

EXISTENCE AND OPTIMALITY OF w -NON-ADJACENT FORMS WITH AN ALGEBRAIC INTEGER BASE

CLEMENS HEUBERGER AND DANIEL KRENN

ABSTRACT. We consider digital expansions in lattices with endomorphisms acting as base. We focus on the w -non-adjacent form (w -NAF), where each block of w consecutive digits contains at most one non-zero digit. We prove that for sufficiently large w and an expanding endomorphism, there is a suitable digit set such that each lattice element has an expansion as a w -NAF.

If the eigenvalues of the endomorphism are large enough and w is sufficiently large, then the w -NAF is shown to minimise the weight among all possible expansions of the same lattice element using the same digit system.

1. INTRODUCTION

One main operation in hyperelliptic curve cryptography is the computation of multiples of a point on a hyperelliptic curve over a finite field. Clearly, we want to perform that scalar multiplication as efficiently as possible. A standard method are double-and-add algorithms. But if the hyperelliptic curve is defined over a field with q elements and we are working in the point group over an extension (i.e., working over a field with q^m elements), then we can use a Frobenius-and-add method instead. There the (expensive) doublings are replaced by the (cheap) evaluations of the q -Frobenius endomorphism in the point group.

In the endomorphism ring of the point group, the Frobenius endomorphism φ acting on the group has a characteristic polynomial $f \in \mathbb{Z}[X]$. Let τ be a complex zero of f . If we write a $z \in \mathbb{Z}[\tau]$ as $z = \sum_{j=0}^{\ell-1} \eta_j \tau^j$ for some η_j out of a digit set \mathcal{D} , then we can calculate zP for a point P on the curve by evaluating $\sum_{j=0}^{\ell-1} \eta_j \varphi^j(P)$. Note that when z is a rational integer, we are calculating multiples of the point P as mentioned at the beginning of this section. Therefore we have to understand numeral systems with an algebraic integer τ as base.

The sums in the previous paragraph are usually evaluated by a Horner scheme. There the number of additions when calculating zP corresponds to the number of non-zero digits (Hamming weight) of our expansion of z . Therefore we are interested in expansions of small weight. Let w be a positive integer. An expansion which gives a low Hamming weight is the w -non-adjacent form, \mathcal{D} - w -NAF for short, cf. [11, 1, 13]. It is defined by the syntactic requirement that every block of w consecutive digits contains at most one non-zero digit. Suitable conditions on \mathcal{D} are required such that it is a w -non-adjacent digit set (w -NADS for short), which means that each element of $\mathbb{Z}[\tau]$ has a representation as a \mathcal{D} - w -NAF.

In the present paper we give positive results on that existence question. Our set-up is more general: In Section 2, which contains the definitions and some basic results, we work in an Abelian group and the base is represented by an injective endomorphism on that group. In the remaining article, starting with Section 3, the set-up is a lattice Λ in \mathbb{R}^n and an injective endomorphism on Λ as base. The case of algebraic integer bases is a special case of this set-up, cf. Examples 2.2 and 2.7.

2010 *Mathematics Subject Classification.* 11A63; 11H06 11R04 94A60.

Key words and phrases. τ -adic expansions, w -non-adjacent forms, redundant digit sets, lattices, existence, hyperelliptic curve cryptography, Koblitz curves, Frobenius endomorphism, scalar multiplication, Hamming weight, optimality, minimal expansions.

The authors are supported by the Austrian Science Fund (FWF): S9606, that is part of the Austrian National Research Network “Analytic Combinatorics and Probabilistic Number Theory”, and by the Austrian Science Fund (FWF): W1230, Doctoral Program “Discrete Mathematics”.

Clemens Heuberger is also supported by the Austrian Exchange Service ÖAD, project number HU 04/2010.

In Section 3 we prove a necessary condition to be a w -NADS, namely that the endomorphism has to be expanding. Section 4 deals with the setting when the digit set comes from a tiling of \mathbb{R}^n . Theorem A states that we have a w -NADS if w is sufficiently large. The bound in that result is explicit. Another result of that kind is given in Section 5, generalising a result of Germán and Kovács [7] to \mathcal{D} - w -NAFs. There minimal norm digit sets are studied. Again we get a w -NADS if w is larger than a constant, which depends (only) on the eigenvalues of Φ , cf. Theorem B. As an important example, we discuss the setting of bases τ coming from hyperelliptic curves, see above, in Example 5.2.

The last section is devoted to the question of minimality: Are the \mathcal{D} - w -NAF-expansions optimal, i.e., does the \mathcal{D} - w -NAF-expansion of an element minimise the weight among all possible expansions of that element with the same digit set? We provide a positive answer for sufficiently large w and sufficiently large eigenvalues of Φ in Theorem C.

2. w -NON-ADJACENT FORMS AND DIGIT SETS

In this section, we formally introduce the notion of w -non-adjacent forms and w -non-adjacent digits sets.

We consider an Abelian group \mathcal{A} , an injective endomorphism Φ of \mathcal{A} and an integer $w \geq 1$. Let \mathcal{D}^\bullet be a system of representatives of those residue classes of \mathcal{A} modulo $\Phi^w(\mathcal{A})$ which are not contained in $\Phi(\mathcal{A})$. We set $\mathcal{D} = \mathcal{D}^\bullet \cup \{0\}$.

We call the triple $(\mathcal{A}, \Phi, \mathcal{D})$ a *pre- w -non-adjacent digit set (pre- w -NADS)*.

Definition 2.1. (1) A word $\boldsymbol{\eta} = \eta_{\ell-1} \dots \eta_0$ over the alphabet \mathcal{D} is said to be a *\mathcal{D} - w -non-adjacent form (\mathcal{D} - w -NAF)*, if every factor $\eta_{j+w-1} \dots \eta_j$, $0 \leq j \leq \ell - w$, contains at most one non-zero letter η_k . Its *value* is defined to be

$$\text{value}(\eta_{\ell-1} \dots \eta_0) = \sum_{j=0}^{\ell-1} \Phi^j(\eta_j).$$

We say that $\boldsymbol{\eta}$ is a *\mathcal{D} - w -NAF of $\alpha \in \mathcal{A}$* if $\text{value}(\boldsymbol{\eta}) = \alpha$.

