Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 26 (2023), No. 2, pp. 387–402
DOI : 10.1080/09720529.2021.1925449

An alternative proof of the minimality of the Hamming weight of width-3 non-adjacent form

Keisuke Hakuta *
Institute of Science and Engineering
Academic Assembly
Shimane University
1060 Nishikawatsu-cho
Matsue
Shimane 690-8504
Japan

Tsukasa Ishikawa †
Interdisciplinary Graduate School of Science and Engineering
Shimane University
1060 Nishikawatsu-cho
Matsue
Shimane 690-8504
Japan

Abstract

In elliptic curve cryptography (ECC for short), point multiplication (or scalar multiplication) is the dominant operation. It is a very important matter to improve the efficiency of point multiplication for practical use. In ECC, recoding methods of the scalars play an important role in the performance of the algorithm used. One such example is the width-w non-adjacent form (w-NAF). Bosma (2001) proved that the Hamming weight of the NAF (2-NAF) is minimal, and Muir and Stinson (2005) proved that the Hamming weight of the w-NAF is minimal. As other examples, the generalized non-adjacent form (GNAF) and the τ -adic non-adjacent form (τ -NAF) are known. Clark and Liang (1973) proved that the Hamming weight of the GNAF is minimal by constructing an injective map. A similar strategy was adopted by Hakuta, Sato, and Takagi (2010) to prove the minimality of the Hamming weight of the τ -NAF. In this paper, we shall give an alternative proof of the

*E-mail: hakuta@cis.shimane-u.ac.jp (Corresponding Author)
†E-mail: tsukasa.ishikawa.m@gmail.com

© Taru Publications

minimality of the Hamming weight of the 3-NAF (w-NAF with $w = 3$). We also discuss that our alternative proof may not work in the case $w \geq 4$.

Subject Classification: *(2010) Primary 11A63; Secondary 11G20, 94A60.*

Keywords: *Elliptic curves, Cryptography, Hamming weight, Point multiplication (scalar multiplication), Width-w non-adjacent form (w-NAF).*

1. Introduction

Elliptic curve cryptography (ECC for short) was proposed in 1985 independently by Koblitz [10] and Miller [13]. ECC provides faster computation speed with a shorter key length. Several cryptographic protocols based on elliptic curves have been proposed (cf. [12]), and there are many discussions on ECC implementation (cf. [6]). For a given point P on an elliptic curve E and a positive integer d, the computation of $[d]P = P + \cdots + P \in E$ (d times) is called point multiplication (or scalar multiplication), and point multiplication is the dominant operation in ECC. It is a very important matter to improve the efficiency of point multiplication for practical use. In ECC, recoding methods of the scalars play an important role in the performance of the algorithm used. For example, the width-w non-adjacent form (w-NAF) is one of the most efficient algorithms of computing point multiplication. The width-2 non-adjacent form is also called the non-adjacent form (NAF). Reitwiesner showed that the Hamming weight of the NAF (2-NAF) is minimal [16]. This result was also shown by Bosma [4]. Muir and Stinson proved that the Hamming weight of the w-NAF is minimal among all 2-adic expansions with respect to the digit set of the w-NAF [15]. The generalized non-adjacent form (GNAF) and the τ-adic non-adjacent form (τ-NAF) are also recoding methods of the scalars. Clark and Liang in [5] proved that the Hamming weight of the GNAF is minimal by constructing an injective map. The minimality of the Hamming weight of the τ-NAF for Koblitz curves [11], [17] was proved by Avanzi, Heuberger, and Prodinger in [1] and [2], and by Hakuta, Sato, and Takagi in [7]. Similar discussions for hyperelliptic Koblitz curves can be found in [8]. In particular, a similar strategy was adopted by Hakuta, Sato, and Takagi in [7] to prove the minimality of the Hamming weight of the τ-NAF.

In this paper, we shall give an alternative proof of the minimality of the Hamming weight of the 3-NAF (w-NAF with $w = 3$) in [15]. Our new proof might be useful to understand whether the minimality of the Hamming weight of other NAF-like expansions (cf. [3], [14]) holds or not.

We also discuss that our alternative proof may not work in the case $w \geq 4$ (Remark 2 in Section 5).

2. Notation and mathematical preliminaries

Throughout the paper, we use the following notations. We use the symbols $\mathbb{N} := \{0,1,2,\ldots\}$, $\mathbb{N}_+ := \mathbb{N} \setminus \{0\} = \{1,2,\ldots\}$, and $\mathbb{Z}$ to represent the natural numbers, the positive integers, and the rational integer ring, respectively. For $x \in \mathbb{Z}$, we denote by $|x|$ the standard absolute value of x.

Let $\ell, \ell' \in \mathbb{N}_+$, and let w be a positive integer satisfying $w \geq 2$. Recall that a non-adjacent form (NAF) of $\alpha \in \mathbb{N}_+$ is an expression $\mathrm{NAF}(\alpha) = (b_{\ell-1}, \ldots, b_0)_2$, where $\alpha = \sum_{i=0}^{\ell-1} b_i 2^i$, $b_i \in \{0, \pm 1\}$, $b_{\ell-1} \neq 0$, and $b_i b_{i+1} = 0$ for $0 \leq i \leq \ell - 2$. Set

$$\mathcal{D}^{(w)} := \{0, \pm 1, \pm 3, \ldots, \pm(2^{w-1} - 1)\}$$

for each $w \geq 2$. For arbitrary $c \in \mathbb{N}_+ \cap \mathcal{D}^{(w)}$, we denote $-c$ by $\overline{c}$ and we sometimes denote an element of $\mathcal{D}^{(w)} \setminus \{0\} = \{\pm 1, \pm 3, \ldots, \pm(2^{w-1} - 1)\}$ by '$*$'. For a finite set $\mathcal{S}$, we denote the cardinality of $\mathcal{S}$ by $\#\mathcal{S}$. We briefly review the definition of the width-w non-adjacent form (w-NAF) and its properties.

