Semi-direct product in groups and Zig-zag product in graphs: Connections and applications

EXTENDED ABSTRACT

Noga Alon* Alexander Lubotzky† Avi Wigderson‡

Abstract

We consider the standard semi-direct product $A \rtimes B$ of finite groups A, B. We show that with certain choices of generators for these three groups, the Cayley graph of $A \rtimes B$ is (essentially) the zigzag product of the Cayley graphs of A and B. Thus, using the results of [RVW00], the new Cayley graph is an expander if and only if its two components are. We develop some general ways of using this construction to obtain large constant-degree *expanding Cayley graphs from small ones.*

In [LW93], Lubotzky and Weiss asked whether expansion is a group property; namely, is being expander for (a Cayley graph of) a group G depend solely on G and not on the choice of generators. We use the above construction to answer the question in negative, by showing an infinite family of groups $A_i \rtimes B_i$ which are expanders with one choice of (constant-size) set of generators and are not with another such choice. It is interesting to note that this problem is still open, though, for "natural" families of groups, like the symmetric groups S_n or the simple groups $PSL(2, p)$.

1 Introduction

This paper reveals yet another bridge that expanders form between Theoretical Computer Science and Graph Theory on one side, and Algebra and Group Theory on the other. This follows from a simple connection that we discover and begin to explore here, between two basic operations: the zigzag product of graphs and the semi-direct product of groups.

The semi-direct product of groups is one of the oldest and most basic constructions of group theory. When a group B acts on another group A in a certain way[1], a larger group $A \rtimes B$ can be constructed, whose elements are all pairs $\{(a, b) : a \in A, b \in B\}$, and group multiplication uses the action above in a nontrivial way. One way to see the power of this operation is that the semi-direct product can have much fewer generators than the group A does. Another is that the semi-direct product of Abelian groups can be non-Abelian.

In contrast, the zigzag product of graphs is very new – it was introduced only last year in the paper [RVW00]. When the vertices of a (small) graph H label the edges around each vertex of a (big) graph G, a larger graph $G \textcircled{z} H$ can be constructed, whose vertices are pairs $\{(g, h) : g \in V(G), h \in V(H)\}$, and adjacency is defined using the above labeling in a nontrivial way. The power of this operation can be seen from two simultaneous properties it has. The degree of the new graph can be much smaller than the degree of the big graph G. Nevertheless, if the two building blocks G and H are good expanders, so is their zigzag product[2].

The link between the two is another step in a long chain of works attempting to understand and construct expander graphs. Expanders are fundamental combinatorial objects, with a wide variety of applications in

*Schools of Mathematics and Computer Science, Tel-Aviv University, Tel Aviv, E-mail: noga@math.tau.ac.il. Partially supported by a US-Israel BSF grant, by the Israel Science Foundation and by the Hermann Minkowski Minerva Center for Geometry at Tel Aviv University.

†Department of Mathematics, The Hebrew University, Jerusalem, E-mail: alexlub@math.huji.ac.il. Partially supported by NSF and US-Israel BSF grants.

‡Institute for Advanced Study, Princeton and the Hebrew University, Jerusalem. E-mail: avi@ias.edu. Partially supported by NSF grants CCR-9987007 and CCR-9987845

[1] Namely, as a subgroup of the automorphisms of A

[2] It is interesting to note that a related construction was proposed and analyzed in a special case by Gromov [G83]

Computer Science (which range from derandomization to network design and error correction) and Mathematics (see for example two recent unexpected applications of expanders: one [G00] for the Baum-Connes Conjecture and one [LP00] for computational group theory).

While random regular graphs are almost always expanders, to give an explicit description of an infinite family of (bounded degree) expanders is a difficult task. Until last year, essentially all explicit constructions were of algebraic nature - they were either Cayley graphs of certain groups (e.g. [AM84, LPS88, Mar88]), or graphs whose vertices are identified with some algebraic structure on which there is a natural action of a group preserving adjacency (e.g. [Mar73, GG81]). This is not surprising, since expansion can be captured by the 2nd largest eigenvalue $\lambda(G)$ of the adjacency matrix of the graph, normalized by the degree, as shown in [Tan84, AM84, A86]. As this is an algebraic parameter - it can be related (as is done in all the papers above) to known tools or results from algebra or number theory when the graph has such a structure.

