Irish Math. Soc. Bulletin
Number 71, Summer 2013, 21–31
ISSN 0791-5578

EXPANDER FAMILIES, GROUP STRUCTURE, AND SEMIDIRECT PRODUCTS

MATTHEW AIVAZIAN AND MIKE KREBS

Abstract. Expander families are, essentially, sequences of large, sparse, pseudorandom graphs. Many such families have been constructed as Cayley graphs. It is an interesting and open question to determine which groups yield Cayley graphs that form expander families. In this paper, we give a brief survey of expander families, with an emphasis on known results pertaining to that question. One minor new result is a necessary but insufficient condition for a sequence of finite solvable groups, each constructed by iterating semidirect products, to yield an expander family as a sequence of Cayley graphs.

1. Introduction

Roughly speaking, expander families model large, fast, cheap, and reliable communication networks. Alternatively, one can view them as large, sparse, pseudorandom regular graphs. In §2, we give the precise definitions. Expander families have a multitude of real-world applications (especially in computer science) as well as connections to many other branches of mathematics. In part for these reasons, a great deal of research has been done on them recently. In §3, we provide a short survey of known results and open problems. For an elementary introduction to the subject, we refer to [9]; for an advanced discussion, see [10].

One common method for forming expander families is the Cayley graph construction. It is an open problem to find necessary and sufficient conditions for a sequence of finite groups to admit an expander family as a sequence of Cayley graphs. The class of

Key words and phrases. expander graph, expander family, solvable group, semidirect product.

Received on 30-7-2012; revised 28-1-2013 and 14-4-2013.

The authors would like to thank the referee for many helpful suggestions, as well as Michael Locke McLendon for his advice on naming conventions.

nonabelian simple groups was resolved (in the affirmative) only recently, after several decades' work; the final case was proved in 2011 by Emmanuel Breuillard, Ben Green, and Terence Tao [4]. In §4, we discuss in more detail what is known about the relationship between group structure and expansion.

Section 5 is guided by the principle that one ought to begin as simply and as generally as possible. It is known that many classes of groups, including abelian groups, do not yield expander families. We begin the section by surveying several previously established positive results concerning solvable groups and iterated semidirect products, as our view is that the family of groups which is easiest to analyze but is not yet excluded is the family of groups constructed by recursively forming semidirect products with cyclic groups. A new result (Theorem 5.1) provides a necessary but insufficient condition for a sequence of groups so constructed to yield an expander family.

2. Basic definitions

Definition 2.1. Let X be a finite graph with vertex set V. Let S be a set of vertices of X. We define the *boundary* of S, denoted ∂S, to be the set of edges in X incident to both a vertex in S and a vertex not in S. We define the *isoperimetric constant* of X, denoted $h(X)$, to be the minimum, over all nonempty subsets S of V containing no more than half the vertices of X, of $|\partial S|/|S|$, where $|A|$ denotes the cardinality of the set A.

Definition 2.2. Let (X_n) be a sequence of finite graphs. We say (X_n) is an *expander family* if

(1) each X_n is regular, each with the same degree, and
(2) $|V_n| \to \infty$, where V_n is the vertex set of X_n, and
(3) there exists a real number $\epsilon > 0$ such that $h(X_n) \geq \epsilon$ for all n.

Let G be a group, and let Γ be a symmetric subset of G. (Recall that to say Γ is *symmetric* means that if $\gamma \in \Gamma$, then $\gamma^{-1} \in \Gamma$.) Recall that the *Cayley graph* $\mathrm{Cay}(G, \Gamma)$ is the graph with vertex set G so that two vertices x and y are adjacent if and only if $xy^{-1} \in \Gamma$. Note that $\mathrm{Cay}(G, \Gamma)$ is regular with degree $|\Gamma|$.

Definition 2.3. Let (G_n) be a sequence of finite groups. We say that (G_n) *yields an expander family* if there exists a positive integer

d and symmetric subsets $\Gamma_n \subset G_n$ with $|\Gamma_n| = d$ for all n such that $(\mathrm{Cay}(G_n, \Gamma_n))$ is an expander family.