Definition 1 ([9, Definition 3.32]) : A width-w non-adjacent form (w-NAF) of $\alpha \in \mathbb{N}_+$ is an expression

$$(b_{\ell-1}, \ldots, b_0)_2,$$

where $\alpha = \sum_{i=0}^{\ell-1} b_i 2^i$, $b_i \in \mathcal{D}^{(w)}$, $b_{\ell-1} \neq 0$, and at most one of any w consecutive digits is nonzero. The length of the w-NAF of $\alpha \in \mathbb{N}_+$ is ℓ.

For a given $\alpha \in \mathbb{N}_+$, the w-NAF of α can be efficiently computed using [9, Algorithm 3.35]. The next theorem (Theorem 1) states important properties of w-NAF, and the theorem shows desired properties for any cryptographic implementation of ECC.

Theorem 1 ([9, Theorem 3.33]) : *Let $\alpha \in \mathbb{N}_+$. Then the followings hold:*

(i) *α has a unique w-NAF denoted $\mathrm{NAF}_w(\alpha)$.*

(ii) *$\mathrm{NAF}_2(\alpha) = \mathrm{NAF}(\alpha)$.*

(iii) *The length of $\mathrm{NAF}_w(\alpha)$ is at most one more than the length of the binary representation of α.*

(iv) *The average density of nonzero digits among all width-w NAFs of length ℓ is approximately $1/(w+1)$.*

We define a 2-adic expansion with digit set $\mathcal{D}^{(w)}$ by the following definition.

Definition 2 : A 2-adic expansion with digit set $\mathcal{D}^{(w)}$ of $\alpha \in \mathbb{N}_+$ is an expression

$$(c_{\ell-1}, \ldots, c_0)_2,$$

where $\alpha = \sum_{i=0}^{\ell-1} c_i 2^i$, $c_i \in \mathcal{D}^{(w)}$ for each i $(i = 0, 1, \ldots, \ell-1)$. We call this expression $\mathcal{D}^{(w)}$-2-*adic expansion* of $\alpha \in \mathbb{N}_+$. For $\alpha \in \mathbb{N}_+$, we denote the Hamming weight of $\mathcal{D}^{(w)}$-2-adic expansion $\alpha = \sum_{i=0}^{\ell-1} c_i 2^i$ by $\mathrm{wt}((c_{\ell-1}, \ldots, c_0)_2) := \#\{i \in \{0, 1, \ldots, \ell-1\} \mid c_i \neq 0\}$.

In general, for a positive integer $\alpha \in \mathbb{N}_+$, there exists several $\mathcal{D}^{(w)}$-2-adic expansions of $\alpha \in \mathbb{N}_+$. Remark that $NAF_w(\alpha)$ is a $\mathcal{D}^{(w)}$-2-adic expansion of $\alpha \in \mathbb{N}_+$. The following example is the 3-NAF (width-3 NAF) and $\mathcal{D}^{(w)}$-2-adic expansions of $\alpha = 111321$.

Example 1 : The 3-NAF of $\alpha = 111321$ is

$$\mathrm{N}AF_w(\alpha) = (b_{15}, \ldots, b_0)_2 = (3, 0, 0, 3, 0, 0, 1, 0, 0, 3, 0, 0, 3, 0, 0, 1)_2,$$

and

$$\begin{aligned}
(c_{16}^{(1)}, \ldots, c_0^{(1)})_2 &= (1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1)_2, \\
(c_{16}^{(2)}, \ldots, c_0^{(2)})_2 &= (1, 0, 3, 0, 0, \overline{1}, 0, \overline{3}, 0, 1, 0, 3, 0, 0, 0, \overline{3}, \overline{1})_2, \\
(c_{17}^{(3)}, \ldots, c_0^{(3)})_2 &= (1, 0, 0, 0, 0, \overline{3}, \overline{3}, 0, \overline{3}, 0, 1, 0, 3, 0, 0, 0, \overline{3}, \overline{1})_2,
\end{aligned}$$

are $\mathcal{D}^{(w)}$-2-adic expansions of $\alpha = 111321$.

The next theorem (Theorem 2) states the minimality of the Hamming weight of the width-w non-adjacent form (w-NAF) among all 2-adic expansions with respect to the digit set $\mathcal{D}^{(w)}$, namely, no other $\mathcal{D}^{(w)}$-2-adic expansion has fewer Hamming weight than that of the w-NAF.

Theorem 2 ([15, Theorem 3.3]) : *Let* $\alpha \in \mathbb{N}_+$. *We assume that* $NAF_w(\alpha) = (b_{\ell-1}, \ldots, b_0)_2$ $(b_i \in \mathcal{D}^{(w)})$ *and* $(c_{\ell'-1}, \ldots, c_0)_2$ $(c_i \in \mathcal{D}^{(w)})$ *is any* $\mathcal{D}^{(w)}$-2-*adic expansion. Set* $\mathcal{S}_\alpha := \{i \in \{0, 1, \ldots, \ell-1\} \mid b_i \neq 0\}$ *and* $\mathcal{T}_\alpha := \{i \in \{0, 1, \ldots, \ell'-1\} \mid c_i \neq 0\}$. *Then, we have* $\#\mathcal{S}_\alpha \leq \#\mathcal{T}_\alpha$, *or equivalently we have* $\mathrm{wt}(\mathrm{N}AF_w(\alpha)) \leq \mathrm{wt}((c_{\ell'-1}, \ldots, c_0)_2)$.

Remark 1 : Bosma proved that for any integer $\alpha \in \mathbb{N}_+$ the NAF (2-NAF) of $\alpha \in \mathbb{N}_+$ has minimal Hamming weight [4, Proposition 2]. This result is a special case $(w = 2)$ of Theorem 2 ([15, Theorem 3.3]).

It is well-known that the point multiplication algorithm using w-NAF ([9, Algorithm 3.36]) is faster than the point multiplication algorithm using binary method ([9, Algorithm 3.26] or [9, Algorithm 3.27]). Thus, in ECC, recoding methods of the scalars play an important role in the performance of the algorithm used. In the following, we focus on Theorem 2 ([15, Theorem 3.3]) for $w = 3$.

