abstract

IAS/PU NUMBER THEORY
Topic:

Speaker:

Affiliation:

Date:

Time/Room:

In inverse problems in arithmetic combinatorics, one is interested in describing internal properties of those finite subsets A of an algebraic structure that ``barely expand'' under its operations. One of the deepest results in the area is Freiman's theorem providing a complete characterization of the sets A in abelian torsion-free groups for which $|A+A|$ is almost linear in A. Nothing non-trivial, however, is known already about sets of integers A with $|A+A|\leq A^{1+\delta}$.

Surprisingly, these questions have turned out to be easier for more complicated algebraic structures like commutative rings or, very recently, non-abelian groups. In particular, Chang (2006) proved that for some fixed δ, any set A in a free group with $|AAA|\leq A^{1+\delta}$ belongs to a cyclic subgroup.

We give a purely combinatorial proof of this result based on the theory of periodic words and their occurrences. Our proof also shows that δ can be chosen arbitrarily close to 1, and this is optimal. This further generalizes to arbitrary virtually free groups (with the respective change in the conclusion); in particular, our result is applicable to the modular group $PSL_2(Z)$.