18.317 Combinatorics, Probability, and Computations on Groups 17 October 2001

Lecture 14

Lecturer: Igor Pak *Scribe: C. Goddard*

Hall Bases Continued

Last lecture we finished with the theorem:

Theorem 1. *Given a ω - complete word in $\overline{B} = (B_1, B_2, \ldots)$, a Hall Basis in G, then $\omega^{\overline{\alpha}}$ - uniform in G.*

Now two lectures ago, we wanted to prove the following lemma:

Lemma 2. $\varkappa$ *for* $\mathrm{U}(n,p) = \left\{ \begin{pmatrix} 1 & * & \cdots & * \\ 0 & 1 & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} * \in \mathbb{F}_p \right\}$ *is strong uniform.*

We proved a corollary to this:

Corollary 3. *The mixing time for a random walk on* $\mathrm{U}(n,p) = \mathrm{O}(n^2 \log n)$.

Now we want to prove Theorem 1 $\Rightarrow$ Lemma 2.

Proof: Let $G = \mathrm{U}(n,p)$, that is the group of $n \times n$ upper triangular matrices with 1's on the diagonal. Consider the basis: $\overline{B} = (B_1, B_2, \ldots, B_{n-1})$ where

$$B_i = \left\{ \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & 1 & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & 1 \end{pmatrix} \text{ with a 1 in the } i\text{th diagonal.} \right\}$$

Thus $|B_i| = n - i$.

Now we have to check $\overline{B}$ is a Hall basis for $\mathrm{U}(n,p)$. This is "obvious" since we know that $<\gamma_i(B_i)> = H_i$ since, firstly $<B_i> = G_i$, where G_i consists of 0's everywhere below the ith diagonal except the main diagonal, and H_i is the quotient G_{i-1}/G_i, so $H_i \cong (\mathbb{Z}_p)^{n-i}$.

For the mixing time, we know $X_t = E_{i_1 j_1}(\alpha_1) \cdot E_{i_2 j_2}(\alpha_2) \cdot \ldots \cdot E_{i_t j_t}(\alpha_t)$ by definition since

$$E_{ij}(\alpha) = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \alpha & 0 \\ \vdots & \ddots & 0 & \vdots \\ 0 & \cdots & 0 & 1 \end{pmatrix} \text{ ie 1's on the diagonal and 0's elsewhere except } \alpha \text{ in the } ij\text{th position}$$

Now we want to look at $\varkappa$, which is the first time all the indices i, j occur in this product. So in the notation of the previous lecture, $\Lambda = \{(i,j), 1 \le i < j \le n\}$. Say that there are N words that contain all i, j and look at the complete words. Thus,

$$\Pr(X_t = h | \varkappa = t) = \frac{1}{N} \cdot \sum_{\omega} \Pr(\omega^{\overline{\alpha}} = h)$$

where we sum over the complete words ω of length t such that no shorter word is a complete word. Therefore from Theorem 1, ω is uniform. So,

$$\Pr(X_t = h | \varkappa = t) = \frac{1}{N} \cdot N \cdot \frac{1}{|G|} = \frac{1}{|G|}$$

Thus, $\varkappa$ is strong uniform. ■

Note, we can generalise this to any nilpotent group with generators corresponding to our generators, and the mixing time $= \mathrm{O}(|\Lambda| \log |\Lambda|)$.

Brief Outline of Open Problems for Research Projects

Hamilton Paths in Cayley Graphs

There are two conflicting conjectures relating to the Hamilton paths in Cayley graphs, namely:

Conjecture 4. (Lovasz) $\forall G,\ <S> = G,\ S = S^{-1}$, *the Cayley graph* $\Gamma(G, S)$ *contains a Hamilton path.*

Conjecture 5. (Babai) $\exists \alpha > 0$ *such that* $\exists$ *infinitely many Cayley graphs with no paths on length* $> (1 - \alpha) \cdot \#vertices$.

