Multiplicative Inverses Validations for Moduli Sets with Dynamic Ranges of $(5n+\beta)$-bit

INESC-ID Technical Report

Hector Pettenghi, Ricardo Chaves, and Leonel Sousa

Instituto de Engenharia de Sistemas e Computadores (INESC-ID),
PO box 1000-029, Lisbon, 1000-029, Portugal

{hector,rjfc,las}@sips.inesc-id.pt

June 4, 2012

Abstract

In this paper the multiplicative inverses proposed for the moduli set vertical extension $\{\mathbf{2^{n+\beta}}, 2^n-1, 2^n+1, 2^n-2^{\frac{n+1}{2}}+1, 2^n+2^{\frac{n+1}{2}}+1\}$ and the hybrid extension $\{\mathbf{2^{n+\beta}}, 2^n-1, 2^n+1, 2^n-2^{\frac{n+1}{2}}+1, 2^n+2^{\frac{n+1}{2}}+1, \mathbf{2^{n\pm1}+1}\}$ presented in the paper [1] are validated.

1 Multiplicative inverses validation associated to the vertical extension moduli set $\{\mathbf{2^{n+\beta}}, 2^n-1, 2^n+1, 2^n-2^{\frac{n+1}{2}}+1, 2^n+2^{\frac{n+1}{2}}+1\}$

The extension of the power of two modulus herein proposed adds a parameter β to the exponent, leading to the five moduli set $\{\mathbf{2^{n+\beta}}, 2^n-1, 2^n+1, 2^n-2^{\frac{n+1}{2}}+1, 2^n+2^{\frac{n+1}{2}}+1\}$, with n an odd integer and $n \geq 5$.

Let us consider the value of $\beta = \phi n + \xi$ with $0 \leq \phi \leq 3$, and $-\frac{(n-1)}{2} \leq \xi \leq +\frac{(n-1)}{2}$, which covers all possible integer values $-\frac{(n-1)}{2} \leq \beta \leq 3n$, to vertically extend the modulus 2^n to $2^{n+\beta}$. Let us also consider from now on that $m_1 = 2^{n+\beta}$, $m_2 = 2^n-1$, $m_3 = 2^n+1$, $m_4 = 2^n - 2^{(\frac{n+1}{2})}+1$, and $m_5 = 2^n + 2^{(\frac{n+1}{2})}+1$. With $m_2 \times m_3 = 2^{2n}-1$ and $m_4 \times m_5 = 2^{2n}+1$, resulting in a DR equal to $M = 2^{n+\beta} \times (2^{4n}-1)$, with:

$$\begin{aligned}
\hat{m}_1 =& (2^{4n}-1); \hat{m}_2 = 2^{n+\beta}(2^n+1)(2^{2n}+1);\\
\hat{m}_3 =& 2^{n+\beta}(2^n-1)(2^{2n}+1); \hat{m}_4 = 2^{n+\beta}(2^{2n}-1)(2^n+2^{\frac{n+1}{2}}+1);\\
\hat{m}_5 =& 2^{n+\beta}(2^{2n}-1)(2^n-2^{\frac{n+1}{2}}+1).
\end{aligned} \tag{1}$$

The multiplicative inverses for the moduli set $\{\mathbf{2^{n+\beta}}, 2^n-1, 2^n+1, 2^n-2^{\frac{n+1}{2}}+1, 2^n+2^{\frac{n+1}{2}}+1\}$ are shown in Table 1. The auxiliary parameter ρ in Table 1, which is used to establish the sign of some multiplicative inverses, is defined as a function of ϕ:

$$\rho = \begin{cases} 1, & \text{if } \phi \in \{0,1\} \\ -1, & \text{if } \phi \in \{2,3\}. \end{cases} \tag{2}$$

The values of the multiplicative inverses shown in Table 1 satisfies the condition:

$$\left|(\hat{m}_i) \times (\hat{m}_i^{-1})\right|_{m_i} = 1, \tag{3}$$

for $(i = 1,2,3,4,5)$, which proof is presented as follows.

Table 1: Multiplicative inverses for moduli set $\{\mathbf{2^{n+\beta}}, 2^n-1, 2^n+1, 2^n-2^{\frac{n+1}{2}}+1, 2^n+2^{\frac{n+1}{2}}+1\}$ for generic $\beta = \phi n + \xi$

Multiplicative Inverse		$-\frac{(\mathbf{n-1})}{\mathbf{2}} \leq \xi < -\mathbf{1}$	$-\mathbf{1} \leq \xi \leq \frac{(\mathbf{n-5})}{\mathbf{2}}$	$\frac{(\mathbf{n-5})}{\mathbf{2}} < \xi \leq \frac{(\mathbf{n-1})}{\mathbf{2}}$
$\lvert\hat{m}_1^{-1}\rvert_{m_1}$		$\lvert -1\rvert_{m_1}$		
$\lvert\hat{m}_2^{-1}\rvert_{m_2}$		$2^{n-2-\xi}$		
$\lvert\hat{m}_3^{-1}\rvert_{m_3}$	**for ϕ even**	$\lvert -2^{n-2-\xi}\rvert_{m_3}$		
	for ϕ odd	$2^{n-2-\xi}$		
$\lvert\hat{m}_4^{-1}\rvert_{m_4}$	**for ϕ even**	$\left\lvert \rho \cdot 2^{\frac{(n-5-2\xi)}{2}}\right\rvert_{m_4}$	$\left\lvert \rho \cdot 2^{\frac{(n-5-2\xi)}{2}}\right\rvert_{m_4}$	$\left\lvert -\rho \cdot 2^{\frac{(3n-5-2\xi)}{2}} + \rho \cdot 2^{(n-2-\xi)}\right\rvert_{m_4}$
	for ϕ odd	$\lvert -\rho \cdot 2^{(n-1-\xi)} + \rho \cdot 2^{-(\xi+2)}\rvert_{m_4}$	$\left\lvert -\rho \cdot 2^{(n-2-\xi)} + \rho \cdot 2^{\frac{(n-5-2\xi)}{2}}\right\rvert_{m_4}$	$\left\lvert -\rho \cdot 2^{\frac{(3n-5-2\xi)}{2}}\right\rvert_{m_4}$
$\lvert\hat{m}_5^{-1}\rvert_{m_5}$	**for ϕ even**	$\left\lvert -\rho \cdot 2^{\frac{(n-5-2\xi)}{2}}\right\rvert_{m_5}$	$\left\lvert -\rho \cdot 2^{\frac{(n-5-2\xi)}{2}}\right\rvert_{m_5}$	$\left\lvert \rho \cdot 2^{\frac{(3n-5-2\xi)}{2}} + \rho \cdot 2^{(n-2-\xi)}\right\rvert_{m_5}$
	for ϕ odd	$\lvert \rho \cdot 2^{(n-1-\xi)} + \rho \cdot 2^{-(\xi+2)}\rvert_{m_5}$	$\left\lvert -\rho \cdot 2^{(n-2-\xi)} - \rho \cdot 2^{\frac{(n-5-2\xi)}{2}}\right\rvert_{m_5}$	$\left\lvert \rho \cdot 2^{\frac{(3n-5-2\xi)}{2}}\right\rvert_{m_5}$

- $i = 1$:

Proof. From Table 1 is derived that $|\hat{m}_1^{-1}|_{m_1} = |-1|_{m_1}$ for all the range of ξ and ϕ. By substituting m_1, $\hat{m}_1$ and $|\hat{m}_1^{-1}|_{m_1}$ in (3):

$$\left|(2^{4n}-1)(-1)\right|_{2^{n+\beta}} = \left|-2^{4n}+1\right|_{2^{n+\beta}} = |(-1)(\overbrace{\left|2^{4n}\right|_{2^{n+\beta}}}^{=0}) + 1|_{2^{n+\beta}} = |0+1|_{2^{n+\beta}} = 1, \tag{4}$$

when $0 \leq \beta \leq 3n$. □

- $i = 2$:

Proof. From Table 1 is derived that $|\hat{m}_2^{-1}|_{m_2} = 2^{n-2-\xi}$ for all the range of ξ and ϕ. By substituting m_2, $\hat{m}_2$ and $|\hat{m}_2^{-1}|_{m_2}$ in (3):

$$\begin{aligned}\left|(2^{n+\beta})(2^n+1)(2^{2n}+1)2^{n-2-\xi}\right|_{2^n-1} &= |(2^{n+\beta})\overbrace{(|2^n|_{2^n-1}+1)}^{=+2}\overbrace{(|2^{2n}|_{2^n-1}+1)}^{=+2}2^{n-2-\xi}|_{2^n-1} = \\ &= \left|(2^{n+\beta+n-2-\xi})2^2\right|_{2^n-1} = \left|(2^{2n+n\phi+\cancel{\xi}-\cancel{2}-\cancel{\xi}+\cancel{2}})\right|_{2^n-1} = \left|(2^{2n+n\phi})\right|_{2^n-1} = 1,\end{aligned} \tag{5}$$

for all the integer values of $0 \leq \phi \leq 3$. □

- $i = 3$:

Proof. From Table 1 is derived that $|\hat{m}_3^{-1}|_{m_3} = |-2^{n-2-\xi}|_{m_3}$ for all the range of ξ, being ϕ an even number, $\phi = 0$ or $\phi = 2$. By substituting m_3, $\hat{m}_3$ and $|\hat{m}_3^{-1}|_{m_3}$ in (3):

$$\begin{aligned}\left|(2^{n+\beta})(2^n-1)(2^{2n}+1)(-2^{n-2-\xi})\right|_{2^n+1} &= |(2^{n+\beta})\overbrace{(|2^n|_{2^n+1}-1)}^{=-2}\overbrace{(|2^{2n}|_{2^n+1}+1)}^{=+2}(-2^{n-2-\xi})|_{2^n+1} = \\ &= \left|(2^{n+\beta+n-2-\xi})2^2\right|_{2^n+1} = \left|(2^{2n+n\phi+\cancel{\xi}-\cancel{2}-\cancel{\xi}+\cancel{2}})\right|_{2^n+1} = \left|(2^{2n+n\phi})\right|_{2^n+1} = 1,\end{aligned} \tag{6}$$

which is true for even values of $(2+\phi)$. Therefore, for even values of ϕ the proof is given by (6). □

Proof. From Table 1 is derived that $|\hat{m}_3^{-1}|_{m_3} = 2^{n-2-\xi}$ for all the range of ξ, being ϕ an odd number, $\phi = 1$ or $\phi = 3$. By substituting m_3, $\hat{m}_3$ and $|\hat{m}_3^{-1}|_{m_3}$ in (3):

$$\begin{aligned}\left|(2^{n+\beta})(2^n-1)(2^{2n}+1)(2^{n-2-\xi})\right|_{2^n+1} &= |(2^{n+\beta})\overbrace{(|2^n|_{2^n+1}-1)}^{=-2}\overbrace{(|2^{2n}|_{2^n+1}+1)}^{=+2}(2^{n-2-\xi})|_{2^n+1} = \\ &= \left|-(2^{n+\beta+n-2-\xi})2^2\right|_{2^n+1} = \left|(-2^{2n+n\phi+\cancel{\xi}-\cancel{2}-\cancel{\xi}+\cancel{2}})\right|_{2^n+1} = \left|(-1)(2^{2n+n\phi})\right|_{2^n+1} = 1,\end{aligned} \tag{7}$$

which is true for odd values of $(2+\phi)$. Therefore, for odd values of ϕ the proof is given by (7). □

- $i = 4$:

Proof. From Table 1 is derived that $|\hat{m}_4^{-1}|_{m_4} = |\rho \cdot 2^{\frac{n-5-2\xi}{2}}|_{m_4}$ for $-\frac{(n-1)}{2} \leq \xi \leq \frac{n-5}{2}$, and being ϕ an even number, $\phi = 0$ or $\phi = 2$. By substituting m_4, $\hat{m}_4$ and $|\hat{m}_4^{-1}|_{m_4}$ in (3):

$$\Big|(2^{n+\beta})(2^{2n}-1)(2^n+2^{\frac{n+1}{2}}+1)(\rho \cdot 2^{\frac{n-5-2\xi}{2}})\Big|_{2^n-2^{\frac{n+1}{2}}+1} =$$

$$= |(2^{n+\beta})(\overbrace{|2^{2n}|_{2^n-2^{\frac{n+1}{2}}+1}}^{=-1}-1)\,(\overbrace{|2^n+2^{\frac{n+1}{2}}+1|_{2^n-2^{\frac{n+1}{2}}+1}}^{=2\times 2^{\frac{n+1}{2}}})(\rho \cdot 2^{\frac{n-5-2\xi}{2}})|_{2^n-2^{\frac{n+1}{2}}+1} =$$

$$= \Big|(-\rho)(2^{n+n\phi+\xi})(2^{\frac{n+5}{2}})(2^{\frac{n-5-2\xi}{2}})\Big|_{2^n-2^{\frac{n+1}{2}}+1} = \Big|(-\rho)(2^{\frac{2n+2n\phi+\cancel{2\xi}+n+\cancel{5}+n-\cancel{5}-\cancel{2\xi}}{2}})\Big|_{2^n-2^{\frac{n+1}{2}}+1} =$$

$$= \Big|(-\rho)(2^{\frac{4n+2n\phi}{2}})\Big|_{2^n-2^{\frac{n+1}{2}}+1} = |(-\rho)\,(\overbrace{|2^{2n}|_{2^n-2^{\frac{n+1}{2}}+1}}^{=-1})(2^{n\phi})|_{2^n-2^{\frac{n+1}{2}}+1} = \Big|\rho \cdot 2^{n\phi}\Big|_{2^n-2^{\frac{n+1}{2}}+1}, \tag{8}$$

where the cases of ϕ derives into the same expression:

$$\phi = \begin{cases} 0, & \rho = +1, \quad \Big|(+1)(2^0)\Big|_{2^n-2^{\frac{n+1}{2}}+1} = 1 \\ 2, & \rho = -1, \quad \Big|(-1)(2^{2n})\Big|_{2^n-2^{\frac{n+1}{2}}+1} = |(-1)\,(\overbrace{|2^{2n}|_{2^n-2^{\frac{n+1}{2}}+1}}^{=-1})|_{2^n-2^{\frac{n+1}{2}}+1} = 1. \end{cases} \tag{9}$$

The range of ξ is defined from two constrains. The first constrain is $\frac{n-5-2\xi}{2} \geq 0$, which is defined in order to have multiplicative inverses based on summation of powers of two integers. Therefore, $\xi \leq \frac{n-5}{2}$ is defined as the upper level. The second constrain is $\frac{n-5-2\xi}{2} < n$ in order to have multiplicative inverses in the range $(-2^n + 2^{\frac{n+1}{2}} - 1, 2^n - 2^{\frac{n+1}{2}} + 1)$. However, $\xi > -\frac{(n+5)}{2}$ derived from the latter constrain is less restrictive than the absolute value of ξ predefined to provide all the possible values of β, $(-\frac{(n-1)}{2} \leq \beta \leq 3n)$. Thus, $\xi \geq -\frac{(n-1)}{2}$ is chosen as the lower level in this case. □

Proof. From Table 1 is derived that $|\hat{m}_4^{-1}|_{m_4} = |\rho \cdot (-2^{\frac{3n-5-2\xi}{2}} + 2^{n-2-\xi})|_{m_4}$ for $\frac{n-1}{2} < \xi \leq \frac{n-1}{2}$, and being ϕ an even number, $\phi = 0$ or $\phi = 2$. By substituting m_4, $\hat{m}_4$ and $|\hat{m}_4^{-1}|_{m_4}$ in (3):

$$\Big|(2^{n+\beta})(2^{2n}-1)(2^n+2^{\frac{n+1}{2}}+1)(\rho)(-2^{\frac{3n-5-2\xi}{2}}+2^{n-2-\xi})\Big|_{2^n-2^{\frac{n+1}{2}}+1} =$$

$$= |(2^{n+\beta})(\overbrace{|2^{2n}|_{2^n-2^{\frac{n+1}{2}}+1}}^{=-1}-1)\,(\overbrace{|2^n+2^{\frac{n+1}{2}}+1|_{2^n-2^{\frac{n+1}{2}}+1}}^{=2\times 2^{\frac{n+1}{2}}})(\rho)(-2^{\frac{3n-5-2\xi}{2}}+2^{\frac{2n-4-4\xi}{2}})|_{2^n-2^{\frac{n+1}{2}}+1} =$$

$$= \Big|(-\rho)(2^{n+n\phi+\xi})(2^{\frac{n+5}{2}})(-2^{\frac{3n-5-2\xi}{2}}+2^{\frac{2n-4-4\xi}{2}})\Big|_{2^n-2^{\frac{n+1}{2}}+1} =$$

$$= \Big|(-\rho)(-2^{\frac{3n+2n\phi+\cancel{2\xi}+\cancel{5}+3n-\cancel{5}-\cancel{2\xi}}{2}}+2^{\frac{3n+2n\phi+\cancel{2\xi}+5+2n-4-\cancel{2\xi}}{2}})\Big|_{2^n-2^{\frac{n+1}{2}}+1} =$$

$$= \Big|(-\rho)(-2^{\frac{6n+2n\phi}{2}}+2^{\frac{5n+2n\phi+1}{2}})\Big|_{2^n-2^{\frac{n+1}{2}}+1} = \Big|(-\rho)(-2^{(3+\phi)n}+2^{\frac{n+1}{2}}2^{(2+\phi)n})\Big|_{2^n-2^{\frac{n+1}{2}}+1}, \tag{10}$$

where the cases of ϕ derives into the same expression:

$$\phi = \begin{cases} 0, & \rho = +1, \quad \Big|(-1)(-2^{3n}+2^{\frac{n+1}{2}}2^{2n})\Big|_{2^n-2^{\frac{n+1}{2}}+1} = \Big|(-1)(2^n-2^{\frac{n+1}{2}})\Big|_{2^n-2^{\frac{n+1}{2}}+1} \\ 2, & \rho = -1, \quad \Big|(+1)(-2^{5n}+2^{\frac{n+1}{2}}2^{4n})\Big|_{2^n-2^{\frac{n+1}{2}}+1} = \Big|(-1)(2^n-2^{\frac{n+1}{2}})\Big|_{2^n-2^{\frac{n+1}{2}}+1}, \end{cases} \tag{11}$$

which can be rewritten as:

$$|(-1)\,(\overbrace{\Big|2^n-2^{\frac{n+1}{2}}\Big|_{2^n-2^{\frac{n+1}{2}}+1}}^{=-1})|_{2^n-2^{\frac{n+1}{2}}+1} = 1. \tag{12}$$