3. Expander families: A brief overview

There are three main approaches to determining whether a sequence of regular graphs forms an expander family: combinatorial, probabilistic, and (in the case of Cayley graphs and related constructions) representation-theoretic.

3.1. **Combinatorial methods.** The definition of the isoperimetric constant is combinatorial in nature. However, of all the existing constructions of expander families, together with the proofs they they are just that, only the one in the paper [2] uses the definition directly to prove the result.

Looking closely at the definition, one can see why it is difficult to work with. It is a minimum that ranges over the collection of all subsets of the vertex set containing no more than half the vertices. The number of possible subsets grows exponentially with the order of the graph. Consequently, most proofs have come at the problem indirectly, tying the isoperimetric constant to other graph invariants that are easier to work with.

3.2. **Probabilistic methods: Random walk theory.** The eigenvalues of the adjacency operator of a graph encode a great deal of information, though not complete information, about its structure. The book [6] provides a thorough overview of many of the connections between graph eigenvalues and other graph invariants. In the study of expander families, the most important such connection is the following double inequality, attributed to Alon, Milman, Tanner, and Dodziuk. Recall that the eigenvalues of the adjacency operator of a finite d-regular graph are all real and that for any such eigenvalue λ, we have $|\lambda| \leq d$.

Theorem 3.1. *Let X be a finite d-regular graph with isoperimetric constant h and second-largest eigenvalue λ_1. Then*

$$\frac{d - \lambda_1}{2} \leq h \leq \sqrt{2d(d - \lambda_1)}.$$

See [9] for a proof of Theorem 3.1.

The significance of Theorem 3.1 is that a sequence of d-regular graphs is an expander family if and only if λ_1 is uniformly bounded

away from d. Tools from linear algebra, such as the Rayleigh-Ritz theorem, can then be brought to bear. The landmark paper [15], which introduces the zig-zag product of graphs as well as other graph constructions, uses this approach to prove that iterating zig-zag products in an appropriate way will yield expander families.

The theory of random walks sheds some light on why we might expect λ_1 to be related to h. A large isoperimetric constant indicates that a graph is "all mixed up," that it is somewhat pseudo-random. Too much structure will cause a graph to have large sets of vertices with small boundary. Even cycle graphs furnish an illustrative example; in a $2n$-cycle, the "bottom half" of the graph forms an isoperimetric set with just two boundary edges, giving us $h = 2/n$, which vanishes as $n \to \infty$.

From the viewpoint of random walks, being "all mixed up" means that a random walker on the graph will get lost quickly on it. For a connected nonbipartite regular graph, it is known that any initial probability distribution will converge to the uniform distribution as one repeatedly takes random steps. Regarding the random walk as a Markov process on the graph, one can see quickly by diagonalizing and taking powers of the adjacency matrix that λ_1 controls the rate of this convergence.

Roughly speaking, Theorem 3.1 tells us that h is large if and only if λ_1 is small. For a d-regular graph with adjacency operator A, the Rayleigh-Ritz theorem asserts that λ_1 equals the maximum, over all unit vectors v orthogonal to the constant vector, of $\langle Av, v\rangle$. (To see why this holds, diagonalize and recall that the largest eigenvalue is d.) So to continue our rough analysis, h is large if and only if $\langle Av, v\rangle$ is small for all unit vectors v orthogonal to the constant vector. But the inner product $\langle Av, v\rangle$ is small if and only if the angle between Av and v is large, which in turn holds if and only if Av is relatively far from v. This fact—the fact that adjacency operators of graphs with large isoperimetric constant move most unit vectors a long distance—conforms with our intuition that graphs in expander families scramble everything up.

For good expansion, then, we want λ_1 to be as small as possible. However, there is an asymptotic lower bound, due to Alon and Boppona, on how small λ_1 can be. More precisely, we have the following theorem.

Theorem 3.2. *Let d be a fixed positive integer, and let (X_n) be a sequence of finite d-regular graphs whose orders approach infinity. Then* $\liminf \lambda_1(X_n) \geq 2\sqrt{d-1}$.

One can prove Theorem 3.2 by obtaining a lower bound for the number of closed walks with a given fixed point in the universal cover of a d-regular graph, that is, a d-regular tree. Alternatively, one can use the Rayleigh-Ritz theorem. Both proofs are presented in [9].

