

Collaborative projects in PARI/GP

1 LLL with symmetries

The goal of the project is to work towards a PARI/GP implementation of effective reduction theory for some arithmetic groups other than SL_n (which corresponds to the reduction theory of lattices).

Such an algorithm is described in [RT25], but the paper does not come with an implementation. However, I think it is possible to simplify the algorithm and make it more efficient at the same time, using the ideas of the FLATTER algorithm [RH23] which is implemented in PARI/GP.

The following steps (not necessarily in this order) would lead to this goal, and some steps would be interesting independently of the full completion.

- Read a bit of theory of semisimple Lie groups (roots, decompositions).
- Choose which group G to work with (e.g. the symplectic group Sp_{2n} or the split orthogonal groups $SO(n, n)$ and $SO(n, n + 1)$, or exceptional groups if you are interested in them). In fact some of the steps below also make sense for non-split groups (for instance orthogonal groups $SO(p, q)$ or complex groups $G = H(\mathbb{C})$) and would be interesting.
- Identify what are its important subgroups (maximal compact subgroup K , maximal split torus A , Borel subgroup $B = AN$, other parabolic subgroups containing B).
- Identify a nice representation of $G \subset GL_m$.
- Implement the Iwasawa decomposition KAN (generalising, and possibly using, the classical QR decomposition).
- Implement the Cartan decomposition KAK (generalising, and possibly using, the classical singular values decomposition).
- Implement size-reduction. The paper [RT25] describes an algorithm, but a simpler version using blocks recursively should be sufficient.
- Implement LLL reduction by a recursive strategy.

Aurel Page will provide guidance for this project.

2 Automorphisms of Hermitian lattices

Let K an imaginary quadratic field, let M be the Gram matrix of an Hermitian lattice L over K of dimension n . Write an algorithm to compute the automorphisms of L by using restriction of scalars to reduce the problem to the computation of the automorphism group of an integral lattice, with additional conditions given by symmetric matrices.

In GP, the function `qfauto` accepts a list of symmetric integral matrices representing bilinear forms B_i , only the first one being required to be positive definite, and returns the group of automorphisms of the lattice that preserve all the input bilinear forms B_i .

We will provide test files. Bill Allombert will provide guidance for this project.

References

- [RH23] Keegan Ryan and Nadia Heninger. Fast practical lattice reduction through iterated compression. In *Advances in cryptology – CRYPTO 2023. 43rd annual international cryptology conference, CRYPTO 2023, Santa Barbara, CA, USA, August 20–24, 2023. Proceedings. Part III*, pages 3–36. Cham: Springer, 2023. <https://zbmath.org/1531.94075> <https://eprint.iacr.org/2023/237>.
- [RT25] Beth Romano and Jack A. Thorne. An LLL algorithm with symmetries. *Int. J. Number Theory*, 21(6):1361–1393, 2025. <https://zbmath.org/8054361>.