List of symbols

Symbol	Description
$\mathbb{N}$	set of nonnegative integers $\{0, 1, 2, 3, \dots\}$
$\mathbb{Z}$	set of integers $\{\dots, -2, -1, 0, 1, 2, \dots\}$
$\mathbb{R}$	set of real numbers
$\mathbb{C}$	set of complex numbers
$\mathbb{Q}$	set of rational numbers
$\mathbb{Q}(\beta)$	the smallest field containing the set $\mathbb{Q}$ and algebraic number β
$\#S$	number of elements of the finite set S
C^*	complex conjugation and transposition of the complex matrix C
m_β	monic minimal polynomial of the algebraic number β
$\deg \beta$	degree of the algebraic number β
$(\beta, \mathcal{A})$	numeration system with the base β and the alphabet $\mathcal{A}$
$(x)_{\beta,\mathcal{A}}$	$(\beta, \mathcal{A})$-representation of the number x
$\mathrm{Fin}_{\mathcal{A}}(\beta)$	set of all complex numbers with a finite $(\beta, \mathcal{A})$-representation
$\mathcal{A}^{\mathbb{Z}}$	set of all bi-infinite sequences of digits in $\mathcal{A}$
$\mathbb{Z}[\omega]$	set of values of all polynomials with integer coefficients evaluated in ω
π	isomorphism from $\mathbb{Z}[\omega]$ to $\mathbb{Z}^d$
$\mathcal{B}$	alphabet of input digits
q_j	weight coefficient for the j-th position
$\mathcal{Q}$	weight coefficients set
$\mathcal{Q}_{[w_j,\dots,w_{j-m+1}]}$	set of possible weight coefficients for the input digits $w_j, \dots, w_{j-m+1}$
$\lfloor x \rfloor$	floor function of the number x
$\mathrm{Re}\, x$	real part of the complex number x
$\mathrm{Im}\, x$	imaginary part of the complex number x

Introduction

Chapter 1

Preliminaries

VLOZENO Z VYZKUMAKU, POTREBA UPRAVIT, ZRUSIT DLOUHE POVIDANI O IZOMORFISMU In this chapter, we recall few definitions and results connected to numeration systems and parallelism. We define the set $\mathbb{Z}[\omega]$ for an algebraic integer ω and we prove that $\mathbb{Z}[\omega]$ is isomorphic to $\mathbb{Z}^d$. This property is used in Theorem

1.1 Numeration systems

Firstly, we give a general definition of numeration system.

Definition 1.1. Let $\beta \in \mathbb{C}, |\beta| > 1$ and $\mathcal{A} \subset \mathbb{C}$ be a finite set containing 0. A pair $(\beta, \mathcal{A})$ is called a *positional numeration system* with *base* β and *digit set* $\mathcal{A}$, usually called *alphabet*.

So-called standard numeration systems have an integer base β and an alphabet $\mathcal{A}$ which is a set of contiguous integers. We restrict ourselves to the base β which is an algebraic integer and possibly non-integer alphabet $\mathcal{A}$.

Definition 1.2. Let $(\beta, \mathcal{A})$ be a positional numeration system. We say that a complex number x has a $(\beta, \mathcal{A})$-*representation* if there exist digits $x_n, x_{n-1}, x_{n-2}, \cdots \in \mathcal{A}, n \geq 0$ such that $x = \sum_{j=-\infty}^{n} x_j \beta^j$.

We write briefly a *representation* instead of a $(\beta, \mathcal{A})$-representation if the base β and the alphabet $\mathcal{A}$ follow from context.

Definition 1.3. Let $(\beta, \mathcal{A})$ be a positional numeration system. The set of all complex numbers with a finite $(\beta, \mathcal{A})$-representation is defined by

$$\mathrm{Fin}_{\mathcal{A}}(\beta) := \left\{ \sum_{j=-m}^{n} x_j \beta^j : n, m \in \mathbb{N}, x_j \in \mathcal{A} \right\}.$$

For $x \in \mathrm{Fin}_{\mathcal{A}}(\beta)$, we write

$$(x)_{\beta,\mathcal{A}} = 0^\omega x_n x_{n-1} \cdots x_1 x_0 \bullet x_{-1} x_{-2} \cdots x_{-m} 0^\omega,$$

where 0^ω denotes right, respectively left-infinite sequence of zeros. Notice that indices are decreasing from left to right as it is usual to write the most significant digits first. In what follows, we omit the starting and ending 0^ω when we work with numbers in $\mathrm{Fin}_{\mathcal{A}}(\beta)$. We remark

that existence of an algorithm (standard or parallel) producing a finite $(\beta, \mathcal{A})$-representation of $x + y$ where $x, y \in \mathrm{Fin}_{\mathcal{A}}(\beta)$ implies that the set $\mathrm{Fin}_{\mathcal{A}}(\beta)$ is closed under addition, i.e.,

$$\mathrm{Fin}_{\mathcal{A}}(\beta) + \mathrm{Fin}_{\mathcal{A}}(\beta) \subset \mathrm{Fin}_{\mathcal{A}}(\beta)\,.$$

Designing an algorithm for parallel addition requires some redundancy in numeration system. According to [**?**], a numeration system $(\beta, \mathcal{A})$ is called *redundant* if there exists $x \in \mathrm{Fin}_{\mathcal{A}}(\beta)$ which has two different $(\beta, \mathcal{A})$-representations. For instance, the number 1 has $(2, \{-1, 0, 1\})$-representations $1\bullet$ and $1(-1)\bullet$. Redundant numeration system can enable us to avoid carry propagation in addition. On the other hand, there are some disadvantages. For example, comparison is problematic.

