MALAYSIAN JOURNAL OF SCIENCE
MJS
ISSN 1394-3065

VIRTUAL SYMPOSIUM ON MULTIDISCIPLINARY SCIENCE 2021 Special Issue

Malaysian Journal of Science 41 (Special Issue 1): 9-16 (September 2022) https://mjs.um.edu.my

ON SOME PATTERNS OF TNAF FOR SCALAR MULTIPLICATION OVER KOBLITZ CURVE

Faridah Yunos [1ac*], Rosimah Rosli[2b], and Norliana Muslim[3cd]

Abstract: A τ-adic non-adjacent form (TNAF) of an element α of the ring $\mathbb{Z}(\tau)$ is an expansion whereby the digits are generated by iteratively dividing α by τ, allowing the remainders of $-1, 0$ or 1. The application of TNAF as a multiplier of scalar multiplication (SM) on the Koblitz curve plays a key role in Elliptical Curve Cryptography (ECC). There are several patterns of TNAF (α) expansion in the form of $[c_0, 0, \ldots, 0, c_{l-1}]$, $[c_0, 0, \ldots, c_{\frac{l-1}{2}}, \ldots, 0, c_{l-1}]$, $2+2k$, $3+4k$, $5+4k$ and $8k_1+8k_2$ that have been produced in prior work in the literature. However, the construction of their properties based upon pyramid number formulas such as Nichomacus's theorem and Faulhaber's formula remains to be rather complex. In this work, we derive such types of TNAF in a more concise manner by applying the power of Frobenius map (τ^m) based on v-simplex and arithmetic sequences.

Keywords: *Non adjacent form, Koblitz curve, scalar multiplication.*

1. Introduction

Koblitz curves are a special type of curve for which the Frobenius endomorphism can be applied to enhance its performance of computing SM (Koblitz, 1992) in ECC. It is defined over $\boldsymbol{F_{2^m}}$ as $\boldsymbol{E_a: y^2 + xy = x^3 + ax^2 + 1}$. The Frobenius map $\boldsymbol{\tau: E_a(F_{2^m}) \to E_a(F_{2^m})}$ is defined by $\boldsymbol{\tau(x,y) = (x^2, y^2)}$ **and** $\boldsymbol{\tau(\infty) = \infty}$, where ∞ represents a point at infinity. Therefore, it satisfies the roots of the polynomial $\boldsymbol{\tau^2 - t\tau + 2}$. Since $\boldsymbol{\tau} = \frac{\boldsymbol{t+\sqrt{-7}}}{\boldsymbol{2}}$ is a quadratic integer, the set $\mathbb{Z}(\boldsymbol{\tau}) = \{\boldsymbol{r + s\tau} \mid \boldsymbol{r, s} \in \mathbb{Z}\}$ forms a ring (Heuberger & Krenn, 2013b). Suppose P and Q are points on a Koblitz curve. SM is $\boldsymbol{n}$ multiple repetitions of a point on the curve, and is denoted as $\boldsymbol{nP = P + P + \cdots + P}$, such that $\boldsymbol{nP = Q}$.

Solinas (1997) introduced a multiplier of SM in the form of TNAF on a Koblitz curve to reduce SM costs. TNAF of nonzero $\boldsymbol{\alpha = r + s\tau}$ in $\mathbb{Z}(\boldsymbol{\tau})$ can be written as TNAF $(\boldsymbol{\alpha}) = \sum_{i=0}^{l-1} \boldsymbol{c_i \tau^i}$ where $\boldsymbol{c_i} \in \{\boldsymbol{-1, 0, 1}\}$ and $\boldsymbol{c_i c_{i+1} = 0}$. If $\boldsymbol{c_{l-1} \neq 0}$, then $\boldsymbol{l}$ is assumed to be the length of TNAF. This $\boldsymbol{\alpha}$ is divisible by $\boldsymbol{\tau}$ *iff* r is even. That is, $\frac{\boldsymbol{\alpha}}{\boldsymbol{\tau}} = \left(\boldsymbol{s + \frac{tr}{2}}\right) - \frac{\boldsymbol{r}}{\boldsymbol{2}}\boldsymbol{\tau}$, where $\boldsymbol{t = (-1)^{1-a}}$ for $\boldsymbol{a} \in \{\boldsymbol{0, 1}\}$. If $\boldsymbol{\alpha}$ is not divisible by $\boldsymbol{\tau}$ (i.e., r is odd), then the remainder is chosen to be either $\boldsymbol{1}$ or $\boldsymbol{-1}$. The coefficients $\boldsymbol{c_i}$ of TNAF are generated successively by dividing $\boldsymbol{\alpha}$ with $\boldsymbol{\tau}$ until $\boldsymbol{r}$ and $\boldsymbol{s}$ are equal to 0. Since $\boldsymbol{c_i\, c_{i+1} = 0}$, the next coefficient $(\boldsymbol{c_{i+1}})$ of TNAF expansion after $\boldsymbol{c_i}$ must be 0. Furthermore, it has a unique digit representation and the average density of nonzero digits in the expansion is approximately $\frac{\boldsymbol{1}}{\boldsymbol{3}}$. The following examples describe the division process of TNAF $(\boldsymbol{1 - 2\tau})$.

Example 1.

Here we consider $\boldsymbol{n = 1 - 2\tau}$ and $\boldsymbol{\bar{\tau} = 1 - \tau}$ represent the conjugate of $\boldsymbol{\tau}$. Firstly, consider the elliptic curve $\boldsymbol{E_1}$ where $\boldsymbol{a = 1}$. Therefore, $\boldsymbol{\tau \cdot \bar{\tau} = -\tau^2 + \tau = (-\tau + 2) + \tau = 2}$ is shown. Next, the following steps are applied for finding TNAF $(\boldsymbol{n})$.

Step 1: Since $\boldsymbol{1 - 2\tau}$ is indivisible by $\boldsymbol{\tau}$, we choose $\boldsymbol{c_0 = 1}$. That is, $\frac{\boldsymbol{1-2\tau-1}}{\boldsymbol{\tau}} = \boldsymbol{-2}$. Thus, TNAF$(\boldsymbol{n}) = [\boldsymbol{1, c_1, c_2, \ldots, c_{l-2}, c_{l-1}}]$. The next coefficient $(\boldsymbol{c_1})$ must be 0.

