Closest Vector Problem

Debadatta Kar, PhD Scholar,
Electrical Engineering and Computer Science,
Indian Institute of Science Education and Research, Bhopal

August, 2025

$\boxed{VI}$

---

1 Introduction

The closest vector problem(CVP) is a hard problem, which we are going to discuss in this article. The fact that CVP is a hard problem was known much before it was known that SVP is hard. László Babai came up with an algorithm in 1986 to solve the approximate version of CVP. This algorithm is often called **Nearest Plane Algorithm**, it obtains an approximation ratio of $2\left(\frac{2}{\sqrt{3}}\right)^n$, where n is the rank of the lattice.

CVP
Input: Basis of lattice B and $t \in \mathbb{R}^n$
Output: $x \in \mathcal{L}(B)$ such that $\|x - t\| \leq \gamma \text{dist}(t, \mathcal{L}(B))$

2 Examples

Example 2.1. *Let* $B = \{(5,1), (-2,8)\}$ *and* $\mathbf{t} = (27,8)$

Consider the linear combinations in the ambient space

$$(27,8) = a(5,1) + b(-2,8)$$

We get a system of equations in two variables a and b

$$5a - 2b = 27$$

$$a + 8b = 8$$

On solving, we end up getting

$$a = \frac{116}{21}, b = \frac{13}{42}$$

To get vectors in lattice, we need integer linear combinations, so we round up the solution to get $\lfloor a \rceil = 6$ and $\lfloor b \rceil = 0$
On applying this to the lattice basis, we obtain

$$\boxed{\mathbf{x} = 6(5,1) + 0(-2,8) = (30,6)}$$

Here $\mathbf{x} = (30,6)$ is a closest vector to the lattice $\mathcal{L}(B)$

Example 2.2. *Let* $B = \{(2,1), (7,3)\}$ *and* $\mathbf{t} = (1.8, 7.5)$

Consider the linear combinations in the ambient space

$$(1.8, 7.5) = a(2, 1) + b(7, 3)$$

We get a system of equations in two variables a and b

$$2a + 7b = 1.8$$

$$a + 3b = 7.5$$

On solving, we have,

$$a = 47.1, b = -13.2$$

To get vectors in lattice, we need integer linear combinations, so we round up the solution to get $\lfloor a \rceil = 47$ and $\lfloor b \rceil = -13$
On applying this to the lattice basis ,we obtain

$$\boxed{\mathbf{x} = 47(2, 1) + (-13)(7, 3) = (3, 8)}$$

Here $\mathbf{x} = (3, 8)$ is a closest vector to the lattice $\mathcal{L}(B)$

Example 2.3. *Let* $B = \{(1, 0), (0, 1)\}$ *and* $\mathbf{t} = (1.8, 7.5)$

Consider the linear combinations in the ambient space

$$(1.8, 7.5) = a(1, 0) + b(0, 1)$$

We then get,

$$a = 1.8, b = 7.5$$

To get vectors in lattice, we need integer linear combinations, so we round up the solution to get $\lfloor a \rceil = 2$ and $\lfloor b \rceil = 8$
On applying this to the lattice basis, we obtain

$$\boxed{\mathbf{x} = 2(1, 0) + 8(0, 1) = (2, 8)}$$

Here $\mathbf{x} = (2, 8)$ is a closest vector to the lattice $\mathcal{L}(B)$.
Observe that in the last two examples, we have choosen two different basis but they generate the same lattice, however the computed closesest vector in both the cases turn out to be different. We can suspect that the closest vector to the target vector can be computed more approximately if we have a reduced basis.

3 The Nearest Plane Algorithm

Algorithm 1 Rounding Algorithm

[1] $B = [\mathbf{b_1}, \mathbf{b_2}, \cdots, \mathbf{b_n}] \in \mathbb{Z}^{m \times n}, \mathbf{t} \in \text{span}(B)$ A vector $\mathbf{x} \in \mathcal{L}(B)$ such that $\|\mathbf{x} - \mathbf{t}\| \leq 2^{n/2}\text{dist}(\mathbf{t}, \mathcal{L}(B))$ Run LLL(B) Find $\alpha_1, \alpha_2, \cdots \alpha_m \in \mathbb{R}$ Such that $t = \alpha_1\mathbf{b_1} + \alpha_2\mathbf{b_2} + \cdots + \alpha_n\mathbf{b_n}$ $\mathbf{x} = \lfloor \alpha_1 \rceil \mathbf{b_1} + \lfloor \alpha_2 \rceil \mathbf{b_2} + \cdots + \lfloor \alpha_n \rceil \mathbf{b_n}$

