On the Upper Bound Lemma - A Brief Presentation by Martin Hildebrand

The Upper Bound Lemma of Diaconis and Shahshahani states that if P is a probability on a finite group G and U is the uniform probability on G, then

$$\|P - U\|^2 \leq \frac{1}{4} \sum_{\rho}^{*} d_\rho Tr(\hat{P}(\rho)\hat{P}(\rho)^*)$$

where the sum is over all non-trivial irreducible representations ρ of G up to equivalence and $\hat{P}(\rho)^*$ is the conjugate transpose of the Fourier transform $\hat{P}(\rho)$. At first glance, this lemma might not appear to be particularly helpful. However, there are some places where it is quite useful, and I used it considerably in some of my earlier work.

If the group is abelian, then the degree of each irreducible representation is 1. This fact not only can be helpful for analyzing random walks on such groups but also can be be useful for studying random processes of the form

$$X_{n+1} = a_n X_n + b_n \pmod p$$

where $X_0 = 0$. This is an extension of a random process described in Ron Graham's talk. To analyze such random processes, I developed a recurrence relation for the Fourier transform of X_n.

For non-abelian groups, if P is constant on conjugacy classes, then $\hat{P}(\rho)$ is a constant times the identity, and the constant can be expressed in terms of the characters of the representation and the degree of the representation. If P^{*m} is the probability distribution after m steps of a random walk starting at the identity element (where $P = P^{*1}$), then $\widehat{P^{*m}}(\rho) = (\hat{P}(\rho))^m$ is relatively easy to compute. This property was used by Diaconis and Shahshahani to study a random walk on the symmetric group where at each step one performs a random transposition (or with a certain probability leaves the permutation alone). I also used this property to study a random walk on $SL_n(F_q)$ where F_q is a finite field with q elements; at each step one multiplies by a random transvection (a matrix which fixes a hyperplane in F_q^n). I actually used representation theory of $GL_n(F_q)$ and studied a related random process on $GL_n(F_q)$ with the same variation distance as the random transvection problem on $SL_n(F_q)$. First I did the case where F_q is the integers mod 2;

there $GL_n(F_q)$ and $SL_n(F_q)$ are identical, but I extended the results to other F_q with an argument that deals with the various determinants of the matrices in $GL_n(F_q)$. The random transvections problem has a sharp cut-off phenomenon. After $n + c$ steps where c is a positive constant, the random walk is close to uniformly distributed in variation distance while after $n - c$ steps, the random walk is far from uniformly distributed.

In his Ph.D. thesis, Carl Dou developed a variation of the Upper Bound Lemma which is useful in studying "random random walks" on finite groups. A number of other works have examined random random walks; some use the Upper Bound Lemma while others use other techniques. A Ph.D. student I'm supervising is working on extending Dou's results. A survey I've authored on random random walks has recently appeared in the new electronic journal *Probability Surveys*.

References

Diaconis, P. *Group Representations in Probability and Statistics*. Institute of Mathematical Statistics, 1988.

Diaconis, P. and Shahshahani, M. Generating a random permutation with random transpositions. *Z. Wahrscheinlichkeitstheorie Verw. Gebiete* **57** (1981), 159-179.

Dou, C. Studies of random walks on groups and random graphs. Ph.D. thesis, Department of Mathematics, Massachusetts Institute of Technology, 1992.

Hildebrand, M. Generating random elements in $SL_n(F_q)$ by random transvections. *J. Alg. Combinatorics* **1** (1992), 133-150.

Hildebrand, M. Random processes of the form $X_{n+1} = a_n X_n + b_n \pmod p$. *Ann. Probab.* **21** (1993), 710-720.

Hildebrand, M. A survey of random random walks on finite groups. *Probability Surveys* **2** (2005), 33-63.