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

Lemma 0.1. *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. $\mu(x + y) = \nu(P(x + y)) = \nu(Px + Py) \leq \nu(Px) + \nu(Py) = \mu(Px) + \mu(Py)\,.$

This verifies that μ is a norm. □

Lemma 0.1 enables us to define a new norm.

Definition 0.1. Let $M \in \mathbb{C}^{n\times n}$ be a diagonalizable matrix and $P \in \mathbb{C}^{n\times n}$ be a nonsingular matrix which diagonalizes M, i.e., $M = P^{-1}DP$ for some diagonal matrix $D \in \mathbb{C}^{n\times n}$. Then we define a vector norm $\|\cdot\|_M$ by

$$\|x\|_M := \|Px\|_2 \tag{1}$$

for all $x \in \mathbb{C}^n$, where $\|\cdot\|_2$ is Euclidean norm. A matrix norm $|||\cdot|||_M$ is induced by the norm $\|\cdot\|_M$.

Theorem 0.2. *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

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

which implies the statement. □

Lemma 0.3. *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 0.2 implies that

$$|||S_\beta|||_{S_\beta} = \rho(S_\beta) = \max\{|\beta'|\colon \beta' \text{ is conjugate of } \beta\}\,.$$

For the second part of the last statement, we use the part *iv)*, Theorem 0.2 and the fact that the eigenvalues of S_β^{-1} are reciprocal for the conjugates of β. □

Definition 0.2. Using the notation of the previous lemma, we define a *MRIZKOVA, NEBO TREBA* β*-NORM ???* $\|\cdot\|_\beta : \mathbb{Z}[\omega] \to \mathbb{R}_0^+$ by

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

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

ASI TO CHCE NEJAKOU POZNAMKU, ZE TO JE NORMA

Theorem 0.4. *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 $\mathbb{N} \subset \mathcal{A}[\beta]$, 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 $m := \max\{|a| : a \in \mathcal{A}\}$. 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 $\tilde{m} := \max\{|\sigma(a)| : a \in \mathcal{A}\}$. 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 0.5. *Let $\mathcal{A} \subset \mathbb{Z}[\beta]$ 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 $(\beta, \mathcal{A})$, then the base β is expanding and the alphabet $\mathcal{A}$ contains at least one representative of each congruence class modulo β in $\mathbb{Z}[\beta]$.*

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 0.4.

TOHLE ASI STEJNE NEMA MOC SMYSL TAM DAVAT POKUD TO NEPUJDE ZOBECNIT NA MOD V ZOMEGA (I NA ZBETA SE MUSI PRIDAT, ZE BETA JE ALG INTEGER):

In order to prove the second part, we have to show that for every $x = \sum_{i=0}^{N} x_i \beta^i \in \mathbb{Z}[\beta]$ there exists $q \in \mathbb{Z}[\beta]$ and $a \in \mathcal{A}$ such that $x = a + \beta q$. A representation of $x = \sum_{i=0}^{N} x_i' \beta^i = \sum_{i=0}^{N} x_i \beta^i + k \cdot m_\beta(\beta)$ such that $x_0' > 0$ can be found by adding an integer multiple of the minimal polynomial m_β evaluated in β. Since $\mathbb{N} \subset \mathcal{A}[\beta]$, we have

$$x_0 = \sum_{i=0}^{n} a_i \beta^i$$

for some $n \in \mathbb{N}$ and $a_i \in \mathcal{A}$. Now

$$x = \underbrace{\sum_{i=0}^{n} a_i \beta^i}_{=x_0} + \sum_{i=1}^{N} x_i \beta^i = \underbrace{a_0}_{\in\mathcal{A}} + \beta \underbrace{\left(\sum_{i=0}^{n-1} a_{i+1} \beta^i + \sum_{i=0}^{N-1} x_{i+1} \beta^i \right)}_{=q\in\mathbb{Z}[\beta]} .$$

□

Lemma 0.6. *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 0.3, we have

$$\left|\left|\left| S_\beta^{-1} \right|\right|\right|_{S_\beta} = \max\{\frac{1}{|\beta'|} : \beta' \text{ is conjugate of } \beta\} = \frac{1}{|\gamma|}\,.$$

Also, $|\gamma| > 1$ as β is an expanding integer. Since $C > 0$, the set $\mathcal{Q}$ is nonempty. Any element $x = b + q \in \mathbb{Z}[\omega]$ with $b \in \mathcal{B}$ and $q \in \mathcal{Q}$ can be written as $x = a + \beta q'$ for some $a \in \mathcal{A}$ and $q' \in \mathbb{Z}[\omega]$ due to existence of a representative of each congruence class in $\mathcal{A}$. Using the isomorphism π, we may write $\pi(q') = S_\beta^{-1} \cdot \pi(b - a + q)$. We prove that q' is in Q:

$$\begin{aligned}\left\|q'\right\|_\beta = \left\|\pi(q')\right\|_{S_\beta} = \left\|S_\beta^{-1} \cdot \pi(b - a + q)\right\|_{S_\beta} &\leq \left|\left|\left| S_\beta^{-1} \right|\right|\right|_{S_\beta} \|b - a + q\|_\beta \\ \leq \frac{1}{|\gamma|}(\|b - a\|_\beta + \|q\|_\beta) = \frac{1}{|\gamma|}(C + R) &= \frac{C}{|\gamma|}(1 + \frac{1}{|\gamma| - 1}) = R\,.\end{aligned}$$

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 0.7. *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 0.6 for the alphabet $\mathcal{A}$ and input alphabet $\mathcal{B}$. We prove by induction that all intermediate weight coefficient sets $\mathcal{Q}_k$ in Algorithm **??** are subsets of the finite set $\mathcal{Q}$.

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 $\mathcal{Q}_0 \subset \mathcal{Q}_1 \subset \mathcal{Q}_2 \subset \cdots$, Phase 1 successfully ends. □