Experiment 2 - Recentering

Before

Hypothesis

Recentering is better, even if strictly speaking the inequalities are not always true (just most of the time). We do not expect a significant difference between exact and nonexact inequalities.

Setup

- The dimensions: D = {50, 52, ..., 140}
- The number of signatures used: N = {500, 600, ..., 7000, 8000, 9000, 10000}
- The data source: data = {real, sim}
- The recentering used: rec = {exact, inexact, none, bad}
- each run 5 times, random sampling $n \in N$ signatures, constructing lattice from $d \in D$ shortest signatures, then doing geometric bounds from 2 bits on. Doing SVP with progressive BKZ (betas: 15, 20, 30, 40, 45, 48, 51, 53, 55).
- In this experiment, we use $l_i + 1$ instead of l_i in the matrix if we are in the **exact** or **inexact** recentering cases. In the **none** case, we do only l_i, in the **bad** case we do $l_i + 1$ but no recentering. Furthermore, the values $2^{l_i+1}u_i$ are replaced with $2^{l_i+1}u_i + 2^{256}$ if the **exact** recentering is used and with $2^{l_i+1}u_i + n$ if the **inexact** recentering is used.

2 * 4 * 68 * 45 = 24 480 tasks

each task does 5 runs of attack: 122 400 runs of attack.

Schedule tasks:

```
for rec in {exact, inexact, none, bad}
    for data in {real, sim}
        for d in D
            for n in N
                schedule one geom task with (rec, data, n, d)
```

That makes 24 480 tasks.

Outputs

Each task outputs {real,sim}_{exact, inexact, none, bad}_{n}_{d}.csv with 5 lines for the 5 runs:

seed, success, duration, last_reduction_step, info, #liars, real_info, bad_info, good_info, result_row, result_norm

Visualizations

For both real and sim data: For both exact and inexact:

- 3D plot, x:N, y:D, z: number of successes.
- 3D plot, x:N, y:D, z: last reduction step.
- 3D plot, x:N, y:D, z: avg. duration of successful run.
- 3D plot, x:N, y:D, z: avg. result row.
- 3D plot, x:N, y:D, z: avg. result norm.
- 2D lineplot, x:N, y:sum over d in D (number of successed).

Why?

- Compares both centering possibilities to the baseline.