Step 2: Since $\boldsymbol{-2}$ is divisible by $\boldsymbol{\tau}$, then $\boldsymbol{c_1 = 0}$. That is, $\frac{\boldsymbol{-2}}{\boldsymbol{\tau}} = \frac{\boldsymbol{-2}}{\boldsymbol{\tau}} \cdot \frac{\boldsymbol{\bar{\tau}}}{\boldsymbol{\bar{\tau}}} = \boldsymbol{-1 + 1\tau}$. Thus, TNAF$(\boldsymbol{n}) = [\boldsymbol{1, 0, c_2, \ldots, c_{l-2}, c_{l-1}}]$.

Step 3: Since $\boldsymbol{-1 + \tau}$ is indivisible by $\boldsymbol{\tau}$, we choose $\boldsymbol{c_2 = 1}$. That is, $\frac{\boldsymbol{-1+1\tau-1}}{\boldsymbol{\tau}} = \boldsymbol{\tau}$. Thus, TNAF$(\boldsymbol{n}) = [\boldsymbol{1, 0, 1, c_3, c_4, \ldots, c_{l-2}, c_{l-1}}]$.

Step 4: Since $\boldsymbol{\tau}$ is divisible by $\boldsymbol{\tau}$ (i.e., $\frac{\boldsymbol{\tau}}{\boldsymbol{\tau}} = \boldsymbol{1}$), then $\boldsymbol{c_3}$ is $\boldsymbol{0}$ and TNAF$(\boldsymbol{n}) = [\boldsymbol{1, 0, 1, 0, c_4, \ldots, c_{l-2}, c_{l-1}}]$.

Authors information:
[a]Department of Mathematics and Statistics, Faculty of Science, Universiti Putra Malaysia, 43400 Serdang, Selangor, Malaysia. Email: faridahy@upm.edu.my[1]
[b]Department of Mathematics, Faculty of Science, Universiti Teknologi Malaysia, 81310 Skudai, Johor Bahru, Johor, Malaysia. E-mail: cymaroslee@gmail.com[2]
[c]Laboratory of Cryptography, Analysis and Structure, Institute for Mathematical Research, 43400 Universiti Putra Malaysia, Serdang, Selangor, Malaysia.
[d]Department of Engineering, Faculty of Engineering and Life Sciences, Universiti Selangor, Jalan Timur Tambahan 45600, Bestari Jaya, Selangor, Malaysia. E-mail: norliana_muslim@unisel.edu.my[3]

*Corresponding Author: faridahy@upm.edu.my

Received: January 21, 2022
Accepted: June 4, 2022
Published: September 30, 2022

DOI: https://doi.org/10.22452/mjs.sp2022no1.2
Malaysian Journal of Science 41 (Special Issue 1): 9-16 (September 2022)

Step 5: Since $\mathbf{1}$ is indivisible by , we choose $c_4 = 1$. That is, $\frac{0}{\tau} = 0$.
Lastly, TNAF$(n) = [1, 0, 1, 0, 1] = 1 + \tau^2 + \tau^4$.

For this example, we utilized a point P in the form of polynomial basis which satisfies E_1. By choosing a certain irreducible polynomial, we can obtain the output of SM in the form of *Q*.

Solinas (2000) also considered other properties of TNAF. That is, α is divisible by τ^2 *iff* $r \equiv 2s \ (mod\ 4)$. For length $l(\alpha) > 30$ then $log_2 N(\alpha) - 0.55 < l(\alpha) < log_2 N(\alpha) + 3.52$, where $N(\alpha) = r^2 + trs + 2s^2$ is denoted as a norm of α. Besides that, he developed among the most efficient algorithms for converting TNAF in the form of $r + s\tau$ into $\sum_{i=0}^{l-1} c_i \tau^i$ as follows. This can eliminate the elliptic doublings in SM, and increase the number of addition operations.

Algorithm 1.1. (Converting $r + s\tau$ to $\sum_{i=0}^{l-1} c_i \tau^i$)
Input: integers r, s
Output: TNAF $(r + s\tau)$
Computation:

1. $c_0 \leftarrow r,\ c_1 \leftarrow s$
2. $S \leftarrow [\,]$
3. *While* $c_0 \neq 0$ *or* $c_1 \neq 0$
4. *If* c_0 *odd then*
5. $u \leftarrow 2 - (c_0 - 2c_1\ mod\ 4)$
6. $c_0 \leftarrow c_0 - u$
7. *Else*
8. $u \leftarrow 0$
9. *Prepend* u *to* S
10. $(c_0, c_1) \leftarrow (c_1 + \frac{tc_0}{2} - \frac{c_0}{2})$
11. *End While*
12. *Output* S

The detailed algorithm for SM of nP where *n* is in the form of TNAF $(r + s\tau)$ can be referred to in Algorithm 3 (see Solinas, 2000). Other concepts of TNAF for SM have also been investigated in prior research (Avanzi et al., 2007, 2011; Blake et al., 2008; Heuberger, 2010; Hakuta et al., 2010; Heuberger & Krenn, 2013a; Yunos & Atan, 2016; Yunos & Suberi, 2018.) on Koblitz curves as well as the other types of curves.

Yunos et al. (2014) introduced τ in the expression in the form of $\tau^i = b_i\, t^i + a_i t^{i+1}\, \tau$, where $a_0 = 0,\ b_0 = 1,\ a_i = a_{i-1} + b_{i-1}$ and $b_i = -2a_{i-1}$ for $i > 0$. It is based on the Lucas sequence and is useful to accelerate the process of transforming TNAF in the form of $\sum_{i=0}^{l-1} c_i \tau^i$ into $r + s\tau$ with $r = \sum_{i=0}^{l-1} c_i\ b_i\, t^i$ and $s = \sum_{i=0}^{l-1} c_i\, a_i\, t^{i+1}$ (Yunos et al., 2015a, b, c).

Based on their theory, we rewrite the conversion process developed by Suberi et al. (2018) as follows: List all the patterns of $\mathbf{TNAF}(A) = [c_0, 0, \dots, 0, c_{l-1}]$ (see Tables 1 and 2) and $\mathbf{TNAF}(B) = [c_0, 0, \dots, c_{\frac{l-1}{2}}, \dots, 0, c_{l-1}]$ for $c_0, c_{\frac{l-1}{2}}, c_{l-1} \in \{-1, 1\}$ (**see Table 3**) and describe the properties of TNAF with the least number of nonzero coefficients, as in Proposition 1.1.