The novelty in the work of [RVW00] was that it gave an entirely combinatorial explicit construction of constant degree expander graphs. Starting with a constant size expander, one can apply successively the zigzag product (as well as some standard graph operations) to obtain larger and larger expanders of the same fixed degree. The central property required for proving this, namely that the zigzag product "preserves" expansion, has a straightforward elementary proof that follows a clear, information theoretic intuition.

It is perhaps ironic that despite the attempt to break from the algebraic mold, the zigzag product can be viewed as a generalization of the semi-direct product - a classical algebraic operation. We show that with appropriate choices of generators for the groups A, B and $A \rtimes B$, the Cayley graph of the semi-direct product $A \rtimes B$ turns out to be the zigzag product[3] of the Cayley graphs of A and B.

Thus the zigzag theorem has implications on the group theory side: whenever the generators satisfy the required properties, the semi-direct product now becomes a tool for constructing large expanding *Cayley graphs* from small ones. Moreover, as noted above, even though A may have a large set of (expanding) generators, the semi-direct product can be expanding with much fewer generators. The main technical part of the paper explores this situation, and we elaborate on it in subsection 1.2 below. But first we motivate (in subsection 1.1) such constructions, describing a consequence of this connection to a basic question in this boundary area of graph theory and group theory - expanding Cayley graphs. We feel that such constructions will find more applications, on both sides of this boundary.

[3]This is not strictly precise - we actually need to generalize the original [RVW00] definition of the zigzag product in a natural way, that preserves its properties.

1.1 Is expansion a group property?

As mentioned above, major examples of expanders are Cayley graphs of certain groups with judicious choice of (constant number of) generators. In some of these constructions, the (infinite) family of groups is obtained in a uniform way – all groups are finite quotients of one infinite group, and the generating sets are the projections of a fixed finite set of generators of the infinite group. Such a construction gives a family of constant degree expanders when the infinite group has the Kazhdan *"Property T"* or even the weaker Lubotzky *"Property τ"* [L94]. In these cases *every* choice of a generating set for the infinite group would work, namely would render all finite graphs expanding. On the other hand, if the infinite group is *"Amenable"* then *no* choice of generators for it would yield a sequence of expanders [LW93].

Of course, for finite groups we have many more choices of (bounded) generating sets, which do not have to be obtained in such uniform fashion. Nevertheless, there was some evidence that this "all or nothing" situation holds in this more general nonuniform setting, at least for some nice families of groups. For example, in the sequence of groups $SL_m(p)$, where m is fixed and p ranges over all primes, every sequence of bounded generating sets for them whose expansion can be analyzed turns out to be expanding. On the other hand, in the sequence of permutation groups S_n where n ranges over the integers, every sequence of bounded generating sets whose expansion can be analyzed turns out to be non-expanding. (See also [LR92] for some experimental evidence). Note however, that if one is interested in unbounded sets of generators, S_n can be expanders and non-expanders — see [R97]. So, the essence of the problem is with bounded sets of generators as, in fact, every group of size n is an expander with respect to most sets of $c \log n$ elements, where $c > 1$, as proved in [AR94].

This led Lubotzky and Weiss to ask whether expansion is a property of a group, rather than a particular choice of generators:

Question 1.1 *[LW93] Fix an integer d. Let A_i be any family of finite groups, and for each i take any two symmetric sets $S_i, \hat{S}_i$ of generators of size at most d. Let $\lambda_i, \hat{\lambda}_i$ be the 2nd eigenvalues of (the random walk on) the Cayley graphs of A_i with generators $S_i, \hat{S}_i$, respectively. Is it true that the sequence λ_i is uniformly bounded above by a fixed constant < 1 if and only if the sequence $\hat{\lambda}_i$ is ?*

We prove that in this generality the answer is no. We use the connection above to describe an infinite family of groups which is expanding with one choice of bounded generating sets and non-expanding with another. In essence, what the connection with zigzag allows us to do is to show that if the conjecture has been true, it would hold even for certain sets of unbounded generators (as we can later reduce them using semi-direct product to a bounded set of generators, maintaining expansion). This leads us to construct appropriate groups which can be expanding or non-expanding depending on the choice of unbounded sets of generators of the required structure, which we explain in the next subsection. Putting everything together, we exhibit a counterexample to the question above. This is the content of Theorem 4.2 in Section 4.

