Abstract

On the Distribution of the Elements of a Finite Group Generated by Random Covers

Nicola Pace

Department of Mathematical Sciences,
Florida Atlantic University,
777 Glades Road, Boca Raton, FL 33431 – USA

Random covers for finite groups are a crucial component for several cryptosystems and because of future potential applications in cryptography, they have received considerable attention over the last few years. In the recent paper "*Discrete logarithms for finite groups*", Klingler et al. define a multiset $\mathcal{S}_k$, which can be considered as a particular type of random cover, and formulate a generalization of the traditional discrete logarithm problem from cyclic to arbitrary finite groups. In this talk, we consider a more general type of random cover and show that a result proved by Klingler et al., on the distribution of elements generated by random covers, still holds for the random covers of this larger family. We consider the particular instance analyzed by Klingler et al. for the groups $\mathrm{PSL}(2, \mathrm{p})$. For the case where α and β are two non-commuting generators of order p, we provide a closed form formula for the multiplicities of elements of $\mathrm{PSL}(2, \mathrm{p})$ in $\mathcal{S}_k(\alpha, \beta)$ and consequently a best possible estimation for the distribution of group elements in $\mathcal{S}_k(\alpha, \beta)$.