Algorithm 1.2. (Converting $\sum_{i=0}^{l-1} c_i \tau^i$ to $r + s\tau$)
Input: coefficient c_i *for* $i = 0, 1, 2, \dots, l-1$ *and trace* $t = (-1)^{1-a}$ *for* $a \in \{0, 1\}$.
Output: $r + s\tau$
Computation:

1. $a_0 \leftarrow 0,\ b_0 \leftarrow 1$
2. *For i from 1 to* $l - 1$ *do*
3. $a_i \leftarrow a_{i-1} + b_{i-1}$
4. $b_i \leftarrow -2a_{i-1}$
5. $g_i \leftarrow a_i t^i$
6. $h_i \leftarrow b_i t^{i+1}$
7. *End do*
8. $r \leftarrow \sum_{i=0}^{l-1} c_i h_i$
9. $s \leftarrow \sum_{i=0}^{l-1} c_i\, g_i$
10. *Return to (r,s)*

Proposition 1.1. *Let,* $a_0 = 0$ *and* $b_0 = 1$. *If* $\tau^i = b_i\, t^i + a_i\, t^{i+1}\tau$ *for* $a_i = a_{i-1} + b_{i-1}$, $b_i = -2a_{i-1}$ *and* $t \in \{-1, 1\}$ *then*

(i) $TNAF(c_0 + c_{l-1}\ \tau^{l-1}) = (c_0 + c_{l-1}\, b_{l-1}\, t^{l-1}) + (c_{l-1}\, a_{l-1}\, t^l)\tau$

for $c_0, c_{l-1} \in \{-1, 1\}$ *and* $l \geq 3$.

(ii) $TNAF(\pm(1 + \tau^{\frac{l-1}{2}} + \tau^{l-1})) = \pm\left(\left(1 + b_{\frac{l-1}{2}}\ t^{\frac{l-1}{2}} + b_{l-1}\, t^{l-1}\right) + \left(a_{\frac{l-1}{2}}\ t^{\frac{l-1}{2}+1} + a_{l-1}\ t^l\right)\tau\right)$

for $l = 3 + 2\eta$ *with* $\eta \in \mathbb{N}$.

The following is an example for Proposition 1.1.

Example 2.
TNAF $([1, 0, 0, 0, 0, 0, 1]) = \tau^6 + 1$ in Table 1 and **TNAF** $([-1, 0, 0, 0, 0, 0, 1]) = -\tau^6 + 1$ in Table 2 can be written as $3 + 5\tau$ and $1 + 5\tau$ respectively. The converting process uses Proposition 1.1 (i) and each expansion has a density of 2/7. Meanwhile, $\mathbf{TNAF}([1, 0, 0, 1, 0, 0, 1]) = \tau^6 + \tau^3 + 1$ in Table 3 can be transformed into $1 + 4\tau$ by using Proposition 1.1 (ii) and its density 3/7.
Yunos et al. (2019) proposes other patterns of TNAF expression (see Table 4) in the form of $\mathbf{TNAF}(C) = [0, c_1, \dots, c_{l-1}]$, $\mathbf{TNAF}(D) = [-1, c_1, \dots, c_{l-1}]$, $\mathbf{TNAF}(E) = [1, c_1, \dots, c_{l-1}]$ and $\mathbf{TNAF}(F) = [0, 0, 0, c_3, c_4, \dots, c_{l-1}]$, which occur between integer γ from 1 to 21, which use Algorithm 1.1 for converting γ into TNAF(γ) (or alternatively, use Algorithm 1.2 for converting TNAF(γ) into γ).

DOI: https://doi.org/10.22452/mjs.sp2022no1.2
Malaysian Journal of Science 41 (Special Issue 1): 9-16 (September 2022)

Table 1. TNAF(A) with $c_0, c_{l-1} = \pm 1$ and $c_i = 0$ for $i = 1,2,\dots,l-2$ with its $r + s\tau$ and length, $3 \le l \le 15$.

TNAF(A)	$r + s\tau$	l	TNAF(A)	$r + s\tau$	l
$\pm[1,0,1]$	$\pm(-1+\tau)$	3	$\pm[1,0,0,0,0,0,0,0,0,1]$	$\pm(7-17\tau)$	10
$\pm[1,0,0,1]$	$\pm(-1-\tau)$	4	$\pm[1,0,0,0,0,0,0,0,0,0,1]$	$\pm(35-11\tau)$	11
$\pm[1,0,0,0,1]$	$\pm(3-3\tau)$	5	$\pm[1,0,0,0,0,0,0,0,0,0,0,1]$	$\pm(23+23\tau)$	12
$\pm[1,0,0,0,0,1]$	$\pm(7-\tau)$	6	$\pm[1,0,0,0,0,0,0,0,0,0,0,0,1]$	$\pm(-45+45\tau)$	13
$\pm[1,0,0,0,0,0,1]$	$\pm(3+5\tau)$	7	$\pm[1,0,0,0,0,0,0,0,0,0,0,0,0,1]$	$\pm(-89-\tau)$	14
$\pm[1,0,0,0,0,0,0,1$	$\pm(-9+7\tau)$	8	$\pm[1,0,0,0,0,0,0,0,0,0,0,0,0,0,1]$	$\pm(3-91\tau)$	15
$\pm[1,0,0,0,0,0,0,0,1]$	$\pm(-13-3\tau)$	9			

Table 2. TNAF(A) with $c_0 = \mp 1, c_{l-1} = \pm 1$ and $c_i = 0$ for $i = 1,2,\dots,l-2$ with its $r + s\tau$ and length, $3 \le l \le 15$.

TNAF(A)	$r + s\tau$	l	TNAF(A)	$r + s\tau$	l
$\pm[-1,0,1]$	$\pm(-3+\tau)$	3	$\pm[-1,0,0,0,0,0,0,0,0,1]$	$\pm(5-17\tau)$	10
$\pm[-1,0,0,1]$	$\pm(-3-\tau)$	4	$\pm[-1,0,0,0,0,0,0,0,0,0,1]$	$\pm(33-11\tau)$	11
$\pm[-1,0,0,0,1]$	$\pm(1-3\tau)$	5	$\pm[-1,0,0,0,0,0,0,0,0,0,0,1]$	$\pm(21+23\tau)$	12
$\pm[-1,0,0,0,0,1]$	$\pm(5-\tau)$	6	$\pm[-1,0,0,0,0,0,0,0,0,0,0,0,1]$	$\pm(-47+45\tau)$	13
$\pm[-1,0,0,0,0,0,1]$	$\pm(1+5\tau)$	7	$\pm[-1,0,0,0,0,0,0,0,0,0,0,0,0,1]$	$\pm(-91-\tau)$	14
$\pm[-1,0,0,0,0,0,0,1]$	$\pm(-11+7\tau)$	8	$\pm[-1,0,0,0,0,0,0,0,0,0,0,0,0,0,1]$	$\pm(181-89\tau)$	15
$\pm[-1,0,0,0,0,0,0,0,1]$	$\pm(-15-3\tau)$	9			

Table 3. TNAF(B) with $c_0, c_{\frac{l-1}{2}}, c_{l-1} = \pm 1$ and $c_i = 0$, $i = 1,2,\dots,l-2$ with its $r + s\tau$ and length, $l = 5,7,9,\dots,21$.

