

# Introduction to LLL “Cryptography”

Di Santi Giovanni

May 25, 2021

# Contents

<b>1</b>	<b>Introduction to Lattices</b>	<b>2</b>
1.1	Vector Spaces . . . . .	2
1.2	Lattices . . . . .	4
<b>2</b>	<b>LLL</b>	<b>6</b>
2.1	Purpose . . . . .	6
2.2	Algorithm . . . . .	6
<b>3</b>	<b>Applications</b>	<b>7</b>
3.1	Attack Knapsack . . . . .	7
3.2	Attack RSA . . . . .	7

# 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  $v_1, v_2, \dots, v_k \in V$ . A linear combination of  $v_1, v_2, \dots, v_k \in V$  is any vector of the form

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

**Definition 1.1.3** *Linear Independence*

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

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

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

**Definition 1.1.4** *Bases*

Given a set of linearly independent vectors  $b = (v_1, \dots, v_n) \in V$  we say that  $b$  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  $v = (x_1, x_2, \dots, x_m)$  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  $v = (x_1, x_2, \dots, x_m), w = (y_1, y_2, \dots, y_m)$ , the dot product of  $v$  and  $w$  is

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

or

$$v \cdot w = \|v\|\|w\|\cos\theta$$

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

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

### Definition 1.1.7 *Orthogonal Basis*

An orthogonal basis for a vector space  $V$  is a basis  $v_1, \dots, v_m$  with the property that

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

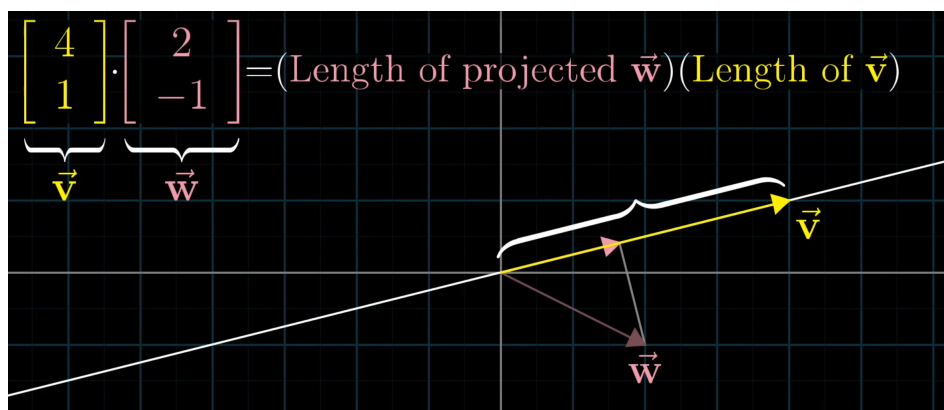


Figure 1.1: Dot Product By 3Blue1Brown

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

### Theorem 1.1.1 *Gram-Schmidt Algorithm*

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

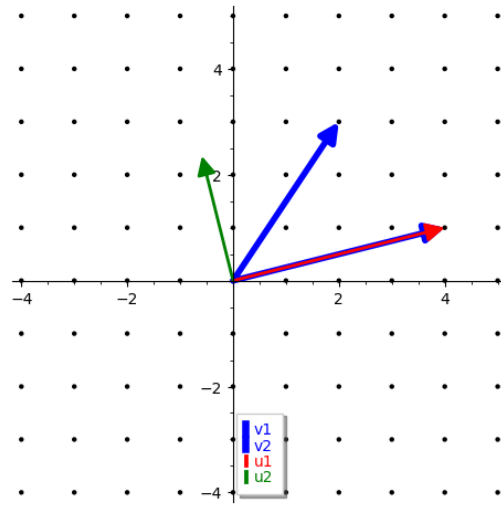


Figure 1.2:

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

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

If  $v_i$  for every  $i = 1, \dots, n$  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  $w = (-1, 1)$ :

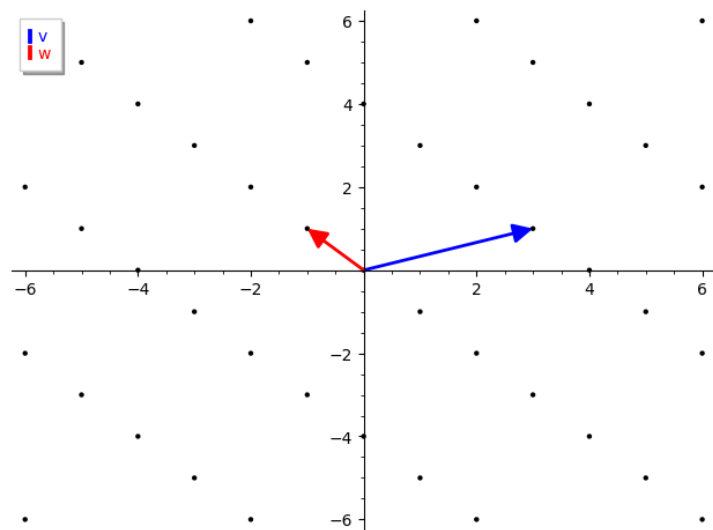


Figure 1.3: Lattice spanned by  $v, w$

# 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