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 $\{2^{n+\beta}, 2^n - 1, 2^n + 1, 2^n + 2^{\frac{n+1}{2}} + 1\}$ and the hybrid extension $\{2^{n+\beta}, 2^n - 1, 2^n + 1, 2^n - 2^{\frac{n+1}{2}} + 1, 2^n + 2^{\frac{n+1}{2}} + 1\}$ presented in the paper [1] are validated.

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

The extension of the power of two modulus herein proposed adds a parameter $\beta$ to the exponent, leading to the five moduli set $\{2^{n+\beta}, 2^n - 1, 2^n + 1, 2^n - 2^{\frac{n+1}{2}} + 1, 2^n + 2^{\frac{n+1}{2}} + 1\}$, 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:

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

(1)

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

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

(2)

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

$$
\left\lfloor (\hat{m}_i) \times (\hat{m}_i^{-1}) \right\rfloor_{m_i} = 1,
$$

(3)

for $i = 1, 2, 3, 4, 5$, which proof is presented as follows.
Table 1: Multiplicative inverses for moduli set \{2^{n+\beta}, 2^n - 1, 2^n + 1, 2^n - 2^{n-\xi}, 1, 2^n + 2^{n-\xi} + 1\} for generic \(\beta = \phi n + \xi\)

<table>
<thead>
<tr>
<th>Multiplicative Inverse</th>
<th>(-\frac{(n-1)}{2} \leq \xi &lt; -1)</th>
<th>(-1 \leq \xi \leq \frac{(n-5)}{2})</th>
<th>(\frac{(n-5)}{2} &lt; \xi \leq \frac{(n-1)}{2})</th>
</tr>
</thead>
<tbody>
<tr>
<td>(\hat{m}_1^{-1}) (m_1) for (\phi) even</td>
<td>(-</td>
<td>1</td>
<td>_{m_1})</td>
</tr>
<tr>
<td>(\hat{m}_2^{-1}) (m_2) for (\phi) odd</td>
<td>(2^n-\xi)</td>
<td>(2^n-\xi)</td>
<td>(2^n-\xi)</td>
</tr>
<tr>
<td>(\hat{m}_3^{-1}) (m_3) for (\phi) even</td>
<td>(-\rho \cdot 2^{n-\xi-2\phi} ) (m_3)</td>
<td>(-\rho \cdot 2^{n-\xi-2\phi} ) (m_3)</td>
<td>(-\rho \cdot 2^{n-\xi-2\phi} ) (m_3)</td>
</tr>
<tr>
<td>(\hat{m}_4^{-1}) (m_4) for (\phi) odd</td>
<td>(-\rho \cdot 2^{n-\xi-2\phi} ) (m_4)</td>
<td>(-\rho \cdot 2^{n-\xi-2\phi} ) (m_4)</td>
<td>(-\rho \cdot 2^{n-\xi-2\phi} ) (m_4)</td>
</tr>
<tr>
<td>(\hat{m}_5^{-1}) (m_5) for (\phi) even</td>
<td>(-\rho \cdot 2^{n-\xi-2\phi} ) (m_5)</td>
<td>(-\rho \cdot 2^{n-\xi-2\phi} ) (m_5)</td>
<td>(-\rho \cdot 2^{n-\xi-2\phi} ) (m_5)</td>
</tr>
<tr>
<td>(\hat{m}_6^{-1}) (m_6) for (\phi) odd</td>
<td>(-\rho \cdot 2^{n-\xi-2\phi} ) (m_6)</td>
<td>(-\rho \cdot 2^{n-\xi-2\phi} ) (m_6)</td>
<td>(-\rho \cdot 2^{n-\xi-2\phi} ) (m_6)</td>
</tr>
</tbody>
</table>

- \(i = 1:\)

Proof. From Table 1 is derived that \(\hat{m}_1^{-1}\) \(m_1\) for all the range of \(\xi\) and \(\phi\). By substituting \(m_1\), \(\hat{m}_1\) and \(\hat{m}_1^{-1}\) \(m_1\) in (3):

\[
\begin{align*}
  |(2^{n+1})(-2^n+1)|_{2n+\beta} & = |2^{n+1} - 2^n|_{2n+\beta} = |(2^{n+1})|_{2n+\beta} + 1|_{2n+\beta} = 0 + 1|_{2n+\beta} = 1,
\end{align*}
\]

when \(0 \leq \beta \leq 3n\).