1.2 Expanding generators with few orbits

Let us start with an example, which is actually related to the counterexample above, and points to the structure of generators required to make the semi-direct product "efficient" in reducing the number of generators.

Example 1.2 *Consider the graph of the Boolean cube. It is the Cayley graph of the Abelian group F_2^n with the generators being the n unit vectors. Note that this generating set is the orbit of* one *unit vector, under the action of the cyclic group Z_n on the coordinates. It is well known that this graph is not an expander, namely the 2nd eigenvalue of the random walk on it tends to 1 as n tends to infinity. Similarly any choice of n vectors will not give expanders, since if the graph is connected, it is isomorphic to the cube. On the other hand it is not difficult to show that $2n$ random vectors will almost surely (that is, with probability tending to 1 and n tends to infinity) make F_2^n into expanders.*

Can one find an expanding generating set of $2n$ vectors which are the orbits of only two *vectors ? In other words, the $2n$ generators should be all possible cyclic shifts of two given vectors. One of the results in this paper is that (if n is a prime and 2 is a primitive root modulo n) in fact such $2n$ vectors can be taken to be the orbits of two random vectors. While this result gives rise to especially elegant linear error correcting codes which are asymptotically good (i.e., have constant rate and linear distance), it falls short of providing the counterexample to Question 1.1. The reason is that the acting group Z_n itself cannot be made an expander with a constant number of generators (and thus cannot provide the required "reduction").*

Back to the general discussion, the main structural requirement for the semi-direct product to reduce the number of generators, is that the set of generators chosen for the group A comprises of a few orbits under the action of B. We will limit ourselves (via a group representation) to the case that B is a matrix group and A is an invariant subspace under this group of linear transformations. Thus A is an Abelian group, and we seek generating sets for A which are the orbits of a constant number of vectors from A under the action of all matrices in B. Our task is to find such sets which are expanding, and others which are not.

Our main technical results provide general criteria for the orbits of a constant number of randomly chosen vectors from A to form an expanding generating set. These are given in Theorems 3.1 and 3.4 in Section 3. For example, we show that such is the case whenever A is a minimal invariant space (i.e. the representation is irreducible). The proofs combine in a simple way a probabilistic argument, linear algebra, and the transitivity of the group action. It is important to note that we do not have a single explicit example of such a generating set.

For the application to the Lubotzky-Weiss question we need to work with a group B which has a constant number of expanding generators, and we choose the group $SL_2(p)$. We also need to pick A for which non-expanding generators can be exhibited. This is done using $A = F_2^{P_1}$, where $P_1 = Z_p \cup \{\infty\}$ is the projective line, and the action of B on A is the permutation of the coordinates according to the Mobius transformations acting on the projective line, as described in Section 4.

Organization of the paper

In Section 2 we give the relevant definitions and results concerning the zigzag product, the semi-direct product, and formulate the connection between them. In Section 3 we derive general conditions under which it is possible to find expanding sets consisting of only a few orbits. In Section 4 we describe the family of groups with expanding and non-expanding sets of generators. We conclude in Section 5 with some open problems.

2 Preliminaries

2.1 Graphs and the Zig-zag product

All graphs discussed in this paper are undirected, regular graphs. We allow multiple edges and self loops, so graphs are best understood as symmetric nonnegative integer matrices with a fixed row-sum, called the *degree*. For a graph G, we let $V(G)$ denote its set of vertices and $E(G)$ its (multiset of) edges.

Let G be a d-regular graph, and M its adjacency matrix. We denote by $\lambda(G)$ the second largest (in absolute value) eigenvalue of M/d. Equivalently, since $\bar{1}$ is the

eigenvector of M/d corresponding to the (largest) eigenvalue 1, $\lambda(G)$ is the largest value $|v^t(M/d)v|$ takes, over all real unit vectors v whose entries sum to zero.

