Improving Lagarias-Odlyzko for Subset-sum

Antoine Joux

@ STACS 2026, March 11th, 2026

Joint work with Karol Węgrzycki

Subset-sum

- Classical NP-complete problem

- Search version:
  - Given values $a_1, a_2, \cdots, a_n$ and target T
  - Find $e_1, e_2, \cdots, e_n$ in $\{0,1\}$ such that:

$$\vec{e} \cdot \vec{a} \equiv \sum_{i=1}^{n} e_i a_i = T$$

Many algorithms for various regimes

Lagarias-Odlyzko idea: turn this into a lattice problem

- Let $\overrightarrow{A} = (a_1, \cdots, a_n, -T)$:

  The set of integers vectors $\overrightarrow{X}$ orthogonal to $\overrightarrow{A}$ is a lattice $\mathscr{L}$

- Furthermore, for any subset-sum solution: $\overrightarrow{E} = (e_1, \cdots, e_n, 1)$ is in $\mathscr{L}$
- And, it is a **short vector**

- Thus, lattice reduction and LLL should find it in polynomial time

Analysis of Lagarias-Odlyzko

- Relies on LLL guarantee on output basis $(\overrightarrow{b_1}, \cdot, \overrightarrow{b_n})$ of $\mathscr{L}$

$$\|b_1\| \leq \gamma_{LLL}^{n} \cdot \lambda_1(\mathscr{L})$$

- If the solution vector $\overrightarrow{E}$ is the shortest with a gap of γ_{LLL}^{n} then LLL finds it

- For random instances — with large enough number size, it works
- More precisely, with a_i uniform in $[1 \cdots \Gamma]$ they need:

$$\Gamma = \gamma_{LLL}^{n^2(1+o(1))}$$

$$\gamma_{LLL} \approx \sqrt{4/3}$$

Our contribution

- New related technique with two main gains

  1- Reduced sampling interval $[1 \cdots \sqrt{\Gamma}]$

  2- It is a preprocessing that then solves quickly for every target

- Reducing the interval could be achieved before with BKZ
  (time vs quality tradeoff)

  - We still gain a $\sqrt{\ }$ factor compared to Lagarias-Odlyzko

  - However, asymptotically, $2^{c\,n^2}$ and $2^{c\,n^2/2}$ (for any c) mean the same

Basic Idea

- Still lattice-based but different

- Let $\overrightarrow{A} = (a_1, \cdots, a_n)$, without the target and choose a prime p

- Our lattice $\mathscr{L}$:

  All vectors congruent to a multiple of $\overrightarrow{A} \pmod{p}$

$$\mathscr{L} = \mathbb{Z}\overrightarrow{A} + p\mathbb{Z}^n$$

Basic Idea — continued

- Let $\overrightarrow{B} \equiv \lambda_B \overrightarrow{A} \pmod{p}$ and $\overrightarrow{E} = (e_1, \cdots, e_n)$ a solution vector, then

$$\overrightarrow{E} \cdot \overrightarrow{B} \equiv \lambda_B T \pmod{p}.$$

- If $\| \overrightarrow{B} \|_1$ is small enough, we get an exact equation:

$$\overrightarrow{E} \cdot \overrightarrow{B} = (\lambda_B T \bmod p).$$

- With many $\overrightarrow{B}$s we get a full rank linear system for any target
- This recovers a candidate solution $\overrightarrow{E}$
  - Then we check that it is 0/1 and that $\overrightarrow{E} \cdot \overrightarrow{A} = T$

Analysis

- We just need to prove that LLL on $\mathscr{L}$ outputs only short vectors

- We need $\|\vec{B}\|_1 < p/2 \Leftarrow \|\vec{B}\| < p/\sqrt{n}$
- Are every vector in the LLL basis short ?

Since $\vec{b}_i = \vec{b}_i^* + \sum_{j=1}^{i-1} \mu_{i,j}\vec{b}_j^*$ we just need to bound the $\|\vec{b}_i^*\|$

Analysis — continued

First vector relies on: $\|\vec{b}_1^{\,*}\| \leq \gamma_{LLL}^{n/2} \det(\mathscr{L})^{1/n} = \gamma_{LLL}^{n/2}\, p^{1-1/n}$

1- For the others (first half) we need: $\|\vec{b}_1^{\,*}\| \geq \det(\mathscr{L})^{1/n}$

2- Last vector needs: $\|\vec{b}_n^{\,*}\| \leq \det(\mathscr{L})^{1/n}$

Ok, with overwhelming prob. on $\overrightarrow{A}$

Second half directly derives from this and $\|\vec{b}_i^{*}\| \leq \gamma_{LLL}\, \|\vec{b}_{i+1}^{*}\|$

CISPA
HELMHOLTZ CENTER FOR INFORMATION SECURITY

Conclusion

Questions?