Let X be a finite regular graph with n vertices. Let $\lambda_0, \lambda_1, \ldots, \lambda_{n-1}$ be the eigenvalues of the adjacency operator of X, listed in nondecreasing order. Define

$$\lambda := \begin{cases} \max\{|\lambda_1|, |\lambda_{n-1}|\} & \text{if } X \text{ is nonbipartite} \\ \max\{|\lambda_1|, |\lambda_{n-2}|\} & \text{if } X \text{ is bipartite.} \end{cases}$$

Motivated in part by Theorem 3.2, we define a d-regular graph X to be *Ramanujan* if $\lambda \leq 2\sqrt{d-1}$. For an integer $d \geq 3$, a short computation shows that a family of d-regular Ramanujan graphs will necessarily be an expander family. Indeed, Ramanujan graphs are in some sense optimal expanders.

If $d \geq 3$ is an integer such that $d-1$ is a prime power, then there exists a family of d-regular Ramanujan graphs [5, 11, 13, 14]. For every $d \geq 3$ not of that form, it is an open problem as to whether a family of d-regular Ramanujan graphs exists.

3.3. **Representation-theoretic methods.** The vast majority of expander families have been constructed via algebraic methods, especially the Cayley graph construction. For such graphs, one can take advantage of the underlying group structure to attack the question of expansion. In particular, the adjacency operator of a finite Cayley graph enjoys a natural direct sum decomposition indexed by the irreducible linear representations of the group—see [3], for example, for a discussion of this useful fact.

In this direct sum, the trivial representation corresponds to the space of constant vectors; the nontrivial representations index the summands in its orthogonal complement. So for Cayley graphs, we expect the isoperimetric constant to be large if and only if the restriction of A to each such summand moves unit vectors far. That motivates the following definition.

Definition 3.3. Let G be a finite group. Let Γ be a subset of G. Define the *Kazhdan constant* $\kappa(G, \Gamma)$ to be the minimum value of $||\pi(\gamma)v - v||$, where γ ranges over Γ; π ranges over all nontrivial irreducible unitary representations of G; and v ranges all unit vectors in the underlying representation space of π.

(Remark: Compactness of unit spheres shows that a minimum is achieved.)

Theorem 3.4. *Let G be a finite group, and let Γ be a symmetric subset of G. Let d, h, and λ_1 be the degree, isoperimetric constant, and second-largest eigenvalue, respectively, of the Cayley graph of G with respect to Γ. Then*

$$2\sqrt{dh} \geq \kappa(G, \Gamma) \geq \sqrt{\frac{2(d - \lambda_1)}{d}}.$$

A proof of Theorem 3.4 can be found in [9] or [12].

It follows immediately from Theorems 3.4 and 3.1 that a sequence of d-regular Cayley graphs is an expander family if and only if the corresponding Kazhdan constants are uniformly bounded away from zero. Many proofs that certain families of groups yield expander families rely primarily on this fact. The point is that for many families of groups, we can use the detailed information we have about their irreducible representations to come up with a lower bound for the Kazhdan constant.

4. Group structure and expansion

Given a sequence of finite groups whose orders approach infinity, does it yield an expander family? Stated in full generality, this question remains open. However, several partial results are known.

Theorem 4.1. *Any sequence of finite nonabelian simple groups whose orders approach infinity yields an expander family.*

Several authors over several decades joined forces to prove Theorem 4.1. The proof relies on the classification of finite simple groups. The survey [8] discusses all cases except Suzuki groups, which had not yet been finished at that time. The case of alternating groups, which is dealt with [7], required special attention. The proof was completed in [4] by showing that Suzuki groups yield expander families.

Although the answer is positive for nonabelian simple groups, not so for perfect groups. The n-fold product G_n of the alternating group on 5 letters provides a counterexample; indeed, given any positive integer d, then for sufficiently large n no set of d elements will generate G_n, so the associated Cayley graphs will be disconnected and therefore have vanishing isoperimetric constant.

We now turn our attention to negative results.

Lemma 4.2. *No sequence of abelian groups yields an expander family.*

The idea of the proof is that expander families have logarithmic diameter (as a function of the number of vertices), whereas for Cayley graphs on abelian groups, the diameter grows at least as fast as a root function. For details, see [9, Prop. 4.25].