We say that a graph G is an $[n, d, \lambda]$-graph if it is a d-regular graph on n vertices, and $\lambda(G) \leq \lambda$.

An infinite family of graphs G_i is called an *expander* family if for some $\lambda < 1$ the normalized second largest eigenvalue of each graph G_i does not exceed λ. It is a *non-expander* family if there is no such uniform bound λ. Note that there is no requirement for the degrees to be bounded in this definition! We shall sometimes abuse notation and refer to a specific graph as an expander or a non-expander, when the family it belongs to is clear from the context. For example, the complete graph is an expander, while the Boolean cube is a non-expander.

We shall now slightly extend the definition of the zig-zag product of [RVW00]. Let H be an $[m, d, \mu]$-graph, and let G be an $[n, cm, \lambda]$-graph, which is the (edge) disjoint union of c m-regular graphs G_i on the same set of vertices (in the original definition, c was 1). Further assume that in each G_i the edges around every vertex are (arbitrarily) labeled by $[m]$ in a 1-1 fashion.

The zigzag product of G and H, denoted $G \textcircled{z} H$, has vertices (v, k) for every $v \in V(G)$ and $k \in V(H)$ (so there is a "cloud" of vertices of H around every original vertex of G). Two vertices (v, k) and (u, l) are adjacent, intuitively if we can travel between them in a "zig-zag" path of length 3: one step on H in the v cloud, then switching to the u cloud according to an edge of G (and the labeling), and a final step on in the u cloud. More formally, they are adjacent if there exist $k', l' \in [m]$ and $i \in [c]$ such that the following conditions hold:

- $(k, k') \in E(H)$ and $(l, l') \in E(H)$.
- An edge $(v, u) \in E(G_i)$ is labeled k' near v and l' near u.

In this slightly more general definition, the middle step in the "zigzag" is stochastic (with c possibilities), whereas it was deterministic in the original definition of [RVW00]. Nevertheless, the basic property that a uniform distribution on the vertices of a cloud around some vertex of G would be dispersed by this step to adjacent clouds according to the random walk on G is maintained. Thus, it is easy to see that the basic eigenvalue bound in [RVW00] carries over without change to this more general definition, to give

Theorem 2.1 *The graph $G \textcircled{z} H$ is an $[nm, cd^2, f(\lambda, \mu)]$-graph, with the function $f(\lambda, \mu)$ satisfying*

- *For every $\lambda < 1, \mu < 1$, we have $f(\lambda, \mu) < 1$.*
- *$f(\lambda, \mu) \leq \lambda + \mu + \mu^2$.*

We will use only the first bound in this paper, to conclude that whenever G and H are expanders, so is $G \textcircled{z} H$. We also use the (easy) reverse direction of this implication, saying that if either G or H fails to be an expander, so does $G \textcircled{z} H$. In particular, it is easy to see that under the notation of the previous theorem $\lambda(G \textcircled{z} H) \geq \lambda(G)$.

2.2 Groups and the semi-direct product

Let A and B be finite groups. Assume that B *acts* on A, namely there is a homomorphism from B to the automorphism group of A. For elements $a \in A, b \in B$ we use a^b to denote the action of b on a. We also use a^B to denote the orbit of a under this action. Here is an example of such action which will be used in the next sections.

Example 2.2 *Let $\rho : B \to GL(n, F)$ be any representation of a group B. Let A be the Abelian group F^n. Then for every $a \in A, b \in B$ we have $a^b = \rho(b) \cdot a$ with $\cdot$ representing matrix vector product over F.*

We will represent groups multiplicatively, and 1 will denote the identity of the group (no confusion should arise between the identity elements of different groups).

The *semi-direct product* of A and B, denoted $A \rtimes B$, is the group whose elements are the ordered pairs $\{(a, b) : a \in A, b \in B\}$, with the group operation defined by

$$(\hat{a}, \hat{b})(a, b) = (\hat{a}a^{\hat{b}^{-1}}, \hat{b}b)$$

It is easy to verify that indeed this operation defines a group[4] when B acts on A.