(2) We say that \mathcal{D} is a *w -non-adjacent digit set (w -NADS)*, if every $\alpha \in \mathcal{A}$ admits a \mathcal{D} - w -NAF.

Example 2.2. Let K be a number field of degree n , \mathfrak{O} be an order in K and $\tau \in \mathfrak{O}$. We consider the endomorphism $\Phi_\tau: \mathfrak{O} \rightarrow \mathfrak{O}$ with $\alpha \mapsto \tau\alpha$, i.e., multiplication by τ . Then let \mathcal{D}^\bullet be a system of representatives of those residue classes of \mathfrak{O} modulo τ^w which are not divisible by τ and $\mathcal{D} = \mathcal{D}^\bullet \cup \{0\}$. Then $(\mathfrak{O}, \Phi_\tau, \mathcal{D})$ is a pre- w -NADS. Note that

$$\text{value}(\eta_{\ell-1} \dots \eta_0) = \sum_{j=0}^{\ell-1} \eta_j \tau^j$$

for a word $\eta_{\ell-1} \dots \eta_0$ over the alphabet \mathcal{D} .

We state a few special cases.

Example 2.3. Let $\tau \in \mathbb{Z}$, $|\tau| \geq 2$ and $w \geq 1$ be an integer. Consider

$$\mathcal{D}^\bullet = \left\{ d \in \mathbb{Z} : -\frac{|\tau|^w}{2} < d \leq \frac{|\tau|^w}{2}, \tau \nmid d \right\}$$

and $\mathcal{D} = \mathcal{D}^\bullet \cup \{0\}$. Then $(\mathbb{Z}, \Phi_\tau, \mathcal{D})$ is a pre- w -NADS, where Φ_τ still denotes multiplication by τ . It can be shown that $(\mathbb{Z}, \Phi_\tau, \mathcal{D})$ is a w -NADS. This will also be a consequence of Theorem B.

Example 2.4. Let τ be an imaginary quadratic integer and \mathcal{D}^\bullet a system of representatives of those residue classes of $\mathbb{Z}[\tau]$ modulo τ^w which are not divisible by τ with the property that

$$\text{if } \alpha \equiv \beta \pmod{\tau^w} \text{ and } \alpha \in \mathcal{D}^\bullet, \text{ then } |\alpha| \leq |\beta|$$

holds for $\alpha, \beta \in \mathbb{Z}[\tau]$ which are not divisible by τ . This means that \mathcal{D} contains a representative of minimal absolute value of each residue class not divisible by τ . As always, we set $\mathcal{D} = \mathcal{D}^\bullet \cup \{0\}$.

Then, for $w \geq 2$, $(\mathbb{Z}[\tau], \Phi_\tau, \mathcal{D})$ is a w -NADS (cf. Heuberger and Krenn [8]), where Φ_τ still denotes multiplication by τ .

For $\tau \in \{(\pm 1 \pm \sqrt{-7})/2, (\pm 3 \pm \sqrt{-3})/2, 1 + \sqrt{-1}, \sqrt{-2}, (1 + \sqrt{-11})/2\}$, this has been shown by Solinas [12, 13] and Blake, Murty and Xu [2, 4], cf. also Blake, Murty and Xu [3] for other digit sets to the bases $(\pm 1 \pm \sqrt{-7})/2$.

At several occurrences, it is useful to consider *equivalent* pre- w -NADS.

Definition 2.5. The pre- w -NADS $(\mathcal{A}, \Phi, \mathcal{D})$ and $(\mathcal{A}', \Phi', \mathcal{D}')$ are said to be *equivalent*, if there is a group isomorphism $Q: \mathcal{A} \rightarrow \mathcal{A}'$ such that the diagram

$$\begin{array}{ccc} \mathcal{A} & \xrightarrow{\Phi} & \mathcal{A} \\ Q \downarrow & & \downarrow Q \\ \mathcal{A}' & \xrightarrow{\Phi'} & \mathcal{A}' \end{array}$$

commutes and such that $\mathcal{D}' = Q(\mathcal{D})$.

It is then clear that the following proposition holds.

Proposition 2.6. *Let $(\mathcal{A}, \Phi, \mathcal{D})$ and $(\mathcal{A}', \Phi', \mathcal{D}')$ two equivalent pre- w -NADS. Then \mathcal{D} is a w -NADS if and only if \mathcal{D}' is a w -NADS.*

Proof. Straightforward. □

Example 2.7. We continue Example 2.2, i.e., K is a number field, \mathfrak{O} an order in K , $\tau \in \mathfrak{O}$, the endomorphism considered is Φ_τ , the multiplication by τ , and the digit set \mathcal{D} is as in Example 2.2.

The real embeddings of K are denoted by $\sigma_1, \dots, \sigma_s$; the non-real complex embeddings of K are denoted by $\sigma_{s+1}, \overline{\sigma_{s+1}}, \dots, \sigma_{s+t}, \overline{\sigma_{s+t}}$, where $\overline{\cdot}$ denotes complex conjugation and $n = s + 2t$. The *Minkowski map* $\Sigma: K \rightarrow \mathbb{R}^n$ maps $\alpha \in K$ to

$$(\sigma_1(\alpha), \dots, \sigma_s(\alpha), \Re\sigma_{s+1}(\alpha), \Im\sigma_{s+1}(\alpha), \dots, \Re\sigma_{s+t}(\alpha), \Im\sigma_{s+t}(\alpha)) \in \mathbb{R}^n.$$

