CAYLEY GRAPHS

CAMERON FRANC

ABSTRACT. In this short note we give an introduction to some elementary properties of Cayley graphs.The first section covers the definition and gives some basic illustrative examples. Section 2 describes what it means to refer to a collection of finite groups as a *family of expanders*. The key result of that section shows that families of abelian groups are not good expanders. This helps gives context to the recent remarkable results about the expansion of families of simple groups. The third section connects eigenvalues of a Cayley graph to representation theory, with a view towards Xander's talk. While preparing this note we have followed chapter 11 of the paper [HLW06].

1. DEFINITION AND FIRST PROPERTIES

Definition 1.1. Let H be a finite group and let $S \subseteq H$ be a subset. The corresponding *Cayley graph* $C(H, S)$ has vertex set equal to H. Two vertices $g, h \in H$ are joined by a directed edge from g to h if and only if there exists $s \in S$ such that $g = sh$. Each edge is labeled to denote that it corresponds to $s \in S$. If G is a graph such that there exists a group H and generating set $S \subseteq H$ with $G \cong C(H, S)$, then G is said to be *Cayley*.

Example 1.2. If $H = \mathbf{Z}/n\mathbf{Z}$ and $S = \{1, -1\}$ then $C(H, S)$ is the cycle on n vertices.

Example 1.3. If $H = \mathbf{F}_2^n$ and $S = \{(1, 0, \ldots, 0), (0, 1, \ldots, 0), \ldots, (0, 0, \ldots, 1)\}$ then $C(H, S)$ is the n-cube.

If S generates H, then the labeled Cayley graph $C(H, S)$ uniquely determines H. However, the edge labelings are necessary for this uniqueness statement to hold.

Example 1.4. Consider $A = \mathbf{Z}/4\mathbf{Z}$ and $B = \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$. Let $S \subseteq A$ be the set $S = \{1, -1\}$ and let $T \subseteq B$ be the set $T = \{(1, 0), (0, 1)\}$. Without the labelings the Cayley graphs $C(A, S)$ and $C(B, T)$ are isomorphic, but they are distinguished via the labels.

In what follows we are concerned with using group theoretic methods to construct expander graphs, so we don't really care about all the extra structure that comes with a Cayley graph. We will thus take our sets $S \subseteq H$ to satisfy the following properties:

(1) they will be generating sets, so that $C(H, S)$ is a connected graph;
(2) we will usually consider *symmetric* sets, that is, sets which satisfy $S = S^{-1}$. Under this assumption we may treat $C(H, S)$ as an undirected graph;
(3) always assume that S does not contain the identity, so that $C(H, S)$ does not contain any loops.

Under these assumptions note that $C(H, S)$ is a connected and undirected regular graph of degree $|S|$ on $|H|$ vertices (without loops).

Inside a single group one can often find different sets of generators with the same numbers of elements, but such that the corresponding Cayley graphs are not isomorhic. For a striking example of this phenomenon one can consult the paper [LSV06] of Lubotzky, Samuels and Vishne, where the authors prove the following remarkable result

Theorem 1.5 (Lubotzky, Samuels, Vishne). *For every $n \geq 5$ ($n \neq 6$) and for every prime power $q > 2$, there exist isospectral yet nonisomorphic Cayely graphs of* $\mathrm{PSL}_n(\mathbf{F}_q)$.

Recall that *isospectral* means that the multisets of eigenvalues of the adjacency matrices of the two Cayley graphs are equal. The proof of Theorem (1.5) gives a nice illustration of the interplay between number theory and graph theory. The isospectral graphs are obtained as the 1-skeletons of certain quotients of the Bruhat-Tits building for $\mathrm{PGL}_n(F)$, where F is a local field of positive characteristic. The proof of their theorem uses infinite-dimensional representations and the theory of division algebras over global fields.

We turn now to the problem of recognizing whether a given graph is Cayley.