Lemma 4.3. *Let (G_n) and (Q_n) be sequences of finite groups such that each Q_n is a homomorphic image of G_n. Suppose that $|Q_n| \to \infty$ and that (Q_n) does not yield an expander family. Then (G_n) does not yield an expander family.*

Proof. The idea of the proof is to project down from a Cayley graph on G_n to a corresponding Cayley graph on Q_n, then take the inverse image of a subset of Q_n that achieves the minimum in the definition of isoperimetric constant. For details, see [9, Prop. 2.20]. □

Lemma 4.4. *Let (G_n) be a sequence of finite groups with $|G_n| \to \infty$. For each n, let H_n be a subgroup of G_n. Suppose that the sequence $[G_n : H_n]$ of indices is bounded. If (H_n) does not yield an expander family, then G_n does not yield an expander family.*

The idea of the proof of Lemma 4.4 is to use Schreier generators to transfer from G_n to H_n. For details, see [9, Prop. 2.46].

The paper [12] also discusses other restrictions to expansion, from a function-analytic point of view.

5. Expanders and semidirect products

Cyclic groups are nearly always the easiest family of groups to work with. However, Lemma 4.2 shows that no sequence of cyclic groups yields an expander family. Next, one might consider dihedral groups, which are in some sense next-easiest. Lemmas 4.2 and 4.4 together imply, though, that the dihedral groups also do not

yield an expander family. More generally, a sequence $(H_n \rtimes K_n)$ of semidirect products of cyclic groups cannot yield an expander family, for either the sequence (K_n) of quotients is unbounded, or else the sequence (H_n) of subgroups has bounded index. Proceeding inductively, we see that no sequence of groups, each constructed by iterating semidirect products of cyclic groups k times for some fixed positive integer k, can yield an expander family.

With that in mind, we consider sequences of groups constructed recursively as follows. Let (K_n) be a sequence of cyclic groups. Let $G_1 = K_1$. Let $G_{n+1} = G_n \rtimes K_n$. Can a sequence (G_n) so constructed yield an expander family?

We begin by discussing several known results relevant to this question, some of which suggest that this construction is not as unpromising as it first appears. We then conclude by proving a necessary condition for such a sequence of iterated semidirect products to yield an expander family and by giving an example to show that this condition is not sufficient.

5.1. **Known results.** Any group constructed by iterating semidirect products of cyclic groups will necessarily be solvable. Perhaps solvability precludes expansion? Almost, but not quite. Lemmas 4.2, 4.3, and 4.4 together imply that no sequence of solvable groups *with bounded derived length* can yield an expander family. Lubotzky and Weiss show in [12], however, that there exists a sequence of solvable groups (indeed, p-groups) that yields an expander family.

If (X_n) is an expander family and each graph X_n has r_n vertices, then $\operatorname{diam}(X_n) = O(\log r_n)$. In other words, expander families have logarithmic diameter. Let C_k denote the cyclic group of order k, and let G_n be the wreath product of C_2 with C_n. That is, $G_n = C_2^n \rtimes C_n$, where C_n acts on C_2^n by cyclically permuting the coordinates. Then (G_n) admits a sequence of 3-regular Cayley graphs (the *cube-connected cycle graphs*) with logarithmic diameter. But each G_n has derived length 2, so this sequence cannot be an expander family. (See [9] for more details of this example.) The point here is that a semidirect products of two abelian groups admit Cayley graphs that in a sense come close to being an expander family.

In [15], Reingold, Vadhan, and Wigderson defined a new graph operation called the zigzag product. They show that iterating zigzag products appropriately will yield an expander family. In [1], Alon, Lubotzky, and Wigderson show that under certain circumstances,

the zigzag product of two Cayley graphs is a Cayley graph on the semidirect product of the two underlying groups. We note that one of the Reingold-Vadhan-Wigderson constructions, the base graph is a Cayley graph on an abelian group. In [16], Rozenman, Shalev, and Wigderson employ the results of [1] to construct expander families as Cayley graphs on iterated wreath products of alternating groups.