- \(i = 2:\)

Proof. From Table 1 is derived that \(\hat{m}_2^{-1}\) \(m_2\) for all the range of \(\xi\) and \(\phi\). By substituting \(m_2\), \(\hat{m}_2\) and \(\hat{m}_2^{-1}\) \(m_2\) in (3):

\[
\begin{align*}
  |(2^{n+\beta})(2^n + 1)|_{2n+\beta} & = |(2^{n+\beta})|_{2n+\beta} + 1|_{2n+\beta} = 0 + 1|_{2n+\beta} = 1,
\end{align*}
\]

for all the integers values of \(0 \leq \phi \leq 3\).

- \(i = 3:\)

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

\[
\begin{align*}
  |(2^{n+\beta})(2^n - 1)|_{2n+\beta} & = |(2^{n+\beta})|_{2n+\beta} + 1|_{2n+\beta} = 0 + 1|_{2n+\beta} = 1,
\end{align*}
\]

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

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

\[
\begin{align*}
  |(2^{n+\beta})(2^n - 1)(2^{n+1})(2^{n+2-\xi})|_{2n+1} & = |(2^{n+\beta})|_{2n+1} + 1|_{2n+1} = 0 + 1|_{2n+1} = 1,
\end{align*}
\]

which is true for odd values of \((2 + \phi)\). Therefore, for odd values of \(\phi\) the proof is given by (7).
\[ i = 4: \]

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

\[
(|(2^{n+\beta})(2^{2n} - 1)(2^n + 2^{n+1} + 1)(\rho \cdot 2^{n-5-2\xi})|_{2^n-2^{n+1}+1} =
\]

\[
= |(2^{n+\beta})(2^{2n} + 2^{n+1} + 1)(\rho \cdot 2^{n-5-2\xi})|_{2^n-2^{n+1}+1} =
\]

\[
= |(-\rho)(2^{n+2\xi}+\xi)2^{n+2}\xi|_{2^n-2^{n+1}+1} = |(-\rho)(2^{n+2\xi})(2^{n+2})|_{2^n-2^{n+1}+1} = |\rho \cdot 2^{n\phi}|_{2^n-2^{n+1}+1},
\]

where the cases of \(\phi\) derive into the same expression:

\[
\phi = \begin{cases} 0, & \rho = +1, \\ 2, & \rho = -1, \end{cases}
\]

\[
(|(1)(2^{2n})|_{2^n-2^{n+1}+1} = 1
\]

The range of \(\xi\) 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 \((-2^n + 2^{n+1} - 1, 2^n - 2^{n+1} + 1)\). However, \(\xi > -\frac{n+3}{2}\) derived from the latter constrain is less restrictive than the absolute value of \(\xi\) predefined to provide all the possible values of \(\beta\), \((-\frac{n+1}{2} \leq \beta \leq 3n)\). Thus, \(n \geq -\frac{n+1}{2}\) is chosen as the lower level in this case. \(\Box\)

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

\[
(|(2^{n+\beta})(2^{2n} - 1)(2^n + 2^{n+1} + 1)(\rho \cdot 2^{n+2\xi} + 2^n - \xi)|_{2^n-2^{n+1}+1} =
\]

\[
= |(2^{n+\beta})(2^{2n} + 2^{n+1} + 1)(\rho \cdot 2^{n+2\xi} + 2^n - \xi)|_{2^n-2^{n+1}+1} =
\]

\[
= |(-\rho)(2^{n+2\xi}+\xi)2^{n+2}\xi|_{2^n-2^{n+1}+1} = |(-\rho)(2^{n+2\xi})(2^{n+2})|_{2^n-2^{n+1}+1} = |\rho \cdot 2^{n\phi}|_{2^n-2^{n+1}+1},
\]

where the cases of \(\phi\) derive into the same expression:

\[
\phi = \begin{cases} 0, & \rho = +1, \\ 2, & \rho = -1, \end{cases}
\]

\[
(|(1)(2^{2n+2})|_{2^n-2^{n+1}+1} = 1
\]

