CAYLEY EXPANDERS AND THE ZIGZAG PRODUCT

TJADEN HESS, LINUS SETIABRATA, COSMO VIOLA

1. Introduction

An expander graph is a regular graph of low degree such that the graph is well-connected in some sense. For a d-regular graph G, define $\lambda(G)$ as the second largest eigenvalue of the normalized adjacency matrix of G. An infinite family of graphs G_n is called a **spectral expander family** if $\lambda(G_n) \leq c$ for some constant $c < 1$. For brevity of notation, we say that a d-regular graph G on n vertices is an (n, d, t)-graph if $\lambda \leq t$.

The construction of explicit infinite families of expander graphs is of significant interest, as such constructions give rise to pseudorandom generators, codes, and other useful objects[1], [2]. A breakthrough in 2002 by Reingold, Vadhan, and Wigderson demonstrated a powerful new technique for constructing such families inductively via a novel combinatorial product, the *zigzag product*, with the property that, if G is a (n_1, d_1, t_1)-graph and H is a (d_1, d_2, t_2)-graph, then the zigzag product $H \textcircled{z} G$ is a $(n_1 d_1, d_2^2, t_1 + t_2)$-graph [3].

While the zigzag product gives a combinatorial construction for expanders, there is interest in generating expander graphs with more algebraic structure; we would like to exhibit families of expanders which are Cayley graphs of some infinite family of groups. To this end, Alon, Lubotzky, and Wigderson demonstrated that the standard semidirect product on groups can, under suitable choices of generators, give a zigzag product on the Cayley graphs of the groups [4]. However, at the time there was no known explicit construction of Cayley expander graphs suitable to act as the seed for this inductive construction. More recently, Kassabov [5] gave generating sets of S_n and A_n of bounded size, from which Rozenman, Shalev and Wigderson [6] constructed a fully explicit family of constant degree Cayley expanders. In this paper, we will explore the construction of Rozenman, Shalev and Wigderson's family of Cayley expanders and the key ideas used in their paper. At the end, we will briefly discuss their extension of the Cayley graph construction to Schreier graphs, which has the additional property that each graph lifts into the next graph.

2. Background

2.1. Graph Theory.

We briefly recall the definition of the zigzag product of an (n, d_1, t_1)-graph G and a (d_1, d_2, t_2)-graph H. Here, observe that the degree of G must be the number of vertices of H (a slightly more general definition which allows G to be the edge disjoint union of $|V(H)|$-regular graphs on the same vertex set can be found in [4]). To each tuple (v, e) of a vertex $v \in V(G)$ and an edge $e \in E(G)$ incident to v, assign a number in $[d_1]$ so that for a fixed vertex v_*, the set of tuples $\{(v_*, e)\}$ are collectively assigned $[d_1]$. The zigzag product of G and H, first defined in [3], is denoted $G \textcircled{z} H$, and is the graph on vertex set $V(G) \times V(H)$, with an edge between (v, i) and (w, j) precisely if there is $i', j' \in V(H)$ so that $(i, i'), (j, j') \in E(H)$ and an edge $e = (v, w) \in E(G)$ so that (v, e) is assigned i' and (w, e) is assigned j'.

This zigzag product has nice properties; one is that $G \textcircled{z} H$ is an $(nd_1, d_2^2, t_1 + t_2)$-graph. For a graph G, define G^2 to be the graph with vertices $V(G)$ and edges corresponding to paths of length exactly 2. If N is the normalized adjacency matrix of G, then N^2 is the normalized adjacency matrix of G^2. Thus, if G is an (n, d_1, t_1)-graph, then G^2 is an (n, d_1^2, t_1^2)-graph.

Following [3], this is enough to combinatorially construct expander graphs: simply fix a $(d^4, d^2, 1/5)$-graph H, define $G_1 := H^2$, and $G_{n+1} := (G_n)^2 \textcircled{z} H$. With a bit more work, a similar construction gives explicit families of expander graphs: neighborhoods of G_{n+1} can be computed in $\operatorname{polylog}(|V(G_{n+1})|)$ time.

2.2. Group Theory.

2.2.1. *Commutators.* We will see that in many of the constructions that we present, there is a clear degenerate case when the groups involved are abelian. In fact, no infinite family of expanding abelian Cayley graphs can have constant degree, and random abelian Cayley graphs are disconnected with high probability [7]. In order for the main construction to work, all of the groups involved need to have the "commutator" property, which in some sense implies that a group is "very" non-abelian.