3. Technical lemmas

In this section, we show some technical lemmas which will be needed in our alternative proof (Section 4) of the minimality of the Hamming weight of the 3-NAF among all 2-adic expansions with respect to the digit set $\mathcal{D}^{(3)}$.

Throughout the section, we assume the followings. Let $\alpha \in \mathbb{N}_+$. We assume that $\mathrm{NAF}_w(\alpha) = (b_{\ell-1}, \ldots, b_0)_2$ $(b_i \in \mathcal{D}^{(w)})$ and $(c_{\ell'-1}, \ldots, c_0)_2$ $(c_i \in \mathcal{D}^{(w)})$ is any $\mathcal{D}^{(w)}$-2-adic expansion. If $\ell > \ell'$ then put $c_{\ell'} = c_{\ell'+1} = \cdots = c_{\ell-1} = 0$. Otherwise, put $b_\ell = b_{\ell+1} = \cdots = b_{\ell'-1} = 0$. Furthermore, replace $\max\{\ell, \ell'\}$ by ℓ if necessary.

We begin with recursive formulas to convert any $\mathcal{D}^{(w)}$-2-adic expansion into the w-NAF. The following lemma is useful to obtain such recursive formulas.

Lemma 1 : *Let* $l \in \mathbb{N}_+$. *If* $\sum_{i=0}^{\ell-1} a_i 2^i = 0$ *and* $a_i \in \mathcal{D}^{(w)}$, *then we have* $a_i = 0$ *for each* i $(0 \le i \le \ell - 1)$.

Proof : We put $\alpha_0 := \sum_{i=0}^{\ell-1} a_i 2^i = 0$. Since $\alpha_0 = a_0 + (\sum_{i=1}^{\ell-1} a_i 2^i)$ and $2 \mid 0$, we have $2 \mid a_0$. By $a_0 \in \mathcal{D}^{(w)}$, we must have $a_0 = 0$. We next put $\alpha_1 := \sum_{i=1}^{\ell-1} a_i 2^i = 0$. 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 $(0 \le i \le \ell - 1)$. □

Since each coefficient $b_i - c_i$ of a 2-adic expansion $(b_{\ell-1} - c_{\ell-1}, \ldots, b_0 - c_0)_2$ satisfies $-2(2^{w-1} - 1) \le b_i - c_i \le 2(2^{w-1} - 1)$, it is not necessary that the 2-adic expansion $(b_{\ell-1} - c_{\ell-1}, \ldots, b_0 - c_0)_2$ is a $\mathcal{D}^{(w)}$-2-adic expansion. 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 the 2-adic expansion $(b_{\ell-1} - c_{\ell-1}, \ldots, b_0 - c_0)_2$ into the w-NAF $(a_{\ell''-1}, \ldots, a_0)_2$

$(a_i \in \mathcal{D}^{(w)})$ for some $\ell'' \in \mathbb{N}_+$. Furthermore, by replacing $\max\{\ell, \ell''\}$ by ℓ if necessary, one obtains the the following recursive formulas:

$$a_i = (b_i - c_i) + \gamma^*_{i-1} + \gamma_i \tag{3.1}$$

for each i $(0 \le i \le \ell - 1)$, where $\gamma^*_{-1} = 0$,

$$\gamma_i := \begin{cases} -\lfloor ((b_i - c_i) + \gamma^*_{i-1}) / 2 \rfloor \times 2, & \text{if } (b_i - c_i) + \gamma^*_{i-1} \ge 0, \\ \lfloor -((b_i - c_i) + \gamma^*_{i-1}) / 2 \rfloor \times 2, & \text{otherwise,} \end{cases} \tag{3.2}$$

for each i $(0 \le i \le \ell - 1)$, and

$$\gamma^*_i = \gamma_i / 2 \tag{3.3}$$

for each i $(0 \le i \le \ell - 1)$. By applying Equation (3.1), Equation (3.2), and Lemma 1 to $(a_{\ell-1}, \ldots, a_0)_2$ $(a_i \in \mathcal{D}^{(w)})$, it follows that $a_i \in \mathcal{D}^{(w)}$ for each i $(0 \le i \le \ell - 1)$. Then we see immediately that $a_i = 0$ for each i $(0 \le i \le \ell - 1)$. Finally, we obtain

$$(b_i - c_i) + \gamma^*_{i-1} + \gamma_i = 0 \tag{3.4}$$

for all i $(0 \le i \le \ell - 1)$.

We prove Lemma 2 on the range of γ^*_i for $w = 3$. Lemma 2 is the most important and technical part of our alternative proof in Section 4.

Lemma 2 : *Suppose that* $w = 3$. *For each* i $(0 \le i \le \ell - 1)$, *we have* $|\gamma^*_i| \le 4$ *and* $|\gamma_i| \le 8$.

Proof : Let us assume the contrary and seek a contradiction. Suppose that there exists $i \ge 0$ such that $|\gamma^*_i| > 4$, and i_0 be the minimal such $i \ge 0$ satisfying $|\gamma^*_i| > 4$, namely,

$$i_0 := \min\{i \in \{0, 1, \ldots, \ell - 1\} \mid |\gamma^*_i| > 4\}.$$

We shall find a lower bound of $|c_{i_0}|$. Since $|\gamma^*_{i_0}| > 4$ and $|\gamma_{i_0}| = 2 \times |\gamma^*_{i_0}| > 8$, we have $|\gamma^*_i| \le 4$ and $|\gamma_i| \le 8$ for all $i < i_0$. By Equation (3.4), it holds that $|\gamma_{i_0}| = |c_{i_0} - b_{i_0} - \gamma^*_{i_0-1}| \le |c_{i_0}| + |b_{i_0}| + |\gamma^*_{i_0-1}|$. By the choice of i_0 and by $|\gamma^*_{i_0-1}| \le 4$, $b_{i_0}, c_{i_0} \in \mathcal{D}^{(3)} = \{0, \pm 1, \pm 3\}$, we have

$$|\gamma_{i_0}| \le |c_{i_0}| + |b_{i_0}| + |\gamma^*_{i_0-1}| \le 3 + 3 + 4 = 10.$$