When we talk about generators of a group, we shall always mean a multiset of generators, that is, we allow repetitions. Let α be a generating (multi)set for A. We will work only with symmetric generating (multi)sets, namely the number of occurrences of a and a^{-1} in α is the same for every $a \in A$.

The Cayley graph of a group A with a (multi)set of generators α, denoted $C(A, \alpha)$, has vertices A and for every vertex $x \in A$ and generator $a \in \alpha$ there is an edge (x, xa). Moreover, the edges are naturally labeled as follows: the label of (x, xa) near x is a (and its label near xa is a^{-1}). Note that the graph is $|\alpha|$-regular.

Now we are ready to describe our main construction. Assume that B acts on A as above. Let α, β be sets of generators for A, B respectively, and further assume that α is a (disjoint) union of B-orbits, namely

[4] In fact $A \rtimes B$ is the smallest group G generated by copies of A and B s.t. A is normal in G and the action of B on A within G by conjugation is the original given action.

$\alpha = \bigcup_{i=1}^{c} a_i^B$. Define the following set of generators for $A \rtimes B$:

$$\gamma = \{(1,b)(a_i,1)(1,b') \,:\, b,b' \in \beta,\, i \in [c]\}$$

Note that $|\gamma| = c|\beta|^2$, and that $G = C(A,\alpha)$ is the edge-disjoint union of the c graphs $G_i = C(A, a_i^B)$, where the edges of G_i around every vertex are labeled by the elements of B in the obvious way. This enables us to define the zigzag product $C(A,\alpha)ⓩC(B,\beta)$ and notice (syntactically using the definitions of semi-direct product and zig-zag product) that following a generator of γ from an element of $A \rtimes B$ leads us to its "zig-zag" neighbour in that group. This gives our main conceptual connection:

Theorem 2.3 $C(A \rtimes B, \gamma) = C(A,\alpha)ⓩC(B,\beta)$

Thus, if $C(A,\alpha)$ and $C(B,\beta)$ are expanders, and $|\beta|, c$ are constants, then regardless of the size of α, the graph $C(A \rtimes B, \gamma)$ is a constant degree expander. This suggests a method for constructing large constant-degree expanders from small ones, that we follow in the next section.

3 Abelian expanders generated by few orbits

It is easy and well known that in order that Cayley graphs of Abelian groups be expanding, the generating set cannot have constant size; indeed, it has to grow logarithmically in the size of the group- [Kl84], see also [AR94]. In this section we show that under very general situations, the orbit (under a natural group action) of a *constant* number of group elements in an Abelian group is an expanding generating set.

Let q be a prime, B a group, F_q the finite field of q elements, and $\rho : B \to GL(r, F_q)$ an irreducible[5] representation over F_q of dimension r. Taking $A = F_q^r$, we have a natural action of B on A, namely $a^b = \rho(b)\cdot a$.

As formally stated in the main theorem of this section below, in this very general situation, the orbits of almost all pairs of vectors in A are expanding!

Theorem 3.1 *For every q there exists $\lambda_q < 1$ such that the following holds.*

For every B and A as above, there exist two elements $a_1, a_2 \in A$, so that

$$\lambda(C(A, \{a_1^B, a_2^B\})) \le \lambda_q$$

Moreover, if a_1, a_2 are chosen independently at random from A, the probability that they fail to satisfy the bound above is $2^{-\Omega(r)}$.

[5] All this means is that there is no nontrivial invariant subspace of F_q^r

Proof: We present the proof for $q = 2$. The argument for general q is similar, but the calculations are a bit more tedious. So from here on $A = F_2^r$, and here we write it additively.

First, since A is Abelian, the eigenvalues of $C(A,\alpha)$ can be expressed in terms of the characters of A. If χ is any character, then the corresponding eigenvalue is $\lambda_\chi = \frac{1}{|\alpha|}\sum_{a\in\alpha}\chi(a)$. Each character χ of A corresponds to a vector $x \in A$ such that $\chi(a) = (-1)^{x\cdot a}$ where $\cdot$ denotes the inner product over F_2. Therefore we have an elegant bound on $\lambda(C(A,\alpha))$: some notations are needed first; define a binary vector of length m to be δ-balanced if at least δm of its coordinates are 0 and at least δm coordinates are 1. Also, for a vector $x \in A$ and a sequence $Y \subseteq A$ let $x \cdot Y$ denote the vector of inner products of x with the members of Y.

