Solving SVP in Two Dimensions

Debadatta Kar
Cryptography Research Lab
Indian Institute of Science Education and Research Bhopal

July 21, 2025

Lecture 4

1 Introduction

The SVP problem, which asks to find the shortest vector in a lattice, was first solved way back in 1805 by the famous German mathematician Carl Friedrich Gauss. The solution provided by Gauss is polynomial time and exact. However, it is only restricted to the case of two dimensions. The algorithm proposed is now named as Gauss Lattice Reduction Algorithm(GLRA). Often it is linked to Euclid's Algorithm, which finds the GCD of two integers. In this article, we will provide a detailed analysis of GLRA for obtaining the reduced basis and its correctness along with the time complexity.

2 Shortest Vector problem(SVP)

Input: Basis of lattice B
Output: $v \in \mathcal{L}$ such that

$$||v|| = \lambda_1$$

This problem specifically finds a short vector v from the lattice vectors.

3 Solving SVP in 2 Dimensions

Definition 3.1. *A babis $[b_1, b_2]$ is said to be reduced iff*

1. $||b_1|| \leq ||b_2||$
2. $|\mu_{2,1}| \leq 1/2$

Where, $\mu_{1,2} = \frac{\langle b_2, b_1 \rangle}{\langle b_1, b_1 \rangle}$

Definition 3.2. *A basis $[b_1, b_2]$ is reduced iff*

$$||b_1|| \leq ||b_2|| \leq ||b_1 - b_2|| \leq ||b_1 + b_2||$$

4 Gauss Lattice Reduction Algorithm

The Gauss lattice reduction algorithm takes as input two linearly independent lattice vectors b_1, b_2 and it outputs two close to orthogonal lattice vectors b'_1, b'_2. This algorithm, provided below, named as the GLRA, is supported by the mathematical results, most of whose proofs are given in this section.

Algorithm 1 GLRA Algorithm

while TRUE **do**
  if $||b_1|| > ||b_2||$ **then**
    SWAP b_1 and b_2
  end if
  $\mu_{2,1} = \frac{\langle b_1, b_2\rangle}{\langle b_1, b_1\rangle}$
  $m = \lfloor \mu_{2,1} \rceil$
  $b_2 = b_2 - m \cdot b_1$
  if $||b_1|| \leq ||b_2||$ and $m = 0$ **then**
    break
  end if
end while
return b_1, b_2 =0

Theorem 4.1. *Let b_1, b_2 be the initial vectors of an iteration of the algorithm and let $b'_1 = b_2 - mb_1$ and $b'_2 = b_1$ be next set of vectors considered in the GLRA. Then except for possibly the last two iterations*

$$||b'_1|| < \frac{||b_1||^2}{3}$$

Proof. Before going ahead, let's note this simple calculation. Consider $-1/2 \leq \epsilon \leq 1/2$

$$m = \lfloor \mu \rceil = \left\lfloor \frac{\langle b_2, b_1\rangle}{\langle b_1, b_1\rangle} \right\rceil = \frac{\langle b_2, b_1\rangle}{\langle b_1, b_2\rangle} + \epsilon \tag{1}$$

Now compute,

$$\begin{aligned}
\left\langle b_1, b'_1 \right\rangle = \langle b_1, b_2 - mb_1\rangle &= \left\langle b_1, b_2 - \left(\frac{\langle b_1, b_2\rangle}{\langle b_1, b_1\rangle} - \epsilon\right) b_1 \right\rangle \\
&= \langle b_1, b_2\rangle - \left(\frac{\langle b_1, b_2\rangle}{\langle b_1, b_1\rangle} - \epsilon\right) \langle b_1, b_1\rangle \\
&= \langle b_1.b_2\rangle - \langle b_1, b_2\rangle - \epsilon \langle b_1, b_1\rangle \\
&= -\epsilon \langle b_1, b_1\rangle = -\epsilon ||b_1||^2
\end{aligned}$$