During

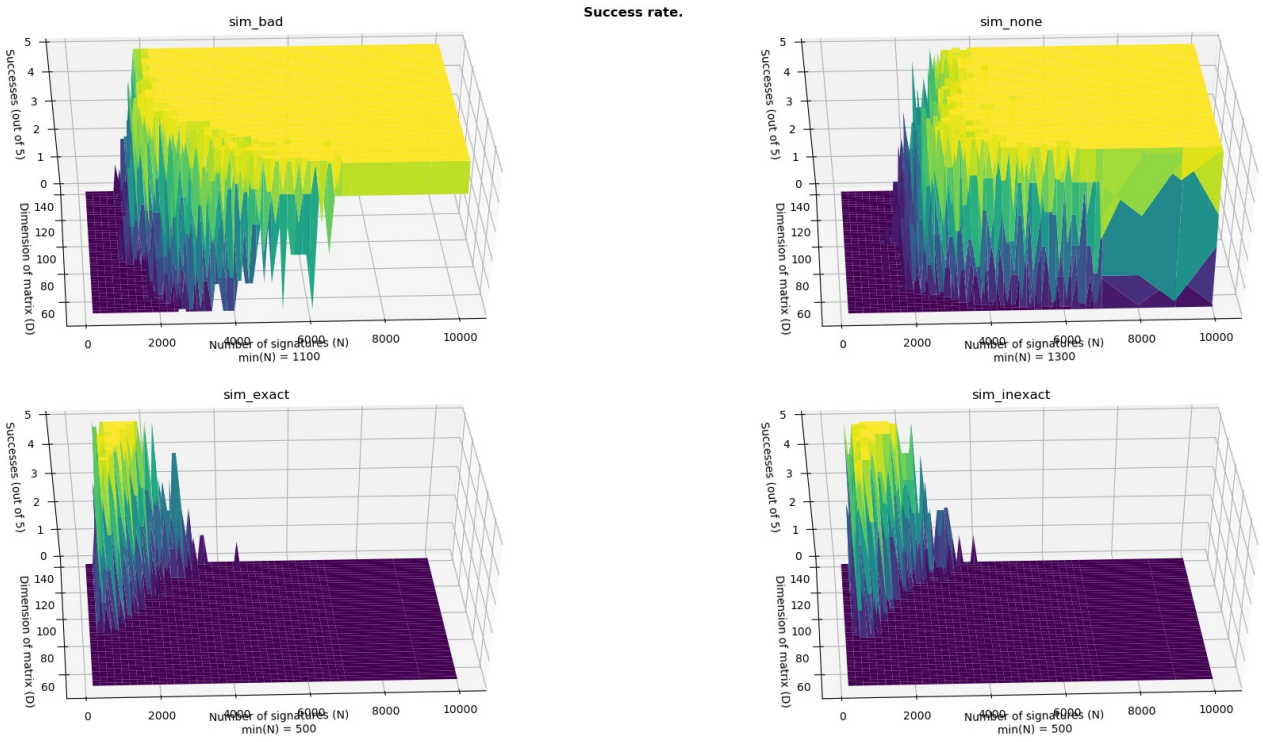
Run 01.10.2019

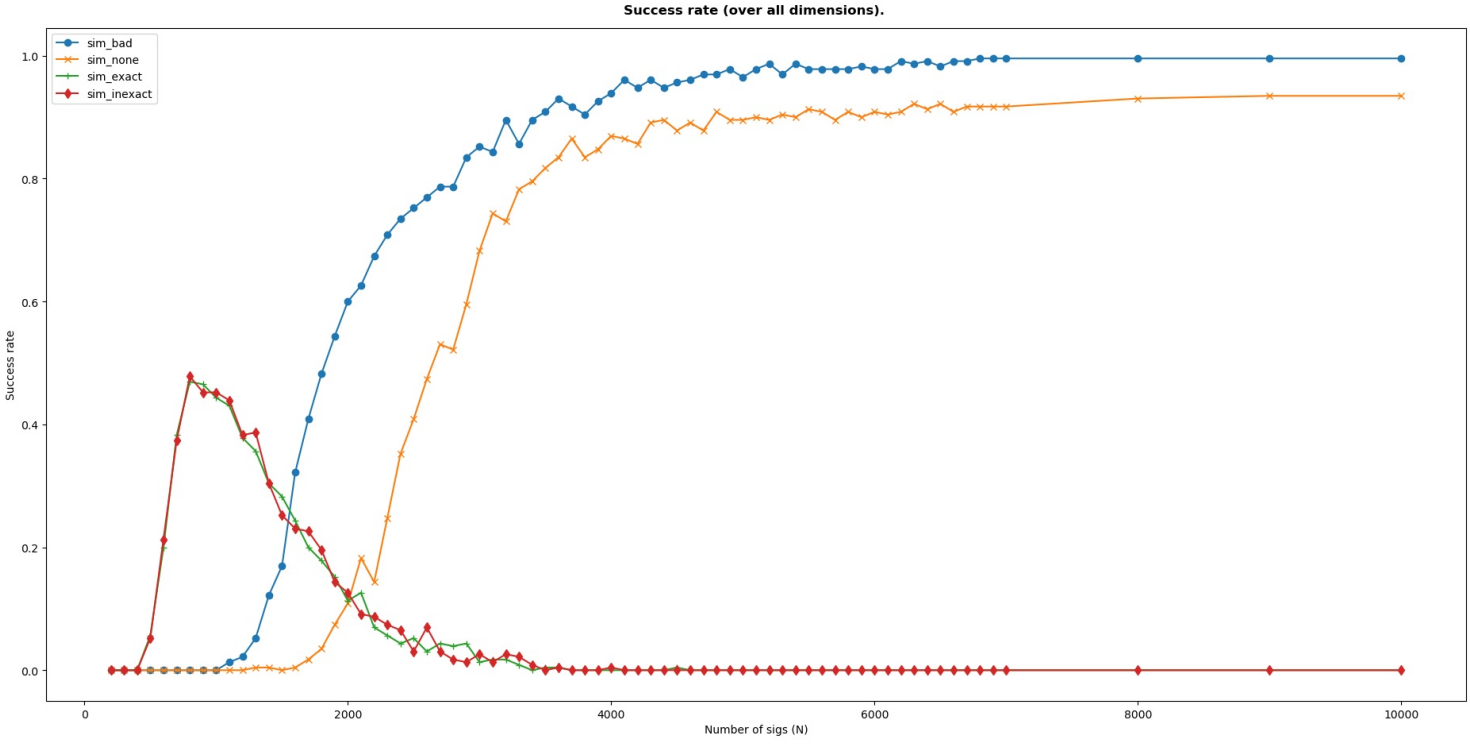
- All went well after a first dry run (had a typo in)
- Then extended the N space to {200, 300, ..., 7000, 8000, 9000, 10000}.
- No significant reruns necessary.

TODO: Real data!!!!!

