18.317 Combinatorics, Probability, and Computations on Groups 26 November 2001

Lecture 29

Lecturer: Igor Pak *Scribe: Etienne Rassart*

Two theorems on the product replacement graph

Let $\Gamma_k(G)$ be the graph with vertex set $\{(g_1, \ldots, g_k) \in G^k : \langle g_1, \ldots, g_k \rangle = G\}$ and edges

$$\begin{aligned}(g_1, \ldots, g_i, \ldots, g_k) \quad &\longleftrightarrow \quad (g_1, \ldots, g_i g_j^{\pm 1}, \ldots, g_k) \\ &\longleftrightarrow \quad (g_1, \ldots, g_j^{\pm 1} g_i, \ldots, g_k)\,,\end{aligned}$$

for a finite group G.

Conjecture $\Gamma_k(G)$ is connected if $k \geq d(G) + 1$.

Theorem *$\Gamma_k(G)$ is connected if $k \geq d(G) + m(G)$.*

Corollary *$\Gamma_k(G)$ is connected if $k \geq 2 \log_2 |G|$.*

Theorem 1 (**Babai**)

If $k = 2\lceil \log_2 |G| \rceil$ then there is a constant $c > 0$ such that $\operatorname{diam} \Gamma_k(G) \leq c \cdot \log_2^2 |G|$.

Proof: Let $r = \lceil \log_2 |G| \rceil$, so that $k = 2r$ and $m(G) \leq r$.

There is a path in $\Gamma_k(G)$ from $(g_1, \ldots, g_k)$ to $(1, \ldots, 1, h_1, 1, \ldots, 1, h_r, 1, \ldots, 1)$, where $\langle h_1, \ldots, h_r \rangle = G$. Since we can exchange elements, we can assume that we send $(g_1, \ldots, g_k)$ to $(h_1, \ldots, h_r, 1, \ldots, 1)$.

We want to go from $(h_1, \ldots, h_r, 1, \ldots, 1)$ to $(h_1, \ldots, h_r, a_1, \ldots, a_r)$ in such a way that

$$\left\{a_1^{\varepsilon_1} \cdots a_r^{\varepsilon_r} : \varepsilon_i \in \{0,1\}\right\} = G\,.$$

Set a_1 to be some $h_i \neq 1$. Then

$$(h_1, \ldots, h_r, 1, \ldots, 1) \longrightarrow (h_1, \ldots, h_r, a_1, 1, \ldots, 1) \quad \text{and} \quad |\{a_1^{\varepsilon_1}\}| = 2\,.$$

From there we proceed by induction. Suppose we have $(g_1, \ldots, g_k)$ connected to $(h_1, \ldots, h_r, a_1, \ldots, a_i, 1, \ldots, 1)$ with $|\{a_1^{\varepsilon_1} \cdots a_i^{\varepsilon_i}\}| = 2^i$.

Let $C = \{a_1^{\varepsilon_1} \cdots a_i^{\varepsilon_i}\}$ and $A = C \cdot C^{-1}$. A first observation is that if $A \neq G$ then we can find x not in A such that x is at distance at most $2i + 1$ from the identity (distance with respect to the generating set $\{h_1, \ldots, h_r, a_1, \ldots, a_i\}$): we take x to be one away from an element on the boundary of A. Then we can use a's to get to the boundary and one of the h's for the final step to x.

So if we let $a_{i+1} = x$ then we can go from $(h_1, \ldots, h_r, a_1, \ldots, a_i, 1, \ldots, 1)$ to $(h_1, \ldots, h_r, a_1, \ldots, a_i, a_{i+1}, 1, \ldots, 1)$ in $O(\log |G|)$ steps (since $i \leq r$). Also, $|\{a_1^{\varepsilon_1} \cdots a_{i+1}^{\varepsilon_{i+1}}\}| = 2^{i+1}$.

So

$$(h_1,\dots,h_r,1,\dots,1) \xrightarrow[\text{steps}]{O(\log^2|G|)} (h_1,\dots,h_r,a_1,\dots,a_r) \xrightarrow[\text{steps}]{O(\log^2|G|)} (1,\dots,1,a_1,\dots,a_r)\,.$$

Hence

$$\begin{tikzcd}
(g'_1,\dots,g'_k) \arrow[r, "O(\log^2|G|)"] & (h'_1,\dots,h'_r,1,\dots,1) \arrow[r, "O(\log^2|G|)"] & (h'_1,\dots,h'_r,a'_1,\dots,a'_r) \arrow[d, "O(\log^2|G|)"] \\
 & & (1,\dots,1,a'_1,\dots,a'_r) \arrow[d, "O(\log|G|)"] \\
 & & (a'_1,\dots,a'_r,1,\dots,1) \arrow[d, "O(\log^2|G|)"] \\
 & & (a'_1,\dots,a'_r,a_1,\dots,a_r) \arrow[d, "O(\log^2|G|)"] \\
 & & (1,\dots,1,a_1,\dots,a_r) \arrow[d, "O(\log^2|G|)"] \\
(g_1,\dots,g_k) & (h_1,\dots,h_r,1,\dots,1) \arrow[l, "O(\log^2|G|)"'] & (h_1,\dots,h_r,a_1,\dots,a_r) \arrow[l, "O(\log^2|G|)"']
\end{tikzcd}$$