This yields that $4 < |\gamma^*_{i_0}| \leq 5$. Thus, one obtains that $|\gamma^*_{i_0}| = 5$ and $|\gamma_{i_0}| = 10$. By Equation (3.4), let us remark that $c_i = b_i + \gamma^*_{i-1} + \gamma_i$. Substituting i in the above equation into i_0 yields $|c_{i_0}| = |b_{i_0} + \gamma^*_{i_0-1} + \gamma_{i_0}|$. Then, again by the choice of i_0, we obtain $|c_{i_0}| \geq |\gamma_{i_0}| - |b_{i_0} + \gamma^*_{i_0-1}| \geq |\gamma_{i_0}| - |\gamma^*_{i_0-1}| - |b_{i_0}| \geq 10 - 4 - |b_{i_0}|$. Hence,

$$|c_{i_0}| \geq 6 - |b_{i_0}|.$$

There are two cases to consider, $b_{i_0} \neq \pm 3$ and $b_{i_0} = \pm 3$.

Case 1. $b_{i_0} \neq \pm 3$.

The inequality $0 \leq |b_{i_0}| \leq 1$ implies $|c_{i_0}| \geq 6 - |b_{i_0}| \geq 6 - 1 = 5$, which contradicts $c_{i_0} \in \mathcal{D}^{(3)}$.

Case 2. $b_{i_0} = \pm 3$.

In this case, we have $|c_{i_0}| \geq 6 - |b_{i_0}| \geq 6 - 3 = 3$. Then by $c_{i_0} \in \mathcal{D}^{(3)}$, we must have $c_{i_0} = \pm 3$. We recall that $|\gamma_{i_0}| = 10$. By Equation (3.4), it is easy to see that $\gamma^*_{i_0-1} = \pm 4$. More precisely, by Equation (3.4), we have $(b_{i_0}, c_{i_0}, \gamma^*_{i_0-1}, \gamma_{i_0}) = (3, -3, 4, -10)$ or $(-3, 3, -4, 10)$. Since substituting i in Equation (3.4) into $i_0 - 1$ yields $|c_{i_0-1}| = |b_{i_0-1} + \gamma^*_{i_0-2} + \gamma_{i_0-1}|$, we obtain $|c_{i_0-1}| \geq ||\gamma_{i_0-1}| - |b_{i_0-1} + \gamma^*_{i_0-2}||$. From the definition of the w-NAF (Definition 1), we must have $b_{i_0-1} = 0$. Thus, by $\gamma^*_{i_0-1} = \pm 4$ (or equivalently $\gamma_{i_0-1} = \mp 8$), we have $|c_{i_0-1}| \geq ||\gamma_{i_0-1}| - |b_{i_0-1} + \gamma^*_{i_0-2}|| \geq 4$, which contradicts $c_{i_0-1} \in \mathcal{D}^{(3)}$.

This concludes the proof of Lemma 2. □

Set

$$\mathcal{S}_\alpha := \{i \in \{0, 1, \ldots, \ell - 1\} \mid b_i \neq 0\},$$

and

$$\mathcal{T}_\alpha := \{i \in \{0, 1, \ldots, \ell - 1\} \mid c_i \neq 0\}.$$

By [15, Theorem 3.3], there exists an injective map $\varphi_\alpha : \mathcal{S}_\alpha \to \mathcal{T}_\alpha$ for each $\alpha \in \mathbb{N}_+$. We remark that guarantees the existence of an injective map $\varphi_\alpha : \mathcal{S}_\alpha \to \mathcal{T}_\alpha$, but does not give any explicit construction of an injective map from $\mathcal{S}_\alpha$ to $\mathcal{T}_\alpha$.

On the other hand, the generalized non-adjacent form (GNAF) and τ-NAF on Koblitz curves have the minimality of the Hamming weight [4], [5], [7]. In the proofs of the minimality of the Hamming weight of GNAF and τ-NAF, the authors construct injective maps φ_α as defined above,

respectively. A quite similar consideration can be found in [4]. Then by a similar discussion as in [4], [5], [7], we shall construct an injective map $\varphi_\alpha : \mathcal{S}_\alpha \to \mathcal{T}_\alpha$ for each $\alpha \in \mathbb{N}_+$.

In [5], [7], if $i \geq 0$ and

$$\begin{pmatrix} b_i \\ c_i \end{pmatrix} = \begin{pmatrix} * \\ * \end{pmatrix},$$

then it is defined that $\varphi_\alpha(i) := i$. In our construction of an injective map $\varphi_\alpha : \mathcal{S}_\alpha \to \mathcal{T}_\alpha$, if $i \geq 0$ and

$$\begin{pmatrix} b_i \\ c_i \end{pmatrix} = \begin{pmatrix} * \\ * \end{pmatrix},$$

then it is natural to define $\varphi_\alpha(i) := i$. Thus, in order to construct an injective map $\varphi_\alpha : \mathcal{S}_\alpha \to \mathcal{T}_\alpha$, we need only consider the case where $i \geq 0$ and

$$\begin{pmatrix} b_i \\ c_i \end{pmatrix} = \begin{pmatrix} * \\ 0 \end{pmatrix}.$$

In the following of this section, we discuss about the case where $i \geq 0$ and

$$\begin{pmatrix} b_i \\ c_i \end{pmatrix} = \begin{pmatrix} * \\ 0 \end{pmatrix}.$$

The main result of this section is to prove the next theorem (Theorem 3).