1.2 Parallel addition

A local function, which is also often called a sliding block code, is used to mathematically formalize parallelism.

Definition 1.4. Let $\mathcal{A}$ and $\mathcal{B}$ be alphabets. A function $\varphi : \mathcal{B}^{\mathbb{Z}} \to \mathcal{A}^{\mathbb{Z}}$ is said to be *p-local* if there exist $r, t \in \mathbb{N}$ satisfying $p = r + t + 1$ and a function $\phi : \mathcal{B}^p \to \mathcal{A}$ such that, for any $w = (w_j)_{j\in\mathbb{Z}} \in \mathcal{B}^{\mathbb{Z}}$ and its image $z = \varphi(w) = (z_j)_{j\in\mathbb{Z}} \in \mathcal{A}^{\mathbb{Z}}$, we have $z_j = \phi(w_{j+t}, \cdots, w_{j-r})$ for every $j \in \mathbb{Z}$. The parameter t, resp. r, is called *anticipation*, resp. *memory*.

This means that each digit of the image $\varphi(w)$ is computed from p digits of w in a sliding window. Suppose that there is a processor on each position with access to t input digits on the left and r input digits on the right. Then computation of $\varphi(w)$, where w is a finite sequence, can be done in constant time independent on the length of w.

Definition 1.5. Let β be a base and $\mathcal{A}$ and $\mathcal{B}$ two alphabets containing 0. A function $\varphi : \mathcal{B}^{\mathbb{Z}} \to \mathcal{A}^{\mathbb{Z}}$ such that

1. for any $w = (w_j)_{j\in\mathbb{Z}} \in \mathcal{B}^{\mathbb{Z}}$ with finitely many non-zero digits, $z = \varphi(w) = (z_j)_{j\in\mathbb{Z}} \in \mathcal{A}^{\mathbb{Z}}$ has only finite number of non-zero digits, and
2. $\sum_{j\in\mathbb{Z}} w_j\beta^j = \sum_{j\in\mathbb{Z}} z_j\beta^j$

is called *digit set conversion* in base β from $\mathcal{B}$ to $\mathcal{A}$. Such a conversion φ is said to be *computable in parallel* if φ is a p-local function for some $p \in \mathbb{N}$.

In fact, addition on $\mathrm{Fin}_{\mathcal{A}}(\beta)$ can be performed in parallel if there is a digit set conversion from $\mathcal{A} + \mathcal{A}$ to $\mathcal{A}$ computable in parallel as we can easily output digitwise sum of two $(\beta, \mathcal{A})$-representations in parallel.

We recall few results about parallel addition in a numeration system with an integer alphabet. C. Frougny, E. Pelantová and M. Svobodová proved the following sufficient condition of existence of an algorithm for parallel addition in [**?**].

Theorem 1.1. *Let $\beta \in \mathbb{C}$ be an algebraic number such that $|\beta| > 1$ and all its conjugates in modulus differ from 1. There exists an alphabet $\mathcal{A}$ of contiguous integers containing 0 such that addition on $Fin_{\mathcal{A}}(\beta)$ can be performed in parallel.*

The proof of the theorem provides the algorithm for the alphabet of the form $\{-a, -a+1, \ldots, 0, \ldots, a-1, a\}$. But in general, a is not minimal.

The same authors showed in [**?**] that the condition on the conjugates of the base β is also necessary:

Theorem 1.2. *Let the base $\beta \in \mathbb{C}, |\beta| > 1$, be an algebraic number with a conjugate β' such that $|\beta'| = 1$. Let $\mathcal{A} \subset \mathbb{Z}$ be an alphabet of contiguous integers containing 0. Then addition on $Fin_{\mathcal{A}}(\beta)$ cannot be computable in parallel.*

The question of minimality of the alphabet is studied in [**?**]. The following lower bound for the size of the alphabet is provided:

Theorem 1.3. *Let $\beta \in \mathbb{C}, |\beta| > 1$, be an algebraic integer with the minimal polynomial p. Let $\mathcal{A} \subset \mathbb{Z}$ be an alphabet of contiguous integers containing 0 and 1. If addition on $Fin_{\mathcal{A}}(\beta)$ is computable in parallel, then $\#\mathcal{A} \geq |p(1)|$. Moreover, if β is a positive real number, $\beta > 1$, then $\#\mathcal{A} \geq |p(1)| + 2$.*

In this thesis, we work in a more general concept as we consider also non-integer alphabets. First, we recall the following definition.

Definition 1.6. Let ω be a complex number. The set of values of all polynomials with integer coefficients evaluated in ω is denoted by

$$\mathbb{Z}[\omega] = \left\{ \sum_{i=0}^{n} a_i \omega^i \colon n \in \mathbb{N}, a_i \in \mathbb{Z} \right\} \subset \mathbb{Q}(\omega)\,.$$

Notice that $\mathbb{Z}[\omega]$ is a commutative ring (for our purposes, a ring is associative under multiplication and there is a multiplicative identity).

From now on, let ω be an algebraic integer which generates the set $\mathbb{Z}[\omega]$ and let the base $\beta \in \mathbb{Z}[\omega]$ be such that $|\beta| > 1$. We remark that β is also an algebraic integer as all elements of $\mathbb{Z}[\omega]$ are algebraic integers. Finally, let the alphabet $\mathcal{A}$ be a finite subset of $\mathbb{Z}[\omega]$ such that $0 \in \mathcal{A}$.

Few parallel addition algorithms for such numeration system with a non-integer alphabet were found ad hoc. We introduce the method for construction of the parallel addition algorithm for a given numeration system $(\beta, \mathcal{A})$ in Chapter **??**.

