18.317 Combinatorics, Probability, and Computations on Groups	21 November 2001
Lecture 28	
Lecturer: Igor Pak	*Scribe: Fumei Lam*

Product Replacement Graphs

Definition 1 *Let G be a finite group and let $k \geq d(G)$, where $d(G)$ is the minimum number of generators of G. The product replacement graph $\Gamma_k(G)$ is a graph on k-tuples $(g_1, g_2, \ldots g_k) \in G^k$ satisfying $< g_1, g_2, \ldots g_k >= G$. The edges of $\Gamma_k(G)$ are*

$$\{\overline{g},\, R_{ij}^{\pm}(\overline{g})\,\},$$
$$\{\overline{g},\, L_{ij}^{\pm}(\overline{g})\,\},$$

where

$$R_{ij}^{\pm}(g_1, \ldots g_i, \ldots g_j, \ldots g_k) = (g_1, \ldots g_i g_j^{\pm 1}, \ldots g_j, \ldots g_k)\},$$
$$L_{ij}^{\pm}(g_1, \ldots g_i, \ldots g_j, \ldots g_k) = (g_1, \ldots g_j^{\pm 1} g_i, \ldots g_j, \ldots g_k)\}.$$

There are $k(k-1)$ choices for pairs (i,j), and two choices each for R or L and $+$ or $-$. By allowing vertices in $\Gamma_k(G)$ to contain loops, this implies $\Gamma_k(G)$ is a $D-$ regular graph with $D = 4k(k-1)$.

Example. For $G = Z_p^m, d(G) = m$, the vertices of $\Gamma_m(Z_p^m)$ are matrices

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2m} \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mm} \end{bmatrix}$$

with $det(A) \neq 0, a_{ij} \in F_p$.

The operations $R_{ij}^{\pm}$ and $L_{ij}^{\pm}$ correspond to left multiplication by

$$E^{\pm} = \begin{cases} 1 \text{ on the diagonal} \\ \pm 1 \text{ in entry ij} \\ 0 \text{ otherwise.} \end{cases}$$

Note that since the group is abelian, the operations L and R are the same. So $\Gamma_m(Z_p^m)$ is the Cayley graph $\Gamma(GL(m,p), \{E_{ij}(\pm 1)\})$. Since $E^{\pm}$ has determinant ± 1, $\Gamma_m(Z_p^m)$ has $p-1$ connected components, each corresponding to different values for the determinant.

Conjecture 2 *If $k \geq d(G) + 1$, then $\Gamma_k(G)$ is connected.*

The following weaker conjecture is also unknown.

Conjecture 3 *If $k \geq 3$, then $\Gamma_k(S_n)$ is connected.*

Lemma 4 *(Higman) Let $k = 2$. Then the conjugacy class of $[g_1, g_2]$ ($< g_1, g_2 >= G$) is invariant on connected components of $\Gamma_2(G)$.*

Proof: For $(g_1, g_2) \in V(\Gamma_2(G))$, $\{L^{\pm}(g_1, g_2), R^{\pm}(g_1, g_2)\} = \{(g_1g_2, g_2), (g_1g_2^{-1}, g_2), (g_2g_1, g_2), (g_2^{-1}g_1, g_2)\}$.

Then

$$
\begin{aligned}
[g_1g_2, g_2] &= g_1g_2g_2g_2^{-1}g_1^{-1}g_2^{-1} = [g_1, g_2], \\
[g_2g_1, g_2] &= g_2g_1g_2g_1^{-1}g_2^{-1}g_2^{-1} = g_2[g_1, g_2]g_2^{-1} = [g_1, g_2]^{g_2^{-1}}, \\
[g_1g_2^{-1}, g_2] &= g_1g_2^{-1}g_2g_2g_1^{-1}g_2^{-1} = [g_1, g_2], \\
[g_2^{-1}g_1, g_2] &= g_2^{-1}g_1g_2g_1^{-1}g_2g_2^{-1} = g_2^{-1}[g_1, g_2]g_2 = [g_1, g_2]^{g_2}.
\end{aligned}
$$

■

Example. Let $G = A_n$ for n odd, $k = 2$ and consider $a = (123 \ldots n), b = (123 \ldots p)$ with $p \not| n$.

Then the commutators lie in different conjugacy classes, implying the number of connected components of $\Gamma_2(A_n) \to \infty$ as $n \to \infty$.

Theorem 5 *Let $m(G)$ denote the maximum size of a nonredundant generating set. For $k \geq d(G) + m(G)$, $\Gamma_k(G)$ is connected.*

In order to prove the theorem, we first define graph $\widetilde{\Gamma}_k(G)$ as the graph $\Gamma_k(G)$ with additional edges defined by the operators

$$
\begin{aligned}
I_m(g_1, g_2, \ldots g_m, \ldots g_k) &= (g_1, g_2, \ldots g_m^{-1}, \ldots g_k) \\
\pi_{ij}(g_1, g_2, \ldots g_i, \ldots g_j, \ldots g_k) &= (g_1, g_2, \ldots g_j, \ldots g_i, \ldots g_k).
\end{aligned}
$$

Then we have the following lemma.