Definition 2.2.2. *A* ***commutator*** $[a, b] \in G$ *is defined as* $(ab)(ba)^{-1}$ *or equivalently* $aba^{-1}b^{-1}$.

Definition 2.2.3. *We say a group* G *has the* ***commutator property*** *if every element* $g \in G$ *can be written as* $g = [a, b]$ *for some* $a, b \in G$.

Note that if a and b commute, then $[a, b] = 1$, and in an abelian group there are no nontrivial commutators. Also note that the commutator property is stronger than the common group theoretic notion of a "perfect group", which requires only that the commutators of G *generate* G.

A recent result relying on the classification of simple groups showed that in fact every finite simple non-abelian group has the commutator property, which is promising for future constructions of this nature [8].

We will see in Section 5 an algorithm for solving the commutator equation $g = [a, b]$ for the groups of interest to this paper.

2.2.4. *Semidirect and Wreath Products.* We assume that the reader is familiar with groups and group actions. Recall the semidirect product:

Definition 2.2.5. *Consider two groups* K, H *with a fixed group action* φ *of* K *on* H*. Then, the group* $H \rtimes_\varphi K$ *is the set* $H \times K$ *with the operation*

$$(h_1, k_1) \cdot (h_2, k_2) = (h_1(k_1 \cdot h_2), k_1k_2).$$

We call this group the ***semidirect*** *product of* H *and* K*. When the group action is obvious, we simply write* $H \rtimes K$*.*

For our purposes, we care about a specific example of a semidirect product, the wreath product.

Definition 2.2.6. *Suppose that* A *is a group and* B *is a subgroup of* S_d*, the group of permutations on* d *elements. Then, denote by* A^d *the direct product* $\prod_{i=1}^d A$*. The group action of* B *onto* $\{1, \ldots, d\}$ *extends to a group action on elements* $(a_1, \ldots, a_d) \in A^d$ *by, for* $\tau \in B$,

$$\tau \cdot (a_1, \ldots, a_d) = \left(a_{\tau(1)}, \ldots, a_{\tau(d)}\right).$$

Then, we call the semidirect product $A^d \rtimes B$ *with this group action the* ***wreath product*** $A \wr B$.

The wreath product can be defined directly, without using the semidirect product, which can help to give a more intuitive idea of how it works. With A and $B \subseteq S_d$ as before, we can define $A \wr B$ as the group with elements $(a_1, \ldots, a_d, \tau)$, with $a_i \in A$ and $\tau \in B$ and with the operation

$$(a_1, \ldots, a_d, \tau) \cdot (b_1, \ldots, b_d, \sigma) = \left(a_1b_{\tau(1)}, \ldots, a_db_{\tau(d)}, \tau\sigma\right).$$

Thus, we can think of the wreath product as pointwise multiplication of vectors in A^d with the second vector permuted by τ, and then with the product of τ and σ appended at the end.

2.3. **Cayley Graphs.** Given a group G and a (multi-)set of generators $Y \subseteq G$, one can construct its Cayley (multi-)graph, denoted $C(G, Y)$, to be the directed graph whose vertices are elements of G and whose edges connect g to h if and only if $g^{-1}h \in Y$. If the element $g^{-1}h$ appears with multiplicity m in Y, then $C(G, Y)$ will have m many directed edges from g to h. Notice that if Y is symmetric, that is, $g^{-1}h \in G$ has the same multiplicity in Y as $(g^{-1}h)^{-1} = h^{-1}g \in G$, then $C(G, Y)$ will have m many directed edges from g to h precisely when it has m many directed edges from h to g. Thus if Y is symmetric we can think of $C(G, Y)$ as an undirected multigraph, with m edges between g and h. Note that according to the definition here, edges are of the form (g, gy) for $g \in G$ and $y \in Y$. So we see that the set of outgoing edges from a vertex g is given by *right* multiplication by generators.

In this construction, we give a family of groups $\{G_i\}$ and generating sets $\{\gamma_i\}$ so that $C(G_i, \gamma_i)$ form an expanding family. For ease of exposition, we introduce a nonstandard definition:

Definition 2.3.1. *For a group A and permutation group $B \leq S_d$ with $\bar{a} \in A^d \trianglelefteq A \wr B$ and a subset $\beta \subset B \leq A \wr B$, define*

$$\gamma(\bar{a}, \beta) = \{x\bar{a}y \colon x, y \in \beta\},$$

where $x, \bar{a}, y$ and multiplication are to be interpreted as inside $A \wr B$.