A graph is said to be *vertex transitive* if its automorphism group acts transitively on the vertices. Note that a vertex transitive graph is necessarily regular. For a Cayley graph $C(H, S)$, left multiplication induces a simply transitive action of H on $C(H, S)$ by graph automorphisms. This shows that every Cayley graph is vertex transitive. Conversely one has the following:

Proposition 1.6. *A connected graph G is Cayley if and only if there exists a subgroup $H \subseteq \mathrm{Aut}(G)$ which acts simply transitively on $V(G)$.*

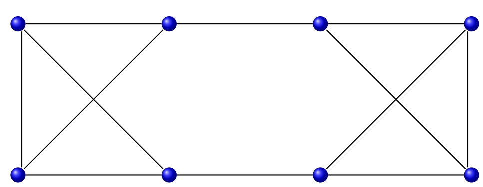
Proof. One direction is clear, so let G be a connected graph with $H \subseteq \mathrm{Aut}(G)$ acting simply transitively on $V(G)$. Fix a vertex $v \in V(G)$ and let

$$S = \{h \in H \mid hv \text{ is adjacent with } v\}.$$

This is symmetric since H acts by graph automorphisms, so that hv is adjacent with v if and only if v is adjacent with $h^{-1}v$. Define $G \cong C(H, S)$ in the following way: if $u \in V(G)$ then there exists a unique $h \in H$ with $hv = u$. Map $u \mapsto h$; similarly for edges. □

This proposition shows that not all connected regular graphs are Cayley.

Example 1.7. This is the smallest example of a connected regular graph which is not Cayley:



It is not vertex transitive: the reader can check that the top left vertex and its neighbour to the right are not mapped to one another via any graph automorphism.

More surprising is the fact that not every vertex transitive graph is a Cayley graph.

Example 1.8. The *Petersen graph*

$$[iwouldbeaPetersengraphifcamwerelesslazy]$$

is the simplest example of a vertex transitive graph which is not Cayley. Chapter 16 of [Big93] suggests proving this by considering the two nonisomorphic groups H with 10 elements, D_5 and $\mathbf{Z}/10\mathbf{Z}$, and all possible symmetric generating sets $S \subseteq H$ of size 3. The Petersen graph has been a common counterexample to many reasonable conjectures in graph theory. See the text [HS93] for more on the Petersen graph.

2. Expansion of Cayley graphs

Recall that if G is a finite graph with n vertices, then we label the eigenvalues of its adjacency matrix as

$$\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_n.$$

This ordering is possible since A is symmetric, so that its eigenvalues are real numbers. We have seen that if G is d-regular, then $\lambda_1 = d$. Also recall the following definitions:

Definition 2.1. Given a subset $S \subseteq V(G)$, the *edge boundary* of S, denoted ∂S, is the set of edges of G going between S and its complement. The (edge) *expansion ratio* of G, denoted $h(G)$, is defined as

$$h(G) = \min_{\{S \subseteq V(G) \mid 2|S| \leq |G|,\ S \neq \emptyset\}} \frac{|\partial S|}{|S|}.$$

If $G = C(H, S)$ is a Cayley graph with $|H| = n$ and $|S| = d$, then G is a graph on n vertices which is regular of degree d. It follows that its largest eigenvalue is d, and the *spectral gap* $d - \lambda_2$ is of interest due to its connection with the expansion constant $h(G)$. Indeed, earlier in our seminar series we saw that

$$\frac{d - \lambda_2}{2} \leq h(g) \leq \sqrt{2d(d - \lambda_2)};$$

for details see [AM85]. This inequality shows that a small second eigenvalue correpsonds to good expansion properties. If $G = C(H, S)$ is Cayley, then we write $\lambda(H, S)$ to denote the second eigenvalue of $C(H, S)$.

We now recall the definition of a family of expanders.

Definition 2.2. A family $\{G_i\}$ of d-regular graphs with $|G_i| \to \infty$ as $i \to \infty$ is said to be a *family of expander graphs*, or a *family of expanders*, if there exists $\varepsilon > 0$ such that $h(G_i) \geq \varepsilon$ for all i.

