of AA^T.

The fact that the second eigenvalue of SUMPROD(p) is small can be interpreted as saying that if we chose m random numbers from $(\mathbf{Z}/p\mathbf{Z})^*$, $a_1, \ldots, a_m$, then the two quantities

$$a_1 + a_2 + \cdots + a_m \quad \text{and} \quad a_1 a_2 \cdots a_m$$

become almost independent very quickly as $m \to \infty$. This will be used to bound the second eigenvalue of SQRT(p). Similarly the statement about POWER(p, k) says that for random numbers $a_1, \ldots, a_m$ chosen among $\mathbf{Z}/p\mathbf{Z}$ the quantities

$$a_1 + \cdots + a_m, \quad a_1^2 + \cdots + a_m^2, \quad \ldots, \quad a_1^k + \cdots + a_m^k$$

become almost independent quickly as $m \to \infty$.

All the above graphs and theorems have a natural generalization for p replaced by a prime power, q, and the arithmetic being done over the finite field with q elements.

It is only for POWER(p, k) with $k \geq 3$ that we use non-trivial facts about exponential sums; we will use a corollary to Weil's Riemann hypothesis for curves, see [Wei48] (though first realized by Hasse [Has] and Hasse-Davenport [?]), a special case of which states that for a polynomial $f = f(x)$ of degree k in $\mathbf{Z}/p\mathbf{Z}$, we have

$$\left| \sum_{a \in \mathbf{Z}/p\mathbf{Z}} e^{\frac{2\pi i}{p} f(a)} \right| \leq (k-1)\sqrt{p}.$$

His corollary also implies on estimate on the exponential sum we estimate for SUMPROD graphs, but this estimate is so easy to derive from scratch that we do it here. In Weil's article, [Wei48], a reference is made to class field theory; this reference can easily be dispensed with, as in [Sch76]. The use of the Riemann hypothesis can also be replaced by weaker estimates which can be proven by elementary means, without too much work; see [Sch76].

In section 2 we discuss the SUMPROD graphs, over $\mathbf{Z}/p\mathbf{Z}$ and other rings. In section 3 we discuss POWER graphs and a variant of them, SYM graphs, which may be more suitable for computing given large p. In section 4 we discuss SQRT graphs and some generalizations. In section 5 we review the representations of the affine transformations, and discuss its implications on the Cayley hypergraphs derived from SQRT and its variants.

The author's interest in AFFINE was due to his work with Avi Wigderson. The author would like to thank him, as well as Nick Pippenger for useful discussions.

2 SUMPROD Graphs

We begin by proving theorem 1.1. It is well known (and easy to see) that the Cayley graph of $\mathbf{Z}/n\mathbf{Z}$ with generators $H = \{h_1, \ldots, h_m\}$, i.e. the graph

with vertex set $\mathbf{Z}/n\mathbf{Z}$ and edges

$$\{(x, x+h) \mid x \in \mathbf{Z}/n\mathbf{Z},\ h \in H\},$$

has eigenvectors which are the real and imaginary parts of

$$\left(1, \zeta, \zeta^2, \ldots, \zeta^{n-1}\right)$$

with ζ ranging over all n-th roots of unity, and corresponding eigenvalue

$$\sum_{j=1}^{m} \zeta^{-h_j}.$$

Since $(\mathbf{Z}/p\mathbf{Z})^*$ is isomorphic to the additive group $\mathbf{Z}/(p-1)\mathbf{Z}$ via the map log, the discrete logarithm with respect to a fixed primitive root (fix one such root), it follows similarly that the eigenvalues of SUMPROD(p) are just

$$\sum_{x=1}^{p-1} \zeta^x \eta^{\log(x)}$$

with ζ and η ranging over all p-th and $(p-1)$-th roots of unity respectively. For $\zeta = \eta = 1$ we get the first eigenvalue, $p-1$. For $\eta = 1$ and $\zeta \neq 1$ the above sum is -1 since any p-th root of unity, $\zeta \neq 1$ satisfies

$$\zeta + \zeta^2 + \cdots + \zeta^{p-1} = -1,$$

and similarly for $\zeta = 1$ and $\eta \neq 1$ we get that the eigenvalue is 0. Finally when neither ζ nor η are not $= 1$, consider the square of absolute value of the eigenvalue,