Given that $\frac{3n-5-2\xi}{2} \geq 0$ and $n-2-\xi \geq 0$ it is possible to have multiplicative inverses based on summation of powers of two integers. Therefore:

$$\begin{cases} \frac{3n-5-2\xi}{2} \geq 0 \Leftrightarrow 3n-5-2\xi \geq 0 \Leftrightarrow \xi \leq \frac{3n-5}{2} \\ n-2-2\xi \geq 0 \Leftrightarrow \xi \leq n-2, \end{cases} \tag{13}$$

However, the condition $\xi \leq \frac{n-1}{2}$ is chosen to define the upper level of ξ given that it is more restrictive than the ones presented in (13). In addition, to derive multiplicative inverses in the range of $(-2^n + 2^{\frac{n+1}{2}} - 1, 2^n - 2^{\frac{n+1}{2}} + 1)$ it is necessary to verify that $\frac{3n-5-2\xi}{2} < n$ and $n - 2 - \xi < n$. Therefore:

$$\begin{cases} \frac{3n-5-2\xi}{2} < n \Leftrightarrow n - 5 - 2\xi < 0 \Leftrightarrow \xi > \frac{n-5}{2} \\ n - 2 - 2\xi < n \Leftrightarrow \xi > -2, \end{cases} \tag{14}$$

where is chosen the most restrictive condition $\xi > \frac{n-5}{2}$ as the lower level. □

Proof. From Table I is derived that $|\hat{m}_4^{-1}|_{m_4} = |\rho \cdot (-2^{\frac{n-5-2\xi}{2}} + 2^{-(\xi+2)})|_{m_4}$ for $-\frac{(n-1)}{2} \leq \xi \leq -1$, and being ϕ an odd number, $\phi = 1$ or $\phi = 3$. By substituting m_4, $\hat{m}_4$ and $|\hat{m}_4^{-1}|_{m_4}$ in (3):

$$\begin{aligned} &\left|(2^{n+\beta})(2^{2n}-1)(2^n + 2^{\frac{n+1}{2}} + 1)(\rho)(-2^{\frac{n-5-2\xi}{2}} + 2^{-(\xi+2)})\right|_{2^n - 2^{\frac{n+1}{2}}+1} = \\ &= |(2^{n+\beta})(\overbrace{|2^{2n}|_{2^n-2^{\frac{n+1}{2}}+1}}^{=-1} - 1)\,(\overbrace{|2^n + 2^{\frac{n+1}{2}} + 1|_{2^n-2^{\frac{n+1}{2}}+1}}^{=2\times 2^{\frac{n+1}{2}}})(\rho)(-2^{\frac{n-5-2\xi}{2}} + 2^{-\frac{(2\xi+4)}{2}})|_{2^n-2^{\frac{n+1}{2}}+1} = \\ &= \left|(-\rho)(2^{n+n\phi+\xi})(2^{\frac{n+5}{2}})(-2^{\frac{n-5-2\xi}{2}} + 2^{-\frac{(2\xi+4)}{2}})\right|_{2^n-2^{\frac{n+1}{2}}+1} = \\ &= \left|(-\rho)(-2^{\frac{3n+2n\phi+\cancel{2\xi}+\cancel{5}+\cancel{n}-\cancel{5}-\cancel{2\xi}}{2}} + 2^{\frac{3n+2n\phi+\cancel{2\xi}+5-4-\cancel{2\xi}}{2}})\right|_{2^n-2^{\frac{n+1}{2}}+1} = \\ &= \left|(-\rho)(-2^{2n+n\phi} + 2^{\frac{3n+2n\phi+1}{2}})\right|_{2^n-2^{\frac{n+1}{2}}+1}, \end{aligned} \tag{15}$$

where the cases of ϕ derives into the same expression:

$$\phi = \begin{cases} 1, \quad \rho = +1, \quad \left|(-1)(-2^{3n} + 2^{\frac{5n+1}{2}})\right|_{2^n-2^{\frac{n+1}{2}}+1} = |(-1)((-2^n)\overbrace{|2^{2n}|_{2^n-2^{\frac{n+1}{2}}+1}}^{=-1} + \\ \qquad +(2^{\frac{n+1}{2}})\overbrace{|2^{2n}|_{2^n-2^{\frac{n+1}{2}}+1}}^{=-1})|_{2^n-2^{\frac{n+1}{2}}+1} = \left|(-1)(2^n - 2^{\frac{n+1}{2}})\right|_{2^n-2^{\frac{n+1}{2}}+1} \\ 3, \quad \rho = -1, \quad \left|(+1)(-2^{5n} + 2^{\frac{7n+1}{2}})\right|_{2^n-2^{\frac{n+1}{2}}+1} = |(-1)((-2^n)\overbrace{|2^{4n}|_{2^n-2^{\frac{n+1}{2}}+1}}^{=+1} + \\ \qquad +(2^{\frac{n+1}{2}})\overbrace{|2^{4n}|_{2^n-2^{\frac{n+1}{2}}+1}}^{=+1})|_{2^n-2^{\frac{n+1}{2}}+1} = \left|(-1)(2^n - 2^{\frac{n+1}{2}})\right|_{2^n-2^{\frac{n+1}{2}}+1}, \end{cases}$$

which can be rewritten as:

$$|(-1)\,(\overbrace{\left|2^n - 2^{\frac{n+1}{2}}\right|_{2^n-2^{\frac{n+1}{2}}+1}}^{=-1})\,|_{2^n-2^{\frac{n+1}{2}}+1} = 1. \tag{16}$$

In order to have multiplicative inverses based on the summation of powers of two integers is needed to set the constrain $n - 1 - \xi \geq 0$ and $-(\xi + 2) \geq 0$. Therefore:

$$\begin{cases} n - 1 - \xi \geq 0 \Leftrightarrow \xi \leq n - 1 \\ -(\xi + 2) \geq 0 \Leftrightarrow \xi \leq -2 \Leftrightarrow \xi < -1, \end{cases} \tag{17}$$

However, the condition $\xi < -1$ is chosen to define the upper level of ξ given that it is more restrictive in comparison with $\xi \leq n - 1$ and $\xi \leq \frac{n-1}{2}$. In addition, to derive multiplicative inverses in the range of $(-2^n + 2^{\frac{n+1}{2}} - 1, 2^n - 2^{\frac{n+1}{2}} + 1)$ is needed to verify that $\frac{n-5-2\xi}{2} < n$ and $-(\xi + 2) < n$. Therefore:

$$\begin{cases} \frac{n-5-2\xi}{2} < n \Leftrightarrow -n - 5 - 2\xi < 0 \Leftrightarrow \xi > -\frac{(n+5)}{2} \\ -\xi - 2 < n \Leftrightarrow \xi > -(n + 2). \end{cases} \tag{18}$$

However, these constrains are less restrictive than the absolute lower level constrain of ξ, $\xi > -\frac{(n-1)}{2}$, which is chosen as the lower level. □