1.3 Isomorphism of $\mathbb{Z}[\omega]$ and $\mathbb{Z}^d$

The goal of this section is to show a connection between the ring $\mathbb{Z}[\omega]$ and the set $\mathbb{Z}^d$. Using Theorem

First we recall the notion of companion matrix which we use to define multiplication in $\mathbb{Z}^d$. By the minimal polynomial of an algebraic integer, we always mean the monic minimal polynomial.

Definition 1.7. Let ω be an algebraic integer of degree $d \geq 1$ with the minimal polynomial $p(x) = x^d + p_{d-1}x^{d-1} + \cdots + p_1 x + p_0 \in \mathbb{Z}[x]$. The matrix

$$S := \begin{pmatrix} 0 & 0 & \cdots & 0 & -p_0 \\ 1 & 0 & \cdots & 0 & -p_1 \\ 0 & 1 & \cdots & 0 & -p_2 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & 1 & -p_{d-1} \end{pmatrix} \in \mathbb{Z}^{d \times d}$$

is called *companion matrix* of the minimal polynomial of ω.

In what follows, the standard basis vectors of $\mathbb{Z}^d$ are denoted by

$$e_0 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, e_1 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \ldots, e_{d-1} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

Definition 1.8. Let ω be an algebraic integer of degree $d \geq 1$, let p be its minimal polynomial and let S be its companion matrix. We define the mapping $\odot_\omega : \mathbb{Z}^d \times \mathbb{Z}^d \to \mathbb{Z}^d$ by

$$u \odot_\omega v := \left(\sum_{i=0}^{d-1} u_i S^i \right) \cdot \begin{pmatrix} v_0 \\ v_1 \\ \vdots \\ v_{d-1} \end{pmatrix} \quad \text{for all } u = \begin{pmatrix} u_0 \\ u_1 \\ \vdots \\ u_{d-1} \end{pmatrix}, v = \begin{pmatrix} v_0 \\ v_1 \\ \vdots \\ v_{d-1} \end{pmatrix} \in \mathbb{Z}^d .$$

and we define powers of $u \in \mathbb{Z}^d$ by

$$\begin{aligned} u^0 &= e_0, \\ u^i &= u^{i-1} \odot_\omega u \text{ for } i \in \mathbb{N} . \end{aligned}$$

We will see later that $\mathbb{Z}^d$ equipped with elementwise addition and multiplication $\odot_\omega$ builds a commutative ring. Let us first recall an important property of a companion matrix – it is a root of its defining polynomial.

Lemma 1.4. *Let ω be an algebraic integer with a minimal polynomial p and let S be its companion matrix. Then*

$$p(S) = 0 .$$

Proof. Following the proof in [**?**], we have

$$\begin{aligned} e_0 &= S^0 e_0 , \\ Se_0 = e_1 &= S^1 e_0 , \\ Se_1 = e_2 &= S^2 e_0 , \\ Se_2 = e_3 &= S^3 e_0 , \\ &\vdots \\ Se_{d-2} = e_{d-1} &= S^{d-1} e_0 , \\ Se_{d-1} &= S^d e_0 , \end{aligned}$$

where the middle column is obtained by multiplication and the right one by using the previous row. Also by multiplying and substituting

$$\begin{aligned} S^d e_0 = Se_{d-1} &= -p_0 e_0 - p_1 e_1 - \cdots - p_{d-1} e_{d-1} \\ &= -p_0 S^0 e_0 - p_1 S^1 e_0 - \cdots - p_{d-1} S^{d-1} e_0 \\ &= (-p_0 S^0 - p_1 S^1 - \cdots - p_{d-1} S^{d-1}) e_0 \\ &= (S^d - p(S)) e_0 . \end{aligned}$$

Hence

$$p(S)e_0 = 0\,.$$

Moreover,

$$p(S)e_k = p(S)S^k e_0 = S^k p(S)e_0 = 0$$

for $k = \{0, 1, \ldots, d-1\}$ which implies the statement. □

The following lemma summarizes basic properties of the mapping $\odot_\omega$ – multiplication by an integer scalar, the identity element, the distributive law and a weaker form of associativity.

Lemma 1.5. *Let ω be an algebraic integer of degree d. The following statements hold for every $u, v, w \in \mathbb{Z}^d$ and $m \in \mathbb{Z}$:*

(i) $(mu) \odot_\omega v = u \odot_\omega (mv) = m(u \odot_\omega v)$,

(ii) $e_0 \odot_\omega v = v \odot_\omega e_0 = v$,

(iii) $(u \odot_\omega e_1^k) \odot_\omega v = u \odot_\omega (e_1^k \odot_\omega v)$ *for* $k \in \mathbb{N}$,

(iv) $(u + v) \odot_\omega w = u \odot_\omega w + v \odot_\omega w$ *and* $u \odot_\omega (v + w) = u \odot_\omega v + u \odot_\omega w$.

Proof. It is easy to see (i) as multiplication of a matrix by a scalar commutes and a scalar can be factored out of a sum.

The first equality of (ii) follows from definition and

$$v \odot_\omega e_0 = \sum_{i=0}^{d-1} v_i S^i \cdot e_0 = \sum_{i=0}^{d-1} v_i e_i = v\,.$$

For (iii), we use Lemma

Now we can prove that there is a correspondence between elements of $\mathbb{Z}[\omega]$ and $\mathbb{Z}^d$.