We write $\Lambda = \Sigma(\mathfrak{O})$ for the image of \mathfrak{O} under Σ . Note that Λ is a lattice in \mathbb{R}^n . We consider the $n \times n$ block diagonal matrix

$$A_\tau := \text{diag} \left(\sigma_1(\tau), \dots, \sigma_s(\tau), \begin{pmatrix} \Re\sigma_{s+1}(\tau) & -\Im\sigma_{s+1}(\tau) \\ \Im\sigma_{s+1}(\tau) & \Re\sigma_{s+1}(\tau) \end{pmatrix}, \dots, \begin{pmatrix} \Re\sigma_{s+t}(\tau) & -\Im\sigma_{s+t}(\tau) \\ \Im\sigma_{s+t}(\tau) & \Re\sigma_{s+t}(\tau) \end{pmatrix} \right)$$

and set $\mathcal{D}' := \Sigma(\mathcal{D})$. Then the pre- w -NADS $(\mathfrak{O}, \Phi_\tau, \mathcal{D})$ and $(\Lambda, \Phi'_\tau, \mathcal{D}')$ are easily seen to be equivalent, where $\Phi'_\tau(x) := A_\tau \cdot x$ for $x \in \mathbb{R}^n$.

Note that if K is an imaginary quadratic number field (cf. Example 2.4), this construction merely corresponds to a straight-forward identification of \mathbb{C} with \mathbb{R}^2 .

In order to investigate the w -NADS property further, it is convenient to consider the following two maps.

Definition 2.8. Let $(\mathcal{A}, \Phi, \mathcal{D})$ be a pre- w -NADS. We define

- (1) $d: \mathcal{A} \rightarrow \mathcal{D}$ with $d(\alpha) = 0$ for $\alpha \in \Phi(\mathcal{A})$ and $d(\alpha) \equiv \alpha \pmod{\Phi^w(\mathcal{A})}$ for all other $\alpha \in \mathcal{A}$,
- (2) $T: \mathcal{A} \rightarrow \mathcal{A}$ with $\alpha \mapsto \Phi^{-1}(\alpha - d(\alpha))$.

Note that the map d is well-defined as \mathcal{D}^\bullet contains exactly one representative of every residue class of \mathcal{A} modulo $\Phi^w(\mathcal{A})$ which is not contained in $\Phi(\mathcal{A})$. Furthermore, we have $\alpha \equiv d(\alpha) \pmod{\Phi(\mathcal{A})}$ for all $\alpha \in \mathcal{A}$. Therefore and by the injectivity of Φ , the map T is well-defined. We remark that by definition, we have $T(0) = 0$.

We get the following characterisation, which corresponds to the backwards division algorithm for computing digital expansions from right (least significant digit) to left (most significant digit).

Lemma 2.9. *Let $\alpha \in \mathcal{A}$. Then α has a \mathcal{D} - w -NAF $\eta_{\ell-1} \dots \eta_0$ if and only if $T^\ell(\alpha) = 0$. In this case, we have $\eta_k = d(T^k(\alpha))$ for $0 \leq k < \ell$. In particular, the \mathcal{D} - w -NAF of an $\alpha \in \mathcal{A}$, if it exists, is unique up to leading zeros.*

Proof. Assume that $\eta_{\ell-1} \dots \eta_0$ is a \mathcal{D} - w -NAF of α . We clearly have $\alpha \equiv \eta_0 \pmod{\Phi(\Lambda)}$, so that α is an element of $\Phi(\Lambda)$ if and only if $\eta_0 = 0$. Otherwise, the w -NAF-condition ensures that $\alpha \equiv \eta_0 \pmod{\Phi^w(\Lambda)}$. In both cases, we get $d(\alpha) = \eta_0$ and therefore

$$T(\alpha) = \text{value}(\eta_{\ell-1} \dots \eta_1).$$

Iterating this process yields $T^k(\alpha) = \text{value}(\eta_{\ell-1} \dots \eta_k)$ for $0 \leq k \leq \ell$, where $\eta_{\ell-1} \dots \eta_k$ is a \mathcal{D} - w -NAF. For $k = \ell$, we see that $T^\ell(\alpha)$ is the value of the empty word, which is zero by the definition of the empty sum.

Conversely, we assume that $T^\ell(\alpha) = 0$. We note that if $d(\beta) \neq 0$ for some $\beta \in \mathcal{A}$, we have $\beta - d(\beta) \equiv 0 \pmod{\Phi^w(\Lambda)}$, which results in $T^j(\beta) = \Phi^{-j}(\beta - d(\beta)) \equiv 0 \pmod{\Phi(\Lambda)}$ and $d(T^j(\beta)) = 0$ for $1 \leq j \leq w-1$. Therefore, the word $\boldsymbol{\eta} = d(T^{\ell-1}(\alpha)) \dots d(T(\alpha))d(\alpha)$ is a \mathcal{D} - w -NAF. Iterating the relation $\beta = \Phi(T(\beta)) + d(\beta)$ valid for all $\beta \in \mathcal{A}$, we conclude that $\alpha = \Phi^\ell(T^\ell(\alpha)) + \text{value}(\boldsymbol{\eta}) = \text{value}(\boldsymbol{\eta})$. \square

3. LATTICES AND \mathcal{D} - w -NAFS

We now specialise our investigations to the case that the abstract Abelian group \mathcal{A} is replaced by a lattice in \mathbb{R}^n , i.e., $\mathcal{A} = \Lambda = w_1\mathbb{Z} \oplus \dots \oplus w_n\mathbb{Z}$ for linearly independent $w_1, \dots, w_n \in \mathbb{R}^n$. Further let Φ be an injective endomorphism of \mathbb{R}^n with $\Phi(\Lambda) \subseteq \Lambda$, $w \geq 1$ be an integer, and \mathcal{D}^\bullet a system of representatives of those residue classes of Λ modulo $\Phi^w(\Lambda)$ which are not contained in $\Phi(\Lambda)$, and set $\mathcal{D} = \mathcal{D}^\bullet \cup \{0\}$.

The results are still applicable to the case of multiplication by τ in the order of a number field, as the purpose of Example 2.7 was to describe it as equivalent to a lattice $\Lambda \subseteq \mathbb{R}^n$ via the isomorphism Σ .