Proof. From Table I is derived that $|\hat{m}_4^{-1}|_{m_4} = |\rho \cdot (-2^{n-2-\xi} + 2^{\frac{n-5-2\xi}{2}})|_{m_4}$ for $-1 \leq \xi \leq \frac{n-5}{2}$, and being ϕ an odd number, $\phi = 1$ or $\phi = 3$. By substituting m_4, $\hat{m}_4$ and $|\hat{m}_4^{-1}|_{m_4}$ in (3):

$$\Big|(2^{n+\beta})(2^{2n}-1)(2^n+2^{\frac{n+1}{2}}+1)(\rho)(-2^{n-2-\xi}+2^{\frac{n-5-2\xi}{2}})\Big|_{2^n-2^{\frac{n+1}{2}}+1} =$$

$$= |(2^{n+\beta})(\overbrace{|2^{2n}|_{2^n-2^{\frac{n+1}{2}}+1}}^{=-1}-1)\,(\overbrace{|2^n+2^{\frac{n+1}{2}}+1|_{2^n-2^{\frac{n+1}{2}}+1}}^{=2\times 2^{\frac{n+1}{2}}})(\rho)(-2^{\frac{2n-4-2\xi}{2}}+2^{\frac{n-5-2\xi}{2}})|_{2^n-2^{\frac{n+1}{2}}+1} =$$

$$= \Big|(-\rho)(2^{n+n\phi+\xi})(2^{\frac{n+5}{2}})(-2^{\frac{2n-4-2\xi}{2}}+2^{\frac{n-5-2\xi}{2}})\Big|_{2^n-2^{\frac{n+1}{2}}+1} =$$

$$= \Big|(-\rho)(-2^{\frac{3n+2n\phi+\cancel{2\xi}+5+2n-4-\cancel{2\xi}}{2}}+2^{\frac{3n+2n\phi+\cancel{2\xi}+5+n-5-\cancel{2\xi}}{2}})\Big|_{2^n-2^{\frac{n+1}{2}}+1} =$$

$$= \Big|(-\rho)(-2^{\frac{5n+2n\phi+1}{2}}+2^{\frac{2n+n\phi}{2}})\Big|_{2^n-2^{\frac{n+1}{2}}+1} = \Big|(\rho)(-2^{\frac{n+1}{2}}+1)(2^{(2+\phi)n}\Big|_{2^n-2^{\frac{n+1}{2}}+1}, \tag{19}$$

where the cases of ϕ derives into the same expression:

$$\phi = \begin{cases} 1, & \rho = +1, \quad \Big|(-1)(-2^{\frac{n+1}{2}}+1)(2^{3n})\Big|_{2^n-2^{\frac{n+1}{2}}+1} = |(-1)(-2^{\frac{n+1}{2}}+1)(2^n)\,\overbrace{|2^{2n}|_{2^n-2^{\frac{n+1}{2}}+1}}^{=-1}|_{2^n-2^{\frac{n+1}{2}}+1} = \\ & \qquad = \Big|(-2^{\frac{n+1}{2}}+1)(2^n)\Big|_{2^n-2^{\frac{n+1}{2}}+1} \\ 3, & \rho = -1, \quad \Big|(+1)(-2^{\frac{n+1}{2}}+1)(2^{5n})\Big|_{2^n-2^{\frac{n+1}{2}}+1} = |(+1)(-2^{\frac{n+1}{2}}+1)(2^n)\,\overbrace{|2^{4n}|_{2^n-2^{\frac{n+1}{2}}+1}}^{=+1}|_{2^n-2^{\frac{n+1}{2}}+1} = \\ & \qquad = \Big|(-2^{\frac{n+1}{2}}+1)(2^n)\Big|_{2^n-2^{\frac{n+1}{2}}+1}, \end{cases}$$

which can be rewritten as:

$$|(-2^n)(2^n)|_{2^n-2^{\frac{n+1}{2}}+1} = |\overbrace{-2^{2n}}^{=+1}|_{2^n-2^{\frac{n+1}{2}}+1} = 1. \tag{20}$$

Given that $\frac{n-5-2\xi}{2} \geq 0$ and $n-2-\xi \geq 0$ it is possible to have multiplicative inverses based on summation of powers of two integers. Therefore:

$$\begin{cases} \frac{n-5-2\xi}{2} \geq 0 \Leftrightarrow n-5-2\xi \geq 0 \Leftrightarrow \xi \leq \frac{n-5}{2} \\ n-2-\xi \geq 0 \Leftrightarrow \xi \leq n-2, \end{cases} \tag{21}$$

where the condition $\xi \leq \frac{n-5}{2}$ is chosen to define the upper level of ξ, given that it is more restrictive than in comparison with $\xi \leq n-1$ and $\xi \leq \frac{n-1}{2}$. In addition, to derive multiplicative inverses in the range of $(-2^n + 2^{\frac{n+1}{2}} - 1, 2^n - 2^{\frac{n+1}{2}} + 1)$ is needed to verify that $\frac{n-5-2\xi}{2} < n$ and $n-2-\xi < n$. Therefore:

$$\begin{cases} \frac{n-5-2\xi}{2} < n \Leftrightarrow -n-5-2\xi < 0 \Leftrightarrow \xi > -\frac{(n+5)}{2} \\ n-2-\xi < n \Leftrightarrow \xi > -2 \Leftrightarrow \xi \geq -1, \end{cases} \tag{22}$$

where the most restrictive condition $\xi \geq -1$ is chosen as lower level, given that it is more restrictive than $-\frac{(n-1)}{2}$. □

Proof. From Table I is derived that $|\hat{m}_4^{-1}|_{m_4} = |(-\rho)(2^{\frac{3n-5-2\xi}{2}})|_{m_5}$ for $\frac{n-5}{2} < \xi \leq \frac{n-1}{2}$, and being ϕ an odd number, $\phi = 1$ or $\phi = 3$. By substituting m_4, $\hat{m}_4$ and $|\hat{m}_4^{-1}|_{m_4}$ in (3):

$$\Big|(2^{n+\beta})(2^{2n}-1)(2^n+2^{\frac{n+1}{2}}+1)(-\rho)(2^{\frac{3n-5-2\xi}{2}})\Big|_{2^n-2^{\frac{n+1}{2}}+1} =$$

$$= |(2^{n+\beta})(\overbrace{|2^{2n}|_{2^n-2^{\frac{n+1}{2}}+1}}^{=-1}-1)\,(\overbrace{|2^n+2^{\frac{n+1}{2}}+1|_{2^n-2^{\frac{n+1}{2}}+1}}^{=2\times 2^{\frac{n+1}{2}}})(-\rho)(2^{\frac{3n-5-2\xi}{2}})|_{2^n-2^{\frac{n+1}{2}}+1} =$$

$$= \Big|(\rho)(2^{\frac{2n+2n\phi+2\xi}{2}})(2^{\frac{n+5}{2}})(2^{\frac{3n-5-2\xi}{2}})\Big|_{2^n-2^{\frac{n+1}{2}}+1} = \Big|(\rho)(2^{\frac{6n+2n\phi+\cancel{2\xi}+\cancel{5}-\cancel{5}-\cancel{2\xi}}{2}})\Big|_{2^n-2^{\frac{n+1}{2}}+1} = \Big|(\rho)(2^{3n+n\phi})\Big|_{2^n-2^{\frac{n+1}{2}}+1}, \tag{23}$$

$$\tag{24}$$

where the cases of ϕ derives into the same expression:

$$\phi = \begin{cases} 1, & \rho = +1, \quad \Big|(+1)(2^{4n})\Big|_{2^n-2^{\frac{n+1}{2}}+1} \\ 3, & \rho = -1, \quad \Big|(-1)(2^{6n})\Big|_{2^n-2^{\frac{n+1}{2}}+1} = |(-1)(2^{4n})(\overbrace{|2^{2n}|_{2^n+2^{\frac{n+1}{2}}+1}}^{=-1})|_{2^n-2^{\frac{n+1}{2}}+1}, \end{cases} \tag{25}$$

which can be rewritten as:

$$|\overbrace{2^{4n}}^{=+1}|_{2^n-2^{\frac{n+1}{2}}+1} = 1, \tag{26}$$

The constrain $\frac{3n-5-2\xi}{2} \geq 0$ needs to be set in order to have multiplicative inverses based on the summation of powers of two integers. However, the constrain $\xi \leq \frac{n-1}{2}$ is chosen as the upper level due to is more restrictive than $\xi \leq \frac{3n-5}{2}$. In addition, to derive multiplicative inverses in the range of $(-2^n + 2^{\frac{n+1}{2}} - 1, 2^n - 2^{\frac{n+1}{2}} + 1)$ is needed to verify that $\frac{3n-5-2\xi}{2} < n$. Therefore, $\xi > \frac{n-5}{2}$ is chosen as lower level due to is more restrictive than $\xi \geq -\frac{(n-1)}{2}$. □

- $i = 5$:

Proof. From Table 1 is derived that $|\hat{m}_5^{-1}|_{m_5} = |(-\rho)(2^{\frac{n-5-2\xi}{2}})|_{m_4}$ for $-\frac{n-1}{2} \leq \xi \leq \frac{n-5}{2}$, and being ϕ an even number, $\phi = 0$ or $\phi = 2$. By substituting m_5, $\hat{m}_5$ and $|\hat{m}_5^{-1}|_{m_5}$ in (3):

$$\begin{aligned}
&\left|(2^{n+\beta})(2^{2n}-1)(2^n+2^{\frac{n+1}{2}}+1)(-\rho)(2^{\frac{n-5-2\xi}{2}})\right|_{2^n+2^{\frac{n+1}{2}}+1} = \\
&= |(2^{n+\beta})(\overbrace{|2^{2n}|_{2^n+2^{\frac{n+1}{2}}+1}}^{=-1}-1)\,(\overbrace{|2^n-2^{\frac{n+1}{2}}+1|_{2^n+2^{\frac{n+1}{2}}+1}}^{=-2\times 2^{\frac{n+1}{2}}})(-\rho)(2^{\frac{n-5-2\xi}{2}})|_{2^n+2^{\frac{n+1}{2}}+1} = \\
&= \left|(-\rho)(2^{n+n\phi+\xi})(2^{\frac{n+5}{2}})(2^{\frac{n-5-2\xi}{2}})\right|_{2^n+2^{\frac{n+1}{2}}+1} = \left|(-\rho)(2^{\frac{2n+2n\phi+\cancel{2\xi}+n+\cancel{5}+n-\cancel{5}-\cancel{2\xi}}{2}})\right|_{2^n+2^{\frac{n+1}{2}}+1} = \\
&= \left|(-\rho)(2^{\frac{4n+2n\phi}{2}})\right|_{2^n+2^{\frac{n+1}{2}}+1} = |(-\rho)\,(\overbrace{|2^{2n}|_{2^n+2^{\frac{n+1}{2}}+1}}^{=-1})(2^{n\phi})|_{2^n+2^{\frac{n+1}{2}}+1} = \left|\rho\cdot 2^{n\phi}\right|_{2^n-2^{\frac{n+1}{2}}+1},
\end{aligned} \tag{27}$$

where the cases of ϕ derives into the same expression:

$$\phi = \begin{cases} 0, & \rho = +1, \quad |(+1)(2^0)|_{2^n+2^{\frac{n+1}{2}}+1} = 1 \\ 2, & \rho = -1, \quad |(-1)(2^{2n})|_{2^n+2^{\frac{n+1}{2}}+1} = |(-1)\,(\overbrace{|2^{2n}|_{2^n+2^{\frac{n+1}{2}}+1}}^{=-1})|_{2^n+2^{\frac{n+1}{2}}+1} = 1. \end{cases} \tag{28}$$

The range of ξ is defined from two constrains. The first constrain is $\frac{n-5-2\xi}{2} \geq 0$, which is defined in order to have multiplicative inverses based on summation of powers of two integers. Therefore, $\xi \leq \frac{n-5}{2}$ is defined as the upper level. The second constrain is $\frac{n-5-2\xi}{2} < n$ in order to have multiplicative inverses in the range $(-2^n - 2^{\frac{n+1}{2}} - 1, 2^n + 2^{\frac{n+1}{2}} + 1)$. However, $\xi > -\frac{(n+5)}{2}$ derived from the latter constrain is less restrictive than the absolute value of ξ predefined to provide all the possible values of β, $(-\frac{(n-1)}{2} \leq \beta \leq 3n)$. Thus, $\xi \geq -\frac{(n-1)}{2}$ is chosen as the lower level in this case. □

Proof. From Table 1 is derived that $|\hat{m}_5^{-1}|_{m_5} = |\rho\cdot(2^{\frac{3n-5-2\xi}{2}} + 2^{n-2-\xi})|_{m_4}$ for $\frac{n-5}{2} < \xi \leq \frac{n-1}{2}$, and being ϕ an even number, $\phi = 0$ or $\phi = 2$. By substituting m_5, $\hat{m}_5$ and $|\hat{m}_5^{-1}|_{m_5}$ in (3):

$$\begin{aligned}
&\left|(2^{n+\beta})(2^{2n}-1)(2^n-2^{\frac{n+1}{2}}+1)(\rho)(2^{\frac{3n-5-2\xi}{2}}+2^{n-2-\xi})\right|_{2^n+2^{\frac{n+1}{2}}+1} = \\
&= |(2^{n+\beta})(\overbrace{|2^{2n}|_{2^n-2^{\frac{n+1}{2}}+1}}^{=-1}-1)\,(\overbrace{|2^n-2^{\frac{n+1}{2}}+1|_{2^n+2^{\frac{n+1}{2}}+1}}^{=-2\times 2^{\frac{n+1}{2}}})(\rho)(2^{\frac{3n-5-2\xi}{2}}+2^{\frac{2n-4-4\xi}{2}}))|_{2^n-2^{\frac{n+1}{2}}+1} = \\
&= \left|(\rho)(2^{n+n\phi+\xi})(2^{\frac{n+5}{2}})(2^{\frac{3n-5-2\xi}{2}}+2^{\frac{2n-4-4\xi}{2}})\right|_{2^n+2^{\frac{n+1}{2}}+1} = \\
&= \left|(\rho)(2^{\frac{3n+2n\phi+\cancel{2\xi}+\cancel{5}+3n-\cancel{5}-\cancel{2\xi}}{2}}+2^{\frac{3n+2n\phi+\cancel{2\xi}+5+2n-4-\cancel{2\xi}}{2}})\right|_{2^n+2^{\frac{n+1}{2}}+1} = \\
&= \left|(\rho)(2^{\frac{6n+2n\phi}{2}}+2^{\frac{5n+2n\phi+1}{2}})\right|_{2^n-2^{\frac{n+1}{2}}+1} = \left|(\rho)(2^{(3+\phi)n}+2^{\frac{n+1}{2}}2^{(2+\phi)n})\right|_{2^n+2^{\frac{n+1}{2}}+1},
\end{aligned} \tag{29}$$

where the cases of ϕ derives into the same expression:

$$\phi = \begin{cases} 0, & \rho = +1, \quad \left|(+1)(2^{3n}+2^{\frac{n+1}{2}}2^{2n})\right|_{2^n+2^{\frac{n+1}{2}}+1} = \left|(-1)(2^n+2^{\frac{n+1}{2}})\right|_{2^n+2^{\frac{n+1}{2}}+1} \\ 2, & \rho = -1, \quad \left|(-1)(2^{5n}+2^{\frac{n+1}{2}}2^{4n})\right|_{2^n+2^{\frac{n+1}{2}}+1} = \left|(-1)(2^n+2^{\frac{n+1}{2}})\right|_{2^n+2^{\frac{n+1}{2}}+1}, \end{cases} \tag{30}$$

which can be rewritten as:

$$|(-1)^{\overbrace{\left(\left|2^n+2^{\frac{n+1}{2}}\right|_{2^n+2^{\frac{n+1}{2}}+}\right)}^{=-1}}|_{2^n+2^{\frac{n+1}{2}}+1}=1. \tag{31}$$

Due to $\frac{3n-5-2\xi}{2}\geq 0$ and $n-2-\xi\geq 0$ in order to have multiplicative inverses based on summation of powers of two integers. Therefore:

$$\begin{cases}\frac{3n-5-2\xi}{2}\geq 0\Leftrightarrow 3n-5-2\xi\geq 0\Leftrightarrow \xi\leq\frac{3n-5}{2}\\ n-2-2\xi\geq 0\Leftrightarrow \xi\leq n-2,\end{cases} \tag{32}$$

However, the condition $\xi\leq\frac{n-1}{2}$ is chosen to define the upper level of ξ given that it is more restrictive than the ones presented in (13). In addition, to derive multiplicative inverses in the range of $(-2^n-2^{\frac{n+1}{2}}-1, 2^n+2^{\frac{n+1}{2}}+1)$ is needed to verify that $\frac{3n-5-2\xi}{2}<n$ and $n-2-\xi<n$. Therefore:

$$\begin{cases}\frac{3n-5-2\xi}{2}<n\Leftrightarrow n-5-2\xi<0\Leftrightarrow \xi>\frac{n-5}{2}\\ n-2-2\xi<n\Leftrightarrow \xi>-2,\end{cases} \tag{33}$$

where the most restrictive condition $\xi>\frac{n-5}{2}$ is chosen as the lower level. □

Proof. From Table I is derived that $|\hat{m}_5^{-1}|_{m_5}=|\rho\cdot(2^{\frac{n-5-2\xi}{2}}+2^{-(\xi+2)})|_{m_5}$ for $-\frac{(n-1)}{2}\leq\xi\leq -1$, and being ϕ an odd number, $\phi=1$ or $\phi=3$. By substituting m_5, $\hat{m}_5$ and $|\hat{m}_5^{-1}|_{m_5}$ in (3):

$$\begin{aligned}&\left|(2^{n+\beta})(2^{2n}-1)(2^n-2^{\frac{n+1}{2}}+1)(\rho)(2^{\frac{n-5-2\xi}{2}}+2^{-(\xi+2)})\right|_{2^n+2^{\frac{n+1}{2}}+1}=\\ &=|(2^{n+\beta})(\overbrace{|2^{2n}|_{2^n+2^{\frac{n+1}{2}}+1}}^{=-1})-1)(\overbrace{|2^n-2^{\frac{n+1}{2}}+1|_{2^n+2^{\frac{n+1}{2}}+1}}^{=-2\times 2^{\frac{n+1}{2}}})(\rho)(2^{\frac{n-5-2\xi}{2}}+2^{-\frac{(2\xi+4)}{2}})|_{2^n+2^{\frac{n+1}{2}}+1}=\\ &=\left|(\rho)(2^{n+n\phi+\xi})(2^{\frac{n+5}{2}})(2^{\frac{n-5-2\xi}{2}}+2^{-\frac{(2\xi+4)}{2}})\right|_{2^n+2^{\frac{n+1}{2}}+1}=\\ &=\left|(\rho)(2^{\frac{3n+2n\phi+\cancel{2\xi}+\cancel{5}+n\cancel{-5}-\cancel{2\xi}}{2}}+2^{\frac{3n+2n\phi+\cancel{2\xi}+5-4-\cancel{2\xi}}{2}})\right|_{2^n+2^{\frac{n+1}{2}}+1}=\\ &=\left|(\rho)(2^{2n+n\phi}+2^{\frac{3n+2n\phi+1}{2}})\right|_{2^n+2^{\frac{n+1}{2}}+1},\end{aligned} \tag{34}$$