After

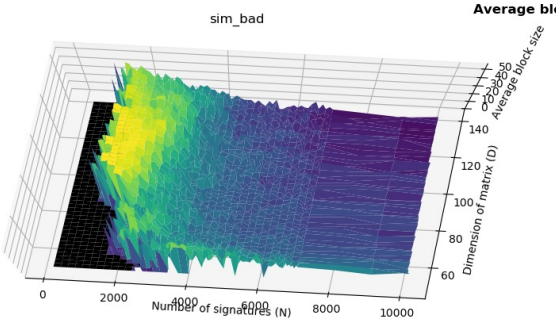
Figures



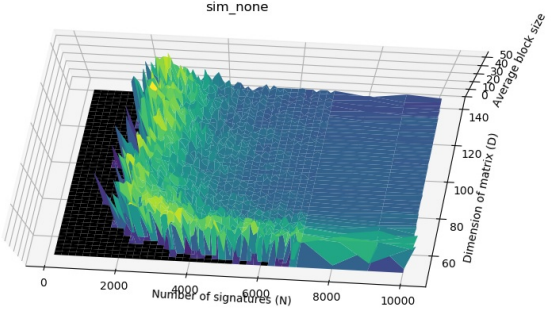


Average block size in successful runs.

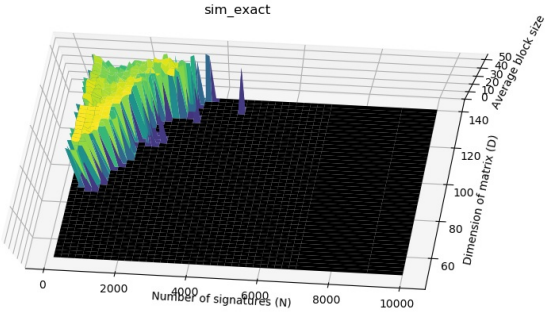
sim_bad



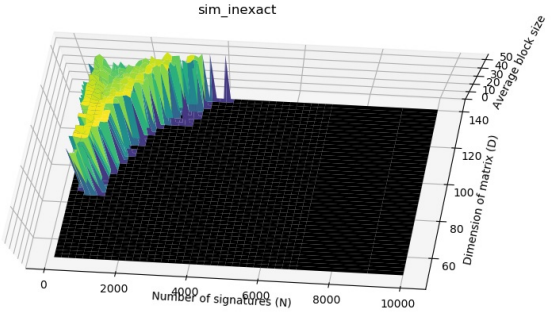
sim_none



sim_exact

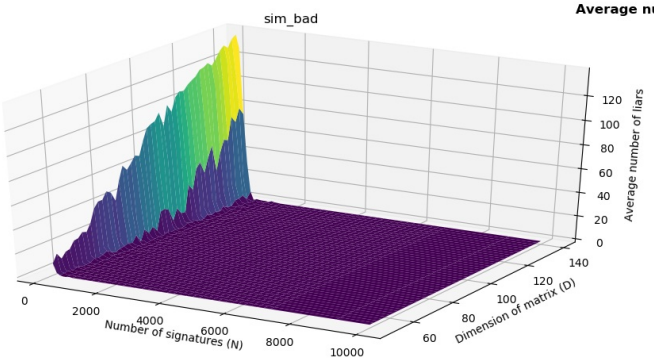


sim_inexact

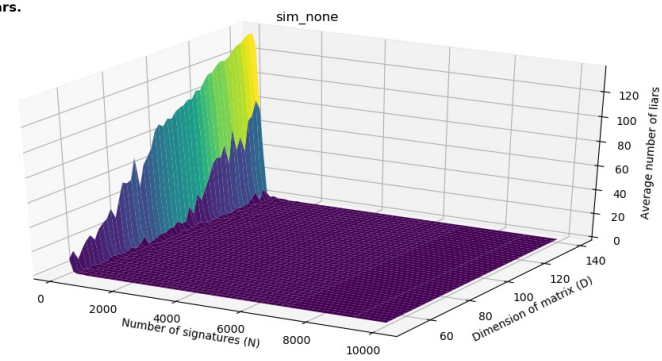


Average number of liars.