Aim: try and find out which one of these is true on a special groups and generating sets.

Examples: 1) Try Hall's 19 (up to automorphisms) Cayley graphs of A_5 with 2 generators (aim for negative answer.)

2) Try S_n and conjugacy classes (aim for positive answer.)

3) Try general nilpotent groups (positive.)

4) Try three involutions in general groups (positive.) NB: every finite simple group can be generated by three involutions.

5) Try wreath and semidirect product of finite groups (positive; easy for direct products.)

Diameter Problem

Suppose we have A_n, S_n and $<S> = A_n$, where S is a set of generators.

Conjecture 6. $\mathrm{diameter}(A_n, S) < cn^2$, c *- constant. Also works for* S_n.

Look at the following weaker versions of this:

1. For the worst case when $|S| = 2$, we have the following:

   Theorem 7. (Babai, Hetyei) $\mathrm{diam} < e^{\sqrt{n} \log n (1+\mathrm{o}(1))}$. *This gives a bound of the maximum order of permuations in* S_n.

Aim: Find something similar for $\mathrm{SL}(n,p)$.

Conjecture 8. *G - simple* $\Rightarrow \operatorname{diam} = \mathrm{O}((\log|G|)^c)$.

So $\operatorname{diam} \leq (n^2 \log p)^2$ which would be hard to prove, but e^n may be manageable.

2. Average Case.

Theorem 9. (Dixon) $<\sigma_1, \sigma_2> = A_n$ *with* $\Pr \to 1$ *as* $n \to \infty$.

Theorem 10. (Babai-Seress) $\operatorname{diam}(\Gamma(A_n, \{\sigma_1, \sigma_2\})) = n^{\mathrm{O}(\log n)}$ *w.h.p.*

Aim: get something close for $\mathrm{PSL}(n,p)$.

3. Problem.

Conjecture 11. (Kantor) $\operatorname{diam}(\Gamma(A_n, \{\sigma_1, \sigma_2\})) = \mathrm{O}(n \log n)$ *w.h.p.*

Some people believe this is not true.

Question: True or False?

Weaker version: Prove that $\Gamma(A_n, \{\sigma_1, \sigma_2\})$ are NOT exanders w.h.p.

Random Graphs vs Random Cayley Graphs

1.

Theorem 12. (Ramsey Theory) *In random undirected graph Γ with n vertices, there exists a $m = c \cdot \log n$ complete subgraph in Γ and a $m = c \cdot \log n$ complete subgraph in $\overline{\Gamma}$ w.h.p.*

Now suppose Γ is a random Cayley graph over a fixed group G. People believe the same is true.

Aim: prove it (N. Alon proved the result with $m = c\sqrt{\log n}$.)

2.

Theorem 13. *Γ - random graph on n vertices* $\Rightarrow \operatorname{Aut}(\Gamma) = 1$ *with high probability.*

NB: Erdős and Rényi proved that one has to remove $\theta(n^2)$ edges before a nontrivial automorphism appears.

Question: if Γ - random Cayley graph, is $\operatorname{Aut}(\Gamma) = G$ with high probability?

L. Goldberg and M. Jerrum conjecture this for $G = \mathbb{Z}_n$.

Percolation on finite Cayley graphs

Fix a Cayley graph Γ and probability p. Delete edges with $\Pr = (1-p)$ independently and look at the connected components. Say $\Gamma \supset$ large cluster if $\exists$ connected component $> \frac{1}{2}|\Gamma|$.

Conjecture 14. (Benjamini) *If* $\operatorname{diam}(\Gamma) < c \cdot \frac{|G|}{\log^2 |G|}$, *then Cayley graph Γ contains large cluster with* $\Pr > \frac{1}{2}$ *for $p < 1 - \varepsilon$ where ε is independent of the size of the graph.*

Itai Benjamini confirms the conjecture for abelian groups.

Question: Is this true for G nilpotent? What about S_n?