Claim 3.2 *If for every $x \in A$, $x \neq 0$ the vector $x \cdot \alpha$ is $\delta/2$-balanced, then $\lambda(C(A,\alpha)) \le 1 - \delta$.*

We will fix $\delta = .01$, and aim to prove the theorem with $\lambda_2 = .99 = 1 - \delta$. As α in our case is the union of two orbits, it would clearly suffice to find a_1, a_2 such that for every $0 \neq x \in A$ at least one of the vectors $x\cdot a_1^B$, $x\cdot a_2^B$ is δ-balanced. This will be done by choosing a_1, a_2 independently at random from A, and using the following bound.

Claim 3.3 *Fix $0 \neq x \in A$, and choose a uniformly at random from A. Then*

$$Pr[x \cdot a^B \text{ is not } \delta - \text{balanced}] \le 2^{-3r/4}$$

We now prove this claim. It is more convenient to consider the vector $x^B \cdot a$ (by doing this we actually replace ρ by its adjoint representation acting on the functionals of A, but this is also an irreducible representation). Since ρ is irreducible and $x \neq 0$, we know that there must be a subset $R \subseteq B$ of size $|R| = r$ such that the set of vectors x^R are linearly independent. Therefore, also the (shifted) sets x^{bR} are linearly independent for every $b \in B$. Set $\epsilon = 2^{-3r/4}/2$, and let $E(b)$ denote the event that $x^{bR} \cdot a$ is not 2δ-balanced. Now the proof follows from three easy observations.

- For every b, $Pr[E_b] \le \epsilon$. This follows (with room to spare) from the Chernoff bound since the vector $x^{bR}\cdot a$ is uniformly distributed in A. This is so since a is chosen uniformly at random, and x^{bR} defines a nonsingular transformation of A.

- The probability that E_b holds for at least half the elements $b \in B$ is at most 2ϵ. This follows by Markov's inequality from the bound above.

- If E_b fails for at least half of $b \in B$, then $x^B \cdot a$ is δ-balanced, as required. This is so since the translates bR cover every element of B exactly r times.

■

One can extend the theorem above to situations in which the representation is not irreducible. Note that the only way irreducibility was used above was to argue that for every $x \in A$, $x \neq 0$ we have $rk(x^B) = r$ (where rk is the rank of this set of vectors, or more precisely, the dimension of the linear space they span).

The probabilistic argument in the proof works just as well when we have sufficiently good bounds on the number of vectors x for which $rk(x^B)$ is small.

Theorem 3.4 *Let $A = F_q^r$ be any invariant space of* any *representation of B. Let k_s be the number of elements $x \in A$ for which $rk(x^B) = s$. Let d be an integer such that $\sum_{s=0}^{r} k_s q^{-ds} \leq 1/2$. Then there are c elements $a_i \in A$, with $c \leq O(d)$, such that*

$$\lambda(C(A, \{a_i^B \ : \ i \in [c]\})) \leq 1/2$$

Proof: (Sketch)
The idea is to use Claim 3.3 (extended naturally for general q, not necessarily $q = 2$) separately for different values of r. The condition of the theorem guarantees that with positive probability, the orbits of c randomly chosen elements a_i will form a balanced set. ■

Two interesting special cases of the above (with a suitable tuned computation) are the following:

Theorem 3.5 *Let $B = SL_2(p)$ for some prime p, and consider the permutational representation on $A = F_2^{p+1}$ induced by the Mobius action of B on the projective line $P_1 = Z_p \cup \{\infty\}$ (defined in Section 4). Then there exist two elements $a_1, a_2 \in A$, so that*

$$\lambda(C(A, \{a_1^B, a_2^B\})) \leq .99.$$

Proof: (Sketch)
While this representation is not irreducible, it decomposes into one representation of dimension 1 and another irreducible representation, so for all vectors $x \in A$ which are not constant in all coordinates, $rk(x^B) = p$, which suffices for the probabilistic argument. ■

A similar argument gives the following.