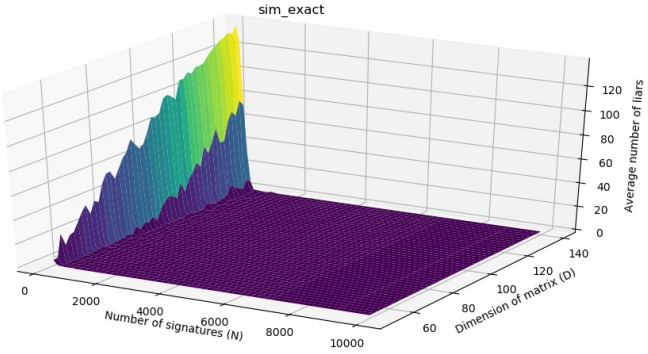
sim_bad



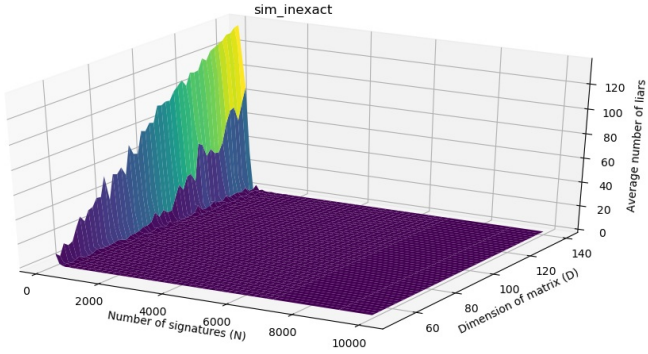
sim_none



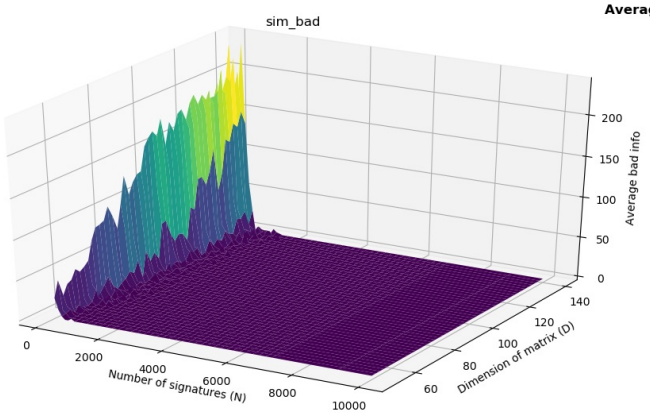
sim_exact

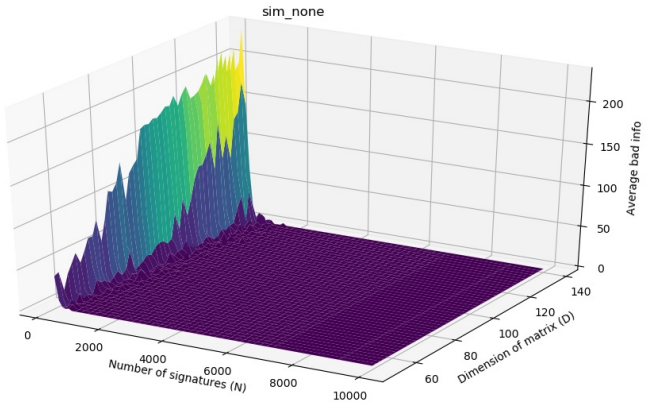


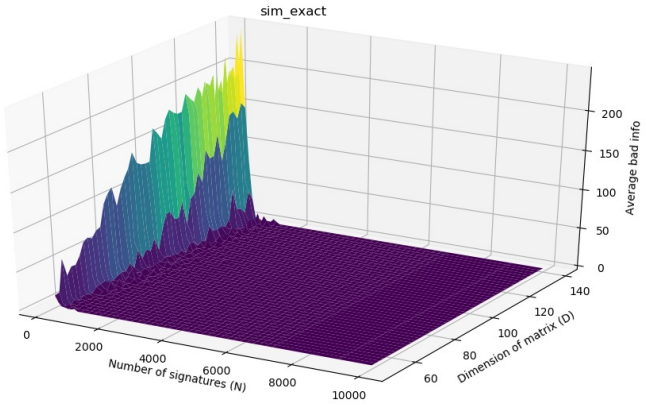
sim_inexact

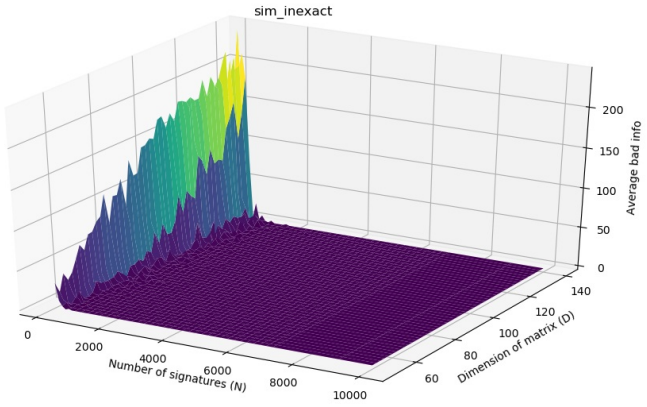


Average bad info.