$$\sum_{x=1}^{p-1} \zeta^x \eta^{\log(x)} \sum_{y=1}^{p-1} \zeta^{-y} \eta^{-\log(y)} = \sum_{x,y=1}^{p-1} \zeta^{x-y} \eta^{\log(x/y)} = \sum_{c,y=1}^{p-1} \zeta^{(c-1)y} \eta^{\log(c)},$$

where the substitution $c = x/y$ was used, as well as the fact that $\bar{\alpha} = \alpha^{-1}$ for $|\alpha| = 1$). For a fixed $c = 2, \ldots, p-1$ we have

$$\sum_{y=1}^{p-1} \zeta^{(c-1)y} \eta^{\log(c)} = (\zeta + \zeta^2 + \cdots + \zeta^{p-1}) \eta^{\log(c)} = -\eta^{\log(c)},$$

while for $c = 1$ we have

$$\sum_{y=1}^{p-1} \zeta^{(c-1)y} \eta^{\log(c)} = \sum_{y=1}^{p-1} \zeta^0 \eta^0 = p-1.$$

Thus

$$\sum_{c,y=1}^{p-1} \zeta^{(c-1)y} \eta^{\log(c)} = p - 1 + (-\eta - \eta^2 - \cdots - \eta^{p-2}) = p,$$

which completes the proof.

□

We remark that while this graph is not undirected, it has a directed variant, due to the following observation which, for example, is implicit in Chung's paper, [Chu]:

Proposition 2.1 *Let the Cayley graph on G with generators H have second eigenvalue λ_2, and let G be commutative. Then its* Cayley sum graph, *i.e. the graph with vertex set G and edges $\{(g, g^{-1}h)\}$ with g and h ranging over G and H respectively, has second eigenvalue of absolute value $|\lambda_2|$.*

Proof If $u = u(g)$ is an eigenvector of the Cayley graph with eigenvalue ν, then it is easy to check that $v(g) \equiv u(g) \pm u(g^{-1})\nu/|\nu|$ is an eigenvector with eigenvalue $\pm|\nu|$; if u is purely real, only one of $\pm$ really appears, since one of "+" or "−" yields the zero vector. It is easy to see that these eigenvectors span the entire space, and therefore give a complete list of the eigenvalues.

□

There are two obvious ways to generalize on this construction. The first is to take a prime power, q, and construct SUMPROD with the sum and product being taken in GF(q), the finite field with q elements. There the same theorem and proof goes through word for word with p replaced by q.

The second generalization is to construct SUMPROD over the ring $\mathbf{Z}/n\mathbf{Z}$ for an integer n, not necessarily prime, with vertex set $(\mathbf{Z}/n\mathbf{Z}) \times (\mathbf{Z}/n\mathbf{Z})^*$ and edges connecting (x, y) to $(x + a, ya)$ where a runs over all elements of $(\mathbf{Z}/n\mathbf{Z})^*$. Here the number of vertices is $n\phi(n)$, where $\phi(n)$ is the size of $(\mathbf{Z}/n\mathbf{Z})^*$. In this case the eigenvalue bounds become much worse. In particular, a similar calculation shows that for n a prime power, $n = p^t$, the eigenvalues have absolute value

$$(p-1)p^{t-1},\ p^{t-(1/2)},\ p^{t-1},\ 0$$

with respective multiplicities

$$1,\ (p-1)(p-2),\ p-1,\ (p-1)p^{2t-1} - p^2 + 2p - 2.$$

It follows that for general n with prime factorization $p_1^{t_1} \dots p_s^{t_s}$ the eigenvalues have absolute values which are products of those for the graph when $n = p_i^{t_i}$, and in particular the second largest eigenvalue is

$$n \max_{1 \le i \le s} \frac{1}{\sqrt{p_i}}.$$

3 POWER Graphs

We begin by proving theorem 1.2. Clearly the vector whose value at $(x_1, \dots, x_k)$ is

$$\zeta_1^{x_1} \cdots \zeta_k^{x_k},$$

with the ζ_i being p-th roots of unity, is an eigenvector with eigenvalue

$$\sum_{a=0}^{p-1} \zeta_1^{-a} \zeta_2^{-a^2} \cdots \zeta_k^{-a^k} = \sum_{a=0}^{p-1} \zeta^{f(a)} \tag{3.1}$$

where $\zeta = e^{2\pi i/p}$ and $f(\,)$ is some polynomial with integer coefficients of degree k with vanishing constant term. Furthermore these p^k eigenvectors are orthogonal to one another, and therefore comprise a complete list of the eigenvectors and eigenvalues. For $\zeta_1 = \cdots = \zeta_k = 1$, i.e. f being the zero polynomial, this sum is p, corresponding to the first eigenvector. It is a standard fact about exponential sums that the sum on the right–hand–side of equation 3.1 is bounded in absolute value by $(k-1)\sqrt{p}$ if f is not the zero polynomial (modulo p); see [Wei74]. For $k = 2$ the above is a Gauss sum, and the bound can be proven directly, using the same "squaring the absolute value" trick used in the previous section.

