Introduction to LLL
“Cryptography”

Di Santi Giovanni

May 26, 2021

Contents

Chapter 1

Introduction to Lattices

1.1 Vector Spaces

Definition 1.1.1 ***Vector space.***

A `vector space` V is a subset of $\mathbb{R}^m$ which is closed under finite vector addition and scalar multiplication, with the property that

$$a_1v_1 + a_2v_2 \in V \text{ for all } v_1, v_2 \in V \text{ and all } a_1, a_2 \in \mathbb{R}$$

Definition 1.1.2 ***Linear Combinations***

Let $v_1, v_2, \ldots, v_k \in V$. A `linear combination` of $v_1, v_2, \ldots, v_k \in V$ is any vector of the form

$$\alpha_1v_1 + \alpha_2v_2 + \cdots + \alpha_kv_k \text{ with } \alpha_1, \ldots, \alpha_k \in \mathbb{R}$$

Definition 1.1.3 ***Lineaer Independece***

A set of vectors $v_1, v_2, \ldots, v_k \in V$ is `linearly independent` if the the only way to get

$$a_1v_1 + a_2v_2 + \cdots + a_kv_k = 0$$

is to have $a_1 = a_2 = \cdots = a_k = 0$.

Definition 1.1.4 ***Bases***

Taken a set of linearly independent vectors $b = (v_1, \ldots, v_n) \in V$ we say that b is a `basis` of V if $\forall w \in V$ we can write

$$w = a_1 v_1 + a_2 v_2 + \cdots + a_n v_n$$

Definition 1.1.5 ***Vector's length***

The vector's length or `Euclidean norm` of $v = (x_1, x_2, \ldots, x_m)$ is

$$\|v\| = \sqrt{x_1^2 + x_2^2 + \cdots + x_m^2}$$

Definition 1.1.6 ***Dot Product***

Let $v, w \in V \subset \mathbb{R}^m$ and $v = (x_1, x_2, \ldots, x_m), w = (y_1, y_2, \ldots, y_m)$, the `dot product` of v and m is

$$v \cdot m = x_1 y_1 + x_2 y_2 + \cdots + x_m y_m$$
or
$$v \cdot m = \|v\| \|w\| \cos\theta$$

where θ is the angle between v and w if we place the starting points of the vectors at the origin O.

Geometrically speaking $v \cdot m$ is the length of w projected to v multiplied by the length of v as shown in 1.1

Definition 1.1.7 ***Ortoghonal Basis***

An `ortoghonal basis` for a vector space V is a basis $v_1, \ldots, v_m$ with the property that

$$v_i \cdot v_j = 0 \text{ for all } i \neq j$$

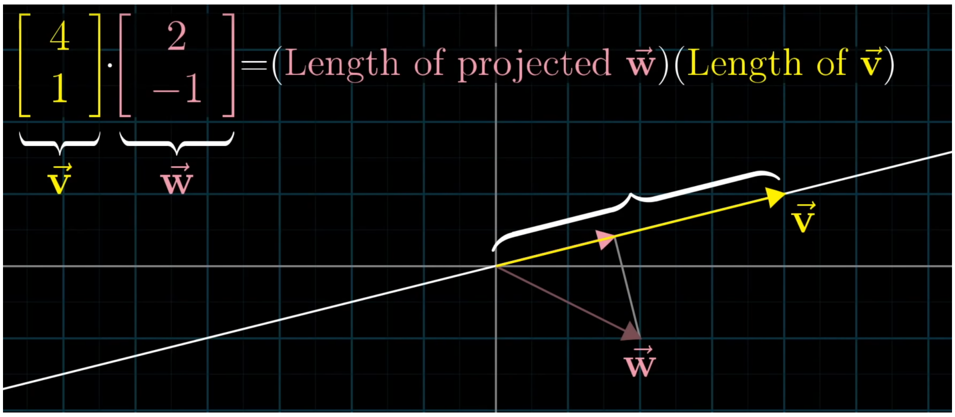

Figure 1.1: Dot Product By 3Blue1Brown

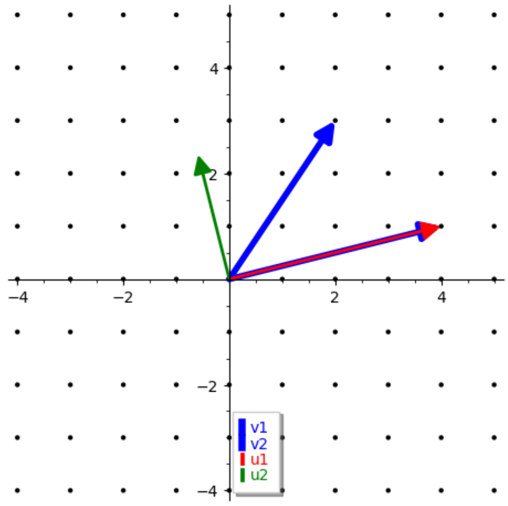

Figure 1.2: Gram Schmidt orthogonalization

If $\|v_i\| = 1$ for all i then the basis is `orthonormal`.