For $\bar{a} \in A^d$, we use the notation $B \cdot \bar{a} := \{b \cdot \bar{a} \colon b \in B\}$ for the B-orbit of $\bar{a}$. Note that inside the group $A \wr B$, the group action of B is given by conjugation, i.e. $b \cdot \bar{a} = b\bar{a}b^{-1}$.

A central theorem of this construction is the Cayley analogue of the zigzag theorem:

Theorem 2.3.2. *For any group A and permutation group $B \subseteq S_d$*

$$\lambda(A \wr B, \gamma(\bar{a}, \beta)) \leq \lambda(A^d, B \cdot \bar{a}) + \lambda(B, \beta).$$

We will see a sketch of a proof in the next section.

3. The Family of Expanders

To construct a family of Cayley expander graphs, Rozenman, Shalev and Wigderson define a sequence of groups $\{G_i\}_{i=1}^{\infty}$ along with generating sets $\{\gamma_i\}_{i=1}^{\infty}$ such that $\{C(G_i, \gamma_i)\}_{i=1}^{\infty}$ form an expanding family. Crucial to this construction is the observation

Lemma 3.0.1. $C(A \wr B, \gamma(\bar{a}, \beta)) = C(A^d, B \cdot \bar{a}) ⓩ C(B, \beta)$.

Proof. The vertex sets are trivially equal, since both are defined to be $A^d \times B$.

Note that because the generating set for A^d is a single B-orbit, there is a natural labeling of the edges near an element $a \in A^d$ by elements in B, where we label the edge $(a, a(b \cdot \bar{a}))$ as b. We then replace each vertex of the graph of A^d with a cloud of B, with the b-th edge of a being replaced by (a, b).

By the definition of the zigzag product, every edge is given by a "zig" from $(a, \sigma) \in A \wr B$ to $(a, \sigma\tau)$, then a "zag" specified by the label, i.e. $(a(\sigma\tau \cdot \bar{a}), \sigma\tau)$ then a final "zig" to $(a(\sigma\tau \cdot \bar{a}), \sigma\tau\zeta)$. Inside the group $A \wr B$ we see that $(a(\sigma\tau \cdot \bar{a}), \sigma\tau\zeta) = (a, \sigma)(1, \tau)(\bar{a}, 1)(1, \zeta)$. This is clearly of the form $(a, \sigma)x\bar{a}y$ for every $x, y \in \beta$, which is exactly the set of neighbors for an arbitrary vertex (a, σ) that are produced by the generating set $\gamma(\bar{a}, \beta)$. Thus, the vertex sets are identical and the neighbors of every vertex are identical, so the two sides of the equation are equal as graphs. $\square$

As a corollary, this implies Theorem 2.3.2 via the expansion properties of the standard zigzag product.

With this in mind we define $G_1 := A_d$ and $G_{n+1} := G_n \wr A_d$. To define γ_{n+1}, we will define $\beta \subseteq A_d$ and $a_n \in G_n$ so that $\lambda(A_d, \beta) < 1/1000$ and $\lambda((G_n)^d, A_d \cdot a_n) < 1/50$. Thus $\lambda(G_n \wr A_d, \gamma(a_n, \beta)) < 1/1000 + 1/50$; define $\gamma_{n+1} := \{xy \colon x, y \in \gamma(a, \beta)\}$ so that

$$\lambda(G_n \wr A_d, \gamma_{n+1}) < (1/1000 + 1/50)^2 < 1/1000.$$

Furthermore, β can be chosen so that $|\beta| < d^{1/28}/10^{40}$, so $|\gamma(a_n, \beta)| = |\beta|^2$ and

$$|\gamma_{n+1}| \leq |\gamma(a_n, \beta)|^2 = |\beta|^4 < d^{1/7}/10^{40}$$

for every n; this means that the $C(G_i, \gamma_i)$ are constant degree expanders.