TNAF(B)	$r + s\tau$	l
$\pm[1,0,1,0,1]$	$\pm(1-2\tau)$	5
$\pm[1,0,0,1,0,0,1]$	$\pm(1+4\tau)$	7
$\pm[1,0,0,0,1,0,0,0,1]$	$\pm(-11-6\tau)$	9
$\pm[1,0,0,0,0,1,0,0,0,0,1]$	$\pm(41-12\tau)$	11
$\pm[1,0,0,0,0,0,1,0,0,0,0,0,1]$	$\pm(-43+50\tau)$	13
$\pm[1,0,0,0,0,0,0,1,0,0,0,0,0,0,1]$	$\pm(-7-84\tau)$	15
$\pm[1,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,1]$	$\pm(165+90\tau)$	17
$\pm[1,0,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,1]$	$\pm(-535+68\tau)$	19
$\pm[1,0,0,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,1]$	$\pm(949-636\tau)$	21

Table 4. TNAF(γ) for integer $1 \le \gamma \le 21$ and its HW and length (l).

γ	TNAF(γ)	HW	l	γ	TNAF(γ)	HW	l
1	$[\mathbf{1}]$	1	1	12	$[\mathbf{0,0,-1,0,-1,0,-1,0,-1}]$	4	9
2	$[\mathbf{0,-1,0,-1}]$	2	4	13	$[\mathbf{1,0,-1,0,-1,0,-1,0,-1}]$	5	9
3	$[\mathbf{-1,0,1,0,0,-1}]$	3	6	14	$[\mathbf{0,1,0,-1,0,0,-1,0,-1}]$	4	9
4	$[\mathbf{0,0,1,0,0,1}]$	2	6	15	$[\mathbf{-1,0,0,0,1,0,0,0,-1}]$	3	9
5	$[\mathbf{1,0,1,0,0,1}]$	3	6	16	$[\mathbf{0,0,0,0,1,0,0,0,-1}]$	2	9
6	$[\mathbf{0,1,0,0,0,1}]$	2	6	17	$[\mathbf{1,0,0,0,1,0,0,0,-1}]$	3	9
7	$[\mathbf{-1,0,0,-1,0,1}]$	3	6	18	$[\mathbf{0,-1,0,1,0,1,0,0,-1}]$	4	9
8	$[\mathbf{0,0,0,-1,0,1}]$	2	6	19	$[\mathbf{-1,0,1,0,-1,0,0,1,0,0,1}]$	5	11
9	$[\mathbf{1,0,0,-1,0,1}]$	3	6	20	$[\mathbf{0,0,1,0,-1,0,0,1,0,0,1}]$	4	11
10	$[\mathbf{0,-1,0,0,-1,0,-1,0,-1}]$	4	9	21	$[\mathbf{1,0,1,0,-1,0,0,1,0,0,1}]$	5	11
11	$[\mathbf{-1,0,-1,0,-1,0,-1,0,-1}]$	5	9				

DOI: https://doi.org/10.22452/mjs.sp2022no1.2
Malaysian Journal of Science 41 (Special Issue 1): 9-16 (September 2022)

Hamming Weight (HW) in Table 4 is defined as the number of nonzero coefficients in the expression of an element in $\mathbb{Z}(\tau)$ (Solinas, 2000; Yunos & Atan, 2013). The following proposition illustrates the pattern of all TNAF (γ) in this table, where γ in terms of $2+2k$, $3+4k$, $5+4k$ and $8k_1+8k_2$.

Proposition 1.2.
Let k be any integer, $k_1, k_2 \in \mathbb{N}$ and $c_i \in \{-1,0,1\}$. Then,
(i) $TNAF(2+2k) = \sum_{i=1}^{l-1} c_i \tau^i$.
(ii) $TNAF(3+4k) = -1 + \sum_{i=1}^{l-1} c_i \tau^i$.
(iii) $TNAF(5+4k) = 1 + \sum_{i=1}^{l-1} c_i \tau^i$.
(iv) $TNAF(8k_1+8k_2) = \sum_{i=3}^{l-1} c_i \tau^i$.

This study then determines the actual formula for TNAF of A-F in the form of $r+s\tau$. Hadani et al. (2019a, b) resolved this issue by applying $\tau^m = -2s_{m-1} + s_m\tau$ for $s_m = \sum_{i=1}^{m} \frac{(-2)^{i-1} t^{m-2i+1}}{(i-1)!} \prod_{j=i}^{2i-2}(m-j)$ as follows.

Proposition 1.3.
If $\tau^m = -2s_{m-1} + s_m\tau$ for $s_m = \sum_{i=1}^{m} \frac{(-2)^{i-1} t^{m-2i+1}}{(i-1)!} \prod_{j=i}^{2i-2}(m-j)$ and $t \in \{-1,1\}$, then

(i) $TNAF(c_0 + c_{l-1}\tau^{l-1}) = \left(c_0 - 2c_{l-1}\left(1 + \sum_{i=2}^{l-2} \frac{(-2)^{i-1} t^{l-1}}{(i-1)!} \prod_{j=i}^{2i-2}(l-2-j)\right)\right) + c_{l-1}\tau\left(t + \sum_{i=2}^{l-1} \frac{(-2)^{i-1} t^{l}}{(i-1)!} \prod_{j=i}^{2i-2}(l-1-j)\right)$ *for* $c_0, c_{l-1} \in \{-1,1\}$ *and* $l \geq 3$.

(ii) $TNAF(\pm\left(1+\tau^{\frac{l-1}{2}}+\tau^{l-1}\right)) = \pm\left[1 - 2\left(t^{\eta+1} + \sum_{i=2}^{\eta} \frac{(-2)^{i-1} t^{\eta+1}}{(i-1)!} \prod_{j=i}^{2i-2}(\eta-j)\right) - 2\left(1 + \sum_{i=2}^{2\eta+1} \frac{(-2)^{i-1}}{(i-1)!} \prod_{j=i}^{2i-2}(2\eta+1-j)\right) + \left(t^{\eta} + \sum_{i=2}^{1+\eta} \frac{(-2)^{i-1} t^{\eta}}{(i-1)!} \prod_{j=i}^{2i-2}(1+\eta-j) + t + \sum_{i=2}^{2+2\eta} \frac{(-2)^{i-1} t}{(i-1)!} \prod_{j=i}^{2i-2}(2+2\eta-j)\right)\tau\right]$ *for* $l = 3+2\eta$ *with integer* $\eta \geq 2$.