Theorem 1.6. *Let ω be an algebraic integer of degree d. Then*

$$\mathbb{Z}[\omega] = \left\{ \sum_{i=0}^{d-1} a_i \omega^i \colon a_i \in \mathbb{Z} \right\},$$

$(\mathbb{Z}^d, +, \odot_\omega)$ is a commutative ring and the mapping $\pi : \mathbb{Z}[\omega] \to \mathbb{Z}^d$ defined by

$$\pi(u) = \begin{pmatrix} u_0 \\ u_1 \\ \vdots \\ u_{d-1} \end{pmatrix} \qquad \text{for every } u = \sum_{i=0}^{d-1} u_i \omega^i \in \mathbb{Z}[\omega]$$

is a ring isomorphism.

Proof. Obviously, $\left\{\sum_{i=0}^{n} a_i \omega^i \colon n \in \mathbb{N}, a_i \in \mathbb{Z}\right\} = \mathbb{Z}[\omega] \supset \left\{\sum_{i=0}^{d-1} a_i \omega^i \colon a_i \in \mathbb{Z}\right\}$. We prove the opposite direction by induction with respect to n. Assume $u \in \mathbb{Z}[\omega]$, $u = \sum_{i=0}^{n} u_i \omega^i$ for some $n \in \mathbb{N}$. We see that $u \in \left\{\sum_{i=0}^{d-1} a_i \omega^i \colon a_i \in \mathbb{Z}\right\}$ for all $n < d$.

Suppose now that the claim holds for $n-1$ and consider $n \geq d$. Let $p(x) = x^d + p_{d-1}x^{d-1} + \dots p_1 x + p_0$ be the minimal polynomial of ω. By $p(\omega) = 0$, we have the equation $\omega^d = -p_{d-1}\omega^{d-1} - \dots - p_1\omega - p_0$ which enables us to write

$$\begin{aligned} u = u_n\omega^n + \sum_{i=0}^{n-1} u_i\omega^i &= u_n\omega^{n-d}(\underbrace{-p_{d-1}\omega^{d-1} - \dots - p_1\omega - p_0}_{\omega^d}) + \sum_{i=0}^{n-1} u_i\omega^i \\ &= \sum_{i=0}^{n-d-1} u_i\omega^i + \sum_{i=n-d}^{n-1} (u_i - u_n \cdot p_{i-n+d})\omega^i = \sum_{i=0}^{n-1} u'_i\omega^i \,. \end{aligned}$$

Thus $u \in \left\{\sum_{i=0}^{d-1} a_i\omega^i \colon a_i \in \mathbb{Z}\right\}$ by the induction assumption.

Let us check now that the mapping π is well-defined. Assume on contrary that there exists $v \in \mathbb{Z}[\omega]$ and $i_0 \in \{0, 1, \dots, d-1\}$ such that $v = \sum_{i=0}^{d-1} v_i\omega^i = \sum_{i=0}^{d-1} v'_i\omega^i$ and $v_{i_0} \neq v'_{i_0}$. Then

$$\sum_{i=0}^{d-1}(v'_i - v_i)\omega^i = 0$$

and $\sum_{i=0}^{d-1}(v'_i - v_i)x^i \in \mathbb{Z}[x]$ is a non-zero polynomial of the degree smaller than the degree d of the minimal polynomial p, a contradiction.

Clearly, π is bijection.

Let $v = \sum_{i=0}^{d-1} v_i\omega^i$ be an element of $\mathbb{Z}[\omega]$. We prove by induction that

$$\pi(\omega^i v) = (\pi(\omega))^i \odot_\omega \pi(v) \,.$$

For $i = 1$, consider

$$\begin{aligned} \omega v = \omega \sum_{i=0}^{d-1} v_i\omega^i &= \sum_{i=0}^{d-2} v_i\omega^{i+1} + v_{d-1}(\underbrace{-p_{d-1}\omega^{d-1} - \dots - p_1\omega - p_0}_{=\omega^d}) \\ &= -p_0 v_{d-1} + \sum_{i=1}^{d-1}(v_{i-1} - v_{d-1}p_i)\omega^i \,. \end{aligned}$$

Hence

$$\begin{aligned} \pi(\omega v) = -p_0 v_{d-1} e_0 + \sum_{i=1}^{d-1}(v_{i-1} - v_{d-1}p_i)e_i &= S \cdot \pi(v) \\ = e_1 \odot_\omega \pi(v) = \pi(\omega) \odot_\omega \pi(v) \,. \end{aligned}$$

Suppose now that

$$\pi(\omega^{i-1} v) = (\pi(\omega))^{i-1} \odot_\omega \pi(v) \,.$$

Then

$$\pi(\omega^i v) = \pi(\omega(\omega^{i-1}v)) = \pi(\omega) \odot_\omega \pi(\omega^{i-1}v) = \pi(\omega) \odot_\omega \big((\pi(\omega))^{i-1} \odot_\omega \pi(v)\big) = (\pi(\omega))^i \odot_\omega \pi(v) \,,$$

where we use (iii) of Lemma

Now we multiply v by $m \in \mathbb{Z} \subset \mathbb{Z}[\omega]$:

$$\pi(mv) = \pi\left(m\sum_{i=0}^{d-1} v_i\omega^i\right) = \pi\left(\sum_{i=0}^{d-1} mv_i\omega^i\right) = m\pi(v) = (me_0) \odot_\omega \pi(v) = \pi(m) \odot_\omega \pi(v)\,.$$

Let $u = \sum_{i=0}^{d-1} u_i\omega^i \in \mathbb{Z}[\omega]$. Since π is obviously additive, we conclude:

$$\begin{aligned}\pi(uv) &= \pi\left(\sum_{i=0}^{d-1} u_i\omega^i v\right) = \sum_{i=0}^{d-1} \pi(\omega^i u_i v) = \sum_{i=0}^{d-1} \pi(\omega)^i \odot_\omega (\pi(u_i) \odot_\omega \pi(v)) \\ &= \sum_{i=0}^{d-1} \pi(\omega^i u_i) \odot_\omega \pi(v) = \pi\left(\sum_{i=0}^{d-1} u_i\omega^i\right) \odot_\omega \pi(v) = \pi(u) \odot_\omega \pi(v)\,.\end{aligned}$$