Suppose that $|||b'_1|| \geq \frac{||b_1||}{3}$ viz $||b_1||^2 \leq 3||b'_1||^2$
Now,

$$|\left\langle b'_1, b'_2 \right\rangle| = |\left\langle b'_1, b_1 \right\rangle| = |-\epsilon|||b_1||^2 \leq \frac{1}{2}||b_1||^2 \leq \frac{3}{2}||b'_1||^2$$

and we have,

$$|\left\langle b'_1, b'_2 \right\rangle| \leq \frac{3}{2}||b'_1||^2$$

this gives

$$\mu = \frac{\langle b'_1, b'_2\rangle}{||b'_1||^2} \leq \frac{3}{2}$$

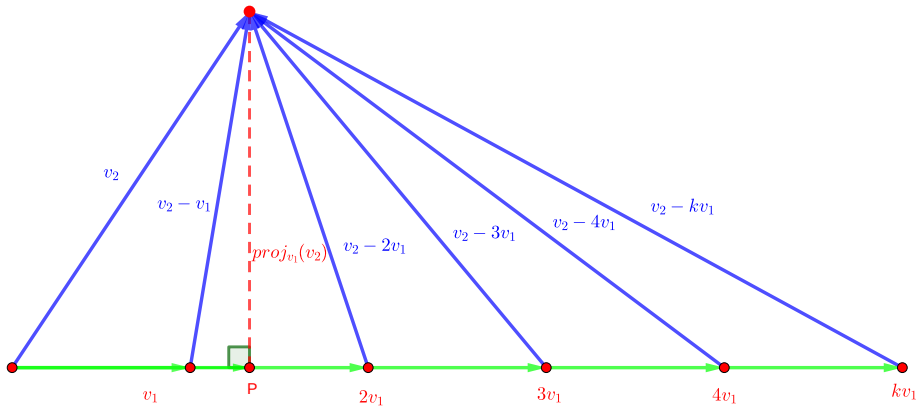

Figure 1: For the proof of Theorem 4.3

Finally, we will have $\lfloor \mu \rceil \in \{-1, 0, 1\}$
Next, we will have $b_2' = b_2' \pm b_1'$ at max.
But if $||b_2'|| < ||b_1'||$, then we would have computed b_1' differently in current iteration.
Thus, the next step is the final step. □

Theorem 4.2. *If b_1, b_2 are some iterations of vectors in the GLRA with $||b_1|| \leq ||b_2||$ and $m = \left\lfloor \frac{\langle b_2, b_1 \rangle}{\langle b_1, b_1 \rangle} \right\rceil$ then for all $k \in \mathbb{Z}$ we have*

$$||b_2 - mb_1|| \leq ||b_2 - kb_1||$$

Proof. The shortest distance between two lines is the perpendicular distance between them.
So, the length of perpendicular distance after calculating the projection of b_2 on b_1 is given by,

$$||v_2 - \frac{\langle v_1, v_2 \rangle}{||v_1||^2} v_1|| \leq ||v_2 - tv_1|| \quad \forall t \in \mathbb{R}$$

Finally,

$$||v_2 - mv_1|| \leq ||v_2 - kv_1|| \quad \forall k \in v_1$$

Figure 1 above supports the proof.

□

Corollary 4.3. *Given the hypothesis of the previous theorem* **(If b_1, b_2 are some iterations of vectors in the GLRA with $||b_1|| \leq ||b_2||$ and $m = \left\lfloor \frac{\langle b_2, b_1 \rangle}{\langle b_1, b_1 \rangle} \right\rceil$)** *if $b_1' = b_2 - mb_1$ and $b_2' = b_1$ then $||b_1'|| \leq ||k'b_2' + b_1'||$ for all $k \in \mathbb{Z}$*

Proof. If $b_1' = b_2 - mb_1$ and $b_2' = b_1$.
The previous theorem suggests,

$$||b_2 - mb_1|| \leq ||b_2 - kb_1|| \quad \forall k \in \mathbb{Z}$$

$$\begin{aligned}||b_1'|| =& ||b_2 - mb_1|| \\ &\leq ||b_2 - kb_1|| \\ &\leq ||b_2 - kb_1 - mb_1 + mb_1|| \\ &\leq || - kb_1 + mb_1 + b_2 - mb_1|| \\ &\leq ||(-k+m)b_1 + b_2 - mb_1|| \\ &\leq ||k'b_1 + b_1'||\end{aligned}$$

And finally, we have,

$$||b_1'|| \leq ||k'b_2' + b_1'||$$

□

Theorem 4.4. *If $m = \pm 1$ then the GLRA algorithm terminates in the next step.*