Recently, Kassabov in [5] showed that for some $d \leq 10^{10^9}$, such a $\beta \subseteq A_d$ exists. It is left to define a suitable a_n (or equivalently, a suitable $A_d \cdot a_n$); we want $\lambda((G_n)^d, A_d \cdot a_n) < 1/50$. To do so, we need:

Definition 3.0.2. *Let G be a group and let $Y \subseteq G$ so that $d > |Y|$. Define $Y^{(d)}$ to be the set of* ***balanced*** *vectors, that is, the vectors $(v_1, \dots, v_d) \subseteq G^d$ such that each $u \in Y$ appears precisely $\lfloor d/|Y| \rfloor$ times and the rest of the elements are $1 \in G$.*

It is easy to see that any $Y^{(d)}$ is an A_d-orbit, as long as d is sufficiently large ($d > 2|Y|$ will do). Now, for each $a \in Y_n$, write $a = [x_a, y_a]$ and define the set

$$Y_n^* := \bigcup_{a \in \gamma_n} \{x_a, y_a, x_a^{-1}, y_a^{-1}, x_a^{-1}y_a^{-1}, y_a x_a\} \cup \{1\}.$$

Now, for some constant $c \in \mathbb{N}$ to be chosen later, we can define

$$X_n := (c \cdot Y_n) \cup Y_n^*$$

where $c \cdot Y_n$ is the multiset consisting of repeating Y_n precisely c times. Then Rozenman, Shalev and Wigderson prove:

Theorem 3.0.3. *Define $\lambda_n := \lambda(G_n, \gamma_n)$. If $d \geq k^2|X_n|^7$, then*

$$\lambda\left((G_n)^d, (X_n)^{(d)}\right) < 0.01 + \max\left\{\frac{\lambda_n + 7}{c}, \exp\left(\frac{-kc(1-\lambda_n)}{10^6}\right)\right\}.$$

Thus, a suitable a_n can be defined by picking $c = 10^3$ and $k = 10^5$. We remark that $|X_n| \leq (c+7)|\gamma_n| \leq d^{1/7}/10^{40}$; thus $k^2|X_n|^7 \leq k^2(c+7)^7 d/10^{280} < d$ and the assumption in the above theorem is always true (for the choice of parameters $c = 10^3$ and $k = 10^5$).

4. Generating sets of G^d

In Rozenman, Shalev and Wigderson's proof of Theorem 3.02, they break into two cases. Denote by $W(G)$ the vector space of real valued functions equipped with the L_2 inner product. Then, to show the theorem, we must see that for all $w \in W(G^d)_\perp$ with $\|w\| = 1$, either

$$\|\mathbb{E}_{x \in X^{(d)}}[P_x(w)]\| \leq 0.01 + \lambda + \frac{7}{c}$$

or

$$\|\mathbb{E}_{x \in X^{(d)}}[P_x(w)]\| \leq 0.01 + e^{-kc(1-\lambda)/10^6}.$$

Ultimately, they find that it is sufficient to prove this for all $w \in W_\perp^{\otimes r} \otimes W_\parallel^{\otimes(d-r)}$, where $W_\parallel$ is the subspace of constant functions and $W_\perp$ is the orthogonal complement of $W_\parallel$. Thus, they can break into two cases based upon r. When r is small, that is, $r \leq 0.1\sqrt{d/|X|}$, the proof follows somewhat quickly, and does not depend upon our choice of G. The tricky case is the case of r large. As has been the theme, the statement does not hold for abelian groups; here, then, we must leverage the properties of our chosen family of graphs. The strategy used is to first show that $G \times G$ is an expander, and then reduce the G^d case to the $G \times G$ case.

To see that $G \times G$ is an expander, first we give the following definition:

Definition 4.0.1. *For $Y \subset G$, with G a group, define $\widetilde{Y} = \{(y, y^{-1}) | y \in Y\}$.*

In this section, we will denote by Y^* the set obtained by the same construction as for γ_n^*. With these definitions in hand, we can obtain the following theorem:

Theorem 4.0.2. *If $\lambda(G, Y) < 1 - \varepsilon$, and all elements of Y are commutators of G, then*

$$\lambda(G \times G, \widetilde{Y^*}) \leq 1 - \frac{\epsilon}{21|Y^*|^2}.$$

As Rozenman, Shalev and Wigderson note, this theorem fails in abelian groups; Y can generate G, but $\widetilde{Y}$ will only generate $\{(g, g^{-1})|g \in G\}$ in this case. Likewise, $\{(y, y)|y \in Y\}$ generates $\{(g, g)|g \in G\}$, rather than the whole of G. The problem, as they note, is that the coordinates here are highly correlated. It is somewhat surprising, then, that the commutator property is sufficient to break this correlation and allow us to generate the whole group. To see why this theorem holds, note that Y^* contains, for all $y \in Y$, a_y, b_y, and $a_y^{-1}b_y^{-1}$, and note $y = [a_y, b_y]$. Thus, if Z is the set of length 3 words in $\widetilde{Y^*}$, we find that we can write

$$(y, 1) = (a_y, a_y^{-1})(b_y, b_y^{-1})(a_y^{-1}b_y^{-1}, (a_y^{-1}b_y^{-1})^{-1}),$$

so $(Y, 1) \subset Z$. Likewise, we find that $(1, Y) \subset Z$. Thus, because we had the commutator property, we are able to take the set $\widetilde{Y^*}$, where we would expect the coordinates to be correlated, and instead use the set $\{(Y, 1) \cup (1, Y)\}$, where the coordinates are uncorrelated. Because of this, we can find that

$$C(G \times G, \{(Y, 1) \cup (1, Y)\}) \subset C(G \times G, Z),$$

so we can bound the spectral gap of $C(G \times G, Z)$ and use this to prove Theorem 3.0.2. The proof of the reduction of the G^d case to the $G \times G$ case is fairly computationally involved, so we will omit it.

5. Commutators

In order for the construction to be explicit, we need an efficient algorithm for constructing an expanding generating set $\alpha \subset G_n^d$ that is a single B-orbit. We have seen that this is possible if we can find a polynomial time algorithm for solving the commutator equation $a = [b, c]$ for all $a \in G_n$. This algorithm will be defined inductively on n. For the base case, a result of [9] gives an algorithm for the commutator equation in A_d for $d \geq 5$.

Nikolov [10] showed that if A and B have the commutator property, then so does $A \wr B$. We would like an algorithmic version of this theorem. Given an oracle to the commutator algorithm for A and B, we want to find a commutator algorithm for $A \wr B$ that is poly-logarithmic in the order of $A \wr B$.

As a matter of notation, since A, A^d and B are isomorphic to subgroups of $A \wr B$, we will sometimes conflate these groups with their respective inclusions in the wreath product.

First, note that every element in $A \wr B$ can be expressed uniquely as a product $\beta\alpha$ for $\beta \in B$ and $\alpha \in A$, with $(a_1, \ldots, a_d, \sigma) = (1_A, \ldots, 1_A, \sigma)(a_1, \ldots, a_d, 1_B)$. Thus, we need to solve the equation $\beta\alpha = [b_1x, b_2y]$. Projecting $[b_1x, b_2y]$ into B, we note that the B-component of the commutator must be $[b_1, b_2]$. One can check that

$$[b_1x, b_2y] = [b_1, b_2]x^{\sigma_1}y^{\sigma_2}x^{-\sigma_3}y^{-\sigma_4}$$

$$\sigma_1 = b_2b_1^{-1}b_2^{-1} \qquad \sigma_2 = \sigma_3 = b_1^{-1}b_2^{-1} \qquad \sigma_4 = b_2^{-1}$$

where x^{σ_i} denotes the conjugation by some $\sigma_i \in B$, or equivalently the action of σ_i on x by permutation of its coordinates. We have by our hypothesis an oracle for $[b_1, b_2]$, so we need only find solutions x and y to $\alpha = x^{\sigma_1}y^{\sigma_2}x^{-\sigma_3}y^{-\sigma_4}$.

For this Rozenman, Shalev, and Wigderson give a general algorithm, which we present an outline of:

Lemma 5.0.1. *For permutations $\sigma_1, \sigma_2, \sigma_3, \sigma_4 \in S_d$ and $\alpha = (\alpha_1, \ldots, \alpha_d) \in A^d$, there exists an algorithm which solves the system of equations*

$$\alpha_i = x_{\sigma_1(i)}y_{\sigma_2(i)}x^{-1}_{\sigma_3(i)}y^{-1}_{\sigma_1(i)} \tag{1}$$

for $1 \leq i \leq d$

Proof. Note first that each $x_i, x_i^{-1}, y_i, y_i^{-1}$ appears exactly once in the system of equations. We would like to have a system of independent equations, i.e. each x_i is found in the same equation as x_i^{-1} and similarly for the y_i. This can be achieved by substitution; for each x_i not in the same equation as its inverse, solve for x_i in one equation and substitute it in the other. This gives a reduced set of independent equations.

