Explicit Lower Bound for the Length of Minimal Weight $\tau$-adic Expansions on Koblitz Curves

Keisuke Hakuta, Hisayoshi Sato and Tsuyoshi Takagi

Received on March 2, 2010

Abstract. Elliptic curve cryptosystems (ECC) are emerging cryptographic standards which can be used instead of RSA cryptosystems, and are practically used. In ECC, scalar multiplication (or point multiplication) is the dominant operation, namely computing an integer multiple for a given integer and a point on an elliptic curve. However, for practical use, it is a very important matter to improve the efficiency of scalar multiplication. The $\tau$-adic non-adjacent form ($\tau$-NAF) proposed by Solinas, is one of the most efficient algorithms to compute scalar multiplications on Koblitz curves. Avanzi, Heuberger, and Prodinger have proven the minimality of the Hamming weight of the $\tau$-NAF on Koblitz curves. However, the lower bound for the length of minimal Hamming weight $\tau$-adic expansions is not known yet. In this paper, we shall derive an explicit lower bound for the length of minimal Hamming weight $\tau$-adic expansions. We shall also give a new proof of the minimality of the Hamming weight of the $\tau$-NAF on Koblitz curves. Further, by using the proof of the lower bound and the new proof of the minimality, we classify a minimal length $\tau$-adic expansion with minimal Hamming weight except for two special cases. The classification shows that the $\tau$-NAF has almost minimal length among all $\tau$-adic expansions of minimal Hamming weight and we can easily convert the $\tau$-NAF into a minimal length $\tau$-adic expansion without changing the Hamming weight. This fact follows immediately from the proof of the lower bound and our new proof.

Keywords. Koblitz Curves (Anomalous Binary Curves), Scalar Multiplication, $\tau$-adic Non-Adjacent Form ($\tau$-NAF), Minimal Length

1. INTRODUCTION

Many public key cryptosystems are based on the computational complexity of number-theoretic problems (i.e. integer factoring problem, discrete logarithm problem in finite fields or elliptic curves). In such cryptosystems, number-theoretic computations are the dominant operations. The de facto standards for public-key cryptosystems are RSA cryptosystems [24], which are based on the difficulty of integer factorization. However, due to advances in algorithms to solve integer factoring problem and improvements of computing power, at least 2048 bit RSA is recommended after 2010 [21]. On the other hand, elliptic curve cryptosystems (ECC) [13], [15] which depend on the elliptic curve discrete logarithm problem, provide shorter key length and faster computation speed than those of RSA cryptosystems. For example, 224 bit ECC provides the same security level as 2048 bit RSA [21]. In ECC, scalar multiplication (or point multiplication) is the dominant operation, namely computing $dP$ from a point $P$ on an elliptic curve and $d$ is an integer, defined as the point resulting of adding $P + P + \cdots + P$, $d$ times. However, for practical use, it is a very important matter to improve the efficiency of scalar multiplication.

A common way for computing scalar multiplication is known as the double-and-add method:

$$dP = 2 \cdot 2(d_{t-1}2P + d_{t-2}P) + \cdots + d_1P + d_0P,$$

where $\sum_{i=0}^{t-1} d_i 2^i = (d_{t-1}, d_{t-2}, \ldots, d_1, d_0)_{2}$ is the binary representation of $d$. In order to improve the performance of scalar multiplication, recoding methods of scalars play an important role. Especially, number systems which have low Hamming weight and short length, are attractive to accelerate scalar multiplication, and many efficient methods have been proposed (cf. [9], [23], [27], [28]).

On the other hand, instead of integer bases, efficiently computable endomorphisms on elliptic curves (as complex numbers) bases number systems are also attractive because it can be expected that the endomorphism-and-add method is more efficient than the double-and-add method (cf. [10], [14], [20], [22], [26]). Koblitz [14] introduced a family of elliptic curves which admit especially fast scalar multiplication. These curves are called Koblitz curves $^*$ (also known as anomalous binary curves). Koblitz curves are defined by

$$E_a : y^2 = x^3 + ax^2 + 1, \quad a \in \mathbb{F}_2$$

$^*$The reason that Koblitz curves are so named is because Koblitz [14] firstly suggested that the curves are suitable for efficient implementation of ECC.

75
over a finite field $\mathbb{F}_2$. We identify \( \{0, 1\} \subset \mathbb{Z} \) with $\mathbb{F}_2$ via the natural map $f : \{0, 1\} \to \mathbb{F}_2$, $a \mapsto a \mod 2$. For some cryptographic usage, we focus on the group of $\mathbb{F}_2$-rational points $E_a(\mathbb{F}_{2^m})$ for some $m \geq 2$. In practical use, the extension degree $m$ is usually chosen to be a prime at least 163 (cf. [8]). Let $\tau$ be the Frobenius map on $E_a$,

\[
(2) \quad \tau : E_a(\mathbb{F}_{2^m}) \to E_a(\mathbb{F}_{2^{m+1}}), \quad (x, y) \mapsto (x^2, y^2).
\]

We can regard $\tau$ as a complex number which satisfies the following characteristic equation

\[
(3) \quad \tau^2 - \mu \tau + 2 = 0, \quad \text{where} \quad \mu = (1)^{1-a}.
\]

The roots of Equation (3) are $\tau = (\mu \pm \sqrt{-7})/2$, that is, the Koblitz curve has complex multiplication by $\tau$. Since the cost of the Frobenius map $\tau$ is cheaper than that of point doubling, and a scalar can be written as a $\tau$-adic expansion, the Frobenius map allows for scalar multiplication without the need for point doubling [14].

