1125-VC-1678 **Bal K. Khadka*** (bkhadkka@gmc.edu), 221 New Petersburg Dr, Apt D, Martinez, GA 30907, and **Spyros M. Magliveras**. *Techniques in Lattice Basis Reduction.*

The credit on *reduction theory* goes back to the work of Lagrange, Gauss, Hermite, Korkin, Zolotarev, and Minkowski. Modern reduction theory is voluminous and includes the work of A. Lenstra, H. Lenstra and L. Lovasz who created the well known LLL algorithm, and many other researchers such as L. Babai and C. P. Schnorr who created significant new variants of basis reduction algorithms. In this paper, we propose and investigate the efficacy of new optimization techniques to be used along with LLL algorithm. The techniques we have proposed are: i) *hill climbing (HC)*, ii) *lattice diffusion-sub lattice fusion (LDSF)*, and iii) *multistage hybrid LDSF-HC*. The first technique relies on the sensitivity of LLL to permutations of the input basis B, and optimization ideas over the symmetric group S_m viewed as a metric space. The second technique relies on partitioning the lattice into sublattices, performing basis reduction in the partition sublattice blocks, fusing the sublattices, and repeating. We also point out places where parallel computation can reduce run-times achieving almost linear speedup. The multistage hybrid technique relies on the lattice diffusion and sublattice fusion and hill climbing algorithms.

(Received September 18, 2016)