Algorithm 2 The Nearest Plane Algorithm

[1] Basis $B \in \mathbb{Z}^{m \times n}$, and target vector $\mathbf{t} \in \text{span}(B)$ $\mathbf{b} \in \mathcal{L}(B)$ close to $\mathbf{t}$ //In our case $\|\mathbf{b} - \mathbf{t}\| \leq 2^{n/2}\|\mathbf{b_{exact}} - \mathbf{t}\|$ Run LLL(B) $\mathbf{b} = \mathbf{0}$ $\mathbf{t_n} \leftarrow \mathbf{t}$ $i = n$ down to 1 Compute $m_i = \frac{\langle \mathbf{t_i}, \mathbf{b_i^*} \rangle}{\langle \mathbf{b_i^*}, \mathbf{b_i^*} \rangle}$ $\mathbf{t_{i-1}} = \mathbf{t_i} - (m_i - \lfloor m_i \rceil)\mathbf{b_i^*} - \lfloor m_i \rceil \mathbf{b_i}$ $\mathbf{b} = \mathbf{b} + \lfloor m_i \rceil \mathbf{b_i}$
$\mathbf{b}$

4 Analysis

Result 4.1. *For any $t \in span(B)$, the output of the algorithm satisfies*

$$\|\mathbf{x} - \mathbf{t}\|^{\mathbf{2}} \leq \frac{\mathbf{1}}{\mathbf{4}} \sum_{\mathbf{i=1}}^{\mathbf{n}} \|\mathbf{b_i^*}\|^{\mathbf{2}}$$

Proof. Let $\mathbf{t} \in \text{span}(B)$.
We can express $\mathbf{t}$ as a linear combination of Gram-Schmidt vectors $\mathbf{b_1^*}, \mathbf{b_2^*}, \cdots, \mathbf{b_n^*}$ and the basis vector of lattice $\mathbf{b_1}, \mathbf{b_2}, \cdots, \mathbf{b_n}$ as:

$$\mathbf{t} = \lfloor m_1 \rceil \, \mathbf{b_1} + (m_1 - \lfloor m_1 \rceil)\mathbf{b_1^*} + \lfloor m_2 \rceil \, \mathbf{b_2} + (m_2 - \lfloor m_2 \rceil)\mathbf{b_2^*} + \cdots + \lfloor m_n \rceil \, \mathbf{b_n} + (m_n - \lfloor m_n \rceil)\mathbf{b_n^*}$$

As we know, the output of the algorithms will give us a linear integer combination of Gram-Schmidt coefficients, rounded up to the nearest decimal we will get,

$$\mathbf{x} = \lfloor m_1 \rceil \, \mathbf{b_1} + \lfloor m_2 \rceil \, \mathbf{b_2} + \cdots + \lfloor m_n \rceil \, \mathbf{b_n}$$

And we have,

$$\mathbf{t} = \lfloor m_1 \rceil \, \mathbf{b_1} + (m_1 - \lfloor m_1 \rceil)\mathbf{b_1^*} + \lfloor m_2 \rceil \, \mathbf{b_2} + (m_2 - \lfloor m_2 \rceil)\mathbf{b_2^*} + \cdots + \lfloor m_n \rceil \, \mathbf{b_n} + (m_n - \lfloor m_n \rceil)\mathbf{b_n^*}$$

or,

$$\mathbf{t} = \mathbf{x} + (m_1 - \lfloor m_1 \rceil)\mathbf{b_1^*} + (m_2 - \lfloor m_2 \rceil)\mathbf{b_2^*} + \cdots + (m_n - \lfloor m_n \rceil)\mathbf{b_n^*}$$

finally,

$$\mathbf{t} - \mathbf{x} = (m_1 - \lfloor m_1 \rceil)\mathbf{b_1^*} + (m_2 - \lfloor m_2 \rceil)\mathbf{b_2^*} + \cdots + (m_n - \lfloor m_n \rceil)\mathbf{b_n^*}$$