Solinas [27] proposed a low Hamming weight $\tau$-adic expansion on Koblitz curves, namely the width-$w$ $\tau$-adic non-adjacent form (w-$\tau$-NAF for short). w-$\tau$-NAF of $d \in \mathbb{Z}[\tau]$ with digit set $D_w$ is a $\tau$-adic expansion $d = \sum_{i=0}^{\ell-1} e_i \tau^i$ such that

\[
(4) \quad e_i \neq 0 \implies e_{i+w-1} = \cdots = e_{i+1} = 0
\]

and $e_i \in D_w$ for all $i$, where $D_w$ is a finite subset of the rational integer ring $\mathbb{Z}$. In this paper, we focus on the digit set of zero and the odd integers with absolute value less than $2^{w-1}$, that is, $D_w = \{0, \pm 1, \pm 3, \ldots, \pm (2^{w-1} - 1)\}$ [27]. Solinas proved some desired properties of the $\tau$-NAF with respect to the Hamming weight, namely, the $\tau$-NAF has the existence and uniqueness, and the non-zero density of the $\tau$-NAF is asymptotically $1/3$ [27]. Subsequently, Avanzi, Heuberger, and Prodinger [1] have proven the minimality of the Hamming weight of the $2$-$\tau$-NAF (or $\tau$-$\tau$-adic expansion).

The computational cost of scalar multiplication $dP$ using the $\tau$-add method with $\tau$-NAF, is approximately $O((\ell/3)A + LF)$, where $\ell$ is the length of the $\tau$-NAF of $d$, and $A, F$ stand for the computational cost of the point addition, the Frobenius map, respectively.

In order to take advantage of the efficiency of the $\tau$-NAF, it is necessary that the $\tau$-NAF has appropriate length. The length of the $\tau$-NAF of $d$ using [27, Algorithm 1] is $\log_2(N_{\mathbb{Z}[\tau]/\mathbb{Z}}(d)) = 2\log_2 d$, which is twice the length of the $\tau$-NAF of $d$. In order to circumvent the problem, Solinas [27] has developed modular reduction in $\mathbb{Z}[\tau]$. This technique is called the reduced $\tau$-NAF. By using modular reduction in $\mathbb{Z}[\tau]$, we can reduce the length $\ell$ to a maximum of $m + a$, where $a$ is the coefficient in Equation (1), and $m$ is the extension degree. However, a lower bound for the length of minimal Hamming weight $\tau$-adic expansions with digit set $\{0, \pm 1\}$, is not known yet. If the lower bound is quite small compared to the length of the $\tau$-NAF, further speed up can be achieved in the case of polynomial basis representation.

In this paper, we shall derive an explicit lower bound for the length of minimal Hamming weight $\tau$-adic expansions. Firstly, we give a lemma which will be needed in the proof of the lower bound and a new proof of the minimality of the Hamming weight of the $\tau$-NAF. Secondly, we derive an explicit lower bound for the length of minimal Hamming weight $\tau$-adic expansions based on the lemma. We also give a new proof of the minimality of the Hamming weight of the $\tau$-NAF. Further, by using the proof of lower bound and the new proof of the minimality of the Hamming weight of the $\tau$-NAF, we classify a minimal length $\tau$-adic expansion with minimal Hamming weight except for two special cases. The classification shows the following two facts. One is that the $\tau$-NAF has almost minimal length among all $\tau$-adic expansions of minimal Hamming weight with digit set $\{0, \pm 1\}$. The other is that we can easily convert the $\tau$-NAF into a minimal length $\tau$-adic expansion without changing the Hamming weight. These facts follow immediately from the proof of the lower bound and our new proof.

This paper is organized as follows. Section 2 prepares some notation. Section 3 shows a key lemma which will be needed in the proof of the lower bound and our new proof of the minimality of the Hamming weight of the $\tau$-NAF. Section 4 derives an explicit lower bound for the length of minimal Hamming weight $\tau$-adic expansions. Section 5 gives the new proof of minimality of the Hamming weight of the $\tau$-NAF on Koblitz curves. Section 6 classifies a minimal length $\tau$-adic expansion except for two special cases.

