Cayley Graphs

Graph Theory (Fall 2011)
Rutgers University
Swastik Kopparty

We will now see a way of producing some very interesting examples of graphs.

Definition 1. *Let H be a group and let $S \subseteq H$. The Cayley graph of H generated by S, denoted $\mathsf{Cay}(H, S)$, is the directed graph $G = (V, E)$ where $V = H$ and $E = \{(x, xs) \mid x \in H, s \in S\}$.*

If $S = S^{-1}$ (i.e., S is closed under inverse), then $\mathsf{Cay}(H, S)$ is an undirected graph.

For example, if $H = \mathbb{Z}_n$ and $S = \{+1, -1\}$, then $\mathsf{Cay}(H, S)$ is the cycle of length n.

1 Spectrum of Cayley Graphs

The spectrum of a Cayley graph can be very conveniently expressed in terms of the representation theory of the underlying group. Here we will restrict ourselves to the case of finite Abelian groups.

Let H be a finite abelian group. A **character** of H is a homomorphism $\psi : H \to \mathbb{C}^\times$.

Lemma 2. *If ψ is a character of H, then ψ is an eigenvector of the adjacency matrix of $G = \mathsf{Cay}(H, S)$, with eigenvalue $\sum_{s \in S} \psi(s)$.*

Proof. Let A_G be the adjacency matrix of G.

We have:

$$(A_G \cdot \psi)(x) = \sum_{y \in \Gamma(x)} \psi(y) = \sum_{s \in S} \psi(xs) = \psi(x) \cdot \left(\sum_{s \in S} \psi(s) \right).$$

□

If H is a finite abelian group, then we know that $H = \bigoplus_{i=1}^{k} \mathbb{Z}_{n_i}$ for some integers n_i. In this case we have a simple description of all the characters of H. For each $\mathbf{a} = (a_1, \ldots, a_k) \in \bigoplus \mathbb{Z}_{n_i}$, we have a character $\psi_{\mathbf{a}} : H \to \mathbb{C}$, given by

$$\psi_{\mathbf{a}}(h_1, \ldots, h_k) = \prod_{i=1}^{k} \omega_{n_i}^{a_i h_i},$$

where $\omega_t = e^{2\pi i/t}$.

These characters are orthogonal to each other: for distinct $\mathbf{a}, \mathbf{b}$, we have

$$\sum_{x \in H} \psi_{\mathbf{a}}(x) \overline{\psi_{\mathbf{b}}(x)} = \sum_{x \in H} \psi_{\mathbf{a}-\mathbf{b}}(x) = 0.$$

Since there are $\prod n_i = |H|$ such characters, this gives a complete description of the eigenvalues of H.

2 A constructive lower bound on $R(3,k)$

We now see an example of how spectral techniques and Cayley graphs can come together in very concrete situations.

We will demonstrate an explicit graph which has no triangles and no large independent sets. This graph will be a Cayley graph of some group; both these conditions will translate into concrete additive-combinatorial properties of the group.

Let p be a large prime. Let $H = \mathbb{Z}_p^3$. Let $S \subseteq \mathbb{Z}_p^3$ be given by:

$$S = \left\{ (xy, xy^2, xy^3) \mid x \in \mathbb{Z}, y \in \mathbb{Z}_p \setminus \{0\}, \frac{p}{3} < x < \frac{2p}{3} \right\}.$$

(Note that S is closed under inverse).

Let $G = \mathsf{Cay}(H, S)$. Let $n = |H|$.

Theorem 3. *G satisfies the following properties:*

1. *G does not contain any triangles,*
2. *G does not contain any independent sets of size $\Omega(n^{2/3} \log n)$.*

This is a simplified version of a beautiful construction due to Alon, which shows how to construct triangle-free graphs with no independent set of size $\Omega(n^{2/3})$. (We saw an even more simplified and even weaker version in class).

The following variant of this construction yields graphs as good as those of Alon. Let $H' = \mathbb{F}_{2^t}^3$ and $S' = \{(xy, xy^2, xy^3) \mid x, y \in \mathbb{F}_{2^t}, \mathsf{Tr}(x) = 1\}$. Then $\mathsf{Cay}(H', S')$ is triangle free and does not contain any independent sets of size $\Omega(n^{2/3})$. The proof of this is completely analogous to the proof below.

Proof. We first prove part 1. It is easy to see that $\mathsf{Cay}(H, S)$ is triangle-free if and only if $0 \notin S + S + S$. Suppose G was not triangle free. Then we have some $p/3 < x_1, x_2, x_3 < 2p/3$ and $y_1, y_2, y_3 \in \mathbb{Z}_p \setminus \{0\}$ such that:

$$(x_1 y_1, x_1 y_1^2, x_1 y_1^3) + (x_2 y_2, x_2 y_2^2, x_2 y_2^3) + (x_3 y_3, x_3 y_3^2, x_3 y_3^3) = 0.$$

If $y_1 = y_2 = y_3$, then we have $x_1 + x_2 + x_3 = 0$, and this is clearly impossible. Otherwise, we have a nonzero linear combination of at most three vectors of the form (y, y^2, y^3) equalling 0, but this is impossible because such vectors are linearly independent (Vandermonde determinant).