We say that a family of groups $\{H_i\}$ *can be made into a family of expanders* if there exists a positive integer d and a symmetric generating set $S_i \subseteq H_i$ of size d for each i, such that $\{C(H_i, S_i)\}$ is a family of expanders.

Many nice families of groups, in particular simple groups, can be made into families of expanders. This is recent work, a summary of which can be found in Xander's notes from his talk. To give an appreciation for these result, and to make use of the expander mixing lemma which we worked hard to prove earlier in the seminar series, we will prove the following negative result:

Proposition 2.3 (Proposition 11.5, [HLW06])**.** *Let H be an abelian group and let S be a symmetric generating set such that $\lambda(H, S) < d/2$. Then $|S| = O(\log |H|)$, where the implied constant depends only on $\lambda(H, S)$.*

Before we go into the proof we should explain why this is a negative result. If we apply this to a family of groups $\{H_i\}$ of increasing size, this proposition says that it is impossible to choose generating sets S_i of fixed size d and maintain the inquality $\lambda(H_i, S_i) < d/2$ for all i. If this holds then, since $|S_i|$ grows as $\log |H_i|$ by the proposition, this forces the size of the S_i's to grow to infinity with i. So there is an inherent restriction on the expansion properties of families of abelian groups: the second eigenvalue must eventually be larger than $d/2$ in such a family.

At this point we recall the definition of an (n, d, α)-graph. This is a graph G on n vertices which is regular of degree d, and such that $\lambda_2(G) \leq \alpha d$. With this notation Proposition 2.3 follows from

Proposition 2.4. *Let H be an abelian group, let $S \subseteq H$ be a symmetric generating set and let $\alpha < 1/2$ be a positive number. If $C(H, S)$ is an (n, d, α)-graph, then $|S| = O(\log |H|)$, where the implied constant depends only on α.*

We begin the proof with a lemma.

Lemma 2.5. *Let $0 \leq \alpha < 1/2$. The diameter of an (n, d, α)-graph is $O(\log n)$, where the implied constant depends only on α.*

Proof. Let G be an (n, d, α)-graph and let S and T be subsets of $V(G)$. Recall that earlier in the seminar Dylan defined $E(S, T)$ to be the collection of edges running between S and T. The *expander mixing lemma* for G gives the inequality

$$|E(S, S)| \leq d\,|S| \left(\alpha + \frac{|S|}{n}\right).$$

Write $\overline{S}$ for the complement of S. Then since G is d-regular, $E(S, S) + E(S, \overline{S}) = d\,|S|$. This relation and the identity above give

$$\left|E(S, \overline{S})\right| \geq d\,|S| \left((1 - \alpha) - \frac{|S|}{n}\right) \tag{1}$$

For each integer $k \geq 0$ and for each vertex v of G, let $B(v, k)$ denote the collection of vertices of G of distance at most k from v. If we set $S = B(v, k)$, then there are at least $\left|E(S, \overline{S})\right|/d$ vertices outside of $B(v, k)$ which are adjacent to $B(v, k)$. Thus, equation (1) implies that

$$\begin{aligned} |B(v, k+1)| &\geq |B(v, k)| + \left|E(S, \overline{S})\right|/d \\ &\geq |B(v, k)| \left((2 - \alpha) - \frac{|B(v, k)|}{n}\right) \end{aligned}$$

for all $v \in V(G)$ and $k \geq 0$. Since $\alpha < 1/2$, we have proved the following: if $|B(v, k)| \leq n/2$ then $|B(v, k+1)| \geq (1 + \varepsilon)\,|B(v, k)|$, where $\varepsilon = 1/2 - \alpha$. It follows that if we take $k \geq \log n / \log(1 + \varepsilon)$ then $|B(v, k)| > n/2$ for all vertices v of G. This means that any two balls of radius k must intersect, and so the diameter of G is at most $2k$. □