Here $|m_i - \lfloor m_i \rceil| \leq \frac{1}{2}$
On computing $\|\mathbf{x} - \mathbf{t}\|^2$ we will obtain

$$\begin{aligned}
\|\mathbf{x} - \mathbf{t}\|^2 &= \|(m_1 - \lfloor m_1 \rceil)b_1^* + (m_2 - \lfloor m_2 \rceil)b_2^* + \cdots + (m_n - \lfloor m_n \rceil)b_n^*\|^2 \\
&\leq \sum_{i=1}^{n} |(m_i - \lfloor m_i \rceil)|^2 \|\mathbf{b_i^*}\|^2 \\
&= \sum_{i=1}^{n} \left(\frac{1}{2}\right)^2 \|\mathbf{b_i^*}\|^2 = \frac{1}{4} \sum_{i=1}^{n} \|\mathbf{b_i^*}\|^2
\end{aligned}$$

□

Result 4.2. *For any $t \in span(B)$, the output of the algorithm satisfies*

$$\|\mathbf{x} - \mathbf{t}\| \leq \frac{1}{2} 2^{n/2} \|\mathbf{b_n^*}\|$$

Proof. Let, $\mathbf{b_1^*}, \mathbf{b_2^*}, \cdots, \mathbf{b_n^*}$ are the Gram–Schmidt orthogonal vectors of B, and $\mathbf{x}$ for the target vector $\mathbf{t}$ be the output of Babai's Nearest Plane algorithm
From the previous result we have,

$$\|\mathbf{x} - \mathbf{t}\|^2 \leq \frac{1}{4} \sum_{i=1}^{n} \|\mathbf{b_i^*}\|^2 \leq \frac{1}{4} 2^n \|\mathbf{b_n^*}\|^2$$

Claim: When B is LLL-reduced with $\delta = \frac{3}{4}$, the Lovász condition and size-reduction imply

$$\|\mathbf{b_i^*}\|^2 \leq 2^{n-i}\,\|\mathbf{b_n^*}\|^2 \quad \text{for } i = 1, \ldots, n.$$

which gives

$$\sum_{i=1}^{n} \|\mathbf{b_i^*}\|^2 \leq (2^n - 1)\|\mathbf{b_n^*}\|^2$$

Proof. Lovász condition implies

$$\delta\|\mathbf{b_i^*}\|^2 \leq \|\mu_{i+1,i}\mathbf{b_i^*} + \mathbf{b_{i+1}^*}\|^2$$

Put $\delta = 3/4$ and $\mu_{i+1,i} = \frac{1}{2}$

$$\begin{aligned}
\frac{3}{4}\|\mathbf{b_i^*}\|^2 &\leq \left\|\frac{1}{2}\mathbf{b_i^*} + \mathbf{b_{i+1}^*}\right\|^2 \leq \frac{1}{4}\|\mathbf{b_i^*}\|^2 + \|\mathbf{b_{i+1}^*}\|^2 \\
\frac{1}{2}\|\mathbf{b_i^*}\|^2 &\leq \|\mathbf{b_{i+1}^*}\|^2 \\
\|\mathbf{b_i^*}\|^2 &\leq 2\|\mathbf{b_{i+1}^*}\|^2
\end{aligned}$$

Now applying induction, we will get,

$$\|\mathbf{b_1^*}\|^2 \leq 2\|\mathbf{b_2^*}\|^2 \leq \cdots \leq 2^i\|\mathbf{b_{i+1}^*}\| \leq \cdots \leq 2^{n-1}\|\mathbf{b_n^*}\|^2$$

No,w looking at each term, we can write,

$$\begin{aligned}
\|\mathbf{b_1^*}\|^2 &\leq 2^{n-1}\|\mathbf{b_n^*}\|^2 \\
\|\mathbf{b_2^*}\|^2 &\leq 2^{n-2}\|\mathbf{b_n^*}\|^2 \\
&\vdots \\
\|\mathbf{b_{n-1}^*}\|^2 &\leq 2\|\mathbf{b_n^*}\|^2 \\
\|\mathbf{b_n^*}\|^2 &\leq \|\mathbf{b_n^*}\|^2
\end{aligned}$$