5.2. **Iterated semidirect products of cyclic groups.** In this subsection, we investigate the question of when groups constructed by iterating semidirect products of cyclic groups can yield expander families. We provide a necessary condition, and then give an example to show that it is not sufficient.

Theorem 5.1. *Suppose (C_n) is a sequence of nontrivial finite cyclic groups, where a_n generates C_n. Let $G_1 = C_1$. Suppose that for all $n \geq 2$, we have that $G_{n+1} = G_n \rtimes_{\theta_n} C_{n+1}$ for some homomorphism $\theta_n : C_{n+1} \to \mathrm{Aut}(G_n)$. If (G_n) yields an expander family, then $\theta_n(a_n)$ must be outer for infinitely many n.*

Proof. We first show that if G, H are groups, where H is cyclic with generator a, and $\theta : H \to \mathrm{Aut}(G)$ is a homomorphism such that $\theta(a)$ is inner, then $(G \rtimes_\theta H)' = G'$. Here we identify G and H as subgroups of $G \rtimes_\theta H$ via the embeddings $g \mapsto (g, 1)$ and $h \mapsto (1, h)$. The inclusion $G' \subset (G \rtimes_\theta H)'$ is immediate.

For the converse, we compute that

$$\begin{aligned} & (g_1 a^r)(g_2 a^s)(g_1 a^r)^{-1}(g_2 a^s)^{-1} \\ = \; & (g_1 a^r)(g_2 a^s)(x^{-r} g_1^{-1} x^r a^{-r})(x^{-s} g_2^{-1} x^s a^{-s}) \\ = \; & (g_1 x^r g_2 x^{-r} a^{r+s})(x^{-r} g_1^{-1} x^{-s} g_2^{-1} x^{r+s} a^{-r-s}) \\ = \; & g_1 x^r g_2 x^{s-r} g_1^{-1} x^{-s} g_2^{-1} x^{-s} \\ = \; & (g_1 x^r)(g_2 x^s)(g_1 x^r)^{-1}(g_2 x^s)^{-1} \end{aligned}$$

where $\theta(a)$ is the inner automorphism $g \mapsto xgx^{-1}$. Therefore $(G \rtimes_\theta H)' = G'$.

Therefore, if only finitely many $\theta(a_n)$ are outer, then $|G_n/G_n'| \to \infty$. Observe, however, that together Lemmas 4.2 and 4.3 imply that if $(|G_n/G_n'|)$ is unbounded, then (G_n) does not yield an expander family. The theorem follows. □

We now show that the converse of Theorem 5.1 fails; that is, we exhibit an example of a sequence (G_n) of groups constructed as in

Theorem 5.1 but with infinitely many (indeed, all but finitely many) of the θ_n outer such that (G_n) does not yield an expander family.

We construct (G_n) as follows. Let $G_1 = \mathbb{Z}_2$, the group of integers modulo 2 under addition. Let $G_2 = \mathbb{Z}_2 \times \mathbb{Z}_2$. (Recall that the direct product is a special case of the semidirect product.) Define $\theta_2 : \mathbb{Z}_2 \to \mathrm{Aut}(G_2)$ by $\theta_2(1) : (a, b) \mapsto (b, a)$. Let $G_3 = G_2 \rtimes_{\theta_2} \mathbb{Z}_2$. Observe that $G_3 \cong D_4$, the dihedral group of order 8. Define the dihedral group of order $2n$ by $D_n := \langle r, s \mid r^n = s^2 = 1, rs = sr^{-1} \rangle$. Define $\tau : \mathbb{Z}_2 \to \mathrm{Aut}(D_n)$ by $\tau(1) : r \mapsto r^{-1}$ and $s \mapsto rs$. For $n \geq 4$, let $G_n = D_{2^{n-2}} \rtimes_\tau \mathbb{Z}_2$. Observe that $D_{2^{n-1}} \cong G_n$ by the isomorphism $r \mapsto (s, 1), s \mapsto (1, 1)$. So the sequence (G_n) is indeed constructed by iterating semidirect products with cyclic groups.

