

1145-06-2804

**Bal K Khadka\*** (bkhadka@gmc.edu) and **Spyros Magliveras**. *Random walks vs Spoke Hub distribution models on a Lattice Basis Reduction under a projective special linear group  $PSL_2(q)$ .*

We present a study on the Lattice Basis Reduction using the famous LLL algorithm. For these experiment, we have used results of our experiments based on permutation techniques of basis reduction. We select permutations from a small subgroup  $G < S_m$ , where  $G$  is isomorphic to a projective special linear group  $PSL_2(q)$ . Then we use random walks and spoke hub distribution models to permute the lattice basis  $B$  using elements of  $G$  to get an *Approximated Shortest Vector* in a given lattice.

This study relies on the sensitivity of LLL to permutations of the input lattice basis  $B$ , and optimization ideas over the symmetric group  $S_m$  viewed as a metric space.

**Keywords:** LLL Lattice Basis Reduction, permutation matrix, Integer unimodular matrix, random walks, spoke-hub distribution, projective special linear group. (Received September 25, 2018)