where the cases of ϕ derives into the same expression:

$$\phi=\begin{cases}1, & \rho=+1, \quad \left|(+1)(2^{3n}+2^{\frac{5n+1}{2}})\right|_{2^n+2^{\frac{n+1}{2}}+1}=|((2^n)\overbrace{|2^{2n}|_{2^n+2^{\frac{n+1}{2}}+1}}^{=-1}+\\ & \quad +(2^{\frac{n+1}{2}})\overbrace{|2^{2n}|_{2^n-2^{\frac{n+1}{2}}+1}}^{=-1})|_{2^n+2^{\frac{n+1}{2}}+1}=\left|(-1)(2^n+2^{\frac{n+1}{2}})\right|_{2^n+2^{\frac{n+1}{2}}+1}\\ 3, & \rho=-1, \quad \left|(-1)(2^{5n}+2^{\frac{7n+1}{2}})\right|_{2^n+2^{\frac{n+1}{2}}+1}=|(-1)((2^n)\overbrace{|2^{4n}|_{2^n+2^{\frac{n+1}{2}}+1}}^{=+1}+\\ & \quad +(2^{\frac{n+1}{2}})\overbrace{|2^{4n}|_{2^n+2^{\frac{n+1}{2}}+1}}^{=+1})|_{2^n+2^{\frac{n+1}{2}}+1}=\left|(-1)(2^n+2^{\frac{n+1}{2}})\right|_{2^n+2^{\frac{n+1}{2}}+1},\end{cases}$$

which can be rewritten as:

$$|(-1)^{\overbrace{\left(\left|2^n+2^{\frac{n+1}{2}}\right|_{2^n+2^{\frac{n+1}{2}}+1}\right)}^{=-1}}|_{2^n+2^{\frac{n+1}{2}}+1}=1, \tag{35}$$

In order to have multiplicative inverses based on summation of powers of two integers is needed to set the constrain $n-1-\xi\geq 0$ and $-(\xi+2)\geq 0$. Therefore:

$$\begin{cases}n-1-\xi\geq 0\Leftrightarrow \xi\leq n-1\\ -(\xi+2)\geq 0\Leftrightarrow \xi\leq -2\Leftrightarrow \xi<-1,\end{cases} \tag{36}$$

However, the condition $\xi < -1$ is chosen to define the upper level of ξ given that it is more restrictive in comparison with $\xi \leq n-1$ and $\xi \leq \frac{n-1}{2}$. In addition, to derive multiplicative inverses in the range of $(-2^n + 2^{\frac{n+1}{2}} - 1, 2^n - 2^{\frac{n+1}{2}} + 1)$ one needs to verify that $\frac{n-5-2\xi}{2} < n$ and $-(\xi+2) < n$. Therefore:

$$\begin{cases} \frac{n-5-2\xi}{2} < n \Leftrightarrow -n-5-2\xi < 0 \Leftrightarrow \xi > -\frac{(n+5)}{2} \\ -\xi - 2 < n \Leftrightarrow \xi > -(n+2). \end{cases} \tag{37}$$

However, these constrains are less restrictive than the absolute lower level constrain of ξ, $\xi > -\frac{(n-1)}{2}$, which is chosen as the lower level. □

Proof. From Table I is derived that $|\hat{m}_5^{-1}|_{m_5} = |\rho \cdot (-2^{n-2-\xi} - 2^{\frac{n-5-2\xi}{2}})|_{m_5}$ for $-1 \leq \xi \leq \frac{n-5}{2}$, and being ϕ an odd number, $\phi = 1$ or $\phi = 3$. By substituting m_5, $\hat{m}_5$ and $|\hat{m}_5^{-1}|_{m_5}$ in (3):

$$\begin{aligned} &\left|(2^{n+\beta})(2^{2n}-1)(2^n - 2^{\frac{n+1}{2}}+1)(-\rho)(2^{n-2-\xi} + 2^{\frac{n-5-2\xi}{2}})\right|_{2^n+2^{\frac{n+1}{2}}+1} = \\ &= |(2^{n+\beta})(\overbrace{|2^{2n}|_{2^n+2^{\frac{n+1}{2}}+1}}^{=-1} - 1)\,(\overbrace{|2^n - 2^{\frac{n+1}{2}}+1|_{2^n+2^{\frac{n+1}{2}}+1}}^{=-2\times 2^{\frac{n+1}{2}}})(-\rho)(2^{\frac{2n-4-2\xi}{2}} + 2^{\frac{n-5-2\xi}{2}})|_{2^n+2^{\frac{n+1}{2}}+1} = \\ &= \left|(-\rho)(2^{n+n\phi+\xi})(2^{\frac{n+5}{2}})(2^{\frac{2n-4-2\xi}{2}} + 2^{\frac{n-5-2\xi}{2}})\right|_{2^n+2^{\frac{n+1}{2}}+1} = \\ &= \left|(-\rho)(2^{\frac{3n+2n\phi+\cancel{2\xi}+5+2n-4-\cancel{2\xi}}{2}} + 2^{\frac{3n+2n\phi+\cancel{2\xi}+5+n-5-\cancel{2\xi}}{2}})\right|_{2^n+2^{\frac{n+1}{2}}+1} = \\ &= \left|(-\rho)(2^{\frac{5n+2n\phi+1}{2}} + 2^{\frac{2n+n\phi}{2}})\right|_{2^n+2^{\frac{n+1}{2}}+1} = \left|(-\rho)(2^{\frac{n+1}{2}}+1)(2^{(2+\phi)n}\right|_{2^n+2^{\frac{n+1}{2}}+1}, \end{aligned} \tag{38}$$

where the cases of ϕ derives into the same expression:

$$\phi = \begin{cases} 1, \quad \rho = +1, & \left|(-1)(2^{\frac{n+1}{2}}+1)(2^{3n})\right|_{2^n+2^{\frac{n+1}{2}}+1} = |(-1)(2^{\frac{n+1}{2}}+1)(2^n)\,\overbrace{|2^{2n}|_{2^n+2^{\frac{n+1}{2}}+1}}^{=-1}|_{2^n+2^{\frac{n+1}{2}}+1} = \\ & \quad = \left|(2^{\frac{n+1}{2}}+1)(2^n)\right|_{2^n+2^{\frac{n+1}{2}}+1} \\ 3, \quad \rho = -1, & \left|(+1)(2^{\frac{n+1}{2}}+1)(2^{5n})\right|_{2^n+2^{\frac{n+1}{2}}+1} = |(+1)(2^{\frac{n+1}{2}}+1)(2^n)\,\overbrace{|2^{4n}|_{2^n-2^{\frac{n+1}{2}}+1}}^{=+1}|_{2^n+2^{\frac{n+1}{2}}+1} = \\ & \quad = \left|(2^{\frac{n+1}{2}}+1)(2^n)\right|_{2^n+2^{\frac{n+1}{2}}+1}, \end{cases}$$

which can be rewritten as:

$$|(-2^n)(2^n)|_{2^n+2^{\frac{n+1}{2}}+1} = |\overbrace{-2^{2n}}^{=+1}|_{2^n+2^{\frac{n+1}{2}}+1} = 1. \tag{39}$$

Due to $\frac{n-5-2\xi}{2} \geq 0$ and $n-2-\xi \geq 0$ in order to have multiplicative inverses based on summation of powers of two integers. Therefore:

$$\begin{cases} \frac{n-5-2\xi}{2} \geq 0 \Leftrightarrow n-5-2\xi \geq 0 \Leftrightarrow \xi \leq \frac{n-5}{2} \\ n-2-\xi \geq 0 \Leftrightarrow \xi \leq n-2, \end{cases} \tag{40}$$

where the condition $\xi \leq \frac{n-5}{2}$ is chosen to define the upper level of ξ due to is more restrictive than in comparison with $\xi \leq n-1$ and $\xi \leq \frac{n-1}{2}$. In addition, to derive multiplicative inverses in the range of $(-2^n - 2^{\frac{n+1}{2}} - 1, 2^n + 2^{\frac{n+1}{2}} + 1)$ is needed to verify that $\frac{n-5-2\xi}{2} < n$ and $n-2-\xi < n$. Therefore:

$$\begin{cases} \frac{n-5-2\xi}{2} < n \Leftrightarrow -n-5-2\xi < 0 \Leftrightarrow \xi > -\frac{(n+5)}{2} \\ n-2-\xi < n \Leftrightarrow \xi > -2 \Leftrightarrow \xi \geq -1, \end{cases} \tag{41}$$

where the most restrictive condition $\xi \geq -1$ is chosen as lower level given that it is more restrictive than $-\frac{(n-1)}{2}$. □