Proposition 1.4.
Let k be any integer, $k_1, k_2 \in \mathbb{N}$ and $c_m \in \{-1,0,1\}$. If $\tau^m = -2s_{m-1} + s_m\tau$ for $s_m = \sum_{i=1}^{m} \frac{(-2)^{i-1} t^{m-2i+1}}{(i-1)!} \prod_{j=i}^{2i-2}(m-j)$, *then*

(i) $TNAF(2+2k) = -2\sum_{m=1}^{l-1} c_m t^m \left(1 + \sum_{i=2}^{m-1} \frac{(-2)^{i-1}}{(i-1)!} \prod_{j=i}^{2i-2}(m-1-j)\right) + \tau \sum_{m=1}^{l-1} c_m t^{m+1}\left(1 + \sum_{i=2}^{m} \frac{(-2)^{i-1}}{(i-1)!} \prod_{j=i}^{2i-2}(m-j)\right)$.

(ii) $TNAF(3+4k) = -1 - 2\sum_{m=1}^{l-1} c_m t^m \left(1 + \sum_{i=2}^{m-1} \frac{(-2)^{i-1}}{(i-1)!} \prod_{j=i}^{2i-2}(m-1-j)\right) + \tau \sum_{m=1}^{l-1} c_m t^{m+1}\left(1 + \sum_{i=2}^{m} \frac{(-2)^{i-1}}{(i-1)!} \prod_{j=i}^{2i-2}(m-j)\right)$.

(iii) $TNAF(5+4k) = 1 - 2\sum_{m=1}^{l-1} c_m t^m \left(1 + \sum_{i=2}^{m-1} \frac{(-2)^{i-1}}{(i-1)!} \prod_{j=i}^{2i-2}(m-1-j)\right) + t\tau \sum_{m=1}^{l-1} c_m t^m \left(1 + \sum_{i=2}^{m} \frac{(-2)^{i-1}}{(i-1)!} \prod_{j=i}^{2i-2}(m-j)\right)$.

(iv) $TNAF(8k_1+8k_2) = -2\sum_{m=3}^{l-1} c_m t^m \left(1 + \sum_{i=2}^{m-1} \frac{(-2)^{i-1}}{(i-1)!} \prod_{j=i}^{2i-2}(m-1-j)\right) + t\tau \sum_{m=3}^{l-1} c_m t^m \left(1 + \sum_{i=2}^{m} \frac{(-2)^{i-1}}{(i-1)!} \prod_{j=i}^{2i-2}(m-j)\right)$.

However, the construction of s_m in Propositions 1.3 and 1.4 are still rather complex. They are based upon the pyramid number formula, Nichomacus's theorem and Faulhaber's formula, as described by Hadani and Yunos (2018). The primary objective of this research is to derive TNAF of A-F in a more concise form by applying $\tau^m = -2s_{m-1} + s_m\tau$, where $s_m = t^{m+1} \sum_{i=1}^{\left\lfloor \frac{m+1}{2} \right\rfloor} (-2)^{i-1} \binom{m-i}{i-1}$, which is based on v-simplex and arithmetic sequences. The detailed development of s_m can be obtained in Yunos et al. (2021).

This paper is structured as follows. In this section, we give some properties describing the patterns for TNAF of A - F (see Propositions 1.1-1.4) produced by previous researchers. In the next section, we describe the preliminaries of this study. In Section 3, we discuss how to improve Propositions 1.3 and 1.4 using a new approach, which is the main objective of this research, and describe its advantages in cryptosystems. The final chapter concludes.

2. Preliminaries

The following are propositions and algorithms that were used throughout this study.

Proposition 2.1. (Hadani et al., 2019a)
Given $\tau^m = r_m + s_m\tau$ an element of $\mathbb{Z}(\tau)$ for $m \in \mathbb{Z}^+$. Let $s_1 = 1$ and $s_2 = t$. If $f_{i_m} = \frac{(-2)^{i-1}}{(i-1)!} \prod_{j=i}^{2i-2}(m-j)$ for $2 \leq i \leq \frac{m+1}{2}$ and $m \geq 2i-1$, then $s_m = \sum_{i=1}^{\left\lfloor \frac{m+1}{2} \right\rfloor} f_{i_m} t^{m-2i+1}$ with $f_{1_m} = 1$ and $m \geq 3$. Subsequently, $r_m = -2s_{m-1}$.

Yunos et al. (2021) described an argument that $f_{i_m} = \frac{(-2)^{i-1}}{(i-1)!} \prod_{j=i}^{2i-2}(m-j)$ is equal to $\beta_{k_m} = (-2)^{k-1}\binom{m-k}{k-1}$ for $m \geq 2$. This new approach reduced the complexity of formula s_m in Proposition 2.1, and obtained a more practical formula for τ^m. That is,

$$\tau^m = -2s_{m-1} + s_m\tau = -2\sum_{k=1}^{\left\lfloor \frac{m}{2} \right\rfloor} \beta_{k_{m-1}} t^m + \tau \sum_{k=1}^{\left\lfloor \frac{m+1}{2} \right\rfloor} \beta_{k_m} t^{m+1} \quad (1)$$

DOI: https://doi.org/10.22452/mjs.sp2022no1.2
Malaysian Journal of Science 41 (Special Issue 1): 9-16 (September 2022)

The first application of using this result is TNAF (α) in the form of $r + s\tau$ can be obtained from $\sum_{m=0}^{l-1} c_m \tau^m$, and its algorithm is developed as follows:

Algorithm 2.2. Converting $\sum_{m=0}^{l-1} c_m \tau^m$ to $r + s\tau$ (Yunos et al., 2021)

Input: $t \leftarrow (-1)^{1-a}$ *for* $a \in \{0,1\}$, *all coefficients* $c_m \in \{-1,0,1\}$ *for* $m = 0,1,\ldots,l-1$.