So there remains to check that we can go from $(g_1,\dots,g_k)$ to $(1,\dots,1,h_1,1,\dots,1,h_r,1,\dots,1)$ in reasonable time. If we had $(h_1,\dots,h_r,t_1,\dots,t_r)$ instead, we could actually use the t_i's instead of x if some of them lie outside of $C\cdot C^{-1}$ (starting with t_1 and adding an element at a time as before; if t_i is inside, we construct x outside as above).

So we can go from $(h_1,\dots,h_r,t_1,\dots,t_r)$ to $(h'_1,\dots,h'_r,t'_1,\dots,t'_r)$ in $O(\log^2|G|)$ steps.

All the transpositions throughout this process are done in $O(\log|G|)$ steps (overall). ■

Theorem 2 (**Dunwoody**)

If G is solvable and $k \geq d(G)+1$ then $\Gamma_k(G)$ is connected.

Proof: Consider the chain

$$\{1\} = G_0 \subseteq G_1 \subseteq \ldots \subseteq G_l = G\,,$$

where G_{i-1} is minimal G-invariant in G_i. We proceed by induction.

If $l=0$, there is nothing to prove. If $l \geq 1$, let $M = G_1$. Because G is solvable, M is normal in G and abelian.

Fix $(h_1,\dots,h_{k-1})$ such that $\langle h_1\dots,h_{k-1}\rangle = G$.

We can go from $(g_1,\dots,g_k)$ to $(m, m_1h_1,\dots,m_{k-1}h_{k-1})$ for $m, m_i \in M$. This is done by working in the quotient group G/M, applying the inductive hypothesis, then lifting back to the whole group by taking a representative in each coset.

Next observe that $(m_ih_i)^{-1}\cdot m\cdot(m_ih_i) = h_i^{-1}\cdot m\cdot h_i = m^{h_i}$ since M is abelian. This implies that

$$\mathit{word}(m_1h_1,\dots,m_{k-1}h_{k-1})^{-1}\cdot m\cdot \mathit{word}(m_1h_1,\dots,m_{k-1}h_{k-1}) = \mathit{word}(h_1,\dots,h_{k-1})^{-1}\cdot m\cdot \mathit{word}(h_1,\dots,h_{k-1})\,.$$

Now $\langle h_1, \ldots, h_{k-1} \rangle = G$, so $(m, m_1 h_1, \ldots, m_{k-1} h_{k-1}) \longrightarrow (m^g, m_1 h_1, \ldots, m_{k-1} h_{k-1})$ for any $g \in G$ (write g as *word*$(h_1, \ldots, h_{k-1})$).

Also, $\langle m^g : g \in G \rangle = M$ since M is minimal, and thus $m_1 = m^{g_{i_1}} m^{g_{i_2}} \cdots m^{g_{i_n}}$ for some $g_{i_j} \in G$.

Therefore

$$
\begin{array}{ccc}
(g_1, \ldots, g_k) & \longrightarrow & (m, m_1 h_1, \ldots, m_{k-1} h_{k-1}) \\
 & & \big\downarrow \\
 & & (m^{g_{i_1}}, m_1 h_1, \ldots, m_{k-1} h_{k-1}) \\
 & & \big\downarrow \\
 & & (m^{g_{i_1}}, (m^{g_{i_1}})^{-1} m_1 h_1, \ldots, m_{k-1} h_{k-1}) \\
 & & \big\downarrow \\
 & & (m^{g_{i_2}}, (m^{g_{i_1}})^{-1} m_1 h_1, \ldots, m_{k-1} h_{k-1}) \\
 & & \big\downarrow \\
 & & (m^{g_{i_2}}, (m^{g_{i_2}})^{-1} (m^{g_{i_1}})^{-1} m_1 h_1, \ldots, m_{k-1} h_{k-1}) \\
 & & \big\downarrow \\
 & & \cdots \\
 & & \big\downarrow \\
 & & (m^a, h_1, m_2 h_2, \ldots, m_{k-1} h_{k-1}) \quad (\text{some } a \in G) \\
 & & \big\downarrow \\
 & & \cdots \\
 & & \big\downarrow \\
 & & (m^z, h_1, h_2, \ldots, h_{k-1}) \quad (\text{some } z \in G) \\
 & & \big\downarrow {\scriptstyle \text{ since } \langle h_1 \ldots, h_{k-1} \rangle = G} \\
 & & (1, h_1, h_2, \ldots, h_{k-1})
\end{array}
$$

Now $(h_1, \ldots, h_{k-1})$ was arbitrary, so any two $(g_1, \ldots, g_k)$ are connected in $\Gamma_k(G)$.

■