□

As a variant of this graph, we can study the graph SYM(p, k), which has vertex set $(\mathbf{Z}/p\mathbf{Z})^k$ and has a directed edge from each vertex

$$(x_1, \dots, x_k)$$

to

$$(x_1 + a, x_2 + ax_1, x_3 + ax_2, \dots, x_k + ax_{k-1})$$

for $a = 0, \dots, p-1$. Similar to the POWER graphs, the fact that the SYM graphs have small second eigenvalue means that the first k symmetric polynomials of m random numbers in $\mathbf{Z}/p\mathbf{Z}$ quickly become almost independent as $m \to \infty$.

Theorem 3.1 *The graph SYM(p,k) has second eigenvalue of absolute value* $\leq (k-1)\sqrt{p}$.

Proof We will give two proofs. The first proof directly uses the fact that POWER graphs have small eigenvalues; the same idea will be carried out in detail for the graphs of the next section. The second, which is more routine, will explicity give the eigenvectors, showing that the eigenvalues are exponential sums like those of equation 3.1.

Consider m random numbers, $a_1, \ldots, a_m$, drawn independently from $\{0, \ldots, p-1\}$ with uniform distribution, and let

$$s_i = a_1^i + \cdots + a_m^i$$

for $i = 1, \ldots, k$. Since the second eigenvalue of POWER(p,k) is bounded by $(k-1)\sqrt{p}$, and since its adjacency matrix is diagonalizable, we have that

$$\Pr\{s_1 = b_1, \cdots, s_k = b_k\} = p^{-k} + O\left(\left(\frac{(k-1)\sqrt{p}}{p}\right)^m\right)$$

for any b_i's in $\mathbf{Z}/p\mathbf{Z}$ where, for the moment, we identify s_i with its representative in $\mathbf{Z}/p\mathbf{Z}$. The symmetric polynomials, $\sigma_1, \ldots, \sigma_k$, of the random a_i's can be written in terms of the s_i's via the "Newton identities"

$$\sigma_j = (-1)^{j+1}\frac{s_j}{j} + f_j(s_1, \ldots, s_{j-1}), \tag{3.2}$$

for some polynomials f_j whose coefficients are rational numbers whose denominators contain only products of powers of integers $\leq j$; the f_j's coefficients (and $1/j$) are therefore defined in $\mathbf{Z}/p\mathbf{Z}$ for $k \leq p-1$. We may assume $k \leq p-1$, or indeed $\leq 1+\sqrt{p}$, for otherwise the theorem is clearly true. Writing

$$\Pr\{\sigma_1 = b_1, \cdots, \sigma_k = b_k\} = \prod_{j=1}^{k} \Pr\{\sigma_j = b_j \mid \sigma_{j-1} = b_{j-1}, \ldots, \sigma_1 = b_1\}$$

we find that

$$\Pr\{\sigma_1 = b_1, \cdots, \sigma_k = b_k\} = p^{-k} + O\left(\left(\frac{(k-1)\sqrt{p}}{p}\right)^m\right).$$

(Here the constant in the $O(\,)$ might, in principle, depend horribly as a function of p and k, but for fixed p and k it is independent of m.) Hence,

if A is the adjacency matrix of SYM(p,k), then every entry of A^m is of the form

$$p^{m-k} + O\Big(((k-1)\sqrt{p})^m\Big),$$

and therefore the second eigenvalue of A is bounded by $(k-1)\sqrt{p}$.