Output: $r + s\tau$

Computation:

1. *For m from 0 to 1 do*
2. $d_m \leftarrow \tau^m$
3. *End do*
4. *For m from 2 to* $l-1$ *do*
5. $h_m \leftarrow \lfloor \frac{m}{2} \rfloor$, $g_m \leftarrow \lfloor \frac{m+1}{2} \rfloor$
6. $r_m \leftarrow t^m \sum_{k=1}^{h_m} \frac{(-2)^k (m-1-k)!}{(k-1)!\,(m-2k)!}$
7. $s_m \leftarrow t^{m+1} \sum_{k=1}^{g_m} \frac{(-2)^{k-1} (m-k)!}{(k-1)!(m-2k+1)!}$
8. $d_m \leftarrow r_m + s_m\tau$
9. *End do*
10. $r + s\tau \leftarrow \sum_{m=1}^{l-1} c_m d_m$

Therefore, it is easy to get back, for example: $1 - 2\tau$ from $1 + \tau^2 + \tau^4$ (refer to the reverse calculation in Example 1). Besides that, transforming $(\rho_0 + \rho_1\tau)\,\frac{\tau^m - 1}{\tau - 1}$ to $r + s\tau$ where τ^m, based on Equation (1), is more efficient than applying the Lucas sequence. Therefore, this can enhance the performance of the conversion process as required in TNAF of *n* modulo $(\rho_0 + \rho_1\tau)\,\frac{\tau^m - 1}{\tau - 1}$ prior to doing SM. Meanwhile, the second advantage of using Equation (1) is given in the following section.

3. Result

The following theorems improve the formulas for TNAF expansions of type A-F that were mentioned in Propositions 1.3 and 1.4.

Theorem 3.1. *If* $\tau^m = -2s_{m-1} + s_m\tau$ *for* $s_m = \sum_{k=1}^{\lfloor \frac{m+1}{2} \rfloor} \beta_{k_m} t^{m+1}$, *then*

(i) $TNAF(c_0 + c_{l-1}\tau^{l-1}) = (c_0 - 2c_{l-1}s_{l-2}) + c_{l-1}s_{l-1}\tau$ *for* $c_0, c_{l-1} \in \{-1,1\}$ **and** $l \geq 3$.

(ii) $TNAF\left(\pm\left(1 + \tau^{\frac{l-1}{2}} + \tau^{l-1}\right)\right) = \pm\left[\left(1 - 2(s_\eta + s_{2\eta+1})\right) + \left(s_{\eta+1} + s_{2\eta+2}\right)\tau\right]$ *for* $l = 3 + 2\eta$ *with integer* $\eta \geq 2$.

Proof.

Let $\tau^m = -2s_{m-1} + s_m\tau$ with $s_m = \sum_{k=1}^{\lfloor \frac{m+1}{2} \rfloor} \beta_{k_m} t^{m+1}$.

(i) By considering $m = l-1$ for $l \geq 3$, we obtain $c_0 + c_{l-1}\tau^{l-1} = c_0 + c_{l-1}(-2s_{l-2} + s_{l-1}\tau) = (c_0 - 2c_{l-1}s_{l-2}) + c_{l-1}s_{l-1}\tau$.

(ii) Suppose $l = 3 + 2\eta$ for integer $\eta \geq 2,$ thus $l - 1 = 2 + 2\eta$ *and* $\frac{l-1}{2} = 1 + \eta$.

Now, $\pm\left(1 + \tau^{\frac{l-1}{2}} + \tau^{l-1}\right) = \pm[1 + \tau^{1+\eta} + \tau^{2+2\eta}]$

$= \pm\left[\left(1 + (-2s_\eta + s_{1+\eta}\tau) + (-2s_{2\eta+1} + s_{2+2\eta}\tau)\right)\right]$

$= \pm[(1 - 2s_\eta - 2s_{2\eta+1}) + (s_{1+\eta} + s_{2+2\eta})\tau]$.

This completes the proof.

Theorem 3.2. *Let* k *be any integer,* $k_1, k_2 \in \mathbb{N}$, *and* $c_m \in \{-1,0,1\}$. *If* $\tau^m = -2s_{m-1} + s_m\tau$ for $s_m = \sum_{k=1}^{\lfloor \frac{m+1}{2} \rfloor} \beta_{k_m} t^{m+1}$, *then*

(i) *TNAF* $(2 + 2k) = -2\sum_{m=1}^{l-1} c_m s_{m-1} + \tau\sum_{m=1}^{l-1} c_m s_m$.

(ii) *TNAF* $(3 + 4k) = -1 - 2\sum_{m=1}^{l-1} c_m s_{m-1} + \tau\sum_{m=1}^{l-1} c_m s_m$.

(iii) *TNAF* $(5 + 4k) = 1 - 2\sum_{m=1}^{l-1} c_m s_{m-1} + \tau\sum_{m=1}^{l-1} c_m s_m$.

(iv) *TNAF*$(8k_1 + 8k_2) = -2\sum_{m=3}^{l-1} c_m s_{m-1} + \tau\sum_{m=3}^{l-1} c_m s_m$.

Proof.

Let $\tau^m = -2s_{m-1} + s_m\tau$ with $s_m = \sum_{k=1}^{\lfloor \frac{m+1}{2} \rfloor} \beta_{k_m} t^{m+1}$.

(i) By using Proposition 1.2 (i), we have

$\mathrm{TNAF}(2 + 2k) = \sum_{m=1}^{l-1} c_m \tau^m = -2\sum_{m=1}^{l-1} c_m s_{m-1} + \tau\sum_{m=1}^{l-1} c_m s_m$.

(ii) By using Proposition 1.2 (ii), we have

$\mathrm{TNAF}(3 + 4k) = -1 + \sum_{m=1}^{l-1} c_m \tau^m$

$= \left(-1 - 2\sum_{m=1}^{l-1} c_m s_{m-1}\right) + \tau\sum_{m=1}^{l-1} c_m s_m$.

(iii) By using Proposition 1.2 (iii), we have

$\mathrm{TNAF}(5 + 4k) = 1 + \sum_{m=1}^{l-1} c_m \tau^m$

$= \left(1 - 2\sum_{m=1}^{l-1} c_m s_{m-1}\right) + \tau\sum_{m=1}^{l-1} c_m s_m$.

(iv) By using Proposition 1.2 (iv), we have

TNAF$(8k_1 + 8k_2) = \sum_{m=3}^{l-1} c_m \tau^m = -2\sum_{m=3}^{l-1} c_m s_{m-1} + \tau\sum_{m=3}^{l-1} c_m s_m$.

This completes the proof.