From above, we can get the sum bounded as,

$$\sum_{i=1}^{n} \|\mathbf{b_i^*}\|^2 \leq (2^{n-1} + 2^{n-1} + \cdots + 2 + 1)\|\mathbf{b_n^*}\|^2 \leq (2^n - 1)\|\mathbf{b_n^*}\|^2$$

□

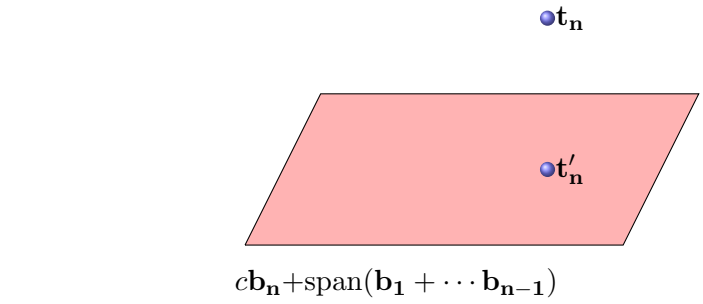
Thus,

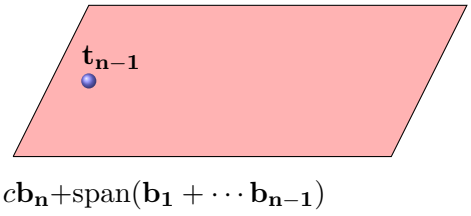
$$\|\mathbf{x} - \mathbf{t}\| \leq \frac{1}{2}\,2^{n/2}\,\|\mathbf{b_n^*}\|$$

□

Lemma 4.3. *Let* $\mathbf{t}$ *be the target vector in* $\mathbb{R}^n$ *and* $\mathbf{x} \in \mathcal{L}(B)$ *be the output of Babai's Algorithm. If* $\mathbf{x}_\xi$ *be the exact closest vector to the target vector* $\mathbf{t}$*. Then,*

$$\|\mathbf{x} - \mathbf{t}\| \leq 2^{n/2}\|\mathbf{x}_\xi - \mathbf{t}\|$$





Some quick remarks before proving the theorem. Assume that

- ✓ $\mathbf{t_n} = \mathbf{t}$ is the target vector.
- ✓ $\mathbf{t'_n} = \mathbf{t} - (m_n - \lfloor m_n \rceil)\mathbf{b_n^*}$
- ✓ $\mathbf{t_{n-1}} = \mathbf{t'_n} - \lfloor m_n \rceil\, \mathbf{b_n} = \mathbf{t} - (m_n - \lfloor m_n \rceil)\mathbf{b_n^*} - c\mathbf{b_n}$

Proof. Let $\mathbf{t_{n-1}}$ be the target vector in the first iteration of the algorithm, and we assume that the property holds in the lower dimension.

$$\begin{aligned} \mathbf{t_{n-1}} &= \mathbf{t'_n} - \lfloor m_n \rceil\, \mathbf{b_n} \\ \mathbf{x_{n-1}} &= \mathbf{x_{n-1}} - \lfloor m_n \rceil\, \mathbf{b_n} \\ \mathbf{x_{\xi(n-1)}} &= \mathbf{x_{\xi(n-1)}} - \lfloor m_n \rceil\, \mathbf{b_n} \end{aligned}$$

So we get,

$$\|\mathbf{x_{n-1}} - \mathbf{t_{n-1}}\| \leq 2^{(n-1)/2} \|\mathbf{x_{\xi(n-1)}} - \mathbf{t_{n-1}}\| \qquad \textbf{(Induction Hypothesis)}$$

Now we will try to get this in the higher dimension,
The LHS of the induction hypothesis can be expressed as

$$\|\mathbf{x_{n-1}} - \mathbf{t_{n-1}}\|^2 = \|\mathbf{x_{n-1}} + \lfloor m_n \rceil\, \mathbf{b_n} - \lfloor m_n \rceil\, \mathbf{b_n} - \mathbf{t_{n-1}}\|^2 = \|\mathbf{x_n} - \mathbf{t_n}'\|^2 \qquad (1)$$