The aim of this section is to prove a necessary criterion for a pre- w -NADS to be a w -NADS.

Proposition 3.1. *Let \mathcal{D} be a w -NADS. Then Φ is expanding, i.e., $|\lambda| > 1$ holds for all eigenvalues λ of Φ .*

Proof. (1) We first consider the case that there is an eigenvalue λ of Φ with $|\lambda| < 1$.

In a somewhat different wording, this has been led to a contradiction by Vince [14]. The idea is the following: After a suitable change of variables, the endomorphism Φ can be represented by a Jordan matrix such that the first k coordinates, say, correspond to the eigenvalue λ . Thus the first k coefficients of $\text{value}(\boldsymbol{\eta})$ are bounded independently of the word $\boldsymbol{\eta}$ over the alphabet \mathcal{D} . Thus it is impossible to have a representation of all elements of Λ . This is completely independent of the w -NAF-condition (and gives, in fact, a stronger result, as representability by any word over the digit set is impossible).

(2) We next consider the case that $|\lambda| \geq 1$ for all eigenvalues λ of Φ with equality $|\lambda_0| = 1$ for at least one eigenvalue λ_0 .

We again follow Vince [14], see also Kovács and Pethő [10], to see that λ_0 must be a root of unity. The idea is that λ_0 is a unit in $\mathbb{Z}[\lambda_0, \overline{\lambda_0}]$, as $\overline{\lambda_0}$ is its inverse. Therefore, λ has absolute norm ± 1 . As we already assumed that all its absolute conjugates are at least 1 in absolute value, this implies that all absolute conjugates of λ_0 lie on the unit circle. Thus λ_0 is a root of unity.

As a consequence, there is some ℓ such that $\lambda_0^\ell = 1$. In other words, 1 is an eigenvalue of Φ^ℓ . After a suitable change of coordinates, Λ can be assumed to be \mathbb{Z}^n and Φ can be represented by a matrix with integer entries. Let α be an eigenvector of Φ^ℓ with eigenvalue 1. Multiplying α by a suitable integer if necessary, we can assume that $\alpha \in \mathbb{Z}^n = \Lambda$. As $\alpha = \Phi^\ell(\alpha)$, we get $\alpha \in \Phi^k(\Lambda)$ for all integers $k \geq 0$, which implies that $d(T^k(\alpha)) = 0$ holds for all k . Furthermore, we cannot have $T^k(\alpha) = 0$ for any $k \geq 0$. Thus, α cannot be represented. \square

4. TILING BASED DIGIT SETS

In this section, we consider a fixed lattice $\Lambda \subseteq \mathbb{R}^n$ and an expanding endomorphism Φ of \mathbb{R}^n with $\Phi(\Lambda) \subseteq \Lambda$. We will discuss digit sets constructed from tilings.

Definition 4.1. Let V be a subset of \mathbb{R}^n . We say that V tiles \mathbb{R}^n by the lattice Λ , if the following two properties hold:

- (1) $\bigcup_{z \in \Lambda} (z + V) = \mathbb{R}^n$,
- (2) $V \cap (z + V) \subseteq \partial V$ holds for all $z \in \Lambda$ with $z \neq 0$.

We now assume that V be a subset of \mathbb{R}^n tiling \mathbb{R}^n by Λ .

Lemma 4.2. Let $w \geq 1$ and

$$\tilde{\mathcal{D}} := \{\alpha \in \Lambda : \Phi^{-w}(\alpha) \in V\}.$$

Then $\tilde{\mathcal{D}}$ contains a complete residue system of Λ modulo $\Phi^w(\Lambda)$.

Furthermore, if $\alpha, \alpha' \in \tilde{\mathcal{D}}$ with $\alpha \neq \alpha'$ and $\alpha \equiv \alpha' \pmod{\Phi^w(\Lambda)}$, then $\Phi^{-w}(\alpha), \Phi^{-w}(\alpha') \in \partial V$.

Proof. Let $\beta \in \Lambda$. Then there is a $\gamma \in \Lambda$ and a $v \in V$ such that $\Phi^{-w}(\beta) = \gamma + v$. Setting $\alpha := \beta - \Phi^w(\gamma)$, this implies that

$$\Phi^{-w}(\alpha) = \Phi^{-w}(\beta) - \gamma = v \in V,$$

i.e., $\alpha \in \tilde{\mathcal{D}}$ and $\beta \equiv \alpha \pmod{\Phi^w(\Lambda)}$.

Assume now $\alpha, \alpha' \in \tilde{\mathcal{D}}$ with $\alpha \neq \alpha'$ and $\alpha \equiv \alpha' \pmod{\Phi^w(\Lambda)}$. We write $\alpha' = \alpha + \Phi^w(\gamma)$ for a suitable $\gamma \in \Lambda$. We obtain

$$\Phi^{-w}(\alpha') = \Phi^{-w}(\alpha) + \gamma,$$

which implies that $\Phi^{-w}(\alpha') \in \partial V$. Analogously, we get $\Phi^{-w}(\alpha) \in \partial V$. \square

For an integer $w \geq 1$, we choose a subset \mathcal{D}^\bullet of $\tilde{\mathcal{D}}$ in such a way that \mathcal{D}^\bullet contains exactly one representative of every residue class modulo $\Phi^w(\Lambda)$ which is not contained in $\Phi(\Lambda)$. We also set $\mathcal{D} := \mathcal{D}^\bullet \cup \{0\}$.

Theorem A. Let $\|\cdot\|$ be a vector norm on \mathbb{R}^n such that for the corresponding induced operator norm, also denoted by $\|\cdot\|$, the inequality $\|\Phi^{-1}\| < 1$ holds. Let r and R be positive reals with

$$\{x \in \mathbb{R}^n : \|x\| \leq r\} \subseteq V \subseteq \{x \in \mathbb{R}^n : \|x\| \leq R\}. \quad (1)$$

If w is a positive integer such that

$$\|\Phi^{-1}\|^w < \frac{1}{1 + R/r}, \quad (2)$$

then \mathcal{D} is a w -NADS.