Now we can show that the operation $\odot_\omega$ is associative and commutative. Let $f, g, h \in \mathbb{Z}^d$ and $u, v, w \in \mathbb{Z}[\omega]$ be such that $f = \pi(u), g = \pi(v)$ and $h = \pi(w)$. Then

$$f \odot_\omega (g \odot_\omega h) = f \odot_\omega \pi(vw) = \pi(u(vw)) = \pi((uv)w) = \pi(uv) \odot_\omega h = (f \odot_\omega g) \odot_\omega h$$

and

$$g \odot_\omega h = \pi(vw) = \pi(wv) = h \odot_\omega g\,.$$

Thus, $(\mathbb{Z}^d, +, \odot_\omega)$ is a commutative ring. □

Due to this theorem we may work with integer vectors instead of elements of $\mathbb{Z}[\omega]$ and multiplication in $\mathbb{Z}[\omega]$ is replaced by multiplying by an appropriate matrix.

The last theorem of this section is a practical tool for divisibility in $\mathbb{Z}[\omega]$. To check whether an element of $\mathbb{Z}[\omega]$ is divisible by another element, we look for an integer solution of a linear system. Moreover, this solution provides the result of division in the positive case.

Theorem 1.7. *Let ω be an algebraic integer of degree d and let S be the companion matrix of its minimal polynomial. Let $\beta = \sum_{i=0}^{d-1} b_i\omega^i$ be a nonzero element of $\mathbb{Z}[\omega]$. Then for every $u \in \mathbb{Z}[\omega]$*

$$u \in \beta\mathbb{Z}[\omega] \iff S_\beta^{-1} \cdot \pi(u) \in \mathbb{Z}^d\,,$$

where $S_\beta = \sum_{i=0}^{d-1} b_i S^i$.

Proof. Observe first that S_β is nonsingular. Otherwise, there exists $y = \begin{pmatrix} y_0 \\ y_1 \\ \vdots \\ y_{d-1} \end{pmatrix} \in \mathbb{Z}^d, y \neq 0$ such that $S_\beta \cdot y = 0$. Thus

$$\pi(\beta) \odot_\omega y = 0 \iff \beta\pi^{-1}(y) = 0\,.$$

Since $\beta \neq 0$, we have

$$0 = \pi^{-1}(y) = \sum_{i=0}^{d-1} y_i\omega^i\,,$$

which contradict that the degree of ω is d.

Now

$$\begin{aligned} u \in \beta\mathbb{Z}[\omega] &\iff (\exists v \in \mathbb{Z}[\omega])(u = \beta v) \\ &\iff (\exists v \in \mathbb{Z}[\omega])(\pi(u) = \pi(\beta) \odot_\omega \pi(v) = S_\beta \cdot \pi(v)) \\ &\iff \pi(v) = S_\beta^{-1} \cdot \pi(u) \in \mathbb{Z}^d \,. \end{aligned}$$

Clearly, if u is divisible by β, then $v = u/\beta = \pi^{-1}(S_\beta^{-1} \cdot \pi(u)) \in \mathbb{Z}[\omega]$. □

MRIZKOVA NORMA - TADY NEBO AZ V KAPITOLE O KONVERGENCI?

1.4 MRIZKOVA NORMA

Lemma 1.8. *Let ν be a norm of the vector space $\mathbb{C}^d$ and P be a nonsingular matrix in $\mathbb{C}^d$. Then the mapping $\mu : \mathbb{C}^d \to \mathbb{R}_0^+$ defined by $\mu(x) = \nu(Px)$ is also a norm of the vector space $\mathbb{C}^d$.*

Proof. Let x and y be vectors in $\mathbb{C}^d$ and $\alpha \in \mathbb{C}$. We use linearity of matrix multiplication, nonsingularity of matrix P and the fact that ν is a norm to prove the following statements:

1. $\mu(x) = \nu(Px) \geq 0$,
2. $\mu(x) = 0 \iff \nu(Px) = 0 \iff Px = 0 \iff x = 0$,
3. $\mu(\alpha x) = \nu(P(\alpha x)) = \nu(\alpha Px) = |\alpha|\nu(Px) = |\alpha|\mu(x)$,
4. $\mu(x + y) = \nu(P(x + y)) = \nu(Px + Py) \leq \nu(Px) + \nu(Py) = \mu(x) + \mu(y)$.

This verifies that μ is a norm. □

Lemma

Theorem 1.9. *Let $M \in \mathbb{C}^{n\times n}$ be a diagonalizable matrix. Then*

$$\rho(M) = |||M|||_M \,,$$

where $\rho(M)$ is the spectral radius of the matrix M.