For the second proof, we note that we can actually write out the eigenvectors without much trouble. Indeed, the Newton identities allow us to write

$$s_j = (-1)^{j+1} j\sigma_j + g_j(\sigma_1, \ldots, \sigma_{j-1})$$

for some polynomials, g_j, with integer coefficients (and therefore defined in $\mathbf{Z}/p\mathbf{Z}$). It is easy to see that the function which takes the value

$$\zeta_1^{x_1} \zeta_2^{g_2(x_1)-2x_2} \cdots \zeta_k^{g_k(x_1,\ldots,x_{k-1})+(-1)^{k+1}kx_k}$$

on the vertex $(x_1, \ldots, x_k)$ is an eigenfunction, for p-th roots of unity ζ_i, with eigenvalue

$$\sum_{a=0}^{p} \zeta_1^{-a} \zeta_2^{-a^2} \cdots \zeta_k^{-a^k},$$

and therefore the same bounds on the eigenvalues hold for SYM as for POWER.

4 Cayley Graphs of AFFINE

We begin by proving theorem 1.3. The proof will work for any prime, p, for Cayley graph on

$$\{r^2x + r,\ cr^2x + r \mid r \in \mathbf{Z}/p\mathbf{Z}\}$$

where c is a fixed non-residue. Let A be SQRT(p)'s adjacency matrix. We will estimate the trace of A^m for a large m. Since the trace of the matrix representing the directed Cayley graph of $\{ax + b\}$ on AFFINE is $p(p-1)$ if $a = 1$ and $b = 0$ and 0 otherwise, and since

$$\begin{aligned}(\pm a_1^2 x + a_1) \circ (\pm a_2^2 x + a_2) \circ \cdots \circ (\pm a_m^2 x + a_m) = \\ \pm(a_1 \cdots a_m)^2 + a_1 \pm a_1^2 a_2 \pm \cdots \pm a_1^2 a_2^2 \cdots a_{m-1}^2 a_m\end{aligned}$$

we have that the trace of A^m is just $p(p-1)$ times the number of solutions to the equations

$$a_1 a_2 \cdots a_m = \pm 1, \tag{4.1}$$

$$a_1 \pm a_1^2 a_2 \pm \cdots \pm a_1^2 a_2^2 \cdots a_{m-1}^2 a_m = 0. \tag{4.2}$$

Using the the first equation to eliminate a_m from the second and substituting $b_i = a_1^2 a_2^2 \cdots a_{i-1}^2 a_i$, the second equation becomes

$$b_1 \pm b_2 \pm \cdots \pm b_{k-1} \pm b_1 b_2^{-1} b_3 b_4^{-1} \cdots b_{m-1}^{(-1)^m} = 0,$$

with the b_i ranging over all values in $(\mathbf{Z}/p\mathbf{Z})^*$.

To count the number of solutions to this equation, recall that SUMPROD(p) has second eigenvalue $\leq \sqrt{p}$. Similarly the three natural variants of SUMPROD(p), namely the graphs that connect each (x, y) to $(x + a, ya^{-1})$, $(x - a, ya)$, or $(x - a, ya^{-1})$ respectively as a ranges over $(\mathbf{Z}/p\mathbf{Z})^*$, also have second eigenvalue $\leq \sqrt{p}$ (and the same eigenvectors). It follows for any fixing of the pluses and minuses, the quantities s and t given by

$$\begin{aligned} s &= b_1 \pm b_2 \pm \cdots \pm b_{m-1}, \\ t &= b_1 b_2^{-1} b_3 b_4^{-1} \cdots b_{m-1}^{(-1)^m} \end{aligned}$$

quickly become independent, in the sense that for any $\alpha \in \mathbf{Z}/p\mathbf{Z}$ and $\beta \in (\mathbf{Z}/p\mathbf{Z})^*$ we have

$$\Pr\{s = \alpha,\ t = \beta\} = \frac{1}{p(p-1)} + O\left(\left(\frac{\sqrt{p}}{p-1}\right)^{m-1}\right)$$

for randomly chosen b_i in $(\mathbf{Z}/p\mathbf{Z})^*$ (independently and with uniform distribution). It follows that

$$\text{Trace}\,(A^m) = 2^m (p-1)^m + O\left(\left(2\sqrt{p}\right)^m\right)$$

with the constant in $O(\,)$ independent of m. Since the first eigenvalue of A is clearly $2(p-1)$, taking $m \to \infty$ gives that the second eigenvalue of SQRT(p) is bounded by $2\sqrt{p}$.