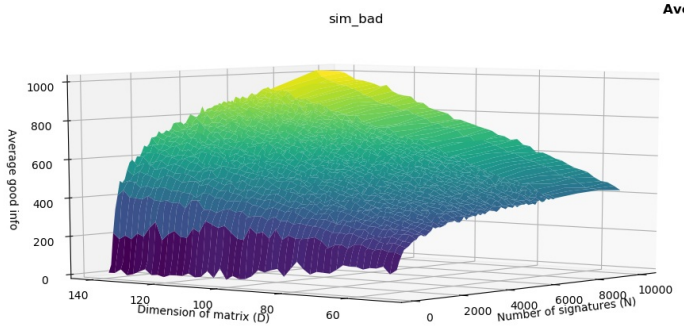


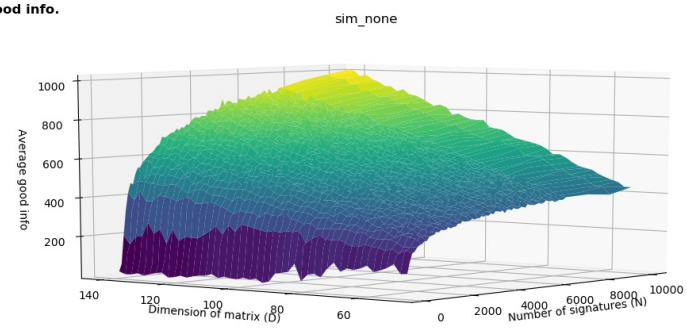


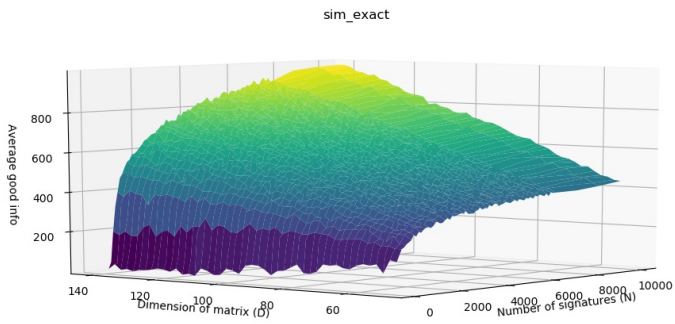


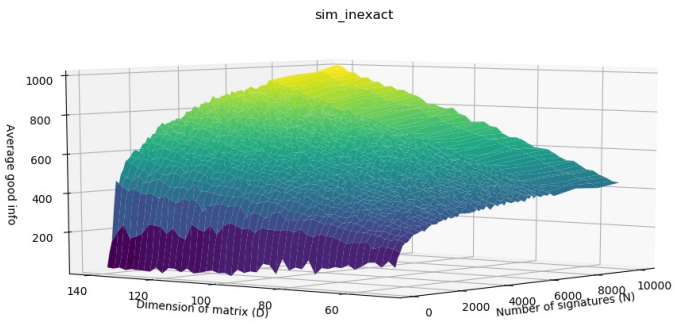


Average good info.

