Introduction to LLL
"Cryptography"

Di Santi Giovanni

May 25, 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

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

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

$$\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_k v_k \text{ with } \alpha_1, \ldots, \alpha_k \in \mathbb{R}$$

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

$$a_1 v_1 + a_2 v_2 + \cdots + a_k v_k = 0$$

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

Definition 1.1.4 ***Bases***

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

$$w = a_1v_1 + a_2v_2 + \cdots + a_nv_n$$

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

$$v \cdot m = x_1y_1 + x_2y_2 + \cdots + x_my_m$$
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

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

1.2 Lattices

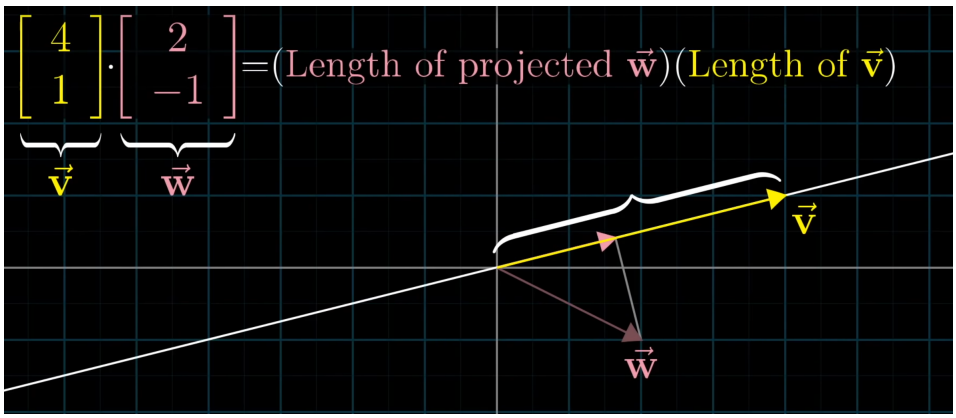

Figure 1.1: Dot Product By 3Blue1Brown

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