Proof. First, we prove that $|||M||| \geq \rho(M)$ for every natural matrix norm induced by $\|\cdot\|$. For all eigenvalues λ in the spectrum $\sigma(M)$ with a respective eigenvector u such that $\|u\| = 1$, we have

$$|||M||| = \max_{\|x\|=1} \|Mx\| \geq \|Mu\| = \|\lambda u\| = |\lambda| \cdot \|u\| = |\lambda| \,.$$

Now, we construct the natural matrix norm $\|\cdot\|_M$ such that $|||M|||_M \leq \rho(M)$. Since M is diagonalizable, there exist nonsingular matrix $P \in \mathbb{C}^{n\times n}$ and diagonal matrix $C \in \mathbb{C}^{n\times n}$ with the eigenvalues of M on the diagonal such that

$$PMP^{-1} = C \,.$$

Now, the natural matrix norm $\|\cdot\|_M$ is induced by the vector norm $\|\cdot\|_M$, i.e.,

$$|||M|||_M = \max_{\|y\|_M=1} \|My\|_M \,.$$

Let y be a vector such that $\|y\|_M = 1$ and set $z = Py$. Notice that

$$\sqrt{z^*z} = \|z\|_2 = \|Py\|_2 = \|y\|_M = 1\,.$$

Consider

$$\begin{aligned}\|My\|_M = \|PMy\|_2 = \|CPy\|_2 = \|Cz\|_2 = \sqrt{z^*C^*Cz}\\ \leq \sqrt{\max_{\lambda\in\sigma(M)} |\lambda|^2 z^*z} = \max_{\lambda\in\sigma(M)} |\lambda| = \rho(M)\ .\end{aligned}$$

which implies the statement. □

Lemma 1.10. *Let ω be an algebraic integer of degree d and let S be the companion matrix of its minimal polynomial. Let $\beta = \sum_{i=0}^{d-1} b_i\omega^i$ be a nonzero element of $\mathbb{Z}[\omega]$. Set $S_\beta = \sum_{i=0}^{d-1} b_i S^i$. Then*

i) The matrix S_β is diagonalizable.

ii) The characteristic polynomial of S_β is m_β^k with $k = d/\deg\beta$.

iii) $|\det S_\beta| = |m_\beta(0)|^k$.

iv) $\|x\|_{S_\beta} = \|x\|_{S_\beta^{-1}}$ *for all* $x \in \mathbb{C}^d$ *and* $|||X|||_{S_\beta} = |||X|||_{S_\beta^{-1}}$ *for all* $X \in \mathbb{C}^{d\times d}$.

v) $|||S_\beta|||_{S_\beta} = \max\{|\beta'|\colon \beta'$ *is conjugate of* $\beta\}$ *and* $\left|\left|\left|S_\beta^{-1}\right|\right|\right|_{S_\beta} = \max\{\frac{1}{|\beta'|}\colon \beta'$ *is conjugate of* $\beta\}$.

Proof. The characteristic polynomial of the companion matrix S is the same as minimal polynomial of ω which has no multiple roots. Hence, S is diagonalizable, i.e., $S = P^{-1}DP$ where D is diagonal matrix with the conjugates of ω on the diagonal and P is a nonsingular complex matrix. The matrix S_β is also diagonalized by P:

$$S_\beta = \sum_{i=0}^{d-1} b_i S^i = \sum_{i=0}^{d-1} b_i \left(P^{-1}DP\right)^i = P^{-1}\underbrace{\left(\sum_{i=0}^{d-1} b_i D^i\right)}_{D_\beta} P\,.$$

By Theorem CONJUGATES SE ZOBRAZUJI NA CONJUGATES, the diagonal elements of the diagonal matrix D_β are conjugates of β. Since $S_\beta \in \mathbb{Z}^{d\times d}$, its characteristic polynomial has integer coefficients. Thus it is k-th power of the minimal polynomial m_β. The value k follows from the equality $d = \deg(m_\beta^k) = k\deg m_\beta$.

The modulus of the determinant of S_β equals the modulus of the absolute coefficient of the characteristic polynomial which is $|m_\beta(0)|^k$.

The matrix S_β^{-1} is also diagonalized by P since $S_\beta^{-1} = (P^{-1}D_\beta P)^{-1} = P^{-1}D_\beta^{-1}P$. Thus, the norms $\|\cdot\|_{S_\beta}$ and $\|\cdot\|_{S_\beta^{-1}}$ are same and so the induced matrix norms $|||\cdot|||_{S_\beta}$ and $|||\cdot|||_{S_\beta^{-1}}$ are.

The matrix S_β is diagonalizable and its eigenvalues are the conjugates of β. Theorem

Definition 1.9. Using the notation of the previous lemma, we define a *β-norm ???* $\|\cdot\|_\beta : \mathbb{Z}[\omega] \to \mathbb{R}_0^+$ by

$$\|x\|_\beta = \|\pi(x)\|_{S_\beta}$$

for all $x \in \mathbb{Z}[\omega]$.

We can easily verify that β-norm is a norm in $\mathbb{Z}[\omega]$:

1. $\|x\|_\beta = \|\pi(x)\|_{S_\beta} \geq 0$,
2. $\|x\|_\beta = 0 \iff \|\pi(x)\|_{S_\beta} = 0 \iff \pi(x) = 0 \iff x = 0$,
3. $\|\alpha x\|_\beta = \|\pi(\alpha x)\|_{S_\beta} = |\alpha| \, \|\pi(x)\|_{S_\beta} = |\alpha| \, \|x\|_\beta$,
4. $\|x + y\|_\beta = \|\pi(x + y)\|_{S_\beta} = \|\pi(x) + \pi(y)\|_{S_\beta} \leq \|\pi(x)\|_{S_\beta} + \|\pi(y)\|_{S_\beta} = \|x\|_\beta + \|y\|_\beta$,

for all $x, y \in \mathbb{Z}[\omega]$ and $\alpha \in \mathbb{Z}[\omega]$.