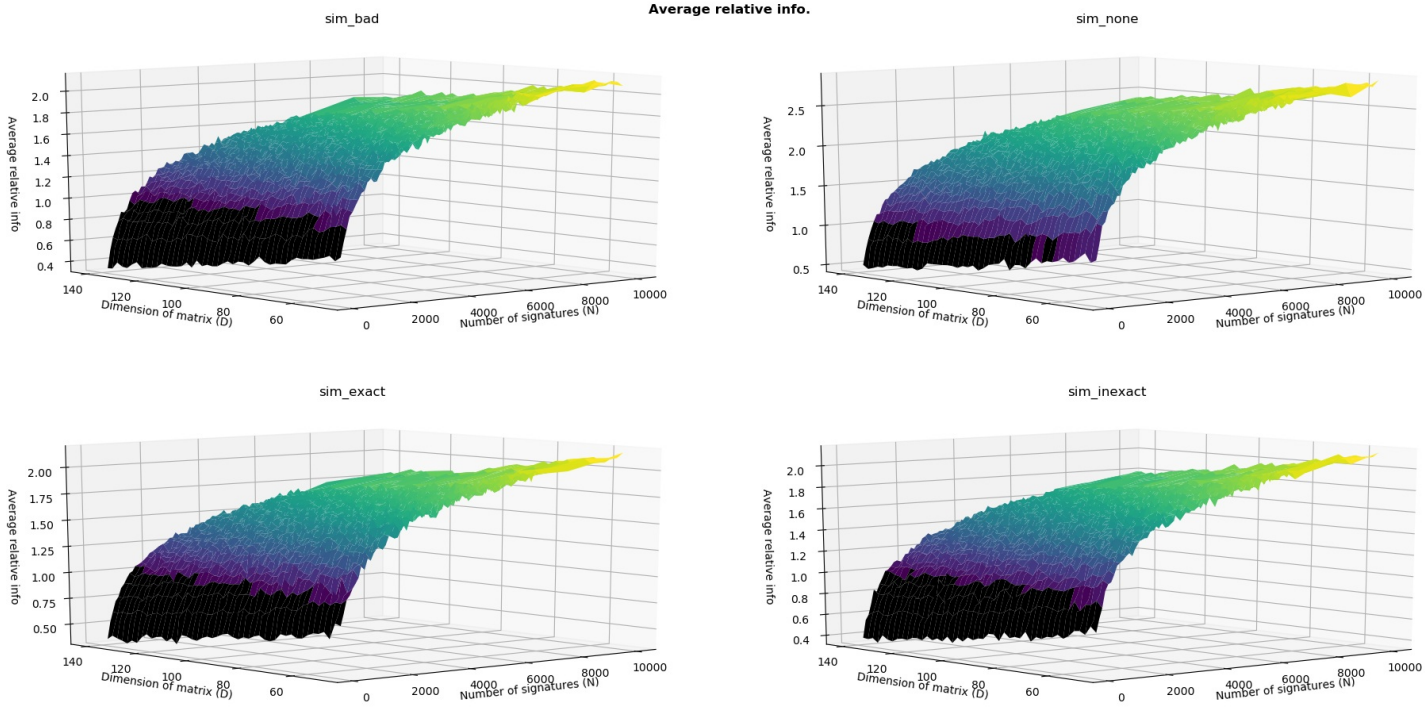




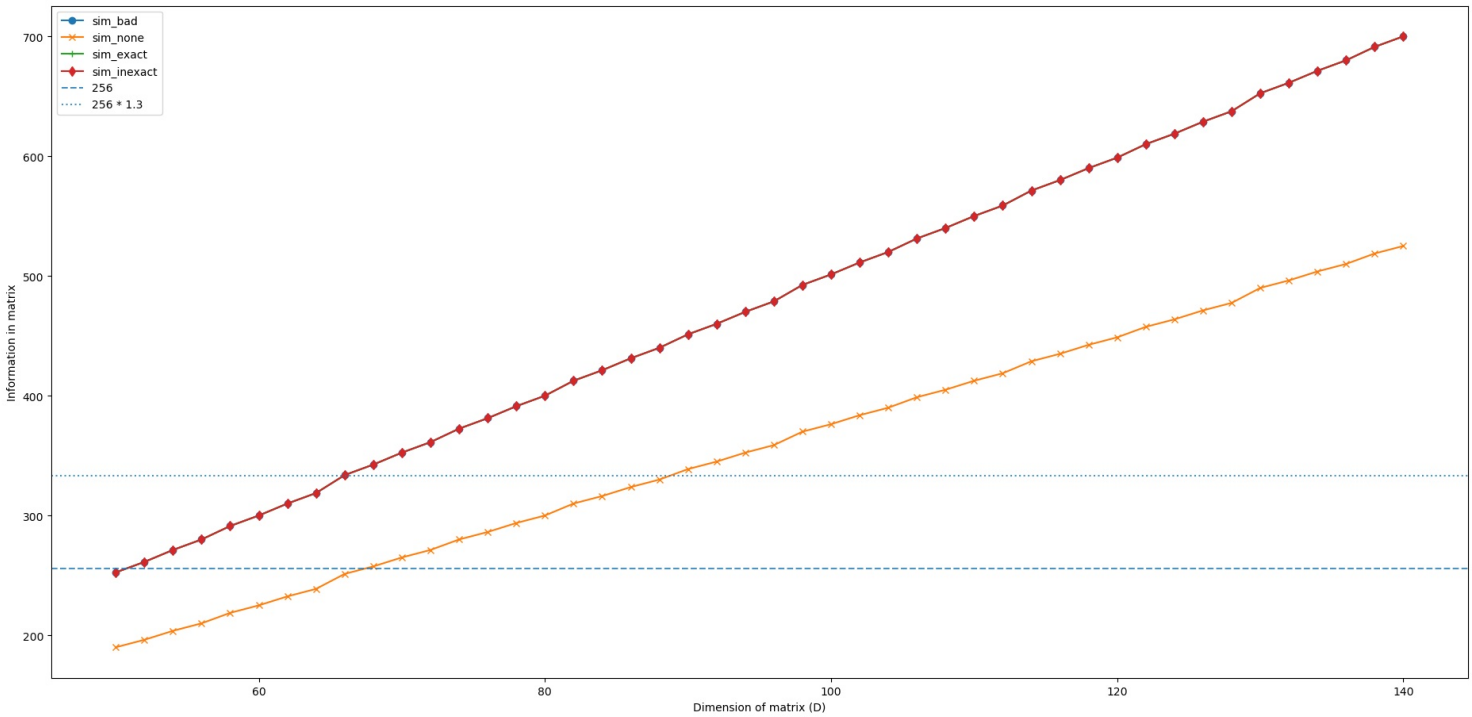




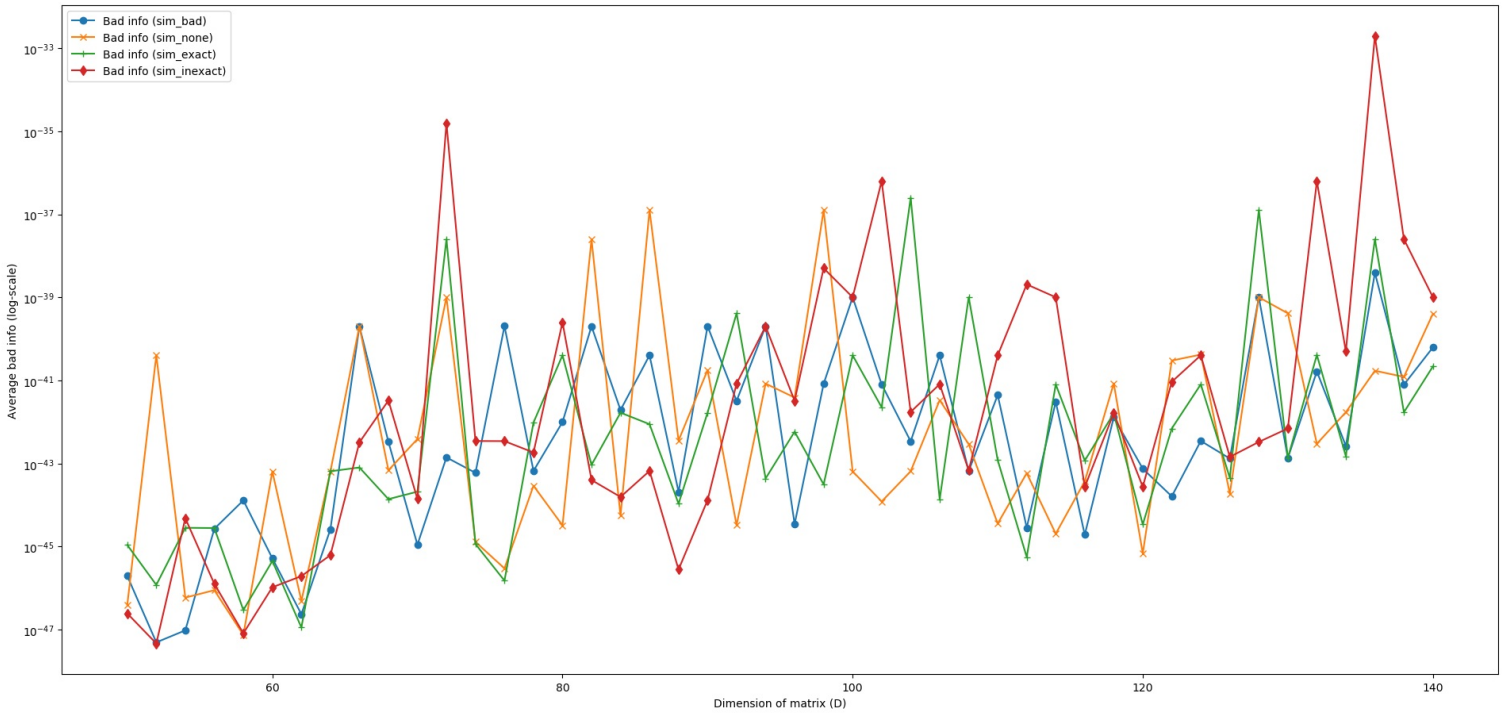
Average relative info.