Consequently, we can create another algorithm that has a similar performance to the running process with Algorithm 2.2 for converting TNAF (for example of types A and E) in the form of $\sum_{m=1}^{l-1} c_m \tau^m$ to $r + s\tau$ (refer to the formulas of *r* and *s* in Theorem 3.1 part (i) and Theorem 3.2 part (iii)) as follows:

Algorithm 3.1.

Input: $t \leftarrow (-1)^{1-a}$ *for* $a \in \{0,1\}$, *all coefficients* $c_m \in \{-1,0,1\}$ *for* $m = 1,\ldots,l-1$.

Output: $r + s\tau$

Computation:

1. *For m from 1 to* $l-1$ *do*
2. $h_m \leftarrow \lfloor \frac{m}{2} \rfloor$, $g_m \leftarrow \lfloor \frac{m+1}{2} \rfloor$
3. $r_m \leftarrow t^m \sum_{k=1}^{h_m} \frac{(-2)^k (m-1-k)!}{(k-1)!\,(m-2k)!}$
4. $s_m \leftarrow t^{m+1} \sum_{k=1}^{g_m} \frac{(-2)^{k-1} (m-k)!}{(k-1)!(m-2k+1)!}$
5. *End do*
6. $r \leftarrow 1 - 2\sum_{m=1}^{l-1} c_m s_{m-1}$
7. $s \leftarrow \sum_{m=1}^{l-1} c_m s_m$

DOI: https://doi.org/10.22452/mjs.sp2022no1.2
Malaysian Journal of Science 41 (Special Issue 1): 9-16 (September 2022)

8. *Return*$(\boldsymbol{r},\boldsymbol{s})$

Besides, Figure A1 illustrates this algorithm by applying Maple programming with a computer with an Intel(R) Core (TM) i7 processor, 8 GB RAM and a 64-bit operating system. This result is also an extension of a prior study (Suberi et al., 2016; Yunos & Suberi, 2018) to scrutinize the property of unsecure keys prior to doing SM on Koblitz Curves. Algorithm 3.1 helps Alice to list down some patterns of unsecure keys and acts as a multiplier of SM before sending a cypher text ($\boldsymbol{Q}$) to Bob. The following example is an impact of being able to identify a plain text ($\boldsymbol{P}$) by choosing some value of $\boldsymbol{r}+\boldsymbol{s\tau}$ and their TNAF and $\boldsymbol{Q}$.

TNAF	$\boldsymbol{r}+\boldsymbol{s\tau}$	$\boldsymbol{Q}=\boldsymbol{nP}$
$[\mathbf{1},\mathbf{0},\mathbf{1}]$	$-\mathbf{1}+\boldsymbol{\tau}$	$(\boldsymbol{x}^{\mathbf{2}}+\boldsymbol{x}+\mathbf{1},\mathbf{0})$
$[\mathbf{1},\mathbf{0},\mathbf{0},\mathbf{1}]$	$-\mathbf{1}-\boldsymbol{\tau}$	$(\boldsymbol{x}+\mathbf{1},\boldsymbol{x}+\mathbf{1})$
$[\mathbf{1},\mathbf{0},\mathbf{0},\mathbf{0},\mathbf{1}]$	$\mathbf{3}-\mathbf{3}\boldsymbol{\tau}$	$(\boldsymbol{x}+\mathbf{1},\mathbf{0})$
$[\mathbf{1},\mathbf{0},\mathbf{0},\mathbf{0},\mathbf{0},\mathbf{1}]$	$\mathbf{7}-\boldsymbol{\tau}$	$(\boldsymbol{x}^{\mathbf{2}}+\boldsymbol{x}+\mathbf{1},\mathbf{0})$

Although Alice sends different values of $\boldsymbol{Q}$ to Bob with different multipliers of *P*, the third parties can attack $\boldsymbol{P}=(\boldsymbol{x},\boldsymbol{x}^{\mathbf{2}}+\mathbf{1})$ easily. Therefore, such keys need to be avoided in real-world scenarios of cryptosystems.

5. Conclusion

In this work, we derive TNAF of types A-F in more concise forms by applying Equation (1), which is based on *v*-simplex and arithmetic sequences. This research can be extended by looking at the nature of such patterns such that TNAF has a low-density. Besides, their possible attacks by third parties need to be explored when implementing such kinds of expansions as secret keys.

6. Acknowledgements

This work was supported by Universiti Putra Malaysia with Putra Grants GP/ 2018/9595400 so that the study has a significant impact on the environment of ECC cryptography systems based on $\boldsymbol{\tau}$ -adic non adjacent.

7. References

Avanzi R M., Heuberger C., Prodinger H. (2007). On redundant τ-adic expansions and non-adjacent digit sets, Proceeding of the 13th International Workshop on Selected Areas in Cryptography, SAC 2006, Lecture Notes in Computer Science, Springer-Verlag 4356: 285-301.

Avanzi R M., Heuberger C., Prodinger H. (2011). Redundant τ-adic expansions I: Non-adjacent digit sets and their applications to scalar multiplication, Des. Codes Cryptography 58 (2): 173-202.

Blake I F V., Murty K., Xu G. (2008). Nonadjacent Radix-τ expansions of integers in euclidean imaginary quadratic number fields, Canadian Journal of Mathematics 60(6): 1267-1282.

Hadani N H., Yunos F. (2018). Alternative formula of τ^m in scalar multiplication on Koblitz curve, Proceeding of the 25th National Symposium on Mathematical Sciences (Sksm25), AIP Publishing, AIP Conference Proceedings 1974(1): 1-9.

Hadani N H., Yunos F., Suberi S. (2019a). On some specific patterns of τ -adic non-adjacent form expansion over ring Z (τ): An alternative formula. In AIP Conference Proceedings 2138 Issue 1; Ibrahim, H., Zulkepli J., Yaakub, A M.; AIP Publishing: 1-10.

Hadani N H., Yunos F., Kamel Arifin M R., Sapar S H. and Rahman N N A. (2019b). Alternative method to find the number of points on Koblitz curve, Malaysian Journal of Science. 13(S) August, Special Issue: The 6th International Cryptology and Information Security Conference: 13-30.

Hankerson D., Menzenes A J., Venstone S. (2006). Guide to elliptic curve cryptography, Springer Science & Business Media.

Heuberger C. (2010). Redundant τ-adic expansions II: non-optimality and chaotic behaviour, Mathematics in Computer Science 3(2):141-157.

Heuberger C., Krenn D. (2013a). Existence and optimality of w-non-adjacent forms with an algebraic integer base, Acta Mathematica Hungarica 140: 90-104.