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:

\[
\begin{align*}
\frac{3n-5-2\xi}{2} \geq 0 & \iff 3n - 5 - 2\xi \geq 0 \iff \xi \leq \frac{3n-5}{2} \\
n - 2 - 2\xi \geq 0 & \iff \xi \leq n - 2,
\end{align*}
\]
However, the condition \( \xi \leq \frac{n-1}{2} \) is chosen to define the upper level of \( \xi \) 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 \( \frac{n-5-2\xi}{2} < n \) and \( n - 2 - \xi < n \). Therefore:

\[
\begin{aligned}
&\begin{cases}
3n-5-2\xi < n \Leftrightarrow n - 5 - 2\xi < 0 \Leftrightarrow \xi > \frac{n-5}{2} \\
n - 2 - \xi < n \Leftrightarrow \xi > -2,
\end{cases}
\end{aligned}
\]

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

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

\[
\begin{aligned}
&\begin{cases}
|(-\rho)(2^n + (\rho + 1)\phi + 5)(2^{\frac{n-5}{2}} + 2^{-\xi+2})|_{2^n-2^{\frac{n+1}{2}}+1} = \\
\end{cases}
\end{aligned}
\]

where the cases of \( \phi \) derives into the same expression:

\[
\phi = \begin{cases}
1, & \rho = +1, \\
3, & \rho = -1,
\end{cases}
\]

which can be rewritten as:

\[
\begin{aligned}
&\begin{cases}
|(-1)(-2^{2n} + 2^{\frac{n+1}{2} + 1})|_{2^n-2^{\frac{n+1}{2}}+1} = \left|(-1)(-2^{2n})\left(2^{2n}\right)_{2^n-2^{\frac{n+1}{2}}+1} + \\
\end{cases}
\end{aligned}
\]

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:

\[
\begin{aligned}
&\begin{cases}
n - 1 - \xi \geq 0 \Leftrightarrow \xi \leq n - 1 \\
-(\xi + 2) \geq 0 \Leftrightarrow \xi \leq -2 \Leftrightarrow \xi < -1,
\end{cases}
\end{aligned}
\]

However, the condition \( \xi < -1 \) is chosen to define the upper level of \( \xi \) 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:

\[
\begin{aligned}
&\begin{cases}
\frac{n-5-2\xi}{2} < n \Leftrightarrow n - 5 - 2\xi < 0 \Leftrightarrow \xi > \frac{n-5}{2} \\
-\xi + 2 < n \Leftrightarrow \xi > -(n + 2).
\end{cases}
\end{aligned}
\]

However, these constrains are less restrictive than the absolute lower level constrain of \( \xi, \xi > \frac{-(n-1)}{2} \), which is chosen as the lower level.
Proof. From Table I is derived that \(|\hat{m}_4^{-1}|_{m_4} = |\rho \cdot (-2^{n-2} - 2^{n-5} - 2^{n-2} + 2^{n-5} + 2)|_{m_4}\) for \(-1 \leq \xi \leq \frac{n-5}{2}\), and being \(\phi\) an odd number, \(\phi = 1\) or \(\phi = 3\). By substituting \(m_4, \hat{m}_4\) and \(|\hat{m}_4^{-1}|_{m_4}\) in (3):

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

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

where the cases of \(\phi\) derives into the same expression:

\[
\phi = \begin{cases} 
1, & \rho = +1, \\
3, & \rho = -1,
\end{cases} \left|\left((-\rho)(2^{n+\beta}(2^{2n^3} - 1)(2^{n + 2^{n+1}} + 1))\right)_{2n-2\frac{n+1}{2}+1}\right| = \left|\left((-\rho)(2^{n+\beta}(2^{2n^3} - 1)(2^{n + 2^{n+1}} + 1))\right)_{2n-2\frac{n+1}{2}+1}\right|
\]

which can be rewritten as:

\[
\left|\left((-\rho)(2^{n+\beta}(2^{2n^3} - 1)(2^{n + 2^{n+1}} + 1))\right)_{2n-2\frac{n+1}{2}+1}\right| = \left|\left((-\rho)(2^{n+\beta}(2^{2n^3} - 1)(2^{n + 2^{n+1}} + 1))\right)_{2n-2\frac{n+1}{2}+1}\right|
\]
which can be rewritten as:

\[
\frac{-n+1}{2^{4n} \mid 2^n - 2 \frac{n+1}{2} + 1} = 1,
\]

(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 \( \xi \leq \frac{n-5}{2} \) 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 \( \xi \geq -\frac{(n-1)}{2} \).