Now for part 2. We will show that G has no large independent sets by studying its spectrum. The eigenvalues of A_G are given by:

$$\lambda_{\mathbf{a}} = \sum_{s \in S} \psi_{\mathbf{a}}(s) = \sum_{p/3 < x < 2p/3} \sum_{y \in \mathbb{Z}_p} \omega^{a_1 xy + a_2 xy^2 + a_3 xy^3}.$$

Rewriting this, we see that:

$$\lambda_{\mathbf{a}} = \sum_{y \in \mathbb{Z}_p} \sum_{p/3 < x < 2p/3} \omega^{x \cdot (a_1 y + a_2 y^2 + a_3 y^3)}.$$

If $\mathbf{a} = (0,0,0)$, then $\lambda_{\mathbf{a}} = |S|$, and this is the largest eigenvalue.

For any other $\mathbf{a}$, we will show that $|\lambda_{\mathbf{a}}| \ll p \log p$. If $z \in \mathbb{Z}_p$, by summing the geometric series we have the following basic bound:

$$|\sum_{p/3<x<2p/3} \omega^{xz}| < \min\{p/3, \frac{2}{|\omega^z - 1|}\}.$$

Let $P(Y) = a_1 Y + a_2 Y^2 + a_3 Y^3$. Then

$$|\lambda_{\mathbf{a}}| \ll \sum_{y \in \mathbb{Z}_p} \min\{p/3, \frac{2}{|\omega^{P(y)} - 1}\}.$$

Note that $P(Y)$ is a nonconstant polynomial of degree at most 3, and hence for any fixed $z \in \mathbb{Z}_p$, the equation $P(Y) = z$ has at most 3 solutions. Thus:

$$|\lambda_{\mathbf{a}}| \ll \sum_{-p/6<z<p/6} \min\{p/3, \frac{2}{|\omega^z - 1|}\}.$$

For $|z| < p$ we have the bound $|\omega^z - 1| \gg \frac{|z|}{p}$.

Thus

$$|\lambda_{\mathbf{a}}| \ll O(p/3) + p \cdot O(\sum_{z=1}^{p/6} \frac{1}{z}) \ll p \log p.$$

We now plug this in to Hoffman's bound on the size of the largest independent set, and tells us that the size of the largest independent set is at most:

$$\frac{-\lambda_n}{|S| - \lambda_n} \cdot n \ll \frac{p \log p}{p^2 + O(p \log p)} \cdot p^3 \ll p^2 \log p.$$

□

3 Graphs of high girth

Now we will see an explicit example of a graph with few edges and high girth (we already saw a probabilistic construction of such graphs).

Let $H = SL_2(p)$ (this is the multiplicative group of 2×2 matrices over $\mathbb{Z}_p$ with determinant 1). Let $n = |H|$ (which is $\Theta(p^3)$). Let $S = \{A, A^{-1}, B, B^{-1}\}$, where

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

$$B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

Theorem 4. *The graph $G = \mathsf{Cay}(H, S)$ has girth $\Omega(\log n)$.*

Proof. We need the following well-known fact: the matrices A and B (treated as matrices in $SL_2(\mathbb{Z})$) generate a free group. (This fact is proved by demonstrating a set X and two subsets X_A, X_B such that $SL_2(\mathbb{Z})$ acts on X, and for every integer $m \neq 0$, we have $A^m \cdot X_A \subseteq X_B$ and $B^m \cdot X_B \subseteq X_A$; the existence of such X, X_A, X_B implies the freeness of the group generated by A, B.)

Given this fact, let us see why $\mathsf{Cay}(H, S)$ has large girth. Suppose there was a cycle $x_1, \ldots, x_g$ in G. For each i, Let $d_i = x_{i+1}^{-1} x_i \in S$ and let $d_g = x_1^{-1} x_g$. Since the x_i are distinct, we have that d_i and d_{i+1} are not inverses of each other. Then $\prod_{i=1}^{g} d_i = I \mod p$, and so we get a relation $A^{m_1} B^{m_2} \cdots A^{m_k} = I \mod p$ where $\sum |m_i| = g$.

On the other hand, by the freeness we know that $A^{m_1} B^{m_2} \cdots A^{m_k} \neq I$ (in $SL_2(\mathbb{Z})$). This implies that $A^{m_1} B^{m_2} \cdots A^{m_k}$ must have some entry which is at least as large as p in absolute value. On the other hand, the largest entry of $A^{m_1} B^{m_2} \cdots A^{m_k}$ is at most $2^{|m_1|+\ldots+|m_k|} = 2^g$. This implies that $g \geq \Omega(\log p)$, as desired. □