18.317 Combinatorics, Probability, and Computations on Groups 16 November 2001

Lecture 26

Lecturer: Igor Pak *Scribe: Igor Pavlovsky*

Babai's Algorithm continued: escape time

Last time, we proved

Theorem 1 *Let C be a subset of the group G, $S = S^{-1}$ a symmetric generating set, $\pi = U(S)$ the uniform distribution on S, and p_π the "one-step evolution" of the random walk (i.e. $p_\pi \varphi = U(S) \star \varphi$). Then for any probability distribution φ,*

$$\|p_\pi \varphi\|^2 \leq \left(1 - \frac{|G \backslash C|}{2 \cdot A \cdot |G|}\right) \cdot \|\varphi\|^2$$

where $A = d \cdot |S| \cdot \max_{s \in S} \max_{g \in \bar{C}} \mu_s(g)$, $d = diam(\bar{C}, G)$. ■

We will use this theorem to bound the escape time of a random walk X_t generated by S. For a subset C of G, set

$$\varphi_t(g) = \Pr[X_t = g \text{ and } X_i \in C \ \forall i = 1 \ldots t]$$

Obviously, supp $\varphi_t \subset C$, $\|\varphi_0\| \leq 1$ (1 if C contains 1_G, 0 otherwise) and

$$\varphi_{t+1}(g) = \begin{cases} (p_\pi \varphi_t)(g) & \text{if } g \in C \\ 0 & \text{otherwise} \end{cases}$$

Inductively applying the above theorem, conclude

Corollary 2 $\|\varphi_t\|^2 \leq \left(1 - \frac{|G \backslash C|}{2 \cdot A \cdot |G|}\right)^t$ ■

Given a bound $\|\varphi_t\|^2 \leq \epsilon$, we'd like to bound the "non-escape" probability $p = \sum_{g \in C} \varphi_t(g)$. It is clear that the worst situation is when $\varphi_t(g) = \frac{p}{|C|}$ is uniform on C. In that case, $\|\varphi_t\|^2 = \sum_{g \in C} (\varphi_t(g))^2 = |C| \frac{p^2}{|C|^2} = \frac{p^2}{|C|}$. Hence, $p^2 \leq |C|\epsilon$. In other words:

Lemma 3 *If $\|\varphi_t\|^2 \leq \frac{\alpha^2}{|C|}$, then $\Pr[X_1, \ldots, X_t \in C] \leq \alpha$.* ■

Combining the last two results, obtain

Corollary 4 *Suppose $|C| \leq |G|/2$. Then $\Pr[X_1, \ldots, X_t \in C] \leq \left(1 - \frac{1}{4A}\right)^{t/2} \sqrt{|C|}$.* ■

The first tool for our main escape-time theorem is now ready:

Proposition 5 *Let C be a subset of a finite group G, let $\{X_t\}_t$ be a random walk on G w.r.t. some symmetric generating set. Suppose $|C| \leq |G|/2$. Then $\Pr[X_1, \ldots, X_t \in C] \leq \frac{1}{e}$ for $t \geq 4A(\log |C| + 2)$.* ■

The following result will provide the remaining tool.

Proposition 6 *Let $C = C^{-1}$ be a symmetric subset of a finite group G, let $\{X_t\}_t$ be a random walk on G w.r.t. some (arbitrary) generating set, and suppose* $\Pr[X_t \in C^2$ *for all* $1 \le t \le T] \le 1-p$. *Then for* $m \ge 2T$,

$$\frac{1}{m}\sum_{t=1}^{m} \Pr[X_t \notin C] \ge \frac{p}{p+1} \cdot \frac{T}{m}$$

Proof: Set τ to be the hitting time of $G \backslash C^2$, i.e. the first t with $X_t \notin C^2$; then $\Pr[\tau \le T] \ge p$. Note that if $\tau \le T$, then $\{\tau, \tau+1, \ldots, \tau+T-1\} \subset \{1, \ldots, m\}$. Set $z = X_\tau$ and observe $(z \cdot C) \cap C = \emptyset$. The idea is that once the random walk wanders outside of C and in fact to a point z outside of the much bigger C^2, it is likely to stay in a C-neighborhood of z (which is outside of C!) for some time. Compute:

$$\begin{aligned}
\frac{1}{m}\sum_{t=1}^{m} \Pr[X_t \notin C] &\ge \frac{1}{m}\Pr[\tau \le T] \cdot \sum_{t=\tau}^{\tau+T-1} \Pr[zX_t \in zC] \\
&\ge \frac{p}{m}\sum_{t=\tau}^{\tau+T-1} \Pr[X_t \in C] \ge \frac{p}{m}\left(\sum_{t=1}^{m} \Pr[X_t \in C] - (m-T)\cdot 1\right) \\
&\ge \frac{p}{m}\left(T - \sum_{t=1}^{m} \Pr[X_t \notin C]\right)
\end{aligned}$$

Here in the first line we used that $X_{\tau+t}$ has the distribution of $z \cdot X_t$, and in the second line that the $m-T$ extra terms $\Pr[X_t \in C]$ on the right all are ≤ 1. Now denote by q the expectation in question: $q = \frac{1}{m}\sum_{t=1}^{m} \Pr[X_t \notin C]$. The above inequality translates into $q \ge p\left(\frac{T}{m} - q\right)$. Solve for q. ■

When $m = 2T$ and $p = 1 - \frac{1}{e}$, the proposition gives $q \ge \frac{e-1}{2e-1} \cdot \frac{1}{2} > \frac{1.5}{5} \cdot \frac{1}{2} > \frac{1}{8}$. Hence, at last,

Theorem 7 *Let $C = C^{-1}$ be a symmetric subset of a finite group G, with $|C^2| \le |G|/2$. Let $\{X_t\}_t$ be a random walk on G w.r.t. some symmetric generating set. Then for $2 \cdot T \ge 2 \cdot 4A(\log|C|^2 + 2) = O(16 \log|C|)$, the escape-expectation is "large":*

$$\frac{1}{2T}\sum_{t=1}^{2T} \Pr[X_t \notin C] > \frac{1}{8}$$

■

Therefore, in Babai's Algorithm, run the random walk on G for a *random* $\alpha \in [1 \ldots L]$ steps ($L = O(\log^3|G|)$ as before, $> O(\log|G|)$). At the end of many – 1/8th – of $l = O(16 \log|G|)$ such runs, we expect to wonder away from any "small" subset. Done!