Remark 4.3. In the case of expansions in an order of a number field (Example 2.7), we may take $\|\cdot\|$ to be the Euclidean norm $\|\cdot\|_2$, as the corresponding operator norm fulfils $\|A_\tau^{-1}\|_2 = \max\{1/|\sigma_j(\tau)| : 1 \leq j \leq s+t\}$. In this case, (2) is equivalent to $|\sigma_j(\tau)|^w > 1 + R/r$ for all $1 \leq j \leq s+t$.

Proof of Theorem A. Let $\alpha \in \Lambda$. We claim that

$$\|T^k(\alpha)\| \leq \frac{R}{1 - \|\Phi^{-1}\|^w} + \|\Phi^{-1}\|^k \cdot \|\alpha\| \quad (3)$$

holds for all k with the property that $d(T^{k'}(\alpha)) = 0$ holds for all non-negative k' with $k - w < k' \leq k$.

For $k = 0$, (3) is obviously true. We assume that (3) holds for some k . As an abbreviation, we write $\beta = T^k(\alpha)$ and $\eta = d(\beta)$. If $\eta = 0$, then we have

$$\|T^{k+1}(\alpha)\| = \|T(\beta)\| = \|\Phi^{-1}(\beta)\| \leq \|\Phi^{-1}\| \cdot \|\beta\| \leq \frac{\|\Phi^{-1}\| \cdot R}{1 - \|\Phi^{-1}\|^w} + \|\Phi^{-1}\|^{k+1} \cdot \|\alpha\|,$$

which proves (3) for $k + 1$.

In the case $\eta \neq 0$, we get

$$\begin{aligned} \|T^{k+w}(\alpha)\| &= \|\Phi^{-w}(\beta - \eta)\| \leq \|\Phi^{-1}\|^w \cdot \|\beta\| + \|\Phi^{-w}(\eta)\| \\ &\leq \|\Phi^{-1}\|^w \left(\frac{R}{1 - \|\Phi^{-1}\|^w} + \|\Phi^{-1}\|^k \cdot \|\alpha\| \right) + R = \frac{R}{1 - \|\Phi^{-1}\|^w} + \|\Phi^{-1}\|^{k+w} \cdot \|\alpha\|, \end{aligned}$$

which is (3) for $k + w$.

By (2) and (3), we can choose a k_0 such that

$$\|\Phi^{-w}(T^k(\alpha))\| \leq \frac{\|\Phi^{-1}\|^w}{1 - \|\Phi^{-1}\|^w} R + \|\Phi^{-1}\|^{k+w} \cdot \|\alpha\| < r \quad (4)$$

holds for all $k \geq k_0$.

If $T^{k_0}(\alpha) = 0$, then α admits a \mathcal{D} - w -NAF by Lemma 2.9. Otherwise, choose $k \geq k_0$ maximally such that $T^{k_0}(\alpha) \in \Phi^{k-k_0}(\Lambda)$. This is possible because Φ is expanding. This results in $T^k(\alpha) \notin \Phi(\Lambda)$. Then (4) implies that

$$\|\Phi^{-w}(T^k(\alpha))\| < r.$$

By (1), we conclude that $\Phi^{-w}(T^k(\alpha))$ is an element of the interior of V .

By Lemma 4.2, we obtain $\Phi^{-w}(T^k(\alpha)) \in \mathcal{D}^\bullet$, hence $d(T^k(\alpha)) = T^k(\alpha)$ and $T^{k+1}(\alpha) = 0$. Thus α admits a \mathcal{D} - w -NAF by Lemma 2.9. \square

5. MINIMAL NORM DIGIT SET

In this section, we study a special digit set, the minimal norm digit set. In the case of an imaginary quadratic integer τ , this notion coincides with the minimal norm representative digit sets introduced by Solinas [12, 13].

Let again Λ be a lattice in \mathbb{R}^n and Φ an expansive endomorphism of \mathbb{R}^n with $\Phi(\Lambda) \subseteq \Lambda$. Choose a positive integer w_0 such that $|\lambda| > 2^{1/w_0}$ holds for all eigenvalues λ of Φ . Thus the spectral radius of Φ^{-1} is less than $1/2^{1/w_0}$. We choose a vector norm $\|\cdot\|$ on \mathbb{R}^n such that the induced operator norm (also denoted by $\|\cdot\|$) fulfils $\|\Phi^{-1}\| < 1/2^{1/w_0}$. As a consequence, we have $\|\Phi^{-1}\|^w < 1/2$ for all $w \geq w_0$.

Again, in the case of expansions in an order of a number field (Example 2.7), we may take $\|\cdot\|$ to be the Euclidean norm $\|\cdot\|_2$, cf. Remark 4.3.

Let V be the Voronoi cell of the origin with respect to the point set Λ and the vector norm $\|\cdot\|$, i.e.,

$$V = \{z \in \mathbb{R}^n : \|z\| \leq \|z + \alpha\| \text{ holds for all } \alpha \in \Lambda\}.$$

While V does not necessarily tile \mathbb{R}^n by Λ (consider the norm $\|\cdot\|_\infty$ and the lattice generated by $(1, 0)$ and $(0, 10)$ in \mathbb{R}^2), for a given integer $w \geq 1$, we can still select a set \mathcal{D}^\bullet of representatives of those residue classes of Λ modulo $\Phi^w(\Lambda)$ which are not contained in $\Phi^w(\Lambda)$ such that

$$\mathcal{D}^\bullet \subseteq \{\alpha \in \Lambda : \Phi^{-w}(\alpha) \in V\}.$$

As usual, we also set $\mathcal{D} := \mathcal{D}^\bullet \cup \{0\}$ and call it a *minimal norm digit set modulo Φ^w* .

Adapting ideas of Germán and Kovács [7] to our setting, we prove the following theorem.