Theorem 3.6 *For every q there is $\lambda_q < 1$ so that the following holds. Let $B = Z_p$ for any prime p, such that q is a generator of the multiplicative group Z_p^*, and let B act on $A = F_q^p$ by cyclic permutation of the coordinates. Then there exist two vectors $a_1, a_2 \in A = F_q^p$, so that*

$$\lambda(C(A, \{a_1^B, a_2^B\})) \leq \lambda_q.$$

It is a good question if the last theorem provides an infinite family of expanders for a given fixed q. The famous Artin Conjecture states that the theorem's hypothesis, namely that q is a generator of Z_p^*, holds for *every* prime q. It was proven by Heath-Brown [HB86] that the Artin Conjecture fails for *at most* two primes, thus e.g. at least one of the primes $q \in \{2, 3, 5\}$ gives an infinite family.

This last family of expanders is particularly interesting, since it yields asymptotically good (constant rate and linear distance) family of linear codes, whose generator matrix is the concatenation of two circulant matrices. It is an interesting problem to construct such codes explicitly.

4 Expansion is not a group property

Consider the group $B_p = SL_2(F_p)$, the group of all 2×2 invertible matrices over F_p with determinant 1. It is well known that it has a bounded set of expanding generators. In particular, let

$$M_1 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, M_2 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

Theorem 4.1 *[L94] There is a constant $\lambda < 1$ such that for every prime p,*

$$\lambda(C(SL_2(F_p), \{M_1, M_2\})) \leq \lambda$$

Let $P_1 = F_p \cup \{\infty\}$ be the projective line, and consider the Mobius action of $SL_2(F_p)$ on P_1 given by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}(x) = \frac{ax + b}{cx + d}.$$

Let $A_p = F_2^{P_1}$, and consider the action of B_p on A_p induced by the Mobius permutation of the coordinates as above.

Now let $a_1(p), a_2(p) \in A_p$ satisfy Theorem 3.5. Further let $e(p)$ be a fixed unit vector in A_p.

Now we are ready to describe a counterexample to the Lubotzky-Weiss question. The proof follows directly from the discussion in the previous sections and the fact that for the Boolean cube C on $p + 1$ vertices, the normalized second largest eigenvalue is $1 - \frac{2}{p+1}$.

Theorem 4.2 • *There is a constant $\delta < 1$ such that for every prime p*

$$\lambda(C(A_p \rtimes B_p, S_1)) \leq \delta,$$

where

$$S_1 = \{(1, M_i)(a_j(p), 1)(a, M_k) \ : \ 1 \leq i, j, k \leq 2\}.$$

- *For every prime p, the (normalized) second largest eigenvalue of $C(A_p \rtimes B_p, S_2)$, where*

  $$S_2 = \{(1, M_i)(e(p), 1)(1, M_k) \ : \ 1 \leq i, k \leq 2\}.$$

  is at least $1 - 2/(p+1)$.

5 Conclusions and Further Directions

The main conceptual contribution of this paper is the connection between zigzag products of graphs and semi-direct products of groups. This connection raises a variety of questions for further study, some of which we have started to look at here, and others that are wide open. We mention a few below.

One interesting possibility this connection raises is that one might be able to construct infinite families of expanding Cayley graphs *from scratch*. Perhaps there is an iterative construction similar to [RVW00] in the group theoretic setting. A step in this direction was recently taken by Meshulam and Wigderson [MW01]. They give an iterative construction of groups G_n and generating sets for them S_n such that $\lambda(C(G_n; S_n)) \leq 1/2$, and $|S_n| = O(\log^{(n/2)} |G_n|)$ (where $\log^{(k)}$ denotes k iterations of the logarithm function). In words, these are expanding groups of nearly constant number of generators. Moreover, they are quite different than other expanding groups – these groups are solvable, and contain huge Abelian subgroups. The analysis extends ideas from this paper, combining it with estimates on the distribution of dimensions of irreducible representations of the groups involved. This is needed to guarantee a distribution of ranks of the type assumed in Theorem 3.4.