Given this system, a theorem of [10] says that every equation contains a "hidden commutator" of the form $\delta_\ell = \zeta_1 x_i \zeta_2 y_j \zeta_3 x_i^{-1} \zeta_4 y_j^{-1} \zeta_5$ for some x_i, y_j. We can then transform this by a change of variables into a true commutator equation. Set $\tilde{x}_i := \zeta_3 x_i \zeta_4$ to see

$$\delta_\ell = \zeta_1 \zeta_4 [\tilde{x}_i, \tilde{y}_j] \zeta_3 \zeta_2 \zeta_5$$
$$[\tilde{x}_i, \tilde{y}_j] = (\zeta_1 \zeta_4)^{-1} \delta_\ell (\zeta_3 \zeta_2 \zeta_5)^{-1}.$$

Using our oracle for commutator equations in A, we can solve this for $\tilde{x}_i$ and then recover x_i via the change of variable equation. Thus, we can find x_i and y_i for all i, and so we have the $x, y \in A^d$ that solves the commutator equation in the wreath product.

In all, this algorithm runs in time $\operatorname{polylog}(|G_n|)$ for all n, and thus is explicit. □

6. Schreier Graphs and Lifts

Another significant set of graphs which are described algebraically are the Schreier graphs. Rozenman, Shalev and Wigderson define them as follows:

Definition 6.0.1. *Fix a finite group H and a subgroup H'. Let U be a symmetric set of elements in H. Then, $\mathrm{Sch}(H, H', U)$ is the graph with vertex set H/H' and edges (gH', ugH'), with $g \in H$ and $u \in U$.*

This will be a $|U|$-regular graph. Notice that if H' is trivial, then this is just the Cayley graph $C(H, U)$. Furthermore, they show that $\lambda(\mathrm{Sch}(H, H', U)) \leq \lambda(C(H, U))$, so we can study the spectral gap of all the Schreier graphs of H just by studying the spectral gap of the Cayley graph of H.

We define the following sequences of groups as Rozenman, Shalev and Wigderson do:

Definition 6.0.2. *For some K a subgroup of S_d, let $K_1 = K$ and $K_{n+1} = K_n \wr K$. Let $T_{n,d}$ be the rooted depth n d-regular tree. Let $Sym(n, d)$ be the symmetry group on $T_{n,d}$. Then, let E_n be the leaves of $T_{n,d}$; note that $Sym(n, d)$ acts naturally on E_n.*

Ultimately, they use these to give a similar theorem as for Cayley graphs:

Theorem 6.0.3. *For a generating set $Q \subset K$ satisfying that $|Q| \leq d^{1/4}/2$ and $\lambda(K, [d], Q) \leq 1/4$, then there exist sets $Q_n \subset K_n$ with $\lambda(K_n, E_n, Q_n) \leq 1/4$, and Q_n is computable in* $\operatorname{polylog}(|E_n|)$ *time.*

This theorem is proven using the zigzag product, as was done using Cayley graphs. Such sets Q exist for many groups K; the authors go on to see specifically that, for $K = S_d$ with d sufficiently large, such a Q exists. This is done by noting that the probability that, for $d \geq 100$, a random subset of 100 permutations satisfied the needed property with probability at least $1/2$, which was shown by Friedman in [11].

Now, we define what it means for a graph to lift.

Definition 6.0.4. *Let X be a graph on vertices $v_1, \ldots, v_n$. Then, a **d-lift** of X is a graph Y with vertices $w_{i,k}$ for $i \in [n], k \in [d]$. Note that there are nd such vertices. Then, the edge set of Y is given by, for all $e = (v_i, v_j)$ in the edge set of X, the edges $(w_{i,k}, w_{i,\sigma_e(k)})$ for all k, with $\sigma_e \in S_d$. We call for any fixed i the set $\{w_{i,k} | k \in d\}$ the **fiber** above v_i.*

Rozenman, Shalev and Wigderson then describe some properties of lifts. Note that if X is d-regular, then a lift of X is also d-regular by definition. Lifts are transitive, in that if X lifts to Y and Y lifts to Z, then X lifts to Z. Finally, they note that $\lambda(Y) \geq \lambda(X)$ if Y is a lift of X.

