Mini Example of Lattice SVP

Dave Ishii • 18 Oct 2025

Here are three example sets of basis vectors for 2D and 3D lattice Shortest Vector Problems (SVP). Each set of vectors defines a lattice; the "problem" is to find the shortest non-zero vector that can be formed by an integer combination of these basis vectors.

2D Lattice SVP Examples

A 2D lattice is defined by a basis of two vectors, $\mathbf{b_1}$ and $\mathbf{b_2}$.

Example 1: Orthogonal Basis (The "Easy" Case)

This is the simplest lattice, where the basis vectors are already short and perpendicular.

- $\mathbf{b_1} = (1, 0)$
- $\mathbf{b_2} = (0, 1)$

This basis generates the standard integer grid Z^2. The shortest non-zero vectors are obviously $\mathbf{b_1}$, $\mathbf{b_2}$, and their negatives, all with a length of 1.

Example 2: Slightly Skewed Basis

This example shows how the shortest vector isn't always one of the basis vectors.

- $\mathbf{b_1} = (5, 3)$
- $\mathbf{b_2} = (2, 2)$

The basis vectors have lengths $\sqrt{5^2 + 3^2} = \sqrt{34} \approx 5.83$ and $\sqrt{2^2 + 2^2} = \sqrt{8} \approx 2.83$. However, a shorter vector can be found by combining them: $\mathbf{v} = \mathbf{b_1} - 2\mathbf{b_2} = (5, 3) - 2(2, 2) = (5 - 4, 3 - 4) = (1, -1)$ The length of $\mathbf{v}$ is $\sqrt{1^2 + (-1)^2} = \sqrt{2} \approx 1.41$, which is the shortest vector in this lattice.

Example 3: Highly Skewed Basis (The "Hard" Case)

This is a "bad" basis, where the vectors are long and nearly parallel. Finding the short vector is non-trivial and demonstrates why reduction algorithms like LLL are needed.

- $\mathbf{b_1} = (65537, 65536)$
- $\mathbf{b_2} = (65536, 65535)$

Both basis vectors are very long (length > 92000). But a simple integer combination reveals a tiny vector:
$\mathbf{v} = \mathbf{b_1} - \mathbf{b_2} = (65537 - 65536, 65536 - 65535) = (1, 1)$ The length of $\mathbf{v}$ is $\sqrt{1^2 + 1^2} = \sqrt{2} \approx 1.41$.

3D Lattice SVP Examples

A 3D lattice is defined by a basis of three vectors, $\mathbf{b_1}$, $\mathbf{b_2}$, and $\mathbf{b_3}$.

Example 1: Orthogonal Basis

Similar to the 2D case, this is the standard Z^3 integer lattice.

- $\mathbf{b_1} = (1, 0, 0)$
- $\mathbf{b_2} = (0, 1, 0)$
- $\mathbf{b_3} = (0, 0, 1)$

The shortest non-zero vectors have a length of 1.

Example 2: Symmetric, Non-Orthogonal Basis

This is a non-trivial but structured lattice.

- $\mathbf{b_1} = (15, -7, -7)$
- $\mathbf{b_2} = (-7, 15, -7)$
- $\mathbf{b_3} = (-7, -7, 15)$

The basis vectors are relatively long (length ≈ 18.2). The shortest vector is not immediately obvious from this basis. (For reference, a short vector in this lattice is $(1, 1, -1)$, which can be formed by a combination like $2\mathbf{b_1} + 3\mathbf{b_2} + 3\mathbf{b_3}$).

Example 3: Highly Skewed "Bad" Basis

This is a classic example used to show the power of the LLL algorithm. The basis vectors are enormous and almost orthogonal, yet they hide a very short vector.

- $\mathbf{b_1} = (1, 1894885908, 0)$
- $\mathbf{b_2} = (0, 1, 1894885908)$
- $\mathbf{b_3} = (0, 0, 2147483648)$

The shortest vector in this lattice is $\mathbf{v} = (-3, 17, 4)$, which has a length of $\sqrt{(-3)^2 + 17^2 + 4^2} = \sqrt{9 + 289 + 16} = \sqrt{314} \approx 17.7$. This vector is found using a massive integer combination:
$\mathbf{v} = -3\mathbf{b_1} + 5684657741\mathbf{b_2} - 5015999938\mathbf{b_3}$