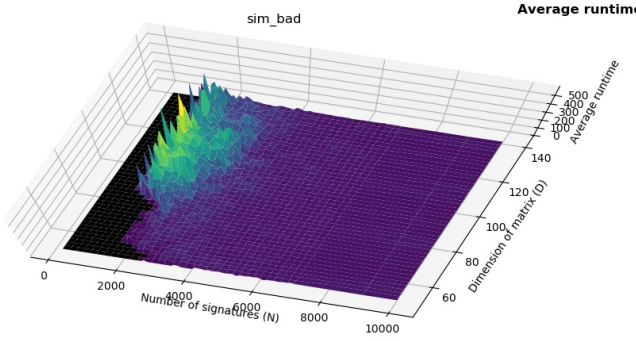
Average info.

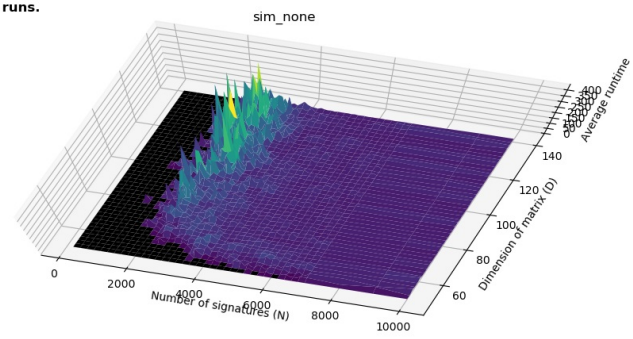


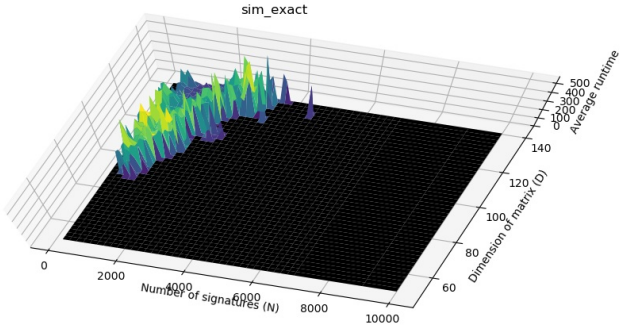
Average bad info.