What distinguishes these graphs from the others is that the associated Cayley hypergraphs have small second eigenvalue. Let us recall some representation theory (Fourier analysis) of finite groups; for proofs see, for example, [Rob83]. Given a finite group, G, the space of complex valued functions on G with the inner product

$$(u, v) = \sum_{g \in G} u(g)\overline{v(g)},$$

denoted $L_2(G)$, can be orthogonally decomposed into subspaces

$$L_2(G) = \bigoplus_{i=1}^{r} E_i$$

with the following conditions:

1. Each E_i is invariant under the natural action of G on $L_2(G)$, given by $g(u(x)) \equiv u(gx)$.
2. $\dim(E_i) = d_i^2$ for some d_i corresponding to the dimension of an irreducible representation of G.
3. r is equal to the number of conjugacy classes in G.

It follows that the matrix A of any Cayley graph on G vanishes outside the $E_i \times E_i$ blocks. The second eigenvalue of the Cayley t-uniform hypergraph derived from A, see [FW], turns out to be

$$\max_{2 \le i \le r} \left(\frac{n}{d_i}\right)^{(t-2)/2} \left\| A|_{E_i} \right\|$$

assuming that E_1 corresponds to the trivial representation (i.e. the all 1's vector). It follows that any Cayley graph whose t-uniform hypergraphs have small second eigenvalue must have some d_i close to $\sqrt{n}$.

The space AFFINE(p) is known to have a particularly simple decomposition, namely as the sum of p subspaces, E_i, where for $1 \le i \le p-1$ they are the span of the functions

$$ax + b \mapsto \zeta^{(i-1)\log a}$$

for a fixed primitive $(p-1)$-th root of unity and a fixed log function (i.e. with a fixed generator of $(\mathbf{Z}/p\mathbf{Z})^*$ as its base); see, for example, [Rob83]. E_p is therefore a $(p-1)^2$ dimensional space. Since the graph SQRT(p) has for each fixed a two generators of the form $ax + b$, it follows that its adjacency matrix A vanishes on all the $E_i \times E_i$ blocks for $2 \le i \le p-1$. Hence the t-uniform Cayley hypergraph derived from SQRT(p) has second eigenvalue

$$\max_{2 \le i \le r} \left(\frac{n}{\sqrt{d_i}}\right)^{(t-2)/2} \left\| A|_{E_i} \right\| = \left(\frac{p(p-1)}{p-1}\right)^{(t-2)/2} 2\sqrt{p},$$

which is within a constant factor of optimal for fixed t among all Cayley graphs with that many vertices and edges.

5 More on AFFINE

Motivated by the discussion, we see that a subset H of AFFINE(p) will yield Cayley hypergraphs with small eigenvalue only if for each $a \in (\mathbf{Z}/p\mathbf{Z})^*$, the number of elements of H of the form $ax + b$ is independent of a. To generalize the construction of the last section, one can try to construct, for any multiple of $p-1$, and subset H of that size in AFFINE(p), such that the associated Cayley hypergraphs have small second eigenvalue. While we don't have an explicit construction for such H's, we will show that a randomly constructed H will yield fairly small eigenvalues, and one can give an algorithm to approximate this construction.

Consider an H of size $2(p-1)k$, constructed by chosing for each $a \in (\mathbf{Z}/p\mathbf{Z})^*$, k numbers $b_{a,1}, \ldots, b_{a,k}$ from $\mathbf{Z}/p\mathbf{Z}$, and setting

$$H = \{ax + b_{a,i},\ a^{-1}x - ab_{a,i}\}.$$

We will prove:

Theorem 5.1 *If $b_{a,i}$ are chosen randomly in $\mathbf{Z}/p\mathbf{Z}$, uniformly and independently, then the expected value of the second eigenvalue is bounded by $C \log p\sqrt{k(p-1)}$ for some absolute constant C. More generally we have*

$$E\{\lambda_2^m + \cdots + \lambda_n^m\} \leq (2emk(p-1))^{m/2}(p-1)^2$$

where $n = p(p-1)$, the number of vertices in the graph.