Theorem B. *If $w \geq w_0$, then \mathcal{D} is a w -NADS.*

Proof. We set $\widetilde{M} := \max\{\|\eta\| : \eta \in \mathcal{D}\}$. For $\beta \in \Lambda$, we have

$$\|T(\beta)\| = \|\Phi^{-1}(\beta - d(\beta))\| \leq \|\Phi^{-1}\|(\|\beta\| + \widetilde{M}).$$

Setting

$$M := \frac{\|\Phi^{-1}\|}{1 - \|\Phi^{-1}\|} \widetilde{M},$$

we see that

$$\begin{aligned} \|T(\beta)\| &< \|\beta\| && \text{if } \|\beta\| > M, \\ \|T(\beta)\| &\leq M && \text{if } \|\beta\| \leq M. \end{aligned}$$

As Λ is a discrete subset of \mathbb{R}^n , we conclude that the sequence $(T^k(\alpha))_{k \geq 0}$ is eventually periodic for all $\alpha \in \Lambda$.

For $\beta \in \Phi(\Lambda)$ with $\beta \neq 0$, we have

$$\|T(\beta)\| = \|\Phi^{-1}(\beta)\| \leq \|\Phi^{-1}\| \cdot \|\beta\| < \|\beta\|.$$

Consider the set

$$P := \{\beta \in \Lambda : \beta \notin \Phi(\Lambda) \text{ and } (T^k(\beta))_{k \geq 0} \text{ is purely periodic}\}.$$

The set P is empty if and only if for each $\alpha \in \Lambda$, there is an ℓ with $T^\ell(\alpha) = 0$, i.e., α admits a \mathcal{D} - w -NAF. Therefore, by Lemma 2.9, P is empty if and only if \mathcal{D} is a w -NADS.

We therefore assume that P is nonempty. We choose an $\alpha \in P$ such that $\|\Phi^{-w}(\alpha)\| \geq \|\Phi^{-w}(\beta)\|$ holds for all $\beta \in P$. This is possible, since all elements β of P fulfil $\|\beta\| \leq M$, which implies that P is a finite set.

Next, we choose $\ell > 0$ with $T^\ell(\alpha) = \alpha$ and set $\eta_k = d(T^k(\alpha))$ for $0 \leq k \leq \ell$. We set

$$N := \{0 \leq k \leq \ell : \eta_k \neq 0\}.$$

By the w -NAF-condition, we have $|k - k'| \geq w$ for distinct elements k and k' of N .

By definition of T , we have

$$\alpha = T^\ell(\alpha) = \Phi^{-\ell} \left(\alpha - \sum_{k=0}^{\ell-1} \Phi^k(\eta_k) \right) = \Phi^{-\ell}(\alpha) - \sum_{k=0}^{\ell-1} \Phi^{k-\ell}(\eta_k).$$

Applying Φ^{-w} once more and rearranging yields

$$\Phi^{-w}(\alpha) = (\text{id} - \Phi^{-\ell})^{-1} \left(- \sum_{\substack{k=0 \\ k \in N}}^{\ell-1} \Phi^{k-\ell}(\Phi^{-w}(\eta_k)) \right). \quad (5)$$

Note that we restricted the sum to those k corresponding to non-zero digits.

We claim that

$$\|\Phi^{-w}(\eta_k)\| \leq \|\Phi^{-w}(T^k(\alpha))\| \leq \|\Phi^{-w}(\alpha)\| \quad (6)$$

holds for $k \in N$. The first inequality is an immediate consequence of the definition of \mathcal{D}^\bullet , as $\Phi^{-w}(T^k(\alpha)) = \Phi^{-w}(\eta_k) + \gamma$ for a suitable $\gamma \in \Lambda$. Here, we used that $\eta_k \neq 0$ implies that $T^k(\alpha) \notin \Phi(\Lambda)$. Therefore and as $T^{k+\ell}(\alpha) = T^k(T^\ell(\alpha)) = T^k(\alpha)$, we also get $T^k(\alpha) \in P$. By the choice of α , we conclude the second inequality in (6).

Taking norms in (5) yields

$$\|\Phi^{-w}(\alpha)\| \leq \frac{\|\Phi^{-w}(\alpha)\|}{1 - \|\Phi^{-1}\|^\ell} \sum_{\substack{k=0 \\ k \in N}}^{\ell-1} \|\Phi^{-1}\|^{\ell-k}. \quad (7)$$

As $\ell \in N$, we have

$$\sum_{\substack{k=0 \\ k \in N}}^{\ell-1} \|\Phi^{-1}\|^{\ell-k} \leq \|\Phi^{-1}\|^w + \|\Phi^{-1}\|^{2w} + \dots + \|\Phi^{-1}\|^{mw} = \|\Phi^{-1}\|^w \frac{1 - \|\Phi^{-1}\|^{mw}}{1 - \|\Phi^{-1}\|^w}, \quad (8)$$

where $m = \lfloor \ell/w \rfloor$. Combining (7) and (8) yields

$$\|\Phi^{-w}(\alpha)\| \leq \frac{\|\Phi^{-1}\|^w}{1 - \|\Phi^{-1}\|^w} \frac{1 - \|\Phi^{-1}\|^{mw}}{1 - \|\Phi^{-1}\|^\ell} \|\Phi^{-w}(\alpha)\| < \|\Phi^{-w}(\alpha)\|,$$

as $\|\Phi^{-1}\|^w < 1/2$, contradiction. \square

We restate this result explicitly for expansion in orders of algebraic number fields.