2. Notation

Throughout this paper, we use the symbols $N, \mathbb{Z}, C, \mathbb{F}_q$ to represent the natural numbers, the integers, complex numbers, and a finite field with $q$ elements respectively. Denote by $\mathbb{Z}_{\geq 0}$ the set of positive integers. For any non-zero complex number $\psi \in C \setminus \{0\}$, we denote $\psi$-adic expansion $\sum_{i=0}^{\ell-1} e_i \psi^i$ with $e_i \in \mathbb{Z}$ by $(e_\ell - 1, \ldots, e_0)_{\psi}$. The symbol $\psi$ means a non-zero digit of $\psi$-adic expansions. We denote by $E_a$ the Koblitz curve defined by Equation (1) and by $\tau$ the Frobenius map on $E_a$ defined by (2). Let $D := D_2 = \{0, \pm 1\}$. Note that for a fixed coefficient $a \in \mathbb{F}_2$ in Equation (1), it satisfies that $D = \{0, \pm \mu\}$. For any element $\alpha \in \mathbb{Z}[\tau]$, we denote by $\alpha = \sum_{i=0}^{\ell-1} b_i \tau^i$ ($b_i \in D$) the $\tau$-NAF of $\alpha$, and by $\alpha = \sum_{i=0}^{\ell-1} c_i \tau^i$ ($c_i \in D$) be any $\tau$-adic expansion of $\alpha$, respectively. The length of $\tau$-NAF of $\alpha$ is denoted by $\ell_{\tau, \text{NAF}}(\alpha)$. We denote by
\( \ell_{\min}(\alpha) \) the length of \( \tau \)-adic expansion of minimal length among all \( \tau \)-adic expansions of minimal Hamming weight with digit set \( \mathcal{D} \). Additionally, we use the following notation in Section 3 and Section 5. If \( \ell > \ell' \) then put \( c_{\ell'} = c_{\ell'+1} = \cdots = c_{\ell+1} = 0 \). Otherwise, put \( b_{\ell} = b_{\ell+1} = \cdots = b_{\ell'} = 0 \). Furthermore, replace \( \max(\ell, \ell') \) by \( \ell \) if necessary. We put \( S_\alpha := \{ i \in [0,1,\ldots,\ell-1] \mid b_i \neq 0 \} \), and \( T_{\alpha} := \{ i \in [0,1,\ldots,\ell-1] \mid c_i \neq 0 \} \).

### 3. Key Lemma

In this section, we show a key lemma (Lemma 2) which will be needed in the proof of the lower bound and the new proof. We begin with recursive formulas to convert any \( \tau \)-adic expansion into the \( \tau \)-NAF. The following lemma is useful to obtain such recursive formulas.

**Lemma 1.** Let \( \ell \in \mathbb{N} \) be a natural number. If \( \sum_{i=0}^{\ell-1} a_i \tau^i = 0 \) \((a_i \in \mathcal{D})\), then \( a_i = 0 \) for all \( i \) \((0 \leq i \leq \ell-1)\).

**Proof.** From \( \sum_{i=0}^{\ell-1} a_i \tau^i = 0 \) and \( \tau(0) \), we have \( 2a_0 \). If \( a_0 \in \mathcal{D} \), we have \( a_0 = 0 \). We put \( \alpha' := \{(\sum_{i=0}^{\ell-1} a_i \tau^i) - a_0\}/\tau \). By the same argument as above, it satisfies \( a_1 = 0 \). Similar to the case of \( a_0 \) and \( a_1 \), we also have \( a_2 = 0, \ldots, a_{\ell-1} = 0 \). Therefore \( a_i = 0 \) for all \( i \). \( \square \)

The \( \tau \)-adic expansion \( \sum_{i=0}^{\ell-1} (b_i - c_i) \tau^i \) is not necessarily \( \tau \)-adic expansion with \( \mathcal{D} \), because \( (b_i - c_i) \in \{0,\pm 1,\pm 2\} \). However, by using the following carry rules from right to left (i.e. from the least significant digit to the most significant digit), we can convert \( \sum_{i=0}^{\ell-1} (b_i - c_i) \tau^i \) into \( \tau \)-adic expansion \( \sum_{i=0}^{\ell-1} a_i \tau^i (a_i \in \mathcal{D}) \). For each \( i \in [0,1,\ldots,\ell-1] \), \( a_i \)'s are obtained by the following recursive formulas:

\begin{align}
(5) \quad a_i &= (b_i - c_i) - \mu D^*_i - 1 + D^*_i - 2 + D_i, \\
(6) \quad D^*_i &= D^*_{i-2}, \text{ for all } i,
\end{align}

where \( D^*_{i-2} \) is \( D_{i-2} \), and for all \( i \),

\begin{align}
(7) \quad D_i &= D_i/2 \text{ (} i \geq 0 \text{)}.
\end{align}

From (5) and (6), it follows that by applying Lemma 1 for \( \sum_{i=0}^{\ell-1} a_i \tau^i \), each \( a_i \) is an element in \( [0,1] \). From Lemma 1, we have \( a_i = 0 \) for all \( i \). In other words, for any \( \alpha \in \mathbb{Z}[\tau] \) and any \( \tau \)-adic expansion \( \alpha = \sum_{i=0}^{\ell-1} a_i \tau^i \) with digit set \( \mathcal{D} \), we can compute the \( \tau \)-NAF of \( \alpha (\alpha = \sum_{i=0}^{\ell-1} b_i \tau^i) \) using the recursive formulas (5), (6), and (7).

The lower bound and our new proof of the minimality of the Hamming weight of the \( \tau \)-NAF are based on the following lemma.

**Lemma 2.** [Key Lemma for Lower Bound and Our New Proof]

Let \( S := \{0,1\} \times \{0,1\} \times \{0,1\} \times \{0,1\} \times \{0,2\} \) be the direct product of four copies of \( \{0,1\} \subset \mathbb{Z} \) and \( \{0,2\} \subset \mathbb{Z} \). Let \( H_i := (b_i, c_i, D^*_{i-1}, D^*_i, D_i) \in S \) for \( 0 \leq i \leq \ell-1 \). Let \( A_1 := \{(\mu,0,0,0,0)\} \), \( A_2 := \{(\mu,0,0,-\mu,0)\} \), \( A_3 := \{(\mu,0,-1,0,-2,\mu)\} \), \( A_4 := \{(\mu,0,0,\mu,0,2,\mu)\} \) be the subset of \( S \), respectively.