Theorem 5.2 *For any ϵ there is a polynomial in n time algorithm to chose $b_{a,i}$ to yield a graph with second eigenvalue bounded by $C(k(p-1))^{\epsilon+1/2}$.*

Proof If A is the adjacency matrix of the corresponding Cayley graph, then

$$\text{Trace}\,(A^m) = \sum_{a_1,\ldots,a_m,i_1,\ldots,i_m} \text{Trace}\,((a_1x + b_{a_1,i_1}) \circ \cdots \circ (a_mx + b_{a_m,i_m})) \tag{5.1}$$

where Trace $(ax+b)$ is $p(p-1)$ if $a = 1$ and $b = 0$, and 0 otherwise. So a summand on the right-hand-side for which $a_1 \cdots a_m \neq 1$ always vanishes; this happens for a fraction $(p-2)/(p-1)$ of the summands. Next consider a fixed summand where $a_1 \cdots a_m = 1$. There

$$(a_1x + b_{a_1,i_1}) \circ \cdots \circ (a_mx + b_{a_m,i_m}) = x + f(b),$$

where b is shorthand for the set of all $b_{a,i}$'s, and f is a linear function depending on the a_j's involved. If f vanishes then the trace of this term

is always $p(p-1)$, whereas if f is non-trivial (i.e. does not vanish) then if the b's are chosen randomly, then $f(b) = 0$ exactly $1/p$ of the time. In particular, if there is an a and i such that the product contains exactly one term from the set

$$\{ax + b_{a,i},\ a^{-1}x - ab_{a,i}\},$$

then $f(b)$ depends non-trivially on $b_{a,i}$. So letting S be the number of summands for which $a_1 \cdots a_m = 1$ and $f(b) \equiv 0$, we have

$$S \leq m^m \binom{k(p-1)}{m/2} \leq (2emk(p-1))^{m/2}$$

where $\binom{a}{b} \leq (ae/b)^b$ was used as well as the fact that $f \equiv 0$ implies that the number of different $b_{a,i}$'s appearing is $\leq m/2$. On the other hand by equation 5.1 we get

$$\mathrm{E}\{(2k(p-1))^m + \lambda_2^m + \cdots + \lambda_n^m\} \leq \Big(\frac{1}{p-1}(2k(p-1))^m - S\Big)\frac{1}{p}p(p-1) + Sp(p-1),$$

and thus

$$\mathrm{E}\{\lambda_2^m + \cdots + \lambda_n^m\} \leq S(p-1)^2 \leq (2emk(p-1))^{m/2}(p-1)^2. \qquad (5.2)$$

The other part of the lemma is proven by taking $m \approx 2\log p$ and even, and applying Jensen's inequality.

□

To give a polynomial time algorithm to approximate the randomized construction, simply fix a value for m in equation 5.1, calculate for each summand on the right-hand-side what $f(b)$ is, and then choose the $b_{a,i}$'s one by one, each time choosing the value for $b_{a,i}$ which makes as many $f(b)$'s non-zero as possible, from those $f(b)$'s which are determined exactly when that $b_{a,i}$'s value is chosen (along with previously chosen b's values); the f's which are not definitely determined by the present $b_{a,i}$'s value (and that of previous b's) we ignore. This procedure will clearly get the number of non-trivial $f(b)$'s to have at least as many non-zero values as is expected by randomly choosing the $b_{a,i}$'s. Thus we can give a polynomial in n time algorithm to construct a graph whose second and smaller eigenvalues satisfy the bound of equation 5.2 (ignoring the $\mathrm{E}\{\}$ in that equation).

References

[Chu] F. R. K. Chung. Diameters and eigenvalues. preprint.

[FW] J. Friedman and A. Wigderson. On the second eigenvalue of hypergraphs. To appear.

[Has34] H. Hasse. Theorie der relativ-zyklischen algebraischen Funktionenkörper, insbesondere bei endlichen Konstantkörper. *J. Reine Angew. Math.*, 172:37–54, 1934.

[HD34] H. Hasse and H. Davenport. Die nullstellen der kongruenzzetafunktionen in gewissen zyklischen fallen. *J. Reine Angew. Math.*, 172:151–182, 1934.

[LPS86] A. Lubotzky, R. Phillips, and P. Sarnak. Explicit expanders and the ramanujan conjectures. In *18th Annual ACM Symposium on Theory of Computing*, pages 240–246, 1986.

[Mar87] G. Margulis. Manuscript in Russian on graphs with large girth, 1987.

[Rob83] Alain Robert. *Introduction to the Representation Theory of Compact and Locally Compact Groups.* Cambridge University Press, Cambridge, 1983.

[Sch76] Wolfgang M. Schmidt. *Lecture Notes in Mathematics, #536: Equations of Finite Fields, An Elementary Approach.* Springer-Verlag, New York, 1976.

[Wei48] André Weil. On some exponential sums. *Proc. Nat. Acad. Sci. USA*, 34:204–207, 1948.

[Wei74] André Weil. *Basic Number Theory.* Springer-Verlag, New York, 1974.