Let $b = (v_1, \ldots, v_n)$, be a basis for a vector space $V \subset \mathbb{R}^m$. There is an algorithm to create an orthogonal basis $b^* = (v_1^*, \ldots, v_n^*)$. The two bases have the property that $\text{Span}\{v_1, \ldots, v_i\} = \text{Span}\{v_1^*, \ldots, v_i^*\}$ for all $i = 1, 2, \ldots, n$

If we take $v_1 = (4, 1), v_2 = (2, 3)$ as basis and apply gram schmidt we obtain $u_1 = v_1 = (4, 1), u_2 = (-10/17, 40/17)$ as shown in 1.2

1.2 Lattices

Definition 1.2.1 *Lattice*

Let $v_1, \ldots, v_n \in \mathbb{R}^m, m \geq n$ be linearly independent vectors. A `Lattice` L spanned by $\{v_1, \ldots, n_n\}$ is the set of all integer linear combinations of $v_1, \ldots, v_n$.

$$L = \left\{ \sum_{i=1}^n a_i v_i, a_i \in \mathbb{Z} \right\}$$

If v_i for every $i = 1, \ldots n$ has integer coordinates then the lattice is called `Integral Lattice`.

On the figure 1.3 we show a lattice L with bases $v = (3, 1)$ and $w = (-1, 1)$, and on 1.4 the same lattice L with a different basis.

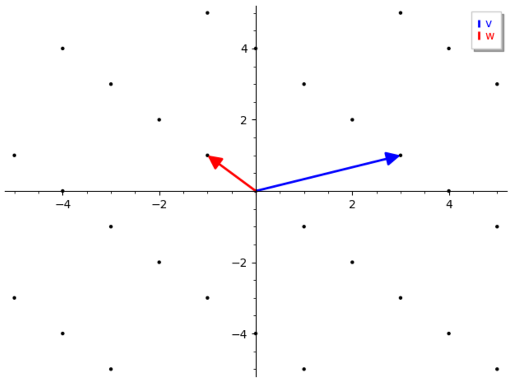

Figure 1.3: Lattice L spanned by v, w

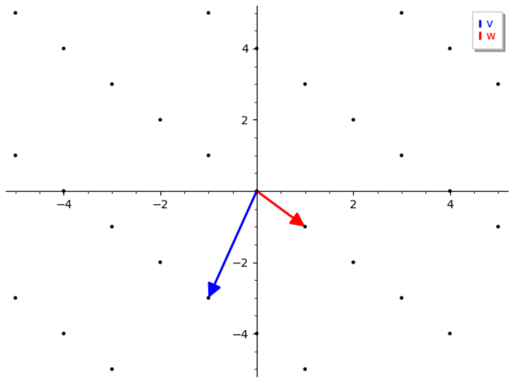

Figure 1.4: Lattice L spanned by v', w'

1.3 Problems

1.3.1 SVP

The Shortest Vector Problem (`SVP`): Find a nonzero vector $v \in L$ that minimez the Euclidean norm $\|v\|$.

Gauss Reduction

Gauss's developed an algorithm to find an optimal basis for a two-dimensional lattice given an arbitrary basis. The output of the algorithm gives the shortest nonzero vector in L and in this way solves the `SVP`.

If we take for example $v_1 = (10, 4), v_2 = (7, 5)$ and apply the gauss reduction algorithm we obtain $w_1 = (3, -1), w_2 = (4, 6)$ 1.5. w_1 is the shortest nonzero vector in the lattice L spanned by v_1, v_2.

However the bigger the dimension of the lattice, the harder is the problem and there isn't a polynomial algorithm to find such vector.

1.3.2 CVP

The Closest Vector Problem (`CVP`): Given a vector $w \in \mathbb{R}^m$ that is not in L, find a vector $v \in L$ that is closest to w, in other words find a vector $v \in L$ that minimizes the Euclidean norm $\|w - v\|$.

Example in 1.6

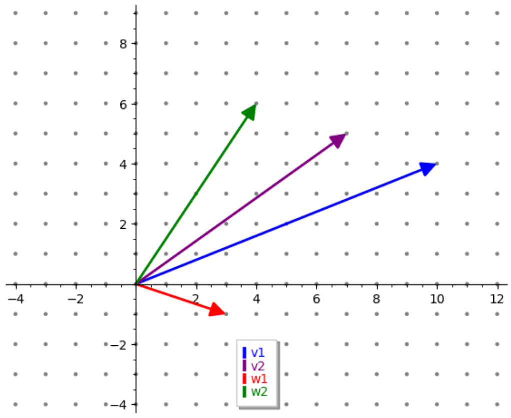

Figure 1.5: Gauss reduction

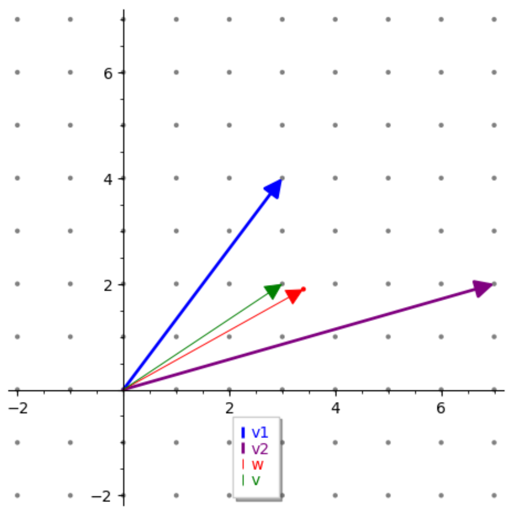

Figure 1.6: CVP

Chapter 2

LLL

2.1 Purpose

2.2 Algorithm

Chapter 3

Applications

3.1 Attack Knapsack

3.2 Attack RSA

End of Paper

gg^2

Bibliography