Theorem 3 : *Suppose that* $i \geq 0$ *and*

$$\begin{pmatrix} b_i \\ c_i \end{pmatrix} = \begin{pmatrix} * \\ 0 \end{pmatrix}.$$

Then one of the following three conditions holds:

(i) $i \geq 1$ *and*

$$\begin{pmatrix} b_i & b_{i-1} \\ c_i & c_{i-1} \end{pmatrix} = \begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix},$$

(ii) $i \geq 2$ *and*

$$\begin{pmatrix} b_i & b_{i-1} & b_{i-2} \\ c_i & c_{i-1} & c_{i-2} \end{pmatrix} = \begin{pmatrix} * & 0 & 0 \\ 0 & 0 & * \end{pmatrix},$$

(iii) and

$$\begin{pmatrix} b_i & b_{i-1} & b_{i-2} & b_{i-3} & b_{i-4} \\ c_i & c_{i-1} & c_{i-2} & c_{i-3} & c_{i-4} \end{pmatrix} = \begin{pmatrix} * & 0 & 0 & * & 0 \\ 0 & 0 & 0 & * & * \end{pmatrix}.$$

Proof : It follows immediately from Lemma 5 below. □

We next show Lemma 3 which will be used to prove Theorem 3.

Lemma 3 : *If* $i \geq 3$ *and*

$$\begin{pmatrix} b_i & b_{i-1} & b_{i-2} \\ c_i & c_{i-1} & c_{i-2} \end{pmatrix} = \begin{pmatrix} * & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

then we have

$$\begin{pmatrix} b_{i-3} \\ c_{i-3} \end{pmatrix} = \begin{pmatrix} * \\ * \end{pmatrix}.$$

Proof : We first show $b_{i-3} \neq 0$ by contradiction. Suppose that $b_{i-3} = 0$. By Equation (3.4), we have $|\gamma^*_{i-1}| = |c_i - b_i - \gamma_i| = |c_i - (b_i + \gamma_i)|$. This yields the inequality $|\gamma^*_{i-1}| \geq ||c_i| - |b_i + \gamma_i||$. From Lemma 2 and Equation (3.3), we must have $\gamma_i = 0, \pm 2, \pm 4, \pm 6, \pm 8$. Since $b_i = \pm 1$ or ± 3 from $b_i \neq 0$, we obtain the inequality $1 \leq |b_i + \gamma_i| \leq 11$, and hence $|\gamma^*_{i-1}| \geq ||c_i| - |b_i + \gamma_i|| \geq 1$. By $|\gamma^*_{i-1}| \geq 1$ and Equation (3.3), we have $|\gamma_{i-1}| \geq 2$. Since $|\gamma^*_{i-2}| \geq ||c_{i-1}| - |b_{i-1} + \gamma_{i-1}|| \geq 2$ from Equation (3.4), it satisfies that $|\gamma_{i-2}| \geq 4$ from Equation (3.3). By a similar way as above, we obtain $|\gamma^*_{i-3}| \geq ||c_{i-2}| - |b_{i-2} + \gamma_{i-2}|| \geq 4$, namely, $|\gamma_{i-3}| \geq 8$. Then since $b_{i-3} = 0$ and $0 \leq |c_{i-3}| \leq 3$, we must have $|\gamma^*_{i-4}| \geq ||c_{i-3}| - |b_{i-3} + \gamma_{i-3}|| \geq 5$, which contradicts Lemma 2.

Next, we prove that $c_{i-3} \neq 0$ by contradiction. Assume that $c_{i-3} = 0$. Then by a similar discussion as in the case of b_{i-3}, we can show that $c_{i-3} \neq 0$. Thus, we have $b_{i-3} \neq 0$ and $c_{i-3} \neq 0$. This concludes the proof of Lemma 3. □

Lemma 4 : *If* $i \geq 3$ *and*

$$\begin{pmatrix} b_i & b_{i-1} & b_{i-2} & b_{i-3} \\ c_i & c_{i-1} & c_{i-2} & c_{i-3} \end{pmatrix} = \begin{pmatrix} * & 0 & 0 & * \\ 0 & 0 & 0 & * \end{pmatrix},$$

then we have $i \geq 5$ *and*

$$\begin{pmatrix} b_{i-4} \\ c_{i-4} \end{pmatrix} = \begin{pmatrix} 0 \\ * \end{pmatrix}.$$

Proof : By $b_{i-3} \neq 0$ and the definition of the w-NAF (Definition 1), we have $b_{i-4} = 0$ and $b_{i-5} = 0$.

We first show $c_{i-4} \neq 0$ by contradiction. Suppose that $c_{i-4} = 0$. By a similar way as in Lemma 3, we have $|\gamma_{i-1}| \geq 2$, $|\gamma_{i-2}| \geq 4$, and $|\gamma_{i-3}| \geq 8$. The assumption that $1 \leq |b_{i-3}| \leq 3$ and $1 \leq |c_{i-3}| \leq 3$ yields the inequality $|\gamma^*_{i-4}| \geq ||c_{i-3}| - |b_{i-3} + \gamma_{i-3}|| \geq 2$. Then, we obtain $|\gamma_{i-4}| \geq 4$ from Equation (3.3). Since $b_{i-4} = 0$, we have $|\gamma^*_{i-5}| \geq ||c_{i-4}| - |b_{i-4} + \gamma_{i-4}|| = |0 - |0 + \gamma_{i-4}|| = |\gamma_{i-4}| \geq 4$ by the assumption $c_{i-4} = 0$ and Equation (3.4), and hence $|\gamma_{i-5}| \geq 8$. From $b_{i-5} = 0$ and $0 \leq |c_{i-5}| \leq 3$, it holds that $|\gamma^*_{i-6}| \geq ||c_{i-5}| - |b_{i-5} + \gamma_{i-5}|| \geq 5$, which contradicts Lemma 2. Thus, we must have $b_{i-4} = 0$ and $c_{i-4} \neq 0$.