Proof. Let b_1, b_2 be basis for the lattice $\mathcal{L}$
Let $b_1' = b_2 - mb_1$ and $b_2' = b_1$ be vectors considered in the next step of the algorithm.
Let,

$$m = \left\lfloor \frac{\langle b_1, b_2\rangle}{\langle b_1, b_1\rangle} \right\rceil = \frac{\langle b_1, b_2\rangle}{\langle b_1, b_1\rangle} + \epsilon \quad \text{where, } \epsilon \leq 1/2$$

So,

$$m - \epsilon = \frac{\langle b_1, b_2\rangle}{\langle b_1, b_1\rangle}$$

Since $m = \pm 1$, almost $b_1' = b_2 \pm b_2'$
We need to show $m' = 0$ in the next iteration.
case I:(Donot Swap)
If $||b_1'|| \geq ||b_2'||$ then $m' = \left\lfloor \frac{\langle b_1', b_2'\rangle}{\langle b_1', b_1'\rangle} \right\rceil$

$$\begin{aligned}\langle b_1', b_2'\rangle &= \langle b_2 \pm b_2', b_2'\rangle \\ &= \langle b_2, b_2'\rangle \pm \langle b_2', b_2'\rangle \\ &= \langle b_2, b_1\rangle \pm \langle b_1, b_1\rangle\end{aligned}$$

Now we can compute

$$\begin{aligned}m' &= \left\lfloor \frac{\langle b_1', b_2'\rangle}{\langle b_1', b_1'\rangle} \right\rceil \\ &= \left\lfloor \frac{\langle b_2, b_1\rangle + \langle b_1, b_1\rangle}{\langle b_1, b_1\rangle} \right\rceil \\ &= \left\lfloor \frac{\langle b_2, b_1\rangle}{\langle b_1, b_1\rangle} + \frac{\langle b_1, b_1\rangle}{\langle b_1, b_1\rangle} \right\rceil \\ &= \lfloor m - \epsilon + 1 \rceil\end{aligned}$$

If $m = 1$ in previous iteration, $m' = \lfloor 1 - \epsilon - 1 \rceil = 0$
If $m = -1$ in previous iteration, $m' = \lfloor -1 - \epsilon + 1 \rceil = 0$
That completes case I.
case II:(Swap)
If $||b_1'|| < ||b_2'||$ then $||b_2 - mb_1|| < ||b_1||$
Also if $m = \pm 1$ then,
$||b_1'|| = || \pm b_2 \pm b_1|| \leq ||b_1||$
We also know, $|| \pm b_2 \pm b_1|| < ||b_2||$ since $||b_1|| \leq ||b_2||$
If $||b_1'|| < ||b_2'||$ then $||kb_1' - b_2|| \geq ||b_1||$ for all $k \in \mathbb{Z}$ by previous theorem(4.2)

consider $k = \pm 1$

$$b_1 \leq || \pm b_2 \pm b_1|| < ||b_1||$$

which is a contradiction.
Thus, algorithm will terminate.

□

Theorem 4.5. *Let $\mathcal{L} \subset \mathbb{R}^2$ be a two dimensional lattice basis with vectors b_1, b_2*

1. *The GLRA terminates and yields a good basis.*
2. *Final vector b_1 is the shortest vector in the lattice $\mathcal{L}$, so the algorithm solves the shortest vector problem in two dimensions.*
3. *The angle θ between b_1, b_2 satisfies $|\cos\theta| \leq \frac{||b_1||}{2||b_2||}$*

Let us assume b_1, b_2 are lattice vectors given as input to the algorithm.
Let at the $k-th$ iteration $b_1' = b - mb_1$ and $b_2' = b_1$.

1. *Proof.* By Theorem 4.1, we have $||b_1'||^2 < \frac{||b_1||^2}{3}$ at each iteration.
   So after $k-$ iterations,
   $$||b_1'||^2 < \frac{||b_1||^2}{3^k} = \frac{||b_2'||^2}{3^k}$$
   From Minkowski's first theorem, we have $\lambda_1(\mathcal{L}) \leq \sqrt{n}(\det(\mathcal{L}))^{1/n}$.
   Since we are dealing with lattices of dimension two, we will have $n = 2$ and
   $$\lambda_1(\mathcal{L}) \leq \sqrt{2(\det(\mathcal{L}))}$$
   Finally we will have
   $$\frac{||b_2'||}{3^k} \leq \sqrt{2\det(\mathcal{L})}$$
   Finally,
   $$\log_3\left(\frac{||b_2'||}{2\det(\mathcal{L})}\right) \leq k$$
   So, the time complexity is
   $$\mathcal{O}\left(\log_3\left(\frac{||b_2'||}{2\det(\mathcal{L})}\right)\right)$$
   Which is polynomial time.
   Thus, the algorithm terminates and gives a good basis.

