Solving the inverse Gram problem over commutative matrix *-algebras over \mathbb{Z} using lattice methods

Assaf Goldberger

Tel-Aviv University

Abstract

Let $G \in \mathbb{Z}^{n \times n}$ be a positive-definite matrix. The inverse Gram problem (IGP) over \mathbb{Z} is to find a solution $X \in \mathbb{Z}^{n \times n}$ to the equation $XX^{\top} = G$. This problem arises naturally in the contexts of Hadamard and weighing matrices, and more generally block designs. In a previous work with Y.Strassler [1] we have suggested a lattice based method for solving the IGP. While in some cases our method is effective, it is usually very bad in the contexts mentioned above. In this work we will study the structured version, where X comes from a commutative matrix *-algebra $\mathcal{A} \subset \mathbb{Z}^{n \times n}$. Our adapted algorithm becomes effective again, even at instances where the general algorithm fails. So for example, solving the IGP for circulant matrices of size 100 can be done very quickly. In this talk we will also give an upper bound to the number of solutions in \mathcal{A} .

References

 A. Goldberger and Y. Strassler. A practical algorithm for completing half-Hadamard matrices using LLL. *Journal of Algebraic Combinatorics*, 55:217–244, 2022.