As the statement is true for $i \geq 4$ from the above discussion, we only prove the case for $i = 5$ here. Let us assume $i = 4$ and seek a contradiction. Since $b_{i-4} = 0$, $c_{i-4} \neq 0$, and $i = 4$, we have $b_{i-4} = b_0 = 0$ and $c_{i-4} = c_0 \neq 0$. Then from $b_0 = 0$, the positive integer $\sum_{i=0}^{\ell-1} b_i 2^i$ $(b_i \in \mathcal{D}^{(3)})$ is even, and from $c_0 \neq 0$, the positive integer $\sum_{i=0}^{\ell-1} c_i 2^i$ $(c_i \in \mathcal{D}^{(3)})$ is odd. This contradicts the equation $\sum_{i=0}^{\ell-1} b_i 2^i = \sum_{i=0}^{\ell-1} c_i 2^i$. Therefore, it satisfies that $i \geq 5$. This concludes the proof of Lemma 4. □

The following result (Lemma 5) follows easily from Lemma 3 and Lemma 4.

Lemma 5 : *If* $i \geq 2$ *and*

$$\begin{pmatrix} b_i & b_{i-1} & b_{i-2} \\ c_i & c_{i-1} & c_{i-2} \end{pmatrix} = \begin{pmatrix} * & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

then we have $i \geq 5$ *and*

$$\begin{pmatrix} b_{i-3} & b_{i-4} \\ c_{i-3} & c_{i-4} \end{pmatrix} = \begin{pmatrix} * & 0 \\ * & * \end{pmatrix}.$$

Proof : Clearly one has

$$\begin{pmatrix} b_{i-3} \\ c_{i-3} \end{pmatrix} = \begin{pmatrix} * \\ * \end{pmatrix}$$

by Lemma 3. Similarly we have

$$\begin{pmatrix} b_{i-4} \\ c_{i-4} \end{pmatrix} = \begin{pmatrix} 0 \\ * \end{pmatrix}$$

by Lemma 4. Thus, we have $i \geq 5$. □

4. Alternative proof of minimality

This section provides our alternative proof of the minimality of the Hamming weight of the 3-NAF among all 2-adic expansions with respect to the digit set $\mathcal{D}^{(3)}$ using lemmas in Section 3.

Alternative proof of [15, Theorem 3.3] for $w = 3$.

Suppose that $w = 3$. Let $\alpha \in \mathbb{N}_+$ and $\mathrm{NAF}_3(\alpha) = (b_{\ell-1}, \ldots, b_0)_2$ $(b_i \in \mathcal{D}^{(3)})$. We remark that the integers $b_0, b_1, \ldots, b_{\ell-1}$ are uniquely determined by $\alpha \in \mathbb{N}_+$ and by [9, Theorem 3.33(i)]. Let $(c_{\ell'-1}, \ldots, c_0)_2$ $(c_i \in \mathcal{D}^{(3)})$ be any $\mathcal{D}^{(3)}$-2-adic expansion of α. If $\ell > \ell'$ then put $c_{\ell'} = c_{\ell'+1} = \cdots = c_{\ell-1} = 0$. Otherwise, put $b_\ell = b_{\ell+1} = \cdots = b_{\ell'-1} = 0$. Furthermore, replace $\max\{\ell, \ell'\}$ by ℓ if necessary. In other words, we assume that the length of $NAF_3(\alpha) = (b_{\ell-1}, \ldots, b_0)_2$ $(b_i \in \mathcal{D}^{(3)})$ and the $\mathcal{D}^{(3)}$-2-adic expansion $(c_{\ell-1}, \ldots, c_0)_2$ $(c_i \in \mathcal{D}^{(3)})$ are equal to each other. Set

$$\mathcal{S}_\alpha := \{i \in \{0, 1, \ldots, \ell-1\} \mid b_i \neq 0\},$$

and

$$\mathcal{T}_\alpha := \{i \in \{0, 1, \ldots, \ell-1\} \mid c_i \neq 0\}.$$

We prove [15, Theorem 3.3] for $w = 3$ by constructing an injective map $\varphi_\alpha : \mathcal{S}_\alpha \to \mathcal{T}_\alpha$ for each $\alpha \in \mathbb{N}_+$. For $0 \leq j \leq i$, we call the matrix of the form

$$\begin{pmatrix} b_i & \cdots & b_j \\ c_i & \cdots & c_j \end{pmatrix}$$

a block. Then by Theorem 3, there exist $m \in \mathbb{N}$, $i_0, i_1, \ldots, i_{m-1} \in \{0, 1, \ldots, \ell-1\}$, $j_0, j_1, \ldots, j_{m-1} \in \{0, 1, \ldots, \ell-1\}$ so that

$$i_0 \geq j_0 > i_1 \geq j_1 > \cdots > i_{m-1} \geq j_{m-1},$$

and for each k $(0 \leq k \leq m-1)$, each block

$$\begin{pmatrix} b_{i_k} & \cdots & b_{j_k} \\ c_{i_k} & \cdots & c_{j_k} \end{pmatrix}$$

has one of the following four forms:

(i) $i \geq 0$ and

$$\begin{pmatrix} b_i \\ c_i \end{pmatrix} = \begin{pmatrix} * \\ * \end{pmatrix},$$

(ii) $i \geq 1$ and

$$\begin{pmatrix} b_i & b_{i-1} \\ c_i & c_{i-1} \end{pmatrix} = \begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix},$$

(iii) $i \geq 2$ and

$$\begin{pmatrix} b_i & b_{i-1} & b_{i-2} \\ c_i & c_{i-1} & c_{i-2} \end{pmatrix} = \begin{pmatrix} * & 0 & 0 \\ 0 & 0 & * \end{pmatrix},$$

(iv) $i \geq 5$ and

$$\begin{pmatrix} b_i & b_{i-1} & b_{i-2} & b_{i-3} & b_{i-4} \\ c_i & c_{i-1} & c_{i-2} & c_{i-3} & c_{i-4} \end{pmatrix} = \begin{pmatrix} * & 0 & 0 & * & 0 \\ 0 & 0 & 0 & * & * \end{pmatrix}.$$