We are now ready for:

Proof of Proposition 2.4. Set $n = |H|$ and $d = |S|$. The lemma shows that the diameter of $C(H, S)$ is $O(\log n)$. Thus every element of H can be written as a product of at most $\beta \log n$ elements of S for β a possibly large constant depending only on α. But in an abelian group the number of possible distinct products of l elements of S is at most the number of monomials of degree l in d variables. Since there are $\binom{l+d-1}{d-1}$ such monomials, we deduce that

$$\sum_{l \leq \beta \log n} \binom{l + d - 1}{d - 1} \geq n.$$

One concludes by using standard approximations for binomial coefficients, for example $\binom{l}{k} \leq (le/k)^k$. □

3. Eigenvalues of Cayley graphs and representation theory

In this section we lay some groundwork for Xander's talk. We begin by recalling some facts about the (complex) representation theory of finite groups.

Let G be a finite group.

Definition 3.1. A *representation* of G is a left $\mathbf{C}[G]$-module which is finite dimensional as a vector space over $\mathbf{C}$. A *subrepresentation* of a representation V is a $\mathbf{C}[G]$-submodule of V. A representation V is said to be *irreducible* if it only contains the trivial subrepresentations (0 and V itself).

Note that to give a representation is the same as giving a finite dimensional complex vector space V, along with a group homomorphism

$$\rho\colon G \to \mathrm{GL}(V)$$

encoding the linear action of G on V. We will represent representations by the vector space V or corresponding homomorphism ρ interchangeably.

The following theorem is fundamental to the theory of representations of finite groups.

Theorem 3.2 (Maschke)**.** *Every representation of G decomposes into a direct sum of irreducible representations.*

We must recall the following facts:

(1) A group G has finitely many isomorphism classes of irreducible representations; in fact, the number of classes is equal to the number of conjugacy classes in G.
(2) The group ring $\mathbf{C}[G]$ is itself a left $\mathbf{C}[G]$-module, called the *regular representation* of G. If $V_1, \ldots, V_k$ are a full set of pairwise nonisomorphic irreducible representations of G, say with $\dim_{\mathbf{C}} V_i = d_i$ for all i, then one has the following decomposition of $\mathbf{C}[G]$ into irreducible subrepresentations:

$$\mathbf{C}[G] \cong \bigoplus_{i=1}^{k} V_i^{d_i}.$$

Given a subset $S \subseteq G$ and a representation ρ of G, write

$$S_\rho = \frac{1}{|S|} \sum_{s \in S} \rho(s) \in \mathrm{End}_{\mathbf{C}}(V).$$

Let $r\colon G \to \mathrm{GL}(\mathbf{C}[G])$ denote the regular representation of G.

Lemma 3.3. *For every symmetric subset $S \subseteq G$, the matrix of S_r in the basis $\{g \in G\}$ for $\mathbf{C}[G]$ is equal to the normalized adjacency matrix of $C(G, S)$.*

Proof. Fix the basis $\{g \in G\}$ for $\mathbf{C}[G]$ so that we may regard each $r(g)$ as a matrix. Then one easily sees that each $r(g)$ is a permutation matrix corresponding to the permutation of G obtained by multiplying on the left by g. Thus for each $s \in S$, the matrix $r(s)$ encodes the edges labeled by s via the Cayley labeling. So $\sum_{s \in S} r(s)$ is the adjacency matrix of $C(G, S)$, and dividing by $|S|$ gives the normalized adjacency matrix since $C(G, S)$ is regular of degree $|S|$. $\square$

If one combines this lemma with the decomposition of the regular representation, then one sees that to understand the eigenvalues of $C(G, S)$, it suffices to understand the eigenvalues of the operators S_ρ as ρ varies over the irreducible representations of G. This is sometimes a very useful strategy.

Unfortunately, as we saw above, not all graphs are Cayley graphs. It would thus be nice to consider a more general construction and hope to apply these same methods to a larger class of graphs.