(1) \( D_0 = 0 \), \( D_1 = 0 \) \((D_i = 0) \) for all \( i \).

(2) \( c_{i+1} = 0 \), \( b_{i+1} = 0 \) for some \( i \geq 0 \), then \( H_{i+1} \in A_1 \cup A_2 \cup A_3 \cup A_4 \).

(3) \( H_{i+1} \in A_1 \cup A_4 \), then \( b_i = 0, c_i \neq 0 \). If \( H_{i+1} \in A_4 \), then it holds \( b_{i+2} = 0 \) and \( c_{i+2} \neq 0 \). In particular, if \( H_i \in A_4 \), then \( H_{i+2} \notin A_1 \cup A_3 \).

(4) For \( i_0 \in \{0,1,\ldots,\ell-1\} \), the following conditions are equivalent:

(a) \( \sum_{i=0}^{\ell-1} b_i \tau^i = \sum_{i=0}^{\ell-1} c_i \tau^i \).

(b) \( D_{\ell-1} = 0 \) and \( D_0 = 0 \).

(5) Suppose that \( H_{i+1} \in A_2 \). If \( (D_{j+1}, D_j) \neq (0,0) \) for all \( j \) \((0 \leq j \leq \ell - 1)\), then \( i \geq 2 \) and

\begin{align}
(8) \quad (b_2 \ b_1 \ b_0) \in \Gamma_1,
\end{align}

or

\begin{align}
(9) \quad (b_2 \ b_1 \ b_0) \in \Gamma_2,
\end{align}

where

\begin{align}
\Gamma_1 &= \left\{ \begin{array}{cc} 0 & 0 \ 0 & 1 \end{array} \right\}, \quad \Gamma_2 = \left\{ \begin{array}{cc} 0 & 0 \ 0 & 1 \end{array} \right\}.
\end{align}

In particular, if \( (b_2 \ b_1 \ b_0) \in \left\{ \begin{array}{cc} 0 & 1 \ 0 & -1 \end{array} \right\} \subset \Gamma_2 \), holds, then \( i \geq 3 \), \( H_2 \in A_4 \), and

(10) \( (b_3 \ b_2 \ b_1 \ b_0) \in \Gamma_3 \),

where

\begin{align}
(11) \quad \Gamma_3 &= \left\{ \begin{array}{cc} 0 & 1 \ 0 & -1 \end{array} \right\}, \quad \Gamma_5 = \left\{ \begin{array}{cc} 0 & 1 \ 0 & -1 \end{array} \right\}.
\end{align}
Proof. (1) Let us assume the contrary and seek a contradiction. Suppose that there exists \(i \in \{0, 1, 2, \ldots, \ell - 1\}\) such that \(i\) does not satisfy \(D_i = 0, \pm 2,\) and \(a_i\) be the minimal such \(i \in \{0, 1, 2, \ldots, \ell - 1\}\). We evaluate the range of \(D_{i_0}\). For \(i\) which satisfies \(i \leq i_0 - 1\), we have \(D_i = 0, \pm 2 (D_i^* = 0, \pm 1)\). Then

\[
|b_{i_0} - c_{i_0} - \mu D_{i_0 - 1} + D_{i_0 - 2}^*| \\
\leq |b_{i_0}| + |c_{i_0}| + |\mu D_{i_0 - 1}| + |D_{i_0 - 2}^*| \\
\leq 1 + 1 + 1 + 1 = 4.
\]

By Equation (6), \(D_i\) is an even number, and \(|D_{i_0}| \geq 2\). There are two cases to consider, \(D_{i_0} = -4\) and \(D_{i_0} = 4\). We only consider the former because the latter may be treated similar to the former case. From \(|b_{i_0}|, |c_{i_0}| \leq 1, |D_{i_0 - 1}^*|, |D_{i_0 - 2}^*| \leq 1\), we must have \(b_{i_0} = 1, c_{i_0} = -1\), \(D_{i_0 - 1}^* = -\mu\), \(D_{i_0 - 2}^* = 1\) in order to satisfy \(0 = a_{i_0} = b_{i_0} - c_{i_0} - \mu D_{i_0 - 1}^* + D_{i_0 - 2}^* + D_i\). So \(D_{i_0 - 1} = 2D_{i_0 - 2} = -2\mu\). On the other hand, \((b_i, \ldots, b_1, b_0)\) is the \(\tau\)-NAF, so \(b_{i_0} = 1\) implies \(b_{i_0 - 1} = 0\). Hence

\[
0 = a_{i_0 - 1} = b_{i_0 - 1} - c_{i_0 - 1} - \mu D_{i_0 - 2}^* + D_{i_0 - 3}^* + D_{i_0 - 1} \\
= -c_{i_0 - 1} - \mu \ast 1 + D_{i_0 - 3}^* - 2\mu \\
= -c_{i_0 - 1} + D_{i_0 - 3}^* - 3\mu,
\]

we obtain \(c_{i_0 - 1} = D_{i_0 - 3}^* - 3\mu\). However, \(D_{i_0 - 3}^* \in \{0, \pm 1\} = \{0, \pm 1\}\), we have \(|c_{i_0 - 1}| = |D_{i_0 - 3}^* - 3\mu| \geq |D_{i_0 - 3}^* - 3\mu| \geq |D_{i_0 - 3}^* - 3\}| \geq 2\). This is a contradiction.

