Universidade Estadual de Campinas
Instituto de Computação

Laura Viglioni

The Dissertation or Thesis Title in English

CAMPINAS
1500

Laura Viglioni

The Dissertation or Thesis Title in English

Dissertação apresentada ao Instituto de Computação da Universidade Estadual de Campinas como parte dos requisitos para a obtenção do título de Mestra em Ciência da Computação.

Dissertation presented to the Institute of Computing of the University of Campinas in partial fulfillment of the requirements for the degree of Master in Computer Science.

Supervisor/Orientador: Prof. Dr. Ricardo Dahab

Este exemplar corresponde à versão da Dissertação entregue à banca antes da defesa.

CAMPINAS
1500

Na versão final esta página será substituída pela ficha catalográfica.

De acordo com o padrão da CCPG: "Quando se tratar de Teses e Dissertações financiadas por agências de fomento, os beneficiados deverão fazer referência ao apoio recebido e inserir esta informação na ficha catalográfica, além do nome da agência, o número do processo pelo qual recebeu o auxílio."
e
"caso a tese de doutorado seja feita em Cotutela, será necessário informar na ficha catalográfica o fato, a Universidade convenente, o país e o nome do orientador."

Na versão final, esta página será substituída por outra informando a composição da banca e que a ata de defesa está arquivada pela Unicamp.

Chapter 1

Introduction

Chapter 2

Mathematical Background

2.1 Groups

Definition 2.1.1. A **group** is a set G closed under a binary operation $\cdot$ defined on G such that:

- **Associativity:** $\forall a, b, c \in G,\ a \cdot (b \cdot c) = (a \cdot b) \cdot c$
- **Identity element:** $\exists e \in G\ ;\ \forall a \in G,\ a \cdot e = e \cdot a = a$
- **Inverse element:** $\forall a \in G,\ \exists b \in G\ ;\ a \cdot b = b \cdot a = e$

And it is denoted by $\langle G, \cdot \rangle$, or simply G if the operation is implied.

Definition 2.1.2. A group is said to be **commutative** or **abelian** if $\forall a, b \in G,\ a \cdot b = b \cdot a$

A group is called **additive** or **multiplicative** if its operation is addition or multiplication, respectively.

Definition 2.1.3. A subset H of G is a **subgroup** of $\langle G, \cdot \rangle$ if it is closed under $\cdot$ induced by $\langle G, \cdot \rangle$.

Definition 2.1.4. The **order** of a group $\langle G, \cdot \rangle$ is the cardinality of the set G.

Definition 2.1.5. A subgroup H of G can be used to decompose G in uniform sized and disjoints subsets called **cosets**. Given an element $g \in G$:

- A **left coset** is defined by $gH := \{g \cdot h\ ;\ h \in H\}$
- A **right coset** is defined by $Hg := \{h \cdot g\ ;\ h \in H\}$

2.2 Rings and Fields

Definition 2.2.1. A **ring** is a set together with two binary operations, we will note by $+$ and $*$ and call it addition and multiplication, respectively, such that:

- $\langle R, + \rangle$ is an abelian group.
- $*$ is associative
- $*$ is distributive over $+$

And it is denoted by $\langle R, +, *\rangle$, or simply G if the operations are implied.

Definition 2.2.2. A ring is said to be **commutative** if its $*$ operation is commutative.

Definition 2.2.3. A ring is said to be **with unity** if $*$ has a identity element. We shall note it by 1 and it is called **unity**.

Definition 2.2.4. A **division ring** is a ring R where $\forall r \in R,\ \exists s \in R\ ;\ r * s = 1$.

Definition 2.2.5. A **field** is a commutative division ring.

2.3 Lattices

Definition 2.3.1. A Lattice $\Lambda \subset \mathbb{R}^n$ is a subgroup of the additive group $\mathbb{R}^n$

In other words, given m linear independent vectors in $\mathbb{R}^n$, the set $\{v_1, v_2, ..., v_m\}$ is called a **basis** for Λ and the Lattice may defined by:

Definition 2.3.2.

$$\Lambda := \left\{ x = \sum_{i=1}^{m} \lambda_i v_i \in \mathbb{R}^n \mid \lambda_i \in \mathbb{Z} \right\} \tag{2.1}$$

2.4 Number Fields

Definition 2.4.1. Let K and L be two fields, L is said to be a **field extension** of K if $L \subseteq K$ and we denote it by L/K

Note that in a field extension L/K, L has a structure of a vector space over K, where vector addition is in L and scalar multiplication $a \in K,\ v \in L \implies av \in L$. The dimension of L as a vector space is called **degree** and it is denoted by $[L : K]$.

Definition 2.4.2. A field extension is called **number field** when it is over $\mathbb{Q}$.

Definition 2.4.3. Let $\alpha \in L$ where L/K is a field extension. We say that α is **algebraic over** K if $\exists p \in K[X]\ ;\ p(\alpha) = 0$. p is said to be **the minimal polynomial of** α **over** K denoted by p_α. If $\alpha \in L = \mathbb{Q}[\theta]$, we simply call α an **algebraic number**.

Example 2.4.1. It is known that $\mathbb{Q}$ is a field. If we add $\sqrt{2}$ to the set, we can build a new field adding also all the powers and multiples of $\mathbb{Q}$. This new field is denoted by $\mathbb{Q}[\sqrt{2}]$, note that $\sqrt{2}$ is algebraic and its minimal polynomial $p_{\sqrt{2}} = x^2 - 2$. All elements of $\mathbb{Q}[\sqrt{2}]$ are in the form $\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ and one of its basis is $\{1, \sqrt{2}\}$, so it has degree is 2.

Example 2.4.2. If we add $\sqrt[3]{2}$ to $\mathbb{Q}$ instead, its elements would have the form $\{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\}$, so one of its basis is $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$, $p_\alpha = x^3 - 2$ and its degree is 3.

Theorem 2.4.1 (add font 45 p.40)**.** *If K is a number field, then $K = \mathbb{Q}[\theta]$ for some algebraic number $\theta \in K$, called primitive element.*

Then we conclude that $\{1, \theta, \theta^2, ..., \theta^{n-1}\}$ is a basis for the vector space $K = \mathbb{Q}[\theta]$ over $\mathbb{Q}$.

2.5 Twisted Embedding

Chapter 3

Literature Review

Chapter 4

Objectives Detailing

Chapter 5

Methodology

Bibliography