Proof. From Table I is derived that $|\hat{m}_5^{-1}|_{m_5} = |(\rho)(2^{\frac{3n-5-2\xi}{2}})|_{m_5}$ for $\frac{n-5}{2} \leq \xi \leq \frac{n-1}{2}$, and being ϕ an odd

number, $\phi = 1$ or $\phi = 3$. By substituting m_5, $\hat{m}_5$ and $|\hat{m}_5^{-1}|_{m_5}$ in (3):

$$\left|(2^{n+\beta})(2^{2n}-1)(2^n+2^{\frac{n+1}{2}}+1)(\rho)(2^{\frac{3n-5-2\xi}{2}})\right|_{2^n+2^{\frac{n+1}{2}}+1} =$$

$$= |(2^{n+\beta})(\overbrace{|2^{2n}|_{2^n+2^{\frac{n+1}{2}}+1}}^{=-1}-1)\,(\overbrace{|2^n-2^{\frac{n+1}{2}}+1|_{2^n+2^{\frac{n+1}{2}}+1}}^{=-2\times 2^{\frac{n+1}{2}}})(\rho)(2^{\frac{3n-5-2\xi}{2}})|_{2^n+2^{\frac{n+1}{2}}+1} =$$

$$= \left|(\rho)(2^{\frac{2n+2n\phi+2\xi}{2}})(2^{\frac{n+5}{2}})(2^{\frac{3n-5-2\xi}{2}})\right|_{2^n+2^{\frac{n+1}{2}}+1} = \left|(\rho)(2^{\frac{6n+2n\phi+\cancel{2\xi}+\cancel{5}-\cancel{5}-\cancel{2\xi}}{2}})\right|_{2^n+2^{\frac{n+1}{2}}+1} = \left|(\rho)(2^{3n+n\phi})\right|_{2^n+2^{\frac{n+1}{2}}+1}, \quad (42)$$

(43)

where the cases of ϕ derives into the same expression:

$$\phi = \begin{cases} 1, & \rho = +1, \quad \left|(+1)(2^{4n})\right|_{2^n+2^{\frac{n+1}{2}}+1} \\ 3, & \rho = -1, \quad \left|(-1)(2^{6n})\right|_{2^n+2^{\frac{n+1}{2}}+1} = |(-1)(2^{4n})(\overbrace{|2^{2n}|_{2^n+2^{\frac{n+1}{2}}+1}}^{=-1})|_{2^n+2^{\frac{n+1}{2}}+1}, \end{cases} \quad (44)$$

which can be rewritten as:

$$|\overbrace{2^{4n}}^{=+1}|_{2^n+2^{\frac{n+1}{2}}+1} = 1, \quad (45)$$

The constrain $\frac{3n-5-2\xi}{2} \geq 0$ needs to be set in order to have multiplicative inverses based on summation of powers of two integers. However, the constrain $\xi \leq \frac{n-1}{2}$ is chosen as the upper level given that it is more restrictive than $\xi \leq \frac{3n-5}{2}$. In addition, to derive multiplicative inverses in the range of $(-2^n+2^{\frac{n+1}{2}}-1, 2^n-2^{\frac{n+1}{2}}+1)$ one needs to verify that $\frac{3n-5-2\xi}{2} < n$. Therefore, $\xi > \frac{n-5}{2}$ is chosen as lower level due to is more restrictive than $\xi \geq -\frac{(n-1)}{2}$. □

2 Multiplicative inverses validation associated to the horizontal and hybrid extension moduli set $\{\mathbf{2^{n+\beta}}, 2^n-1, 2^n+1, 2^n-2^{\frac{n+1}{2}}+1, 2^n+2^{\frac{n+1}{2}}+1, \mathbf{2^{n\pm 1}+1}\}$

In this section the lemmas 3 to 8 related to the multiplicative inverses of the moduli set $\{\mathbf{2^{n+\beta}}, 2^n-1, 2^n+1, 2^n-2^{\frac{n+1}{2}}+1, 2^n+2^{\frac{n+1}{2}}+1, \mathbf{2^{n\pm 1}+1}\}$ presented in the paper [1] are validated.

Proof. To prove that the multiplicative inverse of $(2^{5n}-2^n)$ modulo $2^{n-1}+1$ is:

$$|(2^{5n}-2^n)^{-1}|_{2^{n-1}+1} = \frac{904}{15} \times 2^{n-5} + \frac{56}{15}\ , \quad (46)$$

we have to show that:

$$|(2^{5n}-2^n) \times (\frac{904}{15} \times 2^{n-5} + \frac{56}{15})|_{2^{n-1}+1} = 1. \quad (47)$$

With:

$$\left|(2^{5n}-2^n)\right|_{2^{n-1}+1} = \left|2^{n-1} \times 2^{4n+1}+2)\right|_{2^{n-1}+1} = \left|-2^{4n+1}+2\right|_{2^{n-1}+1} = \left|-2^{n-1} \times 2^{3n+2}+2)\right|_{2^{n-1}+1} =$$
$$= \left|+2^{3n+2}+2\right|_{2^{n-1}+1} = \left|2^{n-1} \times 2^{2n+3}+2)\right|_{2^{n-1}+1} = \left|-2^{2n+3}+2\right|_{2^{n-1}+1} = \left|-2^{n-1} \times 2^{n+4}+2)\right|_{2^{n-1}+1} =$$
$$= \left|2^{n+4}+2\right|_{2^{n-1}+1} = |-30|_{2^{n-1}+1}\,, \quad (48)$$

(47) can be written as:

$$\left|(2^{5n}-2^n) \times (\frac{904}{15} \times 2^{n-5} + \frac{56}{15})\right|_{2^{n-1}+1} = \left|-\frac{30}{15} \times (904 \times \frac{2^{n-1}}{2^4} + 56)\right|_{2^{n-1}+1} = \left|\frac{1808}{2^4} - 112\right|_{2^{n-1}+1} =$$
$$= |113-112|_{2^{n-1}+1} = 1. \quad (49)$$

To finish the proof we have to show that:

$$\frac{904}{15} \times 2^{n-5} + \frac{56}{15} = -2^{n-2} + \sum_{i=0}^{\frac{n-9}{4}} 2^{4i+10} + 2^6 + 2^3\ . \quad (50)$$

For the proof of (50) we use the sum of n terms of a geometric series with common ratio r:

$$\sum_{i=m}^{n} r^i = \frac{r^m - r^{n+1}}{1-r} \quad . \tag{51}$$

Therefore, taking into account that in this case $n = 4k+5,\ k \in \mathbb{N}_0$ it is possible to chose values for $n \geq 5$ that set (50):

$$-2^{n-2} + \sum_{i=0}^{\frac{n-9}{4}} 2^{4i+10} + 2^6 + 2^3 = -2^{n-2} + 2^{10} \times \frac{1-2^{n-5}}{1-2^4} + 72 = -2^3 \times 2^{n-5} - \frac{1024}{15} + \frac{1024 \times 2^{n-5}}{15} + \frac{1080}{15} =$$

$$= -\frac{120 \times 2^{n-5}}{15} + \frac{1024 \times 2^{n-5}}{15} + \frac{56}{15} = \frac{904}{15} \times 2^{n-5} + \frac{56}{15} \quad . \tag{52}$$

Thus, lemma 3 is proved. □

Proof. To prove that the multiplicative inverse of $(2^{5n} - 2^n)$ modulo $2^{n+1}+1$ is:

$$|(2^{5n} - 2^n)^{-1}|_{2^{n+1}+1} = -\frac{256}{15} \times 2^{n-7} + \frac{31}{15} \quad , \tag{53}$$

we have to show that:

$$|(2^{5n} - 2^n) \times (-\frac{256}{15} \times 2^{n-7} + \frac{31}{15})|_{2^{n+1}+1} = 1. \tag{54}$$

With:

$$|2^{5n} - 2^n|_{2^{n+1}+1} = |\frac{1}{32} \times \overbrace{(2^{n+1})^5}^{=-1} + \frac{1}{2}|_{2^{n+1}+1} = \frac{15}{32}, \quad .$$

and operating in the same way than (48), (54) can be written as:

$$|\frac{15}{32} \times (-\frac{256}{15} \times \overbrace{2^{n+1}}^{=-1} \times 2^{-8} + \frac{31}{15})|_{2^{n+1}+1} = 1. \tag{55}$$

To finish the proof we have to show that:

$$\left|(2^{5n} - 2^n)^{-1}\right|_{2^{n+1}+1} = -\sum_{i=0}^{\frac{n-11}{4}} 2^{4i+8} - 2^3 - 2^2 - 2^1 - 2^0 \quad . \tag{56}$$