(2) We assume that \(c_{i + 1} = 0, b_{i + 1} = \pm \mu\). Then we have \(0 = a_{i + 1} = b_{i + 1} - c_{i + 1} = -c_{i + 1} - \mu D_{i_0}^* + D_{i}^* + D_{i + 1}\). It is necessary to treat the cases \(D_{i + 1} = 0\) and \(D_{i + 1} \neq 0\) separately.

\(\text{(Case 1)} \ D_{i + 1} = 0.\)

It is easy to see that \(H_{i + 1} \in A_1 \cup A_2.\)

\(\text{(Case 2)} \ D_{i + 1} \neq 0.\)

If the sign of \(b_{i + 1}\) is same as that of \(D_{i + 1}\), we must have \(|b_{i + 1} + D_{i + 1}| = 3\). So it does not occur that \(b_{i + 1} - \mu D_{i}^* + D_{i}^* + D_{i + 1} = 0\). Hence from \(b_{i + 1}\) and \(D_{i + 1}\) have the opposite signs, we have \(H_{i + 1} \in A_3 \cup A_4.\)

Therefore, if \(c_{i + 1} = 0, b_{i + 1} \neq 0\) then \(H_{i + 1} \in A_1 \cup A_2 \cup A_3 \cup A_4.\)

(3) First, we assume that \(H_{i + 1} \in A_1.\) Since \((b_{i}, \ldots, b_1, b_0)\) is the \(\tau\)-NAF and \(b_{i + 1} \neq 0\), we have \(b_i = 0\). We substitute \(b_i = 0\) into \(a_i = (b_i - c_i) - \mu D_{i - 1}^* + D_{i - 2} + D_i = 0\), we have \(c_i = -\mu D_{i - 1}^* + D_{i - 2} + D_i\). Since \(H_{i + 1} \in A_1\) and \(c_i = -\mu \ast 0 + D_{i - 2} = 2 = D_{i - 2}^* \neq 2 \neq 0\), we have \(c_i \neq 0\).

Next, suppose that \(H_{i + 1} \in A_1.\) Similar to the above case, since \(c_i = -\mu \ast 0 + D_{i - 2} = 2 = D_{i - 2}^* \neq 2 \neq 0\), we also have \(b_i = 0, c_i \neq 0\).

We assume that \(H_{i + 1} \in A_2.\) Since \((b_i, \ldots, b_1, b_0)\) is the \(\tau\)-NAF and \(b_{i + 1} \neq 0\), we have \(b_i \neq 0\). From \(a_{i + 2} = b_{i + 2} - c_{i + 2} - \mu D_{i + 1}^* + D_{i + 2} = 0\) and \(c_{i + 2} = \pm 1 + D_{i + 2} \neq 0\), we have \(c_{i + 2} \neq 0\). Moreover, if \(H_i \in A_4,\) from \(D_i = \mp 2\mu\), we have \(D_i^* = \mp \mu.\) Therefore it does not occur that \(H_{i + 2} \in A_1 \cup A_3.\)
A.1. In the case of \((b_2, c_2, D_2) = (1, 0, 0)\), we have \((D_1, D_2) = (0, 0)\). This is a contradiction.

Hence we obtain

\[
\begin{pmatrix}
  b_2 & b_1 & b_0 \\
  c_2 & c_1 & c_0
\end{pmatrix} \in \Gamma_1 \cup \Gamma_2,
\]

or

\[
\begin{pmatrix}
  b_3 & b_2 & b_1 & b_0 \\
  c_3 & c_2 & c_1 & c_0
\end{pmatrix} \in \Gamma_3.
\]

In particular,

\[
\begin{pmatrix}
  b_2 & b_1 & b_0 \\
  c_2 & c_1 & c_0
\end{pmatrix} = \begin{pmatrix} 0 & 0 & \ast \end{pmatrix} \cdot \begin{pmatrix} \ast & 0 & \ast \\ \ast & \ast & \ast \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 & \ast \\ \ast & \ast & \ast \end{pmatrix}.
\]

or

\[
\begin{pmatrix}
  b_3 & b_2 & b_1 & b_0 \\
  c_3 & c_2 & c_1 & c_0
\end{pmatrix} = \begin{pmatrix} 0 & 0 & \ast \end{pmatrix} \cdot \begin{pmatrix} \ast & 0 & \ast \\ \ast & \ast & \ast \end{pmatrix}.
\]

It is easy to see that \(i \geq 2\) when

\[
\begin{pmatrix}
  b_2 & b_1 & b_0 \\
  c_2 & c_1 & c_0
\end{pmatrix} \in \Gamma_1 \cup \Gamma_2,
\]

and \(i \geq 3\) when

\[
\begin{pmatrix}
  b_3 & b_2 & b_1 & b_0 \\
  c_3 & c_2 & c_1 & c_0
\end{pmatrix} \in \Gamma_3.
\]

4. LOWER BOUND FOR THE LENGTH

This section derives an explicit lower bound for the length of minimal Hamming weight \(\tau\)-adic expansions. From the definition of \(\ell_{\min}\), the following upper bound for \(\ell_{\min}\) is trivially true for all \(\alpha \in \mathbb{Z}[\tau]\):

\[
\ell_{\min}(\alpha) \leq \ell_{\text{NAF}}(\alpha).
\]

An lower bound \(\ell_{\min}\) can also be derived in terms of the length of the \(\tau\)-NAF. The following lower bound for \(\ell_{\min}\) is based on Lemma 2.