For each $i, j \in \mathbb{N}$ satisfying $i \geq j$, we define $\Delta_{i,j}$ as follows:

$$\Delta_{i,j} := (b_i, c_i, b_{i-1}, c_{i-1}, \ldots, b_j, c_j) \in \underbrace{\mathcal{D}^{(3)} \times \mathcal{D}^{(3)} \times \cdots \times \mathcal{D}^{(3)}}_{2(i-j+1)\ times}.$$

Furthermore, we put

$$\Delta_i := \Delta_{i,i}$$

for each i. We now define the map $\varphi_\alpha : \mathcal{S}_\alpha \to \mathcal{T}_\alpha$ as follows:

$$\begin{array}{rccl} \varphi_\alpha : & \mathcal{S}_\alpha & \to & \mathcal{T}_\alpha, \\ & i & \mapsto & i, \quad \text{if } \Delta_i = (*,*), \\ & i & \mapsto & i-1, \quad \text{if } \Delta_{i,i-1} = (*,0,0,*), \\ & i & \mapsto & i-2, \quad \text{if } \Delta_{i,i-2} = (*,0,0,0,0,*), \\ & i & \mapsto & i-4, \quad \text{if } \Delta_{i,i-4} = (*,0,0,0,0,0,*,*,0,*). \end{array}$$

By Theorem 3, the map $\varphi_\alpha : \mathcal{S}_\alpha \to \mathcal{T}_\alpha$ is injective. Thus, for any $\alpha \in \mathbb{N}_+$, the Hamming weight of the 3-NAF is minimal among all 2-adic expansions with respect to the digit set $\mathcal{D}^{(3)}$. This concludes the proof. □

Example 2 : Suppose that $w = 3$. We demonstrate our alternative proof on the three $\mathcal{D}^{(w)}$-2-adic expansions of $\alpha = 111321$ in Example 1. We define

$$\begin{aligned}
\mathcal{T}_\alpha^{(1)} &:= \{j \in \{0,1,\ldots,16\} \mid c_j^{(1)} \in \mathcal{D}^{(3)}, c_j^{(1)} \neq 0\} = \{0,3,4,6,7,9,12,13,15,16\},\\
\mathcal{T}_\alpha^{(2)} &:= \{j \in \{0,1,\ldots,16\} \mid c_j^{(2)} \in \mathcal{D}^{(3)}, c_j^{(2)} \neq 0\} = \{0,1,5,7,9,11,14,16\},\\
\mathcal{T}_\alpha^{(3)} &:= \{j \in \{0,1,\ldots,17\} \mid c_j^{(3)} \in \mathcal{D}^{(3)}, c_j^{(3)} \neq 0\} = \{0,1,5,7,9,11,12,17\}.
\end{aligned}$$

For $\alpha = 111321,$ we have

$$\mathcal{S}_\alpha = \{i \in \{0,1,\ldots,15\} \mid b_i \in \mathcal{D}^{(3)}, b_i \neq 0\} = \{0,3,6,9,12,15\}.$$

By our alternative proof, one can construct the injective maps $\varphi_\alpha^{(i)} : \mathcal{S}_\alpha \to \mathcal{T}_\alpha^{(i)}$ $(i = 1,2,3)$ as follows:

$$\begin{aligned}
\varphi_\alpha^{(1)} : \ \mathcal{S}_\alpha &\to \mathcal{T}_\alpha^{(1)},\\
0 &\mapsto 0,\\
3 &\mapsto 3,\\
6 &\mapsto 6,\\
9 &\mapsto 9,\\
12 &\mapsto 12,\\
15 &\mapsto 15,
\end{aligned}$$

$$\begin{aligned}
\varphi_\alpha^{(2)} : \ \mathcal{S}_\alpha &\to \mathcal{T}_\alpha^{(2)},\\
0 &\mapsto 0,\\
3 &\mapsto 1,\\
6 &\mapsto 5,\\
9 &\mapsto 9,\\
12 &\mapsto 11,\\
15 &\mapsto 14,
\end{aligned}$$

and

$$\begin{aligned}
\varphi_\alpha^{(3)} : \ \mathcal{S}_\alpha &\to \mathcal{T}_\alpha^{(3)},\\
0 &\mapsto 0,\\
3 &\mapsto 1,\\
6 &\mapsto 5,\\
9 &\mapsto 9,\\
12 &\mapsto 12,\\
15 &\mapsto 11.
\end{aligned}$$

5. A concluding remark

In this paper, we gave an alternative proof of the minimality of the Hamming weight of the 3-NAF (w-NAF with $w = 3$) in [15]. Our new proof might be useful to understand whether the minimality of the Hamming weight of other NAF-like expansions (cf. [3], [14]) holds or not. Further investigation is required.

Finally, we conclude the paper by mentioning why our alternative proof in Section 4 may not work in the case $w \geq 4$ in Remark 2.

Remark 2 : In Section 3, we use Lemma 2 to prove Lemma 3, Lemma 4, and Lemma 5. The most technical part in our alternative proof is Theorem 3 which is based on Lemma 3, Lemma 4, and Lemma 5. Therefore, Lemma 2 is the most important result to construct our injective map $\varphi_\alpha : \mathcal{S}_\alpha \to \mathcal{T}_\alpha$ for each $\alpha \in \mathbb{N}_+$ and any $\mathcal{D}^{(3)}$-2-adic expansion of α. To our knowledge, it remains an *open question* whether Lemma 2 holds for $w \geq 4$. We explain the reason why it may be difficult to prove Lemma 2 for $w \geq 4$.