   □

2. *Proof.* Consider $x \in \mathcal{L}$ as a short vector. So it can be written as a linear combination of the reduced basis b_1, b_2
   Note: we have $\mu = \frac{\langle b_2, b_1\rangle}{\langle b_1, b_1\rangle} \leq \frac{1}{2}$. So, $\langle b_2, b_1\rangle \leq \frac{||b_1||^2}{2}$
   we also have
   $$||v_2|| \geq ||v_1||$$

   $$x = \alpha b_1 + \beta b_2 \text{ where } \alpha, \beta \in \mathbb{Z}$$

$$\begin{aligned}
\|x\|^2 &= \alpha^2\|b_1\|^2 + 2\alpha\beta\langle b_1, b_2\rangle + \beta^2\|b_2\|^2 \\
&\geq \alpha^2\|b_1\|^2 - 2|\alpha||\beta||\langle b_1, b_2\rangle| + \beta^2\|b_2\|^2 \\
&\geq \alpha^2\|b_1\|^2 - 2|\alpha||\beta|\frac{\|b_1\|^2}{2} + \beta^2||b_2||^2 \\
&\geq \alpha^2\|b_1\|^2 - 2|\alpha||\beta|\frac{\|b_1\|^2}{2} + \beta^2||b_1||^2 \\
&\geq (\alpha^2 - |\alpha||\beta| + \beta^2)||b_1||^2
\end{aligned}$$

Now we have to show $\alpha^2 - |\alpha||\beta| + \beta^2 \geq 0$

$$\begin{aligned}
\alpha^2 + \alpha\beta + \beta^2 &= \alpha^2 + \alpha\beta + \frac{1}{4}\beta^2 + \frac{3}{4}\beta^2 \\
&= \left(\alpha + \frac{\beta}{2}\right)^2 + \frac{3}{4}\beta^2 \geq 0
\end{aligned} \qquad
\begin{aligned}
\alpha^2 - \alpha\beta + \beta^2 &= \alpha^2 - \alpha\beta + \frac{1}{4}\alpha^2 + \frac{3}{4}\alpha^2 \\
&= \left(\frac{\alpha}{2} + \beta\right)^2 + \frac{3}{4}\alpha^2 \geq 0
\end{aligned}$$

The above part shows that

$$||x|| \geq \text{some integer positive quantity} \times ||b_1||$$

So if x is a short vector, then it must hold equality over here, i.e $||x|| = ||b_1||$. Therefore, b_1 is a short vector.

□

3. *Proof.* For reduced basis b_1, b_2 we have

$$\begin{aligned}
\mu = \frac{\langle b_2, b_1\rangle}{\langle b_1, b_1\rangle} &\leq \frac{1}{2} \\
\implies \frac{\|b_1\| \cdot \|b_2\| \cos\theta}{\|b_1\|^2} &\leq \frac{1}{2} \\
\implies \frac{\|b_2\| \cos\theta}{\|b_1\|} &\leq \frac{1}{2} \\
\implies \cos\theta &\leq \frac{\|b_1\|}{2\|b_2\|} \\
\implies |\cos\theta| &\leq \frac{\|b_1\|}{2\|b_2\|}
\end{aligned}$$

□

5 Conclusion

The GLRA solves the lattice basis reduction efficiently with time complexity $\mathcal{O}\left(\log_3\left(\frac{||b_2'||}{2\det(\mathcal{L})}\right)\right)$. It generates a good basis, and the algorithm is accurate. The problem lies in solving the SVP for lattices of higher dimensions. There is no efficient and exact method to solve SVP even in three dimensions, though the solution for the two-dimensional case was given by Gauss long back in 1805.

References

[1] Oded Regev, *Lecture Notes on Lattices in Computer Science*, Tel Aviv University, Fall 2009.

[2] Vinod Vaikuntanathan, *Advanced Topics in Cryptography: From Lattices to Program Obfuscation*, MIT, Fall 2024.

[3] Deng, Xinyue *An Introduction to Lenstra-Lenstra-Lovasz Lattice Basis Reduction Algorithm*, Massachusetts Institute of Technology, 2016

[4] Galbraith, S. D. *Mathematics of public key cryptography* Cambridge University Press, 2012