**Theorem 1.** [Lower Bound for \(\ell_{\min}(\alpha)\)]

Suppose that \(\ell' < \ell\). Then for any \(\alpha \in \mathbb{Z}[\tau]\),

\[
(12) \quad \ell_{\text{NAF}}(\alpha) - 3 = (\ell - 3) \leq \ell'.
\]

In particular,

\[
(13) \quad \ell_{\text{NAF}}(\alpha) - 3 \leq \ell_{\min}(\alpha).
\]

**Proof.** The latter part follows immediately from the former part. We show the former part. Assume that \(c_{\ell'} = 0, c_{\ell'+1} = \ldots, c_{\ell-1} = 0\). Note that \(b_{\ell-1} \neq 0\) and \(c_{\ell-1} = 0\). From Lemma 2 (2), it satisfies that \(H_{\ell-1} \in A_1 \cup A_2 \cup A_3 \cup A_4\). Since \(\sum_{i=0}^{\ell-1} b_i \tau^i = \sum_{i=0}^{\ell-1} c_i \tau^i\), we have \(D_i = 0\) for all \(i \geq \ell - 2\). It follows that \(H_{\ell-1} \notin A_1 \cup A_3 \cup A_4\). We only deal with the case of \(H_{\ell-1} \in A_2\).

There are two cases to consider, \(H_{\ell-1} = (\mu, 0, 0, -\mu, 0)\) and \(H_{\ell-1} = (-\mu, 0, 0, \mu, 0)\). Without loss of generality, we may assume that \(H_{\ell-1} = (\mu, 0, 0, -\mu, 0)\) because the latter may be treated in exactly the same way. By \(b_{\ell-1} \neq 0\), it satisfies \(b_{\ell-2} = 0\). From

\[
\begin{aligned}
a_{\ell-2} &= (b_{\ell-2} - c_{\ell-2}) - \mu D_{\ell-3} + D_{\ell-4} + D_{\ell-2} \\
&= -c_{\ell-2} + 1 + D_{\ell-4} \\
&= 0,
\end{aligned}
\]

we have \(c_{\ell-2} = D_{\ell-4} + 1\). Hence we obtain \((c_{\ell-2}, D_{\ell-4}) = (1, 0)\) or \((0, -1)\).

(Case 1) \((c_{\ell-2}, D_{\ell-4}) = (1, 0)\).

It is easy to see that \(\ell' = \ell - 1\).

(Case 2) \((c_{\ell-2}, D_{\ell-4}) = (0, -1)\).

It holds that

\[
\begin{aligned}
a_{\ell-3} &= (b_{\ell-3} - c_{\ell-3}) - \mu D_{\ell-3} + D_{\ell-5} - 2\mu \\
&= (b_{\ell-3} - c_{\ell-3}) + D_{\ell-5} - \mu \\
&= 0.
\end{aligned}
\]

So

\[
(b_{\ell-3}, c_{\ell-3}, D_{\ell-5}) = (0, 0, \mu) \in (\mu, 0, 0), \quad (\mu, 0, 0), \quad (\mu, \mu), \quad (\mu, -\mu, -\mu), \quad (-\mu, -\mu, \mu).
\]

However, if \((b_{\ell-3}, c_{\ell-3}, D_{\ell-5}) = (\mu, \mu, \mu)\) or \((-\mu, -\mu, \mu)\), then \(b_{\ell-3} \neq 0\) and \(b_{\ell-4} \neq 0\). This contradicts the fact that \(\alpha = \sum_{i=0}^{\ell-1} b_i \tau^i\) is the \(\tau\)-NAF of \(\alpha\). Therefore it does not occur that \((b_{\ell-3}, c_{\ell-3}, D_{\ell-5}) = (\mu, \mu, \mu)\) and \((-\mu, -\mu, \mu)\).

If \((b_{\ell-3}, c_{\ell-3}, D_{\ell-5}) = (0, -\mu, 0)\) or \((0, -\mu, -\mu)\), then \(\ell' = \ell - 2\).

It remains to consider the case that \((b_{\ell-3}, c_{\ell-3}, D_{\ell-5}) = (0, 0, \mu)\) and \((\mu, 0, 0)\). If \((b_{\ell-3}, c_{\ell-3}, D_{\ell-5}) = (0, 0, \mu)\), then from

\[
\begin{aligned}
a_{\ell-4} &= (b_{\ell-4} - c_{\ell-4}) - \mu D_{\ell-5} + D_{\ell-6} + D_{\ell-4} \\
&= (b_{\ell-4} - c_{\ell-4}) + D_{\ell-6} - 3 \\
&= 0,
\end{aligned}
\]

we have \((b_{\ell-4}, c_{\ell-4}, D_{\ell-6}) = (1, -1, 1)\). This indicates that \(\ell = \ell - 3\). If \((b_{\ell-3}, c_{\ell-3}, D_{\ell-5}) = (\mu, 0, 0)\), we must have \(b_{\ell-4} = 0\). Then

\[
\begin{aligned}
a_{\ell-4} &= (b_{\ell-4} - c_{\ell-4}) - \mu D_{\ell-5} + D_{\ell-6} + D_{\ell-4} \\
&= -c_{\ell-4} + D_{\ell-6} - 2 \\
&= 0.
\end{aligned}
\]

Hence we obtain \((c_{\ell-4}, D_{\ell-6}) = (-1, 1)\). Thus \(\ell' = \ell - 3\).

Combining (Case 1) and (Case 2), we obtain Inequality (12).