1.5 FAZE 1 IFF BETA EXPANDING

Theorem 1.11. *Let ω be a complex number and $\beta \in \mathbb{Z}[\omega]$ be such that $|\beta| > 1$. Let $\mathcal{A} \subset \mathbb{Z}[\omega]$ be an alphabet. If $\mathbb{N} \subset \mathcal{A}[\beta]$, the number β is expanding.*

Proof. For all $n \in \mathbb{N}$ we may write

$$n = \sum_{i=0}^{N} a_i \beta^i \,,$$

where $N \in \mathbb{N}$, $a_i \in \mathcal{A}$ and $a_N \neq 0$.

Set $m := \max\{|a| \colon a \in \mathcal{A}\}$. We take $n \in \mathbb{N}$ such that $n > m$. Since $|a_0| \leq m < n$, we have $N \geq 1$ and there is $i_0 \in \{1, 2, \ldots, N\}$ such that $a_{i_0} \neq 0$. Thus, ω is an algebraic number as $a_i \in \mathcal{A} \subset \mathbb{Z}[\omega]$ and β can be expressed as an integer combination of powers of ω. Therefore, β is also an algebraic number.

Let β' be an algebraic conjugate of β. Since $\beta \in \mathbb{Z}[\omega] \subset \mathbb{Q}(\omega)$, there is an algebraic conjugate ω' of ω and an isomorphism $\sigma : \mathbb{Q}(\omega) \to \mathbb{Q}(\omega')$ such that $\sigma(\beta) = \beta'$. Now

$$n = \sigma(n) = \sum_{i=0}^{N} \sigma(a_i)(\beta')^i \,.$$

Set $\tilde{m} := \max\{|\sigma(a)| \colon a \in \mathcal{A}\}$. For all $n \in \mathbb{N}$, we have

$$n = |n| \leq \sum_{i=0}^{N} |\sigma(a_i)| \cdot |\beta'|^i \leq \sum_{i=0}^{\infty} |\sigma(a_i)| \cdot |\beta'|^i \leq \tilde{m} \sum_{i=0}^{\infty} |\beta'|^i \,.$$

Hence, the sum on the right side diverges which implies that $|\beta'| \geq 1$. Thus, all conjugates of β are at least one in modulus.

If the degree of β is one, the statement is obvious. Therefore, we may assume that $\deg \beta \geq 2$.

Suppose for contradiction that $|\beta'| = 1$ for an algebraic conjugate β' of β. The complex conjugate $\overline{\beta'}$ is also an algebraic conjugate of β. Take any algebraic conjugate γ of β and the isomorphism $\sigma' : \mathbb{Q}(\beta') \to \mathbb{Q}(\gamma)$ given by $\sigma'(\beta') = \gamma$. Now

$$\frac{1}{\gamma} = \frac{1}{\sigma'(\beta')} = \sigma'\left(\frac{1}{\beta'}\right) = \sigma'\left(\frac{\overline{\beta'}}{\beta'\overline{\beta'}}\right) = \sigma'\left(\frac{\overline{\beta'}}{|\beta'|^2}\right) = \sigma'(\overline{\beta'}) \,.$$

Hence, $\frac{1}{\gamma}$ is also an algebraic conjugate of β. From the previous, $\left|\frac{1}{\gamma}\right| \geq 1$ and $|\gamma| \geq 1$ which implies that $|\gamma| = 1$. We may set $\gamma = \beta$ which contradicts $|\beta| > 1$. Thus all conjugates of β are greater than one in modulus, i.e., β is an expanding algebraic number. □

Theorem 1.12. *Let $\mathcal{A} \subset \mathbb{Z}[\omega]$ be an alphabet such that $1 \in \mathcal{A}[\beta]$. If the extending window method with the rewriting rule $x - \beta$ converges for the numeration system $(\beta, \mathcal{A})$, then the base β is expanding.*

Proof. The existence of an algorithm for addition which is computable in parallel implies that the set $\mathrm{Fin}_{\mathcal{A}}(\beta)$ is closed under addition. Moreover, the set $\mathcal{A}[\beta]$ is closed under addition since there is no carry to the right when the rewriting rule $x - \beta$ is used. For any $n \in \mathbb{N}$, the sum $1 + 1 + \cdots + 1 = n$ is in $\mathcal{A}[\beta]$ by the assumption $1 \in \mathcal{A}[\beta]$. Therefore, $\mathbb{N} \subset \mathcal{A}[\beta]$ and thus the base β is expanding by Theorem

Lemma 1.13. *Let ω be an algebraic integer, $\deg \omega = d$, and β be an expanding algebraic integer in $\mathbb{Z}[\omega]$. Let $\mathcal{A}$ and $\mathcal{B}$ be finite subsets of $\mathbb{Z}[\omega]$ such that $\mathcal{A}$ contains at least one representative of each congruence class modulo β in $\mathbb{Z}[\omega]$. Then there exists a finite set $\mathcal{Q} \subset \mathbb{Z}[\omega]$ such that $\mathcal{B} + \mathcal{Q} \subset \mathcal{A} + \beta\mathcal{Q}$.*

Proof. We use the isomorphism $\pi : \mathbb{Z}[\omega] \to \mathbb{Z}^d$ and β-norm $\|\cdot\|_\beta$ to bound the elements of $\mathbb{Z}[\omega]$. Let γ be the smallest conjugate of β in modulus. Denote $C := \max\{\|b - a\|_\beta : a \in \mathcal{A}, b \in \mathcal{B}\}$. Consequently, set $R := \frac{C}{|\gamma|-1}$ and $\mathcal{Q} := \{q \in \mathbb{Z}[\omega] \colon \|q\|_\beta \leq R\}$. By Lemma

Hence $q' \in \mathcal{Q}$ and thus $x = b + q \in \mathcal{A} + \beta\mathcal{Q}$.