Corollary 5.1. *Let K be an algebraic number field of degree n , $\sigma_1, \dots, \sigma_s$ the real embeddings and $\sigma_{s+1}, \overline{\sigma_{s+1}}, \dots, \sigma_{s+t}, \overline{\sigma_{s+t}}$ be the non-real complex embeddings of K .*

Let \mathfrak{D} be an order of K and $\tau \in \mathfrak{D}$ such that $|\sigma_j(\tau)| > 1$ holds for all j . Let w be an integer with

$$w > \max \left\{ \frac{\log 2}{\log |\sigma_j(\tau)|} : 1 \leq j \leq s+t \right\}.$$

Let \mathcal{D}^\bullet be a system of representatives of those residue classes of \mathcal{D} modulo τ^w which are not divisible by τ such that

$$\text{if } \alpha \equiv \beta \pmod{\tau^w} \text{ with } \tau \nmid \alpha \text{ and } \alpha \in \mathcal{D}, \text{ then } \sum_{j=1}^{s+t} a_j \left| \sigma_j \left(\frac{\alpha}{\tau^w} \right) \right|^2 \leq \sum_{j=1}^{s+t} a_j \left| \sigma_j \left(\frac{\beta}{\tau^w} \right) \right|^2,$$

where $a_j = 1$ for $j \in \{1, \dots, s\}$ and $a_j = 2$ for $j \in \{s+1, \dots, s+t\}$. Then $\mathcal{D} := \mathcal{D}^\bullet \cup \{0\}$ is a w -NADS.

Example 5.2. Let C be an algebraic curve of genus g defined over \mathbb{F}_q (a field with q elements). The Frobenius endomorphism operates on the Jacobian variety of C and satisfies a characteristic polynomial $P \in \mathbb{Z}[T]$ of degree $2g$. Let τ be a root of P . Set $K = \mathbb{Q}[\tau]$ and $\mathcal{D} = \mathbb{Z}[\tau]$, and denote the embeddings of K by σ_j . Using Corollary 5.1, a minimal norm digit set modulo τ^w is a w -NADS if

$$w > \frac{\log 4}{\log q}.$$

This is true because of the following reasons: The polynomial P fulfils the equation

$$P(T) = T^{2g} L(1/T),$$

where $L(T)$ denotes the numerator of the zeta-function of C over \mathbb{F}_q , cf. Weil [15, 17]. The Riemann Hypothesis of the Weil Conjectures, cf. Weil [16], Dwork [6] and Deligne [5], state that all zeros of L have absolute value $1/\sqrt{q}$. Therefore $|\sigma_j(\tau)| = \sqrt{q}$, which was to show.

6. OPTIMALITY OF \mathcal{D} - w -NAFS

In this section, we consider a lattice $\Lambda \subseteq \mathbb{R}^n$ and an expanding endomorphism Φ of \mathbb{R}^n with $\Phi(\Lambda) \subseteq \Lambda$.

Definition 6.1. Let $\eta = \eta_{\ell-1} \dots \eta_0$ be a word over the alphabet \mathcal{D} . Its (*Hamming-*)*weight* is the cardinality of $\{j : \eta_j \neq 0\}$, i.e., the number of non-zero digits in η .

Let $z = \text{value}(\eta)$. The expansion η is said to be *optimal* if it minimises the weight among all possible expansions of z , i.e., if the weight of η is at most the weight of ξ for all words ξ over \mathcal{D} with $\text{value}(\xi) = z$.

We will show an optimality result for \mathcal{D} - w -NAFs in Theorem C, where the digit set comes from a tiling as in Section 4.

Lemma 6.2. *We have*

$$\lim_{m \rightarrow \infty} \Phi^m(\Lambda) := \bigcap_{m \in \mathbb{N}_0} \Phi^m(\Lambda) = \{0\}.$$

Proof. Let $\alpha \in \lim_{m \rightarrow \infty} \Phi^m(\Lambda) = \bigcap_{m \in \mathbb{N}_0} \Phi^m(\Lambda)$. Then there is a sequence $(\beta_m)_{m \in \mathbb{N}_0}$, all $\beta_m \in \Lambda$ and with $\beta_m = \Phi^{-m}(\alpha)$. As Φ is expanding, we obtain $\beta_m \rightarrow 0$ as m tends to infinity. The lattice Λ is discrete, so $\beta_m = 0$ for sufficiently large m . We conclude that $\alpha = 0$. \square

Now we define the digit set: We start with a subset V of \mathbb{R}^n tiling \mathbb{R}^n by Λ . For a positive integer w let

$$\tilde{\mathcal{D}} := \{\alpha \in \Lambda : \Phi^{-w}(\alpha) \in V\}$$

and

$$\tilde{\mathcal{D}}_{\text{int}} := \{\alpha \in \Lambda : \Phi^{-w}(\alpha) \in \text{int } V\},$$

where $\text{int } V$ denotes the interior of V . We choose a subset \mathcal{D}^\bullet of $\tilde{\mathcal{D}}$ in such a way that \mathcal{D}^\bullet contains exactly one representative of every residue class modulo $\Phi^w(\Lambda)$ which is not contained in $\Phi(\Lambda)$. We also set $\mathcal{D} := \mathcal{D}^\bullet \cup \{0\}$. This is the same construction as in Section 4.

Lemma 6.3. *Assume that $V \subseteq \Phi(V)$. Then each element of $\tilde{\mathcal{D}}_{\text{int}} \setminus \{0\}$ has an expansion of weight 1.*

Proof. Let $\alpha \in \widetilde{\mathcal{D}}_{\text{int}} \setminus \{0\}$, and let $\beta = \Phi^{-\ell}(\alpha) \in \Lambda$ such that the non-negative integer ℓ is maximal. Therefore $\beta \notin \Phi(\Lambda)$. We have that $\Phi^{-w}(\beta) = \Phi^{-w-\ell}(\alpha)$ is in the interior of $\Phi^{-\ell}(V)$. Using $V \subseteq \Phi(V)$ yields $\Phi^{-w}(\beta) \in \text{int } V$, and therefore, by Lemma 4.2, $\beta \in \mathcal{D}^\bullet$. Thus $\alpha = \Phi^\ell(\beta)$ has an expansion of weight 1. \square

Theorem C. *Assume that $V \subseteq \Phi(V)$, $V = -V$ and that there are a vector norm $\|\cdot\|$ on \mathbb{R}^n and positive reals r and R such that*

$$\{x \in \mathbb{R}^n : \|x\| \leq r\} \subseteq V \subseteq \{x \in \mathbb{R}^n : \|x\| \leq R\} \quad (9)$$

and such that the induced operator norm (also denoted by $\|\cdot\|$) fulfils $\|\Phi^{-1}\| < \frac{r}{R}$.

