

# Asiacrypt Artifact for Dense and smooth lattices in any genus.

This is the artifact belonging to the paper: > Wessel van Woerden, Dense and smooth lattices in any genus, Asiacrypt 2024.

It contains the following parts:

1. The data, plots and utilities to generate the plots in the paper in `data/`, `plots/` and `scripts/plot_*`
2. A patched `QuadraticForm` class named `QuadraticFormFixed` in `scripts/quadratic_form_fixed` which efficiently computes the `local_density(p,k)` at the prime  $p = 2$ .
3. A script that computes the average theta series over the genus of forms of the shape  $I_k + qI_{n-k}$  where  $+$  is an orthogonal sum.

## Dependencies

Dependencies required including the version on which the scripts have been tested.

- SageMath (10.4)
- Numpy (2.0.1)
- Matplotlib (3.9.2)
- LaTeX (e.g. pdfTex, TeXLive)

Generally, it should be sufficient to have a somewhat recent version of Sagemath and a LaTeX distribution installed.

## Plots

To generate the plots in the paper go to the `scripts/` folder and run

```
sage plot_even_unimodular.sage
```

This generates the pdf files `plots/even_packing.pdf` and `plots/even_smoothing.pdf` corresponding to Figures 1 and 2 in section 3.2 of the paper respectively. It computes existence bounds for even unimodular lattices with a good packing and smoothing respectively.

To generate Figure 3 in the eprint go to the `scripts/` folder and run

```
sage plot_concrete.sage
```

This generates the file `plots/concrete_packing.pdf` corresponding to Figure 3 in section 4 of the eprint version. It is a plot of existence bounds for good packings in the genus of  $I_k + 521I_k$  for  $k = 8, 16, 24, 32, 40, 48, 56, 64$ . The data for this is available in the `data/` folder.

## Patch for computing local densities at $p = 2$

The file `scripts/quadratic_form_fixed` contains the class `QuadraticFormFixed` which fixes the inefficient implementation in the `QuadraticForm` class for counting local densities at  $p = 2$ .

Here a small example of its usage. Note that the computation below is extremely slow for the regular `QuadraticForm` class in SageMath version 10.4, but with the patch it is nearly instant.

```
sage: load("quadratic_form_fixed.sage")
sage: Q = QuadraticFormFixed(2*identity_matrix(8))
sage: Q.local_density(2, 1)
1
sage: Q.local_density(2, 4)
71/64
sage: Q.siegel_product(1)
16
sage: Q.siegel_product(2)
112
sage: Q.siegel_product(100)
17893136
```

We also made a pull request to integrate the patch into future version of Sagemath. See: - Issue - Pull request

Update: This pull request has now been integrated into the development branch of SageMath and thus the patch should be available in future versions 10.5+ of SageMath.

## Data generation

The data for Figure 3 of the eprint can be generated using the script `concrete_experiment.sage`. One can run the script with the parameters `n`, `k`, `q`, `start`, `end`, `cores` to compute the coefficients `starts`, `...`, `end-1` of the average theta series over the genus of  $I_k + qI_{n-k}$  where  $+$  is an orthogonal sum.. For example

```
sage concrete_experiment.sage 16 8 521 1 800 2
```

computes the average theta series coefficients  $N_1, \dots, N_{799}$  of the genus of  $I_8 + 521I_8$ . The output is stored in the file `data/siegel_product_{n}_{k}_{q}` where each row contains one space separated pair  $i N_i$ .

At the moment Sagemath contains a bug for computing the average coefficients for odd dimensional lattices, therefore one should only run the above script for even values of  $n$ .

Alternatively, one can execute

```
sh run_small_concrete_experiments.sh
```

to run the same experiment as above. One can uncomment other lines in the same script to also generate the higher dimensional cases. Note that the runtime can be quite significant for the larger dimensional cases. The precomputed data was computed on a machine with 32 cores over several days.