Definition 3.4. Let G be a finite group and let $\pi\colon G \to \mathrm{Aut}(X)$ be an action of G on a finite set X. Let $S \subseteq G$ be any subset. Then the *Schreier graph* of the triple (H, X, S) is the graph with vertex set is equal to X. The (directed) edges are all pairs $(x, \pi(s)x)$ for $s \in S$ and $x \in X$. Each such edge is coloured by $s \in S$. The Schreier graph is denoted $\mathrm{Sch}(G, X, S)$.

As above, one often takes S to be a symmetric subset. In order to assure that $\mathrm{Sch}(G, X, S)$ is connected, one must of course take X to be a *transitive* G-set and S to be a generating set for G.

Example 3.5. If one sets $X = G$ and lets G act on itself by left multiplication, then $\mathrm{Sch}(G, G, S) = C(G, S)$, so that the notion of a Schreier graph includes that of a Cayley graph.

Example 3.6. The most common example of a Schreier graph occurs in the situation where $X = G/H$ for some subgroup $H \subseteq G$. Then by letting G act on cosets by left multiplication $g\colon xH \mapsto gxH$, one obtains Schreier graphs $\mathrm{Sch}(G, G/H, S)$. Note that if one takes $H = \{e\}$ then one recovers the previous example.

Part of the utility of Shreier graphs rests on the fact that most regular graphs are Schreier graphs, unlike the situation with Cayley graphs.

Theorem 3.7 (Gross [Gro77])**.** *Every finite regular graph of even degree is a Schreier graph corresponding to some finite group acting on some finite set.*

The proof is not long or difficult, but we will omit it.

Another useful fact about a Schreier graph is that the eigenvalues of $\mathrm{Sch}(G, X, S)$ are closely related to those of the Cayley graph $C(G, S)$. To make this more precise, let X be a finite G-set and let $S \subseteq G$ be a symmetric subset (without the identity of G, say). Consider the vector space V which is the $\mathbf{C}$-span of the elements of X. Then the action of G on X induces a linear action of G on V, call it $\rho\colon G \to \mathrm{GL}(V)$. This is called a *permutation representation*. One checks as above the following

Lemma 3.8. *The matrix S_ρ for the representation ρ constructed in the preceding paragraph is the normalized adjacency matrix of* $\mathrm{Sch}(G, X, S)$.

But then one can decompose ρ into irreducible subrepresentations, and all of these appear in the regular representation. By Lemma (3.3), one immediately deduces the following

Proposition 3.9. *Let G be a finite group acting on a finite set X. Let $S \subseteq G$ be a symmetric subset and let Z be a connected component of* $\mathrm{Sch}(H, S, X)$*. Then $\lambda(Z) \leq \lambda(C(H, S))$, where λ of a graph denotes its second largest eigenvalue.*

References

[AM85] N. Alon and V. D. Milman. λ_1, isoperimetric inequalities for graphs, and superconcentrators. *J. Combin. Theory Ser. B*, 38(1):73–88, 1985.

[Big93] Norman Biggs. *Algebraic graph theory*. Cambridge Mathematical Library. Cambridge University Press, Cambridge, second edition, 1993.

[Gro77] Jonathan L. Gross. Every connected regular graph of even degree is a Schreier coset graph. *J. Combinatorial Theory Ser. B*, 22(3):227–232, 1977.

[HLW06] Shlomo Hoory, Nathan Linial, and Avi Wigderson. Expander graphs and their applications. *Bull. Amer. Math. Soc. (N.S.)*, 43(4):439–561 (electronic), 2006.

[HS93] D. A. Holton and J. Sheehan. *The Petersen graph*, volume 7 of *Australian Mathematical Society Lecture Series*. Cambridge University Press, Cambridge, 1993.

[LSV06] Alexander Lubotzky, Beth Samuels, and Uzi Vishne. Isospectral Cayley graphs of some finite simple groups. *Duke Math. J.*, 135(2):381–393, 2006.