As already mentioned, \(\tau\)-NAF has the smallest Hamming weight with digit set \([0, \pm 1]\). Further, Theorem 1 tells us that \(\tau\)-NAF also has almost minimal length with digit set \([0, \pm 1]\).

5. OUR NEW PROOF

In this section, we give a new proof of minimality of the Hamming weight of the \(\tau\)-NAF on Koblikt curves.
5.1. The Main Idea of Our New Proof

The minimality of the Hamming weight of the $\tau$-NAF on Kubotiff curves was first proved by Avanzi, Heuberger, and Proding [1], [3]. They have presented two proofs for the minimality. One is referred as the Direct proof, which is induction on the Hamming weight. The other is referred as the Automatic proof, which is based on a weighted digraph induced by the transducer to compute the $\tau$-NAF from any $\tau$-adic expansion from right to left (see [1], [3] for proofs).

The strategy of our new proof of the minimality is as follows. For any $\alpha \in \mathbb{Z}[r]$, we directly construct an injection map from $S_\alpha$ into $T_\alpha$. Notice that if it is possible to construct an injection map from $S_\alpha$ to $T_\alpha$ for any $\alpha$ and any $\tau$-adic expansion of $\alpha$, then the Hamming weight of the $\tau$-NAF of $\alpha$ is always smaller than that of the $\tau$-adic expansion, that is, the $\tau$-NAF minimizes the Hamming weight with digit set $\{0, \pm 1\}$.

A similar strategy is already used for the proof of minimality of the Hamming weight of the generalized non-adic form (GNAF) [9]. We briefly review the strategy to prove the minimality of the Hamming weight of the GNAF. Let $r \geq 2$ be a positive integer, $\beta$ be any element of $\mathbb{Z}_{\geq 0}$. We denote by $\beta = \sum_{i=0}^{[r^n]} g_i r^i$ ($g_i \in D_\beta$) the GNAF of $\beta$, where $D_\beta = \{0, \pm 1, \ldots, \pm (r-1)\}$. Let $\beta = \sum_{i=0}^{[r^n]} h_i r^i$ ($h_i \in D_\beta$) be any $\tau$-adic expansion of $\beta$. If $\ell > \ell'$, then put $h_{\ell'} = h_{\ell'+1} = \cdots = h_{\ell-1} = 0$. Otherwise, put $g_\ell = g_{\ell+1} = \cdots = g_{\ell-1} = 0$. Furthermore, replace $\max\{\ell, \ell'\}$ by $\ell$ if necessary. We put $S_\beta := \{i \in \{0, 1, \ldots, \ell-1\} | g_i \neq 0\}$, and $T_\beta := \{i \in \{0, 1, \ldots, \ell-1\} | h_i \neq 0\}$.

Then the following claim holds.

Claim 1. [The Key Point of the Minimality [9]] If $h_{i+1} = 0$ for some $i \geq 0$, then either $g_{i+1} = 0$ or $h_i \neq 0$ and $g_i = 0$.

Thus from Claim 1, we can construct the following simple injection map.

$$\varphi_\beta : S_\beta \rightarrow T_\beta$$

\[ i \mapsto \begin{cases} 
  i & (g_i \neq 0, \ h_i \neq 0), \\
  i-1 & (g_i \neq 0, \ h_i = 0).
\end{cases} \]

We can see that Lemma 2 is analogous result for $\tau$-adic expansion.

5.2. Our New Proof

We are now in a position to give our new proof of the minimality of the Hamming weight of the $\tau$-NAF on Kubotiff curves.

Our New Proof of the Minimality.

With notation as above, we directly construct an injection map $\varphi_\alpha : S_\alpha \rightarrow T_\alpha$ for each case.

(Case 1) $H_i \not\in A_2$ for all $i (0 \leq i \leq \ell - 1)$.

We define a map $\varphi_\alpha : S_\alpha \rightarrow T_\alpha$ as follows.

$$\varphi_\alpha : S_\alpha \rightarrow T_\alpha$$

\[ i \mapsto \begin{cases} 
  i & (b_i \neq 0, \ c_i \neq 0), \\
  i-1 & (H_i \in A_1 \cup A_3), \\
  i+1 & (H_i \in A_4).
\end{cases} \]

Similarly, replace $\max\{\ell, \ell'\}$ by $\ell$ if necessary. We put $S_B := \{i \in \{0, 1, \ldots, \ell-1\} | g_i \neq 0\}$, and $T_B := \{i \in \{0, 1, \ldots, \ell-1\} | h_i \neq 0\}$.

Then the following claim holds.

Claim 2. [The Key Point of the Minimality [9]] If $h_{i+1} = 0$ for some $i \geq 0$, then either $g_{i+1} = 0$ or $h_i \neq 0$ and $g_i = 0$.

Thus from Claim 2, we can construct the following simple injection map.

$$\varphi_\beta : S_B \rightarrow T_B$$

\[ i \mapsto \begin{cases} 
  i & (g_i \neq 0, \ h_i \neq 0), \\
  i-1 & (g_i \neq 0, \ h_i = 0).
\end{cases} \]

We can see that Lemma 2 is analogous result for $\tau$-adic expansion.
6. \(\tau\)-adic Minimal Length Form

This section classifies a minimal length \(\tau\)-adic expansion with minimal Hamming weight except for two special cases. In the case of the ordinary NAF, minimal length binary representation with minimal Hamming weight is shown in [7, Corollary 3]. From Theorem 1 and our new proof, we now obtain analogous result for \(\tau\)-adic expansion. Corollary 1 shows that we can convert \(\tau\)-NAF into a minimal length \(\tau\)-adic expansion without changing the Hamming weight. This fact follows immediately from the proof of the lower bound and our new proof of the minimality of the Hamming weight of the \(\tau\)-NAF.