In the RHS, we have,

$$\|\mathbf{x_{\xi(n-1)}} - \mathbf{t_{n-1}}\|^2 = \|\mathbf{x_{\xi(n-1)}} + \lfloor m_n \rceil\, \mathbf{b_n} - \lfloor m_n \rceil\, \mathbf{b_n} - \mathbf{t_{n-1}}\|^2 = \|\mathbf{x'_{\xi(n)}} - \mathbf{t_n}'\|^2 \qquad (2)$$

So the initial induction hypothesis

$$\|\mathbf{x_{n-1}} - \mathbf{t_{n-1}}\| \leq 2^{(n-1)/2} \|\mathbf{x_{\xi(n-1)}} - \mathbf{t_{n-1}}\|$$

reduces to,

$$\|\mathbf{x_{(n)}} - \mathbf{t_n}'\|^2 \leq 2^{n-1} \|\mathbf{x'_{\xi(n)}} - \mathbf{t_n}'\|^2$$

$$\|\mathbf{x_n} - \mathbf{t'_n}\|^2 \leq 2^{n-1}\|\mathbf{x'_{\xi(n)}} - \mathbf{t'_n}\|^2$$

$$\|\mathbf{x_n} - \mathbf{t'_n}\|^2 + \|(m_n - \lfloor m_n \rceil)\mathbf{b_n^*}\|^2 \leq 2^{n-1}\left(\|\mathbf{x'_{\xi(n)}} - \mathbf{t'_n}\|^2 + \|(m_n - \lfloor m_n \rceil)\mathbf{b_n^*}\|^2\right)$$

$$\|\mathbf{x_n} - \mathbf{t_n}\|^2 \leq 2^{(n-1)}\|\mathbf{x'_{\xi(n)}} - \mathbf{t_n}\|^2 \qquad \text{[Using pythagoras theorem]}$$

Here, we have two cases

Case 1 $\boxed{\mathbf{x'_{\xi(n)}} = \mathbf{x_{\xi(n)}}}$

For this we have

$$\|\mathbf{x_n} - \mathbf{t_n}\|^2 \leq 2^{(n-1)}\|\mathbf{x'_{\xi(n)}} - \mathbf{t_n}\|^2 = 2^{(n-1)}\|\mathbf{x_{\xi(n)}} - \mathbf{t_n}\|^2$$

Case 2 $\boxed{\mathbf{x'_{\xi(n)}} \neq \mathbf{x_{\xi(n)}}}$

$$\|\mathbf{x_n} - \mathbf{t_n}\|^2 \leq 2^{(n-1)}\|\mathbf{x'_{\xi(n)}} - \mathbf{t_n}\|^2 \leq 2^{n}\|\mathbf{x_{\xi(n)}} - \mathbf{t_n}\|^2$$

$$\begin{aligned}
\|\mathbf{x} - \mathbf{t}\|^2 &= \|\mathbf{x_n} - \mathbf{t_n}\|^2 \\
&= \|\mathbf{x_n} - \mathbf{t'_n} + \mathbf{t'_n} - \mathbf{t_n}\|^2 \\
&= \|\mathbf{x_n} - \mathbf{t'_n}\|^2 + \|\mathbf{t'_n} - \mathbf{t_n}\|^2 && \text{[using pythagoras theorem]} \\
&= \|\mathbf{x_n} - c\mathbf{b_n} + c\mathbf{b_n} - \mathbf{t'_n}\|^2 + \|\mathbf{t'_n} - \mathbf{t_n}\|^2 \\
&= \|\mathbf{x_{n-1}} - \mathbf{t_{n-1}}\|^2 + \|\mathbf{t'_n} - \mathbf{t_n}\|^2 \\
&\leq 2^{n-1}\|\mathbf{x_{\xi(n-1)}} - \mathbf{t_{n-1}}\|^2 + \|\mathbf{t'_n} - \mathbf{t_n}\|^2 \\
&\leq 2^{n-1}\|\mathbf{x_{\xi(n-1)}} + c\mathbf{b_n} - c\mathbf{b_n} - \mathbf{t_{n-1}}\|^2 + \|\mathbf{t'_n} - \mathbf{t_n}\|^2 \\
&\leq 2^{n-1}\|\mathbf{x'_{\xi(n)}} - \mathbf{t'_n}\|^2 + \|\mathbf{t'_n} - \mathbf{t_n}\|^2 \\
&\leq 2^{n-1}\|\mathbf{x'_{\xi(n)}} - \mathbf{t'_n}\|^2 + \|\mathbf{t'_n} - \mathbf{t_n}\|^2
\end{aligned}$$