Since there are only finitely many elements of $\mathbb{Z}^d$ bounded by the constant R, the set Q is finite. □

Theorem 1.14. *Let ω be an algebraic integer and $\beta \in \mathbb{Z}[\omega]$. Let the alphabet $\mathcal{A} \subset \mathbb{Z}[\omega]$ be such that $\mathcal{A}$ contains at least one representative of each congruence class modulo β in $\mathbb{Z}[\omega]$. Let $\mathcal{B} \subset \mathbb{Z}[\omega]$ be the input alphabet.*

If β is expanding, Phase 1 of the extending window method converges.

Proof. We have the constant R and finite set $\mathcal{Q}$ from Lemma

We start with $\mathcal{Q}_0 = \{0\}$ which is bounded by any positive constant. Suppose that the intermediate weight coefficients set $\mathcal{Q}_k$ has elements bounded by the constant R. We see from the previous proof that the candidates obtained by Algorithm **??** for the set $\mathcal{Q}_k$ are also bounded by R. Thus, the next intermediate weight coefficients set $\mathcal{Q}_{k+1}$ has elements bounded by the constant R, i.e., $\mathcal{Q}_{k+1} \subset \mathcal{Q}$.

Since $\#\mathcal{Q}$ is finite and $\mathcal{Q}_0 \subset \mathcal{Q}_1 \subset \mathcal{Q}_2 \subset \cdots \mathcal{Q}$, Phase 1 successfully ends. □

1.6 NUTNOST REPREZENTANTU + DOLNI ODHAD VELIKOSTI ABECEDY

Theorem 1.15. *Let β be an algebraic integer such that $|\beta| > 1$. Let $0 \in \mathcal{A} \subset \mathbb{Z}[\beta]$ be an alphabet such that $1 \in \mathcal{A}[\beta]$. If the extending window method with the rewriting rule $x - \beta$ converges for the numeration system $(\beta, \mathcal{A})$, the alphabet $\mathcal{A}$ contains at least one representative of each congruence class modulo β and $\beta - 1$ in $\mathbb{Z}[\beta]$.*

Proof. The existence of an algorithm for addition with the rewriting rule $x - \beta$ implies that the set $\mathcal{A}[\beta]$ is closed under addition. By the assumption $1 \in \mathcal{A}[\beta]$, the set $\mathbb{N}$ is subset of $\mathcal{A}[\beta]$. Since $0 \in \mathcal{A}$, we have $\beta \cdot \mathcal{A}[\beta] \subset \mathcal{A}[\beta]$. Hence, $\mathbb{N}[\beta] \subset \mathcal{A}[\beta]$.

For any element $x = \sum_{i=0}^{N} x_i\beta^i \in \mathbb{Z}[\beta]$ there is an element $x' = \sum_{i=0}^{N} x'_i\beta^i \in \mathbb{N}[\beta]$ such that $x \equiv_\beta x'$ since $m_\beta(0) \equiv_\beta 0$ and $\beta^i \equiv_\beta 0$. As $x' \in \mathbb{N}[\beta] \subset \mathcal{A}[\beta]$, we have

$$x \equiv_\beta x' = \sum_{i=0}^{n} a_i\beta^i \equiv_\beta a_0\,,$$

where $a_i \in \mathcal{A}$. Hence, for any element $x \in \mathbb{Z}[\omega]$, there is a letter $a_0 \in \mathcal{A}$ such that $x \equiv_\beta a_0$.

In order to prove that there is at least one representative of each congruence class modulo $\beta - 1$ in the alphabet $\mathcal{A}$, we consider again an element $x = \sum_{i=0}^{N} x_i\beta^i \in \mathbb{Z}[\beta]$. Similarly, there is an element $x' = \sum_{i=0}^{N} x'_i\beta^i \in \mathbb{N}[\beta]$ such that $x \equiv_{\beta-1} x'$ since $m_{\beta-1}(0) \equiv_{\beta-1} 0$ and $(\beta-1)^i \equiv_{\beta-1} 0$.

Since $x' \in \mathbb{N} \subset \mathcal{A}[\beta]$,

$$x' = \sum_{i=0}^{n} a_i\beta^i\,,$$

where $a_i \in \mathcal{A}$. We prove by induction with respect to n that $x' \equiv_{\beta-1} a$ for some $a \in \mathcal{A}$. If $n = 0$, $x' = a_0$. Now we use the fact, that if there is a parallel addition algorithm, for each letter $b \in \mathcal{A} + \mathcal{A}$, there is $a \in \mathcal{A}$ such that $b \equiv_{\beta-1} a$ ODKAZ NA PRISLUSNOU VETU. For $n + 1$, we have

$$\begin{aligned} x' &= \sum_{i=0}^{n+1} a_i\beta^i = a_0 + \sum_{i=1}^{n+1} a_i\beta^i \\ &= a_0 + \beta\sum_{i=0}^{n} a_{i+1}\beta^i - \sum_{i=0}^{n} a_{i+1}\beta^i + \sum_{i=0}^{n} a_{i+1}\beta^i \\ &\equiv_{\beta-1} a_0 + (\beta-1)\sum_{i=0}^{n} a_{i+1}\beta^i + a \equiv_{\beta-1} a_0 + a \equiv_{\beta-1} a' \in \mathcal{A}\,, \end{aligned}$$

where we use the induction assumption

$$\sum_{i=0}^{n} a_{i+1}\beta^i \equiv_{\beta-1} a\,.$$

□

CHYBI VETA ZE POCET REPREZENTANTU JE DETERMINANT=> DOLNI ODHAD VELIKOSTI ABECEDY

BYLO BY FAJN TO JESTE ZOBECNIT NA Z[OMEGA]

Summary