Corollary 1. \([\tau\text{-adic Minimal Length Expansion}]

Let \(d\) be an element of \(\mathbb{Z}[\tau]\), and \(\sum_{i=0}^{\ell-1} e_i \tau^i (e_i \in D, e_{\ell-1} \neq 0)\) be the \(\tau\)-NAF of \(d\). We convert the \(\tau\)-NAF \(d = \sum_{i=0}^{\ell-1} e_i \tau^i \) into \(d = \sum_{i=0}^{\ell-1} e'_i \tau^i (e'_i \in D, e'_{\ell-1} \neq 0)\) as follows.

\[(\ell \leq 6)\]

Table 1: Conversion of the \(\tau\)-NAF into the \(\tau\)-MLF (\(\ell \leq 6\))

<table>
<thead>
<tr>
<th>((e_{\ell-1}, \ldots, e_0)_\tau)</th>
<th>((e'<em>{\ell-1}, \ldots, e'</em>{0})_\tau)</th>
<th>(\ell)</th>
<th>(\ell')</th>
</tr>
</thead>
<tbody>
<tr>
<td>((\pm \mu, 0, 0, 1, \tau))</td>
<td>((\mp \mu, 1, 0, \tau))</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>((\pm \mu, 0, 0, 1, \tau))</td>
<td>((\pm \tau, 0, 1, \tau))</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>((\pm \mu, 0, \pm 1, \tau))</td>
<td>((\pm \tau, 0, 1, \tau))</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>((\pm \mu, 0, 0, 0, \tau))</td>
<td>((\pm \tau, 0, 0, \tau))</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>((\pm \mu, 0, 0, 0, \tau))</td>
<td>((\pm \tau, 0, 0, \tau))</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>((\pm \mu, 0, 0, 0, \tau))</td>
<td>((\pm \tau, 0, 0, \tau))</td>
<td>5</td>
<td>4</td>
</tr>
<tr>
<td>((\pm \mu, 0, 0, 0, \tau))</td>
<td>((\pm \tau, 0, 0, \tau))</td>
<td>5</td>
<td>4</td>
</tr>
<tr>
<td>((\pm \mu, 0, 0, 0, \tau))</td>
<td>((\pm \tau, 0, 0, \tau))</td>
<td>5</td>
<td>4</td>
</tr>
</tbody>
</table>

\[(\ell \geq 7)\]

\[\text{Remark 1. As described in Corollary 1, if (e_{\ell-1}, \ldots, e_0)_{\tau} = (\pm \mu, 0, \pm 1, \mp \tau)_{\tau}, then the \(\tau\)-adic expansion d = \sum_{i=0}^{\ell-1} e_i \tau^i\) is not necessarily a minimal length \(\tau\)-adic expansion with minimal Hamming weight.} \]

\[\text{For example, consider } d = -11\mu. \text{ The } \tau\text{-NAF of } d \text{ is } (\mu, 0, \mu, 0, 0, 0, \tau), \text{ and } \ell = 9. \text{ From Corollary 1, } \ell' = \ell - 2 \text{ and the } \tau\text{-MLF of } d \text{ is } (\mu, -1, 0, 0, 0, 0, -1, \tau). \]

\[\text{However, minimal length } \tau\text{-adic expansion with minimal Hamming weight of } d \text{ is } (-1, 0, 1, \mu, -1, \mu, -1, \tau) \text{ and } \ell_{\min}(d) = \ell - 3. \text{ These issues remain to be discussed.} \]

7. Conclusion

In this paper, we derived an explicit lower bound for the length of minimal Hamming weight \(\tau\)-adic expansions. We also gave a new proof of the minimality of the Hamming weight of the \(\tau\)-NAF on Koblytski curves. Further, by using the proof of the lower bound and the new proof of the minimality of the Hamming weight of the \(\tau\)-NAF, we classified a minimal length \(\tau\)-adic expansion with minimal
Hamming weight except for two special cases. The classification shows that the $\tau$-NAF has almost minimal length among all $\tau$-adic expansions of minimal Hamming weight and we can easily convert the $\tau$-NAF into a minimal length $\tau$-adic expansion without changing the Hamming weight.

ACKNOWLEDGMENTS

The authors would like to thank anonymous reviewers for their careful reading and very helpful comments on earlier versions of this manuscript.

REFERENCES


Keisuke Hakuta  
Hitachi, Ltd., Systems Development Laboratory, 292, Yoshida-cho, Totsuka-ku, Yokohama, 244-0817, Japan.  
E-mail: keisuke.hakuta.cw(at)hitachi.com

Hisayoshi Sato  
Hitachi, Ltd., Systems Development Laboratory, 292, Yoshida-cho, Totsuka-ku, Yokohama, 244-0817, Japan.  
E-mail: hisayoshi.sato.th(at)hitachi.com

Tsuyoshi Takagi  
School of Systems Information Science, Future University Hakodate, 116-2, Kameda-nakano-cho, Hakodate, 041-8655, Japan.  
E-mail: takagi(at)fun.ac.jp