There is still much to do in this direction. For one, it would be nice to get the generating sets down to constant size. But a more serious problem is the probabilistic nature of the argument. It would be nice to find explicit balanced sets which are the union of few orbits even for special cases. Doing so e.g. for the cube F_2^n under the action of the cyclic group C_n would give an extremely concisely described, asymptotically good, linear error correcting code obver $GF(2)$.

Finally, while we have exhibited groups whose expansion in (constant degree) Cayley graphs depends on the choice of generators, these groups are somewhat "nonstandard". It would be interesting to decide whether the groups $SL_2(p)$ are expanding with *every* choice of generators, and whether the groups S_n are expanding with *none*.

Acknowledgments

We are grateful to R. Meshulam, A. Potapchik, A. Rapinchuk, and S. Vadhan for fruitful conversations.

References

[A86] N. Alon, "Eigenvalues and expanders", Combinatorica 6(1986), pp. 83-96.

[AM84] N. Alon and V.D. Milman, "Eigenvalues, expanders and superconcentrators", Proc. 25^{th} Annual Symp. on Foundations of Computer Science (FOCS), Singer Island, Florida, IEEE(1984), pp. 320-322. Also: "λ_1, Isoperimetric Inequalities for Graphs and Superconcentrators," *J. Combinatorial Theory Ser. B* 38 (1985), pp. 73-88.

[AR94] N. Alon and Y. Roichman, "Random Cayley graphs and expanders", Random Structures and Algorithms 5 (1994), pp. 271-284.

[GG81] O. Gabber and Z. Galil, "Explicit Construction of Linear Sized Superconcentrators," *J. Comp. and Sys. Sci* 22 (1981), pp. 407-420.

[G00] M. Gromov, "Spaces and Questions", GAFA 2000, Special Volume, Part I, Birkhäuser Verlag, Basel (2000), pp. 118-161.

[G83] M. Gromov, "Filling Riemanian Manifolds" Journal of Differential Geometry, 18, pp. 1–147, 1983.

[HB86] R. Heath-Brown, "Artin conjecture for primitive roots" *Quarterly J. of Math. Oxford* (2) 37 (1986) pp. 27-38.

[Kl84] M. Klawe, "Limitation on explicit constructions of expanding graphs", SIAM J. Comput. 13 (1984), 156–166.

[LPS88] A. Lubotzky, R. Philips, P. Sarnak, "Ramanujan Graphs", *Combinatorica* 8 (1988), pp. 261-277.

[L94] A. Lubotzky, Discrete Groups, Expanding Graphs and Invariant Measures, Progress in Math. 125, Birkhaüser Verlag, Basel 1994.

[LW93] A. Lubotzky, B. Weiss, Groups and expanders, in: "Expanding Graphs" (ed. J. Friedman), DIMACS Ser. Discrete Math. Theoret. Compt. Sci. 10 pp. 95–109, Amer. Math. Soc., Providence, RI 1993.

[LP00] A. Lubotzky, I. Pak, "The product replacement algorithm and Kazhdan property (T)", J. of the AMS 14 (2000), 347-363.

[LR92] J.D. Lafferty, D. Rockmore, Fast Fourier analysis for SL_2 over a finite field and related numerical experiments, Experiment. Math 1 (1992), 115–139.

[Mar73] G.A. Margulis, "Explicit Construction of Concentrators," *Problems of Inform. Transmission* (1973), pp. 325-332.

[Mar88] G. A. Margulis, "Explicit group-theoretical constructions of combinatorial schemes and their application to the design of expanders and superconcentrators", Problems of Information Transmission 24(1988), pp. 39-46.

[MW01] R. Meshulam and A. Wigderson, "Expanders in Group algebras", in preparation.

[R97] Y. Roichman, "Expansion properties of Cayley graphs of the alternating group", J. Combin. Theory Ser. A 79 (1997), 281–297.

[RVW00] O. Reingold, S. Vadhan and A. Wigderson, "Entropy Waves, The Zig-Zag Graph Product, and New Constant-Degree Expanders and Extractors" *Proc. of the 41st FOCS* (2000), pp. 3–13.

[Tan84] R.M. Tanner, "Explicit Construction of Concentrators from Generalized N-gons," *SIAM J. Alg. Discr. Meth.* 5 (1984), pp. 287-293.