Heuberger C., Krenn D. (2013b). Analysis of width-w non-adjacent forms to imaginary quadratic, Journal of Number Theory 133(5): 1752-1808.

Hakuta K., Sato H., Takagi T., Jarvinen K. (2010). Explicit lower bound for the length of minimal weight τ-adic expansions on Koblitz curves, Journal of Math-for-Industry 2 (2010A-7): 75-83.

Koblitz N. (1987). Elliptic curve cryptosystem, Mathematics Computation 48 (177): 203-209. https://doi.org/10.1090/S0025-5718-1987-0866109-5.

Koblitz N. (1992). CM curves with good cryptographic properties. In Advances in cryptology CRYPTO 91: Proceedings 576; Feigenbaum J.; Springer: Berlin, Heidelberg: 279-287. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.137.6778

Solinas J A. (1997). An improved algorithm for arithmetic on a family of elliptic curves, Advance in Cryptology-CRYPTO'97, 1294, Burton S., and Kaliski Jr.; Springer: Berlin, Heidelberg: 357-371.

Solinas J A. (2000). Efficient arithmetic on Koblitz curves, Kluwer Academic Publishers, Design, Codes, and Cryptography, J.A.; Springer: Boston, Massachusetts 19:

DOI: https://doi.org/10.22452/mjs.sp2022no1.2
Malaysian Journal of Science 41 (Special Issue 1): 9-16 (September 2022)

195-249. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.157.2469

Suberi S., Yunos F., Md Said M R. (2016). An even and odd situation for the multiplier of scalar multiplication with pseudo τ -adic non-adjacent form. In AIP Conference Proceedings 1750, AIP Publishing: 1-9. https://doi.org/10.1063/1.4954597

Suberi S., Yunos F., Md Said M R., Sapar S H., Said Husain Sh K. (2018). Formula of τ-adic nonadjacent form with the least number of non-zero coefficients, Jurnal Karya Asli Lorekan Ahli Matematik 11(1): 23-30.

Yunos F., Atan M K A. (2013). An average density of τ-adic naf (τ-NAF) representation: An alternative proof, Malaysian Journal of Mathematical Sciences *7*(1): 111-123.

Yunos F., Atan M K A., Md Said M R., Ariffin M R K. (2014). A reduced τ-NAF (RTNAF) representation for scalar multiplication on anomalous binary curves (ABC), Pertanika Journal of Science and Technology 22(2): 489-506.

Yunos F., Atan M K A., Md Said M R., Ariffin M R K. (2015a). Pseudo T-Adic nonadjacent form for scalar multiplication on Koblitz curves, Malaysian Journal of Mathematical Sciences 9(S) (Special Issue: The 4th International Cryptology and Information Security Conference 2014): 71-88.

Yunos F., Atan M K A., Md Said M R., Ariffin M R K. (2015b). Pseudo T-adic nonadjacent form for scalar multiplication on Koblitz curves, Conference Proceeding of the 4th International Cryptology and Information Security Conference 2014: 120-130.

Yunos F., Atan M K A., Md Said M R., Ariffin M R K. (2015c). Kembangan Pseudotnaf bagi pendaraban skalar ke atas lengkuk Koblitz, Ph.D. thesis, Universiti Putra Malaysia.

Yunos F., Atan M K A. (2016). Improvement to scalar multiplication on Koblitz curves by using Pseudo τ-adic non-adjacent form, Advances in Industrial and Applied Mathematics, Proceedings of 23rd Malaysian National Symposium of Mathematical Sciences (SKSM23), AIP Publishing 1750: 050006.

Yunos F., Suberi S. (2018). Even and odd nature for pseudo τ-adic non-adjacent form, Malaysian Journal of Science 37(2): 94-102.

Yunos F., Suberi S., Said Husain Sh K., Ariffin M R K., Asbullah M A. (2019). On some specific patterns of τ -adic non-adjacent form expansion over ring Z (τ), Journal of Engineering and Applied Sciences.

Yunos F., Mohd Yusof A., Hadani N H., Kamel Arifin M R., Sapar S H. (2021). Power of frobenius endomorphism and its performance on PseudoTNAF system, new ideas in Cryptology in Malaysian Journal of Mathematical Sciences 15(S) December: 105-121.

DOI: https://doi.org/10.22452/mjs.sp2022no1.2
Malaysian Journal of Science 41 (Special Issue 1): 9-16 (September 2022)

Appendix

$$> \; a := 1; \; c := [1, 0, 0, 0, 0, 0, 1]; \; \#\text{input } a \text{ either } 0 \text{ or } 1$$

$$l := nops(c); \#\text{length of } c$$

$$c := array(0..l-1, c); \; \#\text{need to used array since maple cannot read } c[0] \text{ directly from inpu}$$

$$t := (-1)^{1-a}; \; s[0] := 0;$$

$$\text{for } m \text{ from } 1 \text{ to } l-1 \text{ do}$$

$$g[m] := floor\left(\frac{m+1}{2}\right); \; h[m] := floor\left(\frac{m}{2}\right);$$

$$r[m] := t^{m} \cdot \left(-2 + add\left(\frac{(-2)^{k} \cdot (m-1-k)!}{(k-1)! \cdot (m-2 \cdot k)!}, k = 2..h[m]\right)\right);$$

$$\#r[m] = \sum_{k=1}^{h[m]} \frac{(-2)^{k} \cdot (m-1-k)!}{(k-1)! \cdot (m-2 \cdot k)!} \cdot t^{m}$$

$$s[m] := t^{m+1} \cdot \left(1 + add\left(\frac{(-2)^{k-1} \cdot (m-k)!}{(k-1)! \cdot (m-2 \cdot k+1)!}, k = 2..g[m]\right)\right);$$

$$\#s[m] = \sum_{k=1}^{g[m]} \frac{(-2)^{k-1} \cdot (m-k)!}{(k-1)! \cdot (m-2 \cdot k+1)!} \cdot t^{m+1}, \; s_1 = 1 \text{ and } s_2 = t$$

$$\text{end do;}$$

$$g := 1 - 2 \cdot add(c[m].(s[m-1]), m = 1..l-1);$$

$$h := add(c[m] \cdot s[m], m = 1..l-1);$$

$$\#\text{assume } g + h\tau = r + s\tau \text{ since maple cannot read the repeated used of } r \text{ and } s.$$

Figure A1. Programming for Algorithm 3.1 by Using Maple

DOI: https://doi.org/10.22452/mjs.sp2022no1.2
Malaysian Journal of Science 41 (Special Issue 1): 9-16 (September 2022)