The question is, then, what are interesting examples of lifts in graphs? As it turns out, the set of Schreier graphs they gave above satisfy this lifting property:

Theorem 6.0.5. $\mathrm{Sch}(K_n, E_n, Q_n)$ *d-lifts to* $\mathrm{Sch}(K_{n+1}, E_{n+1}, Q_{n+1})$.

Then, letting $K = S_d$ where $d \geq 4 \cdot 100^4$. The Q shown to exist earlier will work for this construction. This is shown inductively, and hinges on the existence of an infinite set Q_∞. This set has the following property:

Theorem 6.0.6. *There is a natural map from $Sym(n,d)$ to $Sym(k,d)$, given by restricting $\tau \in Sym(n,d)$ to the first k levels of $T_{n,d}$. We call this map the restriction map. We can also define $Sym(\infty,d)$, the group of symmetries on the infinite d-regular tree. Then, there exists a subset Q_∞ of $Sym(\infty,d)$ such that, for all n, Q_n is the restriction of Q_∞ to $Sym(n,d)$.*

Using this, Rozenman, Shalev, and Wigderson obtain a sequence of expander graphs with the desired lifting property. This exemplifies the potential of the wreath product construction. Though we originally used it to construct Cayley expanders, it can be used to produce other types of expanders too, which may themselves have other interesting properties.

7. Future Directions

While the construction of Rozenman, Shalev, and Wigderson is explicit in the sense that the neighbors of a vertex can be found in time polynomial in the length of the index of the vertex, the construction suffers from large constants in that the main theorem holds only for A_d with $d \geq 10^{10^9}$, and thus the smallest usable seed group in this construction has size $(10^{10^9})!$ which is too large for any practical application. Thus, we should be interested in other similar iterative constructions using the semidirect product but with alternative seed groups. The recent proof of the Ore conjecture gives hope that possibly some other family of finite simple groups may give rise to an analogous expander family. Using the semidirect product construction, [4] shows that expansion is not a group property, that is there exist groups for which only certain bounded size generating sets give rise to expanding Cayley graphs. Thus, constructing expanding Cayley graphs is as much an exercise in constructing good generating sets as it is about choosing amenable families of groups.

8. Acknowledgements

This paper was written for Eshan Chattopadhyay's CS 6815 class on pseudorandomness at Cornell University.

References

[1] Avi Wigderson and David Zuckerman. Expanders That Beat the Eigenvalue Bound: Explicit Construction and Applications. *Combinatorica*, 19(1):125–138, January 1999.
[2] Hoory, Shlomo, Linial, Nathan, Wigderson, and Avi. Expander Graphs and Their Applications. *Bull. Amer. Math. Soc.*, 43(4):439–561, 2006.
[3] Omer Reingold, Salil Vadhan, and Avi Wigderson. Entropy Waves, the Zig-Zag Graph Product, and New Constant-Degree Expanders. *arXiv:math/0406038*, June 2004.
[4] N. Alon, A. Lubotzky, and A. Wigderson. Semi-Direct Product in Groups and Zig-Zag Product in Graphs: Connections and Applications. In *Proceedings 2001 IEEE International Conference on Cluster Computing*, pages 630–637, October 2001.
[5] Martin Kassabov. Symmetric Groups and Expander Graphs. *Invent. math.*, 170(2):327–354, November 2007.
[6] Eyal Rozenman, Aner Shalev, and Avi Wigderson. Iterative Construction of Cayley Expander Graphs. *Theory of Computing*, 2, 2006.
[7] Sebastian M. Cioabă. Closed walks and eigenvalues of Abelian Cayley graphs. *Comptes Rendus Mathematique*, 342(9):635 – 638, 2006.
[8] Liebeck, Martin, and O'Brien. The Ore conjecture. *Journal of the European Mathematical Society*, 012(4):939–1008, 2010.
[9] Oystein Ore. Some Remarks on Commutators. *Proceedings of the American Mathematical Society*, 2(2):307–314, 1951.
[10] Nikolay Nikolov. On the Commutator Width of Perfect Groups. *Bulletin of the London Mathematical Society*, 36(1):30–36, January 2004.
[11] Joel Friedman. A proof of Alon's second eigenvalue conjecture and related problems. *CoRR*, cs.DM/0405020, 2004.