If w is a positive integer such that

$$\|\Phi^{-1}\|^w < \frac{1}{2} \left(\frac{r}{R} - \|\Phi^{-1}\| \right) \quad (10)$$

and \mathcal{D} is a w -NADS, then the \mathcal{D} - w -NAF-expansion of each element of Λ is optimal.

The proof relies on the following optimality result.

Theorem (Heuberger and Krenn [9]). *If*

$$\lim_{m \rightarrow \infty} \Phi^m(\Lambda) = \{0\}, \quad (11)$$

and if there are sets U and S such that $\mathcal{D} \subseteq U$, $-\mathcal{D} \subseteq U$, $U \subseteq \Phi(U)$, all elements in $S \cap \Lambda$ are singletons (have expansions of weight 1) and if

$$(\Phi^{-1}(U) + \Phi^{-w}(U) + \Phi^{-w}(U)) \cap \Lambda \subseteq S \cup \{0\},$$

then every \mathcal{D} - w -NAF is optimal.

Proof of Theorem C. Condition (11) is shown in Lemma 6.2. For the second condition, we choose $U = \Phi^w(V)$ and $S = \Phi^w(\text{int } V) \setminus \{0\}$, and we show

$$(\Phi^{-1}(V) + \Phi^{-w}(V) + \Phi^{-w}(V)) \subseteq \text{int } V.$$

Optimality then follows, since each element in $S \cap \Lambda$ has a weight 1 expansion by Lemma 6.3. So let z be an element of the left hand side of the inclusion above. Using (9) and (10) yields

$$\|z\| \leq \|\Phi^{-1}\|R + 2\|\Phi^{-1}\|^w R < r,$$

therefore z is in the interior of V . \square

REFERENCES

- [1] Roberto Maria Avanzi, *A Note on the Signed Sliding Window Integer Recoding and a Left-to-Right Analogue*, Selected Areas in Cryptography: 11th International Workshop, SAC 2004, Waterloo, Canada, August 9–10, 2004, Revised Selected Papers, Lecture Notes in Comput. Sci., vol. 3357, Springer-Verlag, Berlin, 2004, pp. 130–143.
- [2] Ian F. Blake, V. Kumar Murty, and Guangwu Xu, *Efficient algorithms for Koblitz curves over fields of characteristic three*, J. Discrete Algorithms **3** (2005), no. 1, 113–124.
- [3] ———, *A note on window τ -NAF algorithm*, Inform. Process. Lett. **95** (2005), 496–502.
- [4] ———, *Nonadjacent radix- τ expansions of integers in Euclidean imaginary quadratic number fields*, Canad. J. Math. **60** (2008), no. 6, 1267–1282.
- [5] Pierre Deligne, *La conjecture de Weil. I*, Inst. Hautes Études Sci. Publ. Math. (1974), no. 43, 273–307.
- [6] Bernard Dwork, *On the rationality of the zeta function of an algebraic variety*, Amer. J. Math. **82** (1960), 631–648.
- [7] L. Germán and A. Kovács, *On number system constructions*, Acta Math. Hungar. **115** (2007), no. 1-2, 155–167.
- [8] Clemens Heuberger and Daniel Krenn, *Analysis of width- w non-adjacent forms to imaginary quadratic bases*, arXiv:1009.0488v2 [math.NT], 2010.
- [9] ———, *Optimality of the width- w non-adjacent form: General characterisation and the case of imaginary quadratic bases*, arXiv:1110.0966v1 [math.NT], 2011.
- [10] B. Kovács and A. Pethő, *Number systems in integral domains, especially in orders of algebraic number fields*, Acta Sci. Math. (Szeged) **55** (1991), 287–299.
- [11] James A. Muir and Douglas R. Stinson, *Alternative digit sets for nonadjacent representations*, SIAM J. Discrete Math. **19** (2005), 165–191.

- [12] Jerome A. Solinas, *An improved algorithm for arithmetic on a family of elliptic curves*, Advances in Cryptology — CRYPTO '97. 17th annual international cryptology conference. Santa Barbara, CA, USA. August 17–21, 1997. Proceedings (B. S. Kaliski, jun., ed.), Lecture Notes in Comput. Sci., vol. 1294, Springer, Berlin, 1997, pp. 357–371.
- [13] ———, *Efficient arithmetic on Koblitz curves*, Des. Codes Cryptogr. **19** (2000), 195–249.
- [14] Andrew Vince, *Replicating tessellations*, SIAM J. Discrete Math. **6** (1993), no. 3, 501–521.
- [15] André Weil, *Variétés abéliennes et courbes algébriques*, Actualités scientifiques et industrielles, no. 1064, Hermann & Cie, 1948.
- [16] ———, *Numbers of solutions of equations in finite fields*, Bull. Amer. Math. Soc. **55** (1949), 497–508.
- [17] ———, *Courbes algébriques et variétés abéliennes*, Hermann, 1971.

CLEMENS HEUBERGER
INSTITUTE OF MATHEMATICS
ALPEN-ADRIA-UNIVERSITÄT
UNIVERSITÄTSSTRASSE 65–67, A-9020 KLAGENFURT AM WÖRTHERSEE, AUSTRIA

E-mail address: `clemens.heuberger@aau.at`

DANIEL KRENN
INSTITUTE OF OPTIMISATION AND DISCRETE MATHEMATICS (MATH B)
GRAZ UNIVERSITY OF TECHNOLOGY
STEYRERGASSE 30/II, A-8010 GRAZ, AUSTRIA

E-mail address: `math@danielkrenn.at` or `krenn@math.tugraz.at`