18.317 Combinatorics, Probability, and Computations on Groups	12 October 2001
Lecture 14	
Lecturer: Igor Pak	*Scribe: D. Jacob Wildstrom*

Random Walks on Nilpotent Groups

Example 1. Let

$$G = \left\{ \begin{pmatrix} 1 & * & \cdots & * \\ 0 & 1 & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} * \in \mathbb{F}_p \right\},$$

that is to say, the group of upper triangular matrices with ones on the diagonal. Let the generator set S consist of the *elementary transvections* – that is, matrices equivalent to the identity matrix except that the (i, j)-th entry is a, for $1 < i < j < n$, $a \in \mathbb{F}_p$. For purposes of simplicity we regard each matrix defined by an (i, j, a) triple as distinct, even those which are identical (for instance, all matrices with $a = 0$ are identical). With this enumeration, we may easily find that $|S| = \binom{n}{2}p$, and that $|G| = p^{\binom{n}{2}}$. Now let us design a random process in the usual fashion: let $X_0 = I$, and $X_{t+1} = X_t E_{ij}(a)$ where $E_{ij}(a)$ is a random variable uniformly distributed in S.

We may more intuitively represent $XE_{ij}(a)$ as identical to X, but with the ith row increased by the jth row multiplied by a.

Theorem 1. *The mixing time of a random walk $\{X_t\}$ on $\Gamma(G, S)$ is $O(n^2 \log n)$.*

Proof: Let us define the stopping time $\varkappa$ by the following rule: we wait until all pairs i, j have been used in the walk (we place no restrictions on the value of a). By the Coupon Collector's problem, $E(\varkappa) \approx \binom{n}{2} \log \binom{n}{2} = O(n^2 \log n)$, and by the following lemma, $\tau_3 \leq E(\varkappa)$. ■

Lemma 2. *$\varkappa$ is strong uniform.*

Before we address random walks further though, we'll want to discuss the non-probabilistic properties of nilpotent groups.

General Group Theory

First, let's review some facts we all learned in kindergarten. For a finite group G and subgroup H normal in G, G/H is the quotient group; the multiplicative group of cosets of H. Note that $|G/H| = \frac{|G|}{|H|} = [G : H]$.

Another important concept is the commutator group: for $H \triangleleft G$, we define $[G, H]$ as the group generated by all products of the form $ghg^{-1}h^{-1}$, for $g \in G$ and $h \in H$.

Proposition 3. *If $H \triangleleft G$, then $[G, H] \triangleleft G$. Moreover, $G/[G, G]$ is abelian.*

Proof:

Since the conjugate of a product is the product of conjugates, it is only necessary to show that the generators of $[G,H]$, under conjugation by elements of G, remain in $[G,H]$, and from this the normality of the entire group $[G,H]$ follows. Let $a \in G$, and $ghg^{-1}h^{-1}$ be a generator of $[G,H]$. Then

$$(ghg^{-1}h^{-1})^a = g^a h^a (g^a)^{-1}(h^a)^{-1}$$

Since $H \triangleleft G$, $g^a \in G$ and $h^a \in H$, so $g^a h^a (g^a)^{-1}(h^a)^{-1}$ is in the commutator group [G,H].

From here, proving that $G/[G,G]$ is abelian is quite straightforward: let $a, x \in G$, and let $[a]$ and $[x]$ be the associated elements of $G/[G,G]$. Then

$$[x][a] = [xa] = [xa(a^{-1}x^{-1}ax)] = [ax] = [a][x]$$

■

Finally, we shall discuss application of these properties to nilpotent groups.

Definition 4. The *lower central series* of a group G is the chain of groups $G_0 \triangleright G_1 \triangleright G_2 \triangleright \cdots$ defined by $G_0 = G$ and $G_{i+1} = [G, G_i]$. Group G is called *nilpotent* if some G_ℓ in the lower central series of G is trivial.

Let $H_i = G_{i-1}/G_i$. Each H_i is abelian since $G_i = [G, G_{i-1}] \supset [G_{i-1}, G_{i-1}]$, thus $G_{i-1}/G_i \subset G_{i-1}/[G_{i-1}, G_{i-1}]$, which was shown earlier to be abelian.

Definition 5. For prime p, a finite group G is called a *p-group* if $|G| = p^m$ for some integer m.

Theorem 6. *If G is a finite p-group, then G is nilpotent.*

Example 2. The group of upper triangular matrices $U(n,p)$ of $\mathbb{F}_p$ is a p-group, hence nilpotent. Calculation of the lower central series yields:

$$G_1 = \begin{pmatrix} 1 & 0 & * & * & \cdots & * \\ & 1 & 0 & * & \cdots & * \\ & & 1 & 0 & \cdots & * \\ & & & \ddots & \ddots & \vdots \\ & & & & 1 & 0 \\ & & & & & 1 \end{pmatrix}, \qquad G_2 = \begin{pmatrix} 1 & 0 & 0 & * & \cdots & * \\ & 1 & 0 & 0 & \cdots & * \\ & & 1 & 0 & \cdots & * \\ & & & \ddots & \ddots & \vdots \\ & & & & 1 & 0 \\ & & & & & 1 \end{pmatrix},$$

and so forth, so that G_{n-1} consists only of the identity matrix. Interestingly enough, we can deduce from this that $H_i \simeq \mathbb{Z}_p^{n-1}$.

Finally, another probabilistic result:

Lemma 7. *Suppose $N \triangleleft G$. Let $H = G/N$, and let $\gamma : G \to H$ be the standard onto map from $g \in G$ to the coset $gN \in H$. For any map $\psi : H \to G$ such that $\gamma(\psi(h)) = h$ for all $h \in H$, the formula $\psi(h)n$ is uniform in G given that h and n are uniform in H and N.*

Proof: This is obvious, according to Pak's notes. To go into slightly more detail, it's a well-known fact from algebra that the cosets of N are disjoint, equal size, and cover G. For ψ to satisfy the given condition, it must map each coset aN to one of its elements. SO, the product $\psi(h)n$ is essentially a uniform selection from the cosets aN, then a uniform selection from the cosets elements. The partition and equality conditions of cosets guarantee that such a selection process is uniform. ■