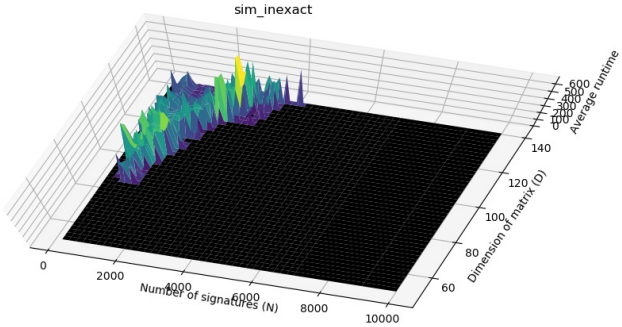


Average runtime in successful runs.

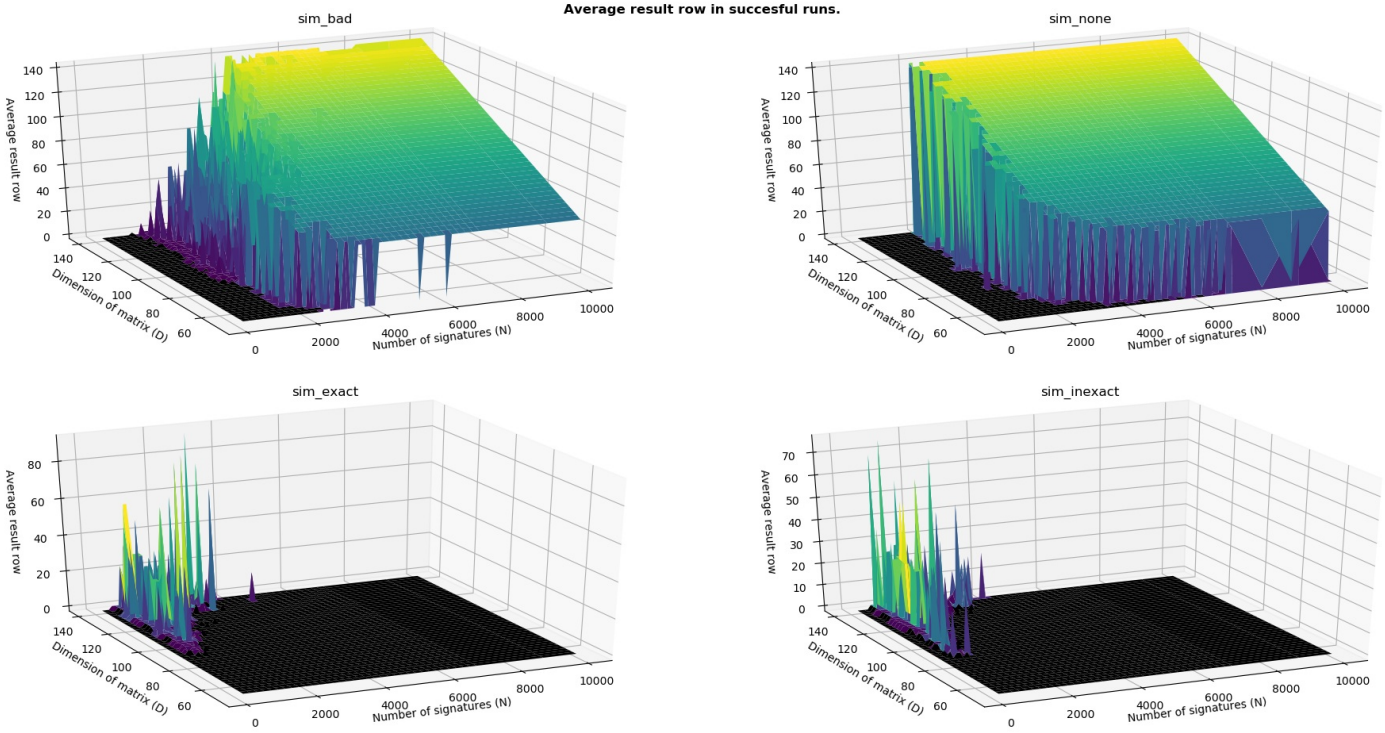








Average result row in succesful runs.



Average result norm in succesful runs.