Bounding the expression $\|\mathbf{x} - \mathbf{t'}\|^2$

case 1:

$$\|\mathbf{x_\xi} - \mathbf{t'}\| < \frac{\|\mathbf{b_n^*}\|}{2}$$

$$\mathbf{x_\xi} \in c\mathbf{b_n^*} + \text{span}(\mathbf{b_1}, \mathbf{b_2}, \cdots, \mathbf{b_{n-1}}) = cb_n + \text{span}(\mathbf{b_1}, \mathbf{b_2}, \cdots, \mathbf{b_{n-1}})$$

By induction,

$$\begin{aligned}
\|\mathbf{x} - \mathbf{t'}\| &= \|\mathbf{x'} - \mathbf{t''}\| \\
&\leq 2^{\frac{n-1}{2}}\|\mathbf{x_\xi}' - \mathbf{t''}\| \\
&\leq 2^{\frac{n-1}{2}}\|\mathbf{x_\xi} - \mathbf{t''}\| \\
&\leq 2^{\frac{n}{2}}\|\mathbf{x_\xi} - \mathbf{t'}\|
\end{aligned}$$

case 2:

$$\|\mathbf{x}_\xi - \mathbf{t}'\| \geq \frac{\|\mathbf{b}_\mathbf{n}^*\|}{2}$$

$$\mathbf{x}_\xi \notin c\mathbf{b}_\mathbf{n}^* + \text{span}(\mathbf{b_1}, \mathbf{b_2}, \cdots, \mathbf{b_{n-1}}) = c\mathbf{b_n} + \text{span}(\mathbf{b_1}, \mathbf{b_2}, \cdots, \mathbf{b_{n-1}})$$

$$\mathbf{x}_\xi \in c\mathbf{b}_\mathbf{n}^* + \text{span}(\mathbf{b_1}, \mathbf{b_2}, \cdots, \mathbf{b_{n-1}}) \pm \mathbf{b}_\mathbf{n}^* = c\mathbf{b_n} + \text{span}(\mathbf{b_1}, \mathbf{b_2}, \cdots, \mathbf{b_{n-1}}) \pm \mathbf{b_n}$$

But we have,

$$\|\mathbf{x} - \mathbf{t}'\| \leq \frac{1}{2} 2^{\frac{n}{2}} \|\mathbf{b}_\mathbf{n}^*\| \leq 2^{\frac{n}{2}} \|\mathbf{x}_\xi - \mathbf{t}'\|$$

□

5 Questions

✓✓ Why do I need to use LLL before the second step?

References

[Bla14] Richard E. Blahut. *Cryptography and Secure Communication*. Cambridge University Press, Mar. 2014. ISBN: 9781139013673. DOI: 10.1017/cbo9781139013673. URL: http://dx.doi.org/10.1017/CBO9781139013673.

[Gal12] Steven D. Galbraith. *Mathematics of Public Key Cryptography*. Cambridge University Press, 2012. ISBN: 978-1107013926. URL: https://www.cambridge.org/core/books/mathematics-of-public-key-cryptography/DDDFA3874A53C4E6846EB3AB06161E43.

[LLL82] A. K. Lenstra, H. W. Lenstra, and L. Lovász. "Factoring polynomials with rational coefficients". In: *Mathematische Annalen* 261.4 (Dec. 1982), pp. 515–534. ISSN: 1432-1807. DOI: 10.1007/bf01457454. URL: http://dx.doi.org/10.1007/BF01457454.

[Reg09] Regev. *Lecture Notes on Lattices in Computer Science*. Tel Aviv University, 2009.

[Vai24] Vinod Vaikuntanathan. "Advanced Topics in Cryptography: From Lattices to Program Obfuscation". In: *MIT* (2024).