\( \bullet \) \( i = 5 \):

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

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

\[
\left| -2 \times \frac{n+1}{2} \right|_{2^n + 2 \frac{n+1}{2} + 1} - 1 \left| (2^n - 2^{\frac{n+1}{2}} + 1) \right|_{2^n + 2 \frac{n+1}{2} + 1} =
\]

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

\[
\left| (-\rho)(2^{n+\phi+\xi})(2^{\frac{n+1}{2}})(2^{\frac{n-5-2\xi}{2}}) \right|_{2^n + 2 \frac{n+1}{2} + 1} =
\]

\[
\left| \rho \cdot 2^{\phi} \right|_{2^n + 2 \frac{n+1}{2} + 1},
\]

(27)

where the cases of \( \phi \) derives into the same expression:

\[
\phi = \begin{cases} 
0, & \rho = +1, \\
\rho = +1, & (-1)(2^n)_{2^n + 2 \frac{n+1}{2} + 1} = 1 \\
2, & \rho = -1, \\
\end{cases}
\]

(28)

The range of \( \xi \) is defined from two constraints. 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, \( \xi > -\frac{(n-5)}{2} \) is derived from the latter constrain is less restrictive than the absolute value of \( \xi \) predefined to provide all the possible values of \( \beta \), \(-\frac{(n-1)}{2} \leq \beta \leq 3n \). Thus, \( \xi \geq -\frac{(n-1)}{2} \) is chosen as the lower level in this case.

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

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

\[
\left| -2 \times \frac{n+1}{2} \right|_{2^n + 2 \frac{n+1}{2} + 1} - 1 \left| (2^n - 2^{\frac{n+1}{2}} + 1) \right|_{2^n + 2 \frac{n+1}{2} + 1} =
\]

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

\[
\left| (\rho)(2^{6n+2n+2\xi+3n} + 2^{n+2\xi+3n} + 2^{n+2\xi+3n}) \right|_{2^n + 2 \frac{n+1}{2} + 1} =
\]

\[
\left| (\rho)(2^{6n+2n+2\xi+3n} + 2^{n+2\xi+3n} + 2^{n+2\xi+3n}) \right|_{2^n + 2 \frac{n+1}{2} + 1} =
\]

\[
\left| \rho \right|_{2^n + 2 \frac{n+1}{2} + 1} \left| (\rho)(2^{6n+2n+2\xi+3n} + 2^{n+2\xi+3n} + 2^{n+2\xi+3n}) \right|_{2^n + 2 \frac{n+1}{2} + 1},
\]

(29)

where the cases of \( \phi \) derives into the same expression:

\[
\phi = \begin{cases} 
0, & \rho = +1, \\
\rho = +1, & (-1)(2^n + 2^{\frac{n+1}{2}} 2^{2n})_{2^n + 2 \frac{n+1}{2} + 1} = 1 \\
2, & \rho = -1, \\
\end{cases}
\]

(30)
which can be rewritten as:

$$\frac{(-1)}{(2^n + 2^{\frac{n+1}{2}})} \left(2^{n+2} \frac{n+1}{2} \right)\frac{n+1}{2} + 1 = 1. \quad (31)$$

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:

$$\begin{align*}
\begin{cases}
\frac{3n-5-2\xi}{2} \geq 0 \iff 3n - 5 - 2\xi \geq 0 \iff \xi \leq \frac{3n-5}{2} \\
n - 2 - \xi \geq 0 \iff \xi \leq n - 2,
\end{cases}
\end{align*} \quad (32)$$

However, the condition $\xi \leq \frac{n-1}{2}$ is chosen to define the upper level of $\xi$ 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:

$$\begin{align*}
\begin{cases}
\frac{3n-5-2\xi}{2} < n \iff n - 5 - 2\xi < 0 \iff \xi > \frac{3n-5}{2} \\
n - 2 - \xi < n \iff \xi > -2,
\end{cases}
\end{align*} \quad (33)$$

where the most restrictive condition $\xi > \frac{n-1}{2}$ is chosen as the lower level.

