18.317 Combinatorics, Probability, and Computations on Groups	15 October 2001
Lecture 15	
Lecturer: Igor Pak	*Scribe: Fumei Lam*

Hall Bases

Definition 1 *Let H be an abelian p-group. A set $B = \{b_1.b_2, \ldots b_r\} \subseteq H$ is a Hall basis if $\forall h \in H,\ \exists\, \alpha_1, \alpha_2, \ldots \alpha_r \in \{0, 1, \ldots p-1\}$ such that $h = b_1^{\alpha_1} b_2^{\alpha_2} \ldots b_r^{\alpha_r}$.*

The following lemma shows that for a Hall basis B, the distribution of $B^{\overline{\alpha}}$ over $\overline{\alpha}$ is uniform in H.

Lemma 2 *If $B = \{b_1, b_2, \ldots b_r\}$ is a Hall basis in H, then*

$$Pr_{\overline{\alpha}}(b_1^{\alpha_1} b_2^{\alpha_2} \ldots b_r^{\alpha_r} = h) = \frac{1}{|H|} \quad \forall\, h \in H$$

Proof: Consider H as a vector space. Since B is a Hall basis, it is a spanning set and contains a basis, say $b_1, b_2, \ldots b_k$. Then for uniform $\alpha_i \in \{0, 1, \ldots p-1\}$, we have

$$\underbrace{b_1^{\alpha_1} b_2^{\alpha_2} \ldots b_k^{\alpha_k}}_{\text{uniform in } H}\, b_{k+1}^{\alpha_{k+1}} b_{k+2}^{\alpha_{k+2}} \ldots b_r^{\alpha_r},$$

which is uniform in H.

■

Recall that G is nilpotent if some G_l in the lower central series

$$G = G_0 \supset G_1 \supset G_2 \supset G_3 \supset \cdots \supset G_l = \{1\}$$

is the identity element (where $G_i = [G_{i-1}, G]$ for $i = 1, 2, 3 \ldots$).

Let $H_i = G_{i-1}/G_i$ and let $\gamma_i : G_{i-1} \to H_i$ denote the standard map of G_{i-1} onto the cosets of G_i. From last time, if $\psi_i : H_i \to G_{i-1}$ is a map such that $\gamma_i(\psi_i(h)) = h$ for all $h \in H$, then we have the following lemma.

Lemma 3 *For h_i uniform in H_i and g_i uniform in G_i, $\psi(h_i)g_i$ is uniform in G_{i-1}.*

In what follows, we will assume G is nilpotent with $G = G_0 \supset G_1 \supset G_2 \supset \ldots \supset G_l = \{1\}$.

Definition 4 *Let $\overline{B} = (B_1, B_2, \ldots B_l)$, $B_i \subset G_{i-1}$. $\overline{B}$ is a Hall basis if $\gamma_i(B_{i+1})$ is a Hall basis of H_{i+1} for all $i = 0, 1, \ldots l-1$.*

Lemma 5 *Let $\overline{B} = (B_1, B_2, \ldots B_l), B_i = \{b_{i_1}, b_{i_2}, \ldots b_{i_{r_i}}\}$, and suppose α_{ij} is uniform in $\{0, 1, \ldots p-1\}$. Then*

$$g = \prod_{i=1,2,\ldots l}^{\rightarrow} \prod_{j=1,2,\ldots r_i}^{\rightarrow} b_{ij}^{\alpha_{ij}}$$

is uniform in G, where $\prod\limits_{i=1,2,\ldots l}^{\rightarrow}$ denotes the product in the order $1, 2 \ldots l$.

Proof: Note that since $\overline{B}$ is a Hall basis, g can be written as $g = g_1 g_2 \ldots g_l$ with $g_i \in G_{i-1}$ and $h_i = \gamma_i(g_i)$ uniform in H_i.

Since $H_l = G_{l-1}$, $h_l = \gamma_l(g_l) = g_l$ is uniform in G_{l-1}. Furthermore, $h_{l-1} = \gamma_{l-1}(g_{l-1})$ is uniform in H_{l-1} and by the previous lemma, this implies $g_{l-1}g_l$ is uniform in G_{l-2}. Continuing by induction, we obtain $g = g_1 g_2 \ldots g_l$ is uniform in $G_0 = G$. ■

In fact, the lemma remains true even if we remove the restriction on the product order of the b_{ij}, as we will show in the following theorem.

Definition 6 *Let $\Lambda = \{(i,j) : i = 1, 2, \ldots l, j = 1, 2, \ldots r_i\}$. A word w in $b_{ij}, (i,j) \in \Lambda$ is complete if b_{ij} occurs in w for all $(i,j) \in \Lambda$.*

Theorem 7 *If $\overline{B}$ is a Hall basis and w is a complete word, then $w^{\overline{\alpha}}$ is uniform in G.*

Proof: First, consider all the elements $b_{l*} \in B_l$ in w. Since $B_l \subseteq G_{l-1}$, and G_{l-1} is contained in the center of G, each element b_{l*} commutes with all other elements in the word w and we can express w as

$$w = * * \cdots * \underbrace{\boxed{}}_{B_l}.$$

Now, observe that if $a \in B_i, b \in B_j$, then $ab \in ba[a^{-1}, b^{-1}]$ with $[a^{-1}, b^{-1}] \in G_c$ for some $c > i, j$. So we can move all the elements $b_{l-1*} \in B_{l-1}$ in w to the right and write w in the form

$$w = * * \cdots * \underbrace{\boxed{}}_{B_{l-1}} \blacksquare \underbrace{\boxed{}}_{B_l},$$

where the shaded box represents a product of terms in G_{l-1} accumulated by commuting the elements b_{l-1*}.

Continuing in this way, we obtain

$$w = \underbrace{\square}_{B_1}\,\blacksquare\,\underbrace{\square}_{B_2}\cdots\blacksquare\,\underbrace{\square}_{B_{l-1}}\,\blacksquare\,\underbrace{\square}_{B_l}.$$

Since each of the products in B_i corresponds to a uniform element in H_i under γ_i, we have

$$w = \underbrace{\square\,\blacksquare\,\square\cdots\cdots\underbrace{\blacksquare\,\square\,\underbrace{\blacksquare\,\square}_{\text{uniform in } G_{l-1}}}_{\text{uniform in } G_{l-2}}}_{\text{uniform in } G_0 = G},$$

proving the theorem.

■