Therefore, by using (51) and taking into account that in this case $n = 4k+7,\ k \in \mathbb{N}_0$ it is possible to chose values for $n \geq 7$ that set (56):

$$-\sum_{i=0}^{\frac{n-11}{4}} 2^{4i+8} - 2^3 - 2^2 - 2^1 - 2^0 = -2^8 \times \frac{1-2^{n-7}}{1-2^4} - 15 = \frac{256}{15} - \frac{256 \times 2^{n-7}}{15} - \frac{225}{15} = -\frac{256}{15} \times 2^{n-7} + \frac{31}{15}. \tag{57}$$

Thus, lemma 4 is proved. □

Proof. To prove that the multiplicative inverse of $(2^{6n} - 2^{2n})$ modulo $2^{n-1}+1$ is:

$$|(2^{6n} - 2^{2n})^{-1}|_{2^{n-1}+1} = -\frac{452}{15} \times 2^{n-5} - \frac{28}{15} \quad , \tag{58}$$

we have to show that:

$$|(2^{6n} - 2^{2n}) \times (-\frac{452}{15} \times 2^{n-5} - \frac{28}{15})|_{2^{n-1}+1} = 1. \tag{59}$$

With:

$$|(2^{6n} - 2^{2n})|_{2^{n-1}+1} = |64 \times \overbrace{(2^{n-1})^6}^{=1} - \overbrace{(2^{n-1})^2}^{=1} \times 2^2|_{2^{n-1}+1} = 60,$$

(59) can be written as:

$$|60 \times (-\frac{452}{15} \times \overbrace{2^{n-1}}^{=-1} \times 2^{-4} - \frac{28}{15})|_{2^{n-1}+1} = 1. \tag{60}$$

To finish the proof we have to show that:

$$-\frac{452}{15} \times 2^{n-5} - \frac{28}{15} = 2^{n-3} - \sum_{i=0}^{\frac{n-9}{4}} 2^{4i+9} - 2^5 - 2^2 \ . \tag{61}$$

By using (51):

$$2^{n-3} - \sum_{i=0}^{\frac{n-9}{4}} 2^{4i+9} - 2^5 - 2^2 = 2^{n-3} - 2^9 \times \frac{1-2^{n-5}}{1-2^4} - 36 = 2^2 \times 2^{n-5} + \frac{512}{15} - \frac{512 \times 2^{n-5}}{15} - \frac{540}{15} =$$
$$= \frac{60 \times 2^{n-5}}{15} - \frac{512 \times 2^{n-5}}{15} - \frac{28}{15} = -\frac{452}{15} \times 2^{n-5} - \frac{28}{15} \ . \tag{62}$$

Thus, lemma 5 is proved. □

Proof. To prove that the multiplicative inverse of $(2^{6n} - 2^{2n})$ modulo $2^{n+1} + 1$ is:

$$\left|(2^{6n} - 2^{2n})^{-1}\right|_{2^{n+1}+1} = \frac{512}{15} \times 2^{n-7} - \frac{62}{15} \ , \tag{63}$$

we have to show that:

$$\left|(2^{6n} - 2^{2n}) \times (\frac{512}{15} \times 2^{n-7} - \frac{62}{15})\right|_{2^{n+1}+1} = 1. \tag{64}$$

With:

$$\left|2^{6n} - 2^{2n}\right|_{2^{n+1}+1} =$$
$$= |\frac{1}{64} \times \overbrace{(2^{n+1})^6}^{=1} - \frac{1}{4} \times \overbrace{(2^{n+1})^2}^{=1}|_{2^{n+1}+1} = |-\frac{15}{64}|_{2^{n+1}+1},$$

(64) can be written as:

$$|(-\frac{15}{64}) \times (\frac{512}{15} \times \overbrace{2^{n+1}}^{=-1} \times 2^{-8} - \frac{62}{15})|_{2^{n+1}+1} = 1. \tag{65}$$

To finish the proof we have to show that:

$$\left|(2^{6n} - 2^{2n})^{-1}\right|_{2^{n+1}+1} = \sum_{i=0}^{\frac{n-11}{4}} 2^{4i+9} + 2^4 + 2^3 + 2^2 + 2^1. \tag{66}$$

By using (51):

$$\sum_{i=0}^{\frac{n-11}{4}} 2^{4i+9} + 2^4 + 2^3 + 2^2 + 2^1 = 2^9 \times \frac{1-2^{n-7}}{1-2^4} + 30 = -\frac{512}{15} + \frac{512 \times 2^{n-7}}{15} + \frac{450}{15}\frac{512}{15} \times 2^{n-7} - \frac{62}{15}. \tag{67}$$

Thus, lemma 6 is proved. □

Proof. To prove that the multiplicative inverse of $(2^{7n} - 2^{3n})$ modulo $2^{n-1} + 1$ is:

$$\left|(2^{7n} - 2^{3n})^{-1}\right|_{2^{n-1}+1} = \frac{226}{15} \times 2^{n-5} + \frac{14}{15} \ , \tag{68}$$

we have to show that:

$$\left|(2^{7n} - 2^{3n}) \times (\frac{226}{15} \times 2^{n-5} + \frac{14}{15})\right|_{2^{n-1}+1} = 1. \tag{69}$$

With:

$$\left|(2^{7n}-2^{3n})\right|_{2^{n-1}+1} =$$
$$= |128 \times \overbrace{(2^{n-1})^7}^{=-1} - 8 \times \overbrace{(2^{n-1})^3}^{=-1}|_{2^{n-1}+1} = |-120|_{2^{n-1}+1},$$

(69) can be written as:

$$|(-120) \times (\frac{226}{15} \times \overbrace{2^{n-1}}^{=-1} \times 2^{-4} + \frac{14}{15})|_{2^{n-1}+1} = 1. \tag{70}$$

To finish the proof we have to show that:

$$\frac{226}{15} \times 2^{n-5} + \frac{14}{15} = -2^{n-4} + \sum_{i=0}^{\frac{n-9}{4}} 2^{4i+8} + 2^4 + 2^1 \quad . \tag{71}$$

By using (51):

$$-2^{n-4} + \sum_{i=0}^{\frac{n-9}{4}} 2^{4i+8} + 2^4 + 2^1 = -2^{n-4} + 2^8 \times \frac{1-2^{n-5}}{1-2^4} + 18 = -2^1 \times 2^{n-5} - \frac{256}{15} + \frac{256 \times 2^{n-5}}{15} + \frac{270}{15} =$$
$$= -\frac{30 \times 2^{n-5}}{15} + \frac{256 \times 2^{n-5}}{15} + \frac{14}{15} = \frac{226}{15} \times 2^{n-5} + \frac{14}{15} \quad . \tag{72}$$

Thus, lemma 7 is proved. □

Proof. To prove that the multiplicative inverse of $(2^{7n} - 2^{3n})$ modulo $2^{n+1} + 1$ is:

$$\left|(2^{7n}-2^{3n})^{-1}\right|_{2^{n+1}+1} = -\frac{1024}{15} \times 2^{n-7} + \frac{124}{15}, \tag{73}$$

we have to show that:

$$\left|(2^{7n}-2^{3n}) \times (-\frac{1024}{15} \times 2^{n-7} + \frac{124}{15})\right|_{2^{n+1}+1} = 1. \tag{74}$$

With:

$$|2^{7n}-2^{3n}|_{2^{n+1}+1} = |\frac{1}{128} \times \overbrace{(2^{n+1})^7}^{=-1} - \frac{1}{8} \times \overbrace{(2^{n+1})^3}^{=-1}|_{2^{n+1}+1} = \frac{15}{128},$$

(74) can be written as:

$$|(\frac{15}{128}) \times (-\frac{1024}{15} \times \overbrace{2^{n+1}}^{=-1} \times 2^{-8} + \frac{124}{15})|_{2^{n+1}+1} = 1. \tag{75}$$

To finish the proof we have to show that:

$$\left|(2^{7n}-2^{3n})^{-1}\right|_{2^{n+1}+1} = -\sum_{i=0}^{\frac{n-11}{4}} 2^{4i+10} - 2^5 - 2^4 - 2^3 - 2^2. \tag{76}$$

By using (51):

$$-\sum_{i=0}^{\frac{n-11}{4}} 2^{4i+10} - 2^5 - 2^4 - 2^3 - 2^2 = -2^{10} \times \frac{1-2^{n-7}}{1-2^4} - 60 = \frac{1024}{15} - \frac{1024 \times 2^{n-7}}{15} - \frac{900}{15} = -\frac{1024}{15} \times 2^{n-7} + \frac{124}{15}. \tag{77}$$

Thus, lemma 8 is proved. □

Acknowledgments

This work was partially supported by FCT (INESC-ID multiannual funding) through the PIDDAC Program funds and the European Network of Excellence on High Performance and Embedded Architecture and Compilation (HiPEAC) funds.

References

[1] H. Pettenghi, R. Chaves and L. Sousa, "RNS Reverse Converters for Moduli Sets with Dynamic Ranges up to $(8n+1)$-bit", *Submitted in IEEE Transactions on Circuits and Systems I*, (2012).