When n is even, the commutator subgroup of D_n is generated by r^2 and so has order $n/2$. Hence, for $n \geq 4$, we have

$$|(D_{2^{n-2}} \rtimes_\tau \mathbb{Z}_2)'| = |D'_{2^{n-1}}| = 2^{n-2},$$

whereas $|D'_{2^{n-2}}| = 2^{n-3}$. From the first half of the proof of Theorem 5.1, then, it follows that τ is outer.

It remains to be shown that (G_n) does not yield an expander family. First observe that for all n, the group G_n admits $\mathbb{Z}_{2^{n-2}}$ as a subgroup of index 2. From Lemma 4.2, we know that $(\mathbb{Z}_{2^{n-2}})$ does not yield an expander family. It then follows from Lemma 4.4 that (G_n) does not yield an expander family.

References

1. N. Alon, A. Lubotzky, and A. Wigderson, *Semi-direct product in groups and zig-zag product in graphs: connections and applications (extended abstract)*, 42nd IEEE Symposium on Foundations of Computer Science (Las Vegas, NV, 2001), IEEE Computer Soc., Los Alamitos, CA, 2001, pp. 630–637.
2. N. Alon, O. Schwartz, and A. Shapira, *An elementary construction of constant-degree expanders*, Combin. Probab. Comput. **17** (2008), no. 3, 319–327. MR MR2410389 (2009b:05070)
3. L. Babai, *Spectra of Cayley graphs*, Journal of Combinatorial Theory, Series B **27** (1979), 180–189.
4. E. Breuillard, B. Green, and T. Tao, *Suzuki groups as expanders*, Groups Geom. Dyn. **5** (2011), no. 2, 281–299.
5. P. Chiu, *Cubic Ramanujan graphs*, Combinatrica **12** (1992), 275–285.
6. F. R. K. Chung, *Spectral graph theory*, CBMS Regional Conference Series in Mathematics, vol. 92, Published for the Conference Board of the Mathematical Sciences, Washington, DC, 1997. MR MR1421568 (97k:58183)
7. M. Kassabov, *Symmetric groups and expander graphs*, Invent. Math. **170** (2007), no. 2, 327–354. MR MR2342639

8. M. Kassabov, A. Lubotzky, and Nikolov N., *Finite simple groups as expanders*, Proceedings of the National Academy of Sciences of the United States of America **103** (2006), no. 16, 6116–6119.
9. M. Krebs and A. Shaheen, *Expander families and Cayley graphs: A beginner's guide*, Oxford University Press, USA, 2011.
10. A. Lubotzky, *Expander graphs in pure and applied mathematics*, Bull. Amer. Math. Soc. **49** (2012), no. 1, 113–162.
11. A. Lubotzky, R. Phillips, and P. Sarnak, *Ramanujan graphs*, Combinatorica **8** (1988), no. 3, 261–277.
12. A. Lubotzky and B. Weiss, *Groups and expanders*, Expanding Graphs, DIMACS Series in Discrete Mathematics and Theoretical Computer Science, vol. 10, American Mathematical Society, 1993, pp. 95–109.
13. G. A. Margulis, *Explicit group-theoretical constructions of combinatorial schemes and their application to the design of expanders and concentrators*, Problems of Information Transmission **24** (1988), no. 1, 39–46.
14. M. Morgenstern, *Existence and explicit constructions of $q + 1$ regular Ramanujan graphs for every prime power q*, J. Comb. Theory, Ser. B **62** (1994), 44–62.
15. O. Reingold, S. Vadhan, and A. Wigderson, *Entropy waves, the zig-zag graph product, and new constant-degree expanders*, Ann. of Math. (2) **155** (2002), no. 1, 157–187.
16. E. Rozenman, A. Shalev, and A. Wigderson, *Iterative construction of Cayley expander graphs*, Theory Comput. **2** (2006), 91–120.

M. Aivazian received his Master's Degree in Mathematics from California State University, Los Angeles.

M. Krebs is an associate professor of mathematics at California State University, Los Angeles.

(M. Aivazian) Department of Mathematics, California State University - Los Angeles, 5151 State University Drive, Los Angeles, California 90032

(M. Krebs) Department of Mathematics, California State University - Los Angeles, 5151 State University Drive, Los Angeles, California 90032

E-mail address: maivazian@calstatela.edu, mkrebs@calstatela.edu