We assume that the inequality

$$|\gamma_i^*| \leq 2^{w-1}$$

(or equivalently, $|\gamma_i| \leq 2^w$) holds for each $i\,(0 \leq i \leq \ell - 1)$ and for each $w \geq 4$. We would like to show the above inequality using the same strategy as in the proof of Lemma 2 for $w \geq 4$ by deriving a contradiction. Set

$$i_0 := \min\{i \in \{0,1,\ldots,\ell-1\} \mid |\gamma_i^*| > 2^{w-1}\}.$$

Then we have $|\gamma_{i_0}^*| > 2^{w-1}$ and $|\gamma_{i_0}| = 2 \times |\gamma_{i_0}^*| > 2^w$. In addition, we also have $|\gamma_i^*| \leq 2^{w-1}$ and $|\gamma_i| \leq 2^w$ for $i < i_0$. Since $|\gamma_{i_0}| = |c_{i_0} - b_{i_0} - \gamma_{i_0-1}^*| \leq |c_{i_0}| + |b_{i_0}| + |\gamma_{i_0-1}^*|$ and $|\gamma_{i_0-1}^*| \leq 2^{w-1}$, one can see that

$$\begin{aligned} |\gamma_{i_0}| &\leq |c_{i_0}| + |b_{i_0}| + |\gamma_{i_0-1}^*| \\ &\leq (2^{w-1}-1) + (2^{w-1}-1) + (2^{w-1}) \\ &= 3 \times 2^{w-1} - 2. \end{aligned} \tag{5.1}$$

On the other hand, by $|\gamma_{i_0}| > 2^w$, Equation (3.2), and Equation (3.3), we have

$$|\gamma_{i_0}| \geq 2^w + 2. \tag{5.2}$$

Therefore, combining Equation (5.1) and Equation (5.2) yields

$$2^w + 2 \le |\gamma_{i_0}| \le 3 \times 2^{w-1} - 2. \tag{5.3}$$

If $w = 3$, then by $2^3 + 2 = 10$ and $3 \times 2^{3-1} - 2 = 10$, we obtain $|\gamma_{i_0}| = 10$ from Equation (5.3) (see the proof of Lemma 2). However, the number of possible values of $|\gamma_{i_0}|$ grows exponentially with w. For example, the equation $|\gamma_{i_0}| = 18, 20, 22$ holds for the case $w = 4$, and the equation $|\gamma_{i_0}| = 34, 36, 38, 40, 42, 44, 46$ holds for the case $w = 5$. From the above observation, our alternative proof in Section 4 may not work in the case $w \ge 4$. It might exist a systematic way to take care of the special case $w = 4$ ($|\gamma_{i_0}| = 18, 20, 22$), but this is not clear. Further investigation will be required to give an alternative proof of the minimality of the Hamming weight of the w-NAF for $w \ge 4$ along with a similar result for Lemma 2.

Acknowledgement

The authors would like to thank the anonymous referees for their valuable comments.

References

[1] R.M. Avanzi, C. Heuberger, and H. Prodinger, Minimality of the Hamming Weight of the τ-NAF for Koblitz Curves and Improved Combination with Point Halving, In: B. Preneel, S. Tavares (eds.), Selected Areas in Cryptography – SAC 2005, Lecture Notes in Computer Science, vol. 3897 (2006), 332–344.

[2] R.M. Avanzi, C. Heuberger, and H. Prodinger, Scalar multiplication on Koblitz curves using the Frobenius endomorphism and its combination with point halving: extensions and mathematical analysis, Algorithmica 46 (2006), no. 3–4, 249–270.

[3] G. Avoine, J. Monnerat, and T. Peyrin, Advances in Alternative Non-adjacent Form Representations, In: A. Canteaut and K. Viswanathan (eds.), Progress in Cryptology – INDOCRYPT 2004, Lecture Notes in Computer Science, vol. 3348 (2004), 260–274.

[4] W. Bosma, Signed bits and fast exponentiation, J. Théor. Nombres Bordeaux 13 (2001), 27–41.

[5] W.E. Clark and J.J. Liang, On arithmetic weight for a general radix representation of integers, *IEEE Trans. Inform. Theory* 19 (1973), no. 6, 823–826.

[6] S.S. Dhanda, B. Singh, and P. Jindal, Demystifying elliptic curve cryptography: Curve selection, implementation and countermeasures to attacks, *J. Interdiscip. Math.* 23 (2020), 463–470.

[7] K. Hakuta, H. Sato, and T. Takagi, Explicit lower bound for the length of minimal weight τ-adic expansions on Koblitz curves, *J. Math-for-Ind*. 2A (2010), 75–83.

[8] K. Hakuta, H. Sato, and T. Takagi, Some properties of τ-adic expansions on hyperelliptic Koblitz curves, *J. Appl. Math. Comput.* 58 (2018), 367–388.

[9] D. Hankerson, A.J. Menezes, and S. Vanstone, Guide to elliptic curve cryptography, Springer Professional Computing, Springer, New York, NY (2004).

[10] N. Koblitz, Elliptic curve cryptosystems, Math. Comp. 48 (1987), no. 177, 203–209.

[11] N. Koblitz, CM-curves with good cryptographic properties, In: J. Feigenbaum (eds.), Advances in Cryptology – CRYPTO '91, Lecture Notes in Computer Science, vol. 576 (1992), 279–287.

[12] K.A. Kumar, A.V.N. Krishna, and K.S. Chatrapati, New secure routing protocol with elliptic curve cryptography for military heterogeneous wireless sensor networks, *Journal of Information and Optimization Sciences* 38 (2017), 341–365.

[13] V. Miller, Use of elliptic curves in cryptography, In: H.C. Williams (eds.), Advances in Cryptology – CRYPTO '85, Lecture Notes in Computer Science, vol. 218 (1986), 417–426.

[14] J.A. Muir and D.R. Stinson, Alternative digit sets for nonadjacent representations, SIAM J. Discrete Math. 19 (2005), no. 1, 165–191.

[15] J.A. Muir and D.R. Stinson, Minimality and other properties of the width-w nonadjacent form, Math. Comp. 75 (2005), no. 253, 369–384.

[16] G.W. Reitwiesner, Binary Arithmetic, Adv. Comput. 1 (1960), 231–308.

[17] J.A. Solinas, Efficient arithmetic on Koblitz curves, Des. Codes Cryptogr. 19 (2000), 195–249.

Received October, 2020

Revised February, 2021