Lemma 6 *The number of connected components of $\Gamma_k(G)$ is less than or equal to the number of connected components of $\widetilde{\Gamma}_k(G)$.*

Proof: Define the operation $T_{ij}(g_1, g_2, \ldots g_i, \ldots g_j, \ldots g_k) = (g_1, g_2, \ldots g_j^{-1}, \ldots g_i, \ldots g_k)$, i.e., T_{ij} switches entries g_i and g_j and inverts g_j. Note that $T_{ij} = L_{ij}^{-}L_{ji}^{+}R_{ij}^{-}$ and

$$
T_{ij}^2(g_1, g_2, \ldots g_i, \ldots g_j, \ldots g_k) = (g_1, g_2, \ldots g_i^{-1} \ldots g_j^{-1} \ldots g_k).
$$

Now note that since $\Gamma_k(G)$ is a subgraph of $\widetilde{\Gamma}_k(G)$, this implies every connected component of $\widetilde{\Gamma}_k(G)$ splits into at most 2 components in $\Gamma_k(G)$.

■

As a corollary, if $\widetilde{\Gamma}_k(G)$ is connected for $k \geq d(G) + 1$, then $\Gamma_k(G)$ is connected.

Since $m(G) \geq 1$ for all groups, we need only consider $\widetilde{\Gamma}_k(G)$ to prove the theorem.

Theorem 7 *For $k \geq d(G) + m(G)$, $\widetilde{\Gamma}_k(G)$ is connected.*

Proof:

By definition of $m = m(G)$, any element $(g_1, g_2, \ldots g_k) \in \Gamma_k(G)$ contains a generating subset of m elements $g_{i_1}, g_{i_2}, \ldots g_{i_m}$. Use the operators π_{ij} to obtain

$$(g_1, g_2, \ldots g_k) \to (g_{i_1}, g_{i_2}, \ldots g_{i_m}, \ldots)$$

where the remaining $k - m$ elements are those not in $\{g_{i_1}, g_{i_2}, \ldots g_{i_m}\}$. Now since $g_{i_1}, g_{i_2}, \ldots g_{i_m}$ form a generating set, we can use the $L^{\pm}$ and $R^{\pm}$ operations to obtain

$$\begin{aligned}(g_{i_1}, g_{i_2}, \ldots g_{i_m}, \ldots) &\to (g_{i_1}, g_{i_2}, \ldots g_{i_m}, 1, 1, \ldots 1)\\ &\to (g_{i_1}, g_{i_2}, \ldots g_{i_m}, h_1, h_2, \ldots h_{k-m}),\end{aligned}$$

where $h_1, h_2, \ldots h_{k-m}$ is a generating set of G (this is possible, since $k - m \geq d$). Then we again use the $L^{\pm}, R^{\pm}$ operators to obtain

$$(g_{i_1}, g_{i_2}, \ldots g_{i_m}, h_1, h_2, \ldots h_{k-m}) \to (1, 1, \ldots 1, h_1, h_2, \ldots h_{k-m}).$$

Therefore, every element in $\widetilde{\Gamma}_k(G)$ is connected to the element $(1, 1, \ldots 1, h_1, h_2, \ldots h_{k-m})$, implying $\widetilde{\Gamma}_k(G)$ is connected.

■

Now Theorem 5 follows immediately from Lemma 6 and Theorem 7. We also have the following corollary.

Corollary 8 *For $k \geq 2\lfloor \log_2 |G| \rfloor, \Gamma_k(G)$ is connected.*

The following theorem shows that $\Gamma_3(A_n)$ contains very large connected components.

Theorem 9 *There exists $\Gamma' \subset \Gamma_k(A_n)$ such that Γ' is connected for all $k \geq 3$ and*

$$\frac{|\Gamma'|}{|\Gamma_k(A_n)|} \to 1 \text{ as } n \to \infty.$$

Proof: For $k = 3$, pick $g_1, g_2, g_3, h_1, h_2, h_3 \in A_n$ uniformly and independently. We will show that with high probability, the elements $(g_1, g_2, g_3), (h_1, h_2, h_3) \in \Gamma_3(A_n)$ are connected. Since $< g_1, g_2 >= A_n$ with high probability, we can use $L^{\pm}, R^{\pm}$ operations to obtain

$$(g_1, g_2, g_3) \to (g_1, g_2, h_3).$$

Similarly, since h_2 and h_3 were chosen uniformly, $< g_1, h_3 >=< h_2, h_3 >= A_n$ with high probability, so we have

$$(g_1, g_2, h_3) \to (g_1, h_2, h_3) \to (h_1, h_2, h_3).$$

Since the probability two random elements generate A_n is at least $1 - \frac{1}{n}$, the probability two random elements are connected is at least $1 - \frac{1}{3n}$ and the theorem follows.

■