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

$$\begin{align*}
\begin{align*}
|\rho \cdot (2^{n+2}\phi + 2^{\xi+1})|_{\hat{m}_5} & = |\rho \cdot (2^{n+2}\phi + 2^{\xi+1})|_{\hat{m}_5} \\
& = |\rho \cdot (2^{n+2}\phi + 2^{\xi+1})|_{\hat{m}_5} \\
& = |\rho \cdot (2^{n+2}\phi + 2^{\xi+1})|_{\hat{m}_5} \\
& = |\rho \cdot (2^{n+2}\phi + 2^{\xi+1})|_{\hat{m}_5}
\end{align*}
\end{align*}$$

where the cases of $\phi$ derive into the same expression:

$$\phi = \begin{cases} 
1, & \rho = +1, \\
3, & \rho = -1,
\end{cases} \quad (34)$$

which can be rewritten as:

$$\begin{align*}
\begin{align*}
\begin{cases}
\frac{(-1)}{(2^n + 2^{\frac{n+1}{2}})} \left(2^{n+2} \frac{n+1}{2} \right)\frac{n+1}{2} + 1 = 1,
\end{cases}
\end{align*}
\end{align*} \quad (35)$$

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:

$$\begin{align*}
\begin{cases}
n - 1 - \xi \geq 0 \iff \xi \leq n - 1 \\
-(\xi + 2) \geq 0 \iff \xi \leq -2 \iff \phi < -1,
\end{cases}
\end{align*} \quad (36)$$
However, the condition $\xi < -1$ is chosen to define the upper level of $\xi$ given that it is more restrictive in comparison with $\xi \leq n - 1$ and $\xi \leq \frac{n-5}{2}$. 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 $\frac{n-5-2\xi}{2} < n$ and $-(\xi + 2) < n$. Therefore:

\[
\begin{align*}
\frac{n-5-2\xi}{2} < n & \iff -n - 5 - 2\xi < 0 \iff \xi > \frac{-(n+5)}{2} \\
-\xi - 2 < n & \iff \xi > -(n + 2).
\end{align*}
\]

(37)

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

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

\[
\begin{align*}
|\tilde{m}_5^{-1}|_{m_5} &= |\rho \cdot (-2^{n-2-\xi} - 2 \frac{n-5-2\xi}{2})|_{m_5} \\
&= |\rho \cdot (2^n - 2^{\frac{n+1}{2}} + 1)(-\rho)(2^{n-2-\xi} + 2^{\frac{n-5-2\xi}{2}})|_{2^n+2^{\frac{n+1}{2}}+1} = \\
&= |(-\rho)(2^{\frac{n+1}{2}})2^n(2^{n+2\frac{n+1}{2}} + 1)(-\rho)(2^{n-2-\xi} + 2^{\frac{n-5-2\xi}{2}})|_{2^n+2^{\frac{n+1}{2}}+1} = \\
&= |(-\rho)(2^{\frac{5n+2n+1}{2}} + 2^{\frac{5n+1}{2}})|_{2^n+2^{\frac{n+1}{2}}+1} = |(-\rho)(2^{\frac{n+1}{2}} + 1)(2^{2+\phi}n)|_{2^n+2^{\frac{n+1}{2}}+1},
\end{align*}
\]

(38)

where the cases of $\phi$ derives into the same expression:

\[
\phi = \begin{cases} 
1, & \rho = +1, \\
3, & \rho = -1,
\end{cases}
\]

\[
\begin{align*}
&\frac{n-5-2\xi}{2} < n \iff -n - 5 - 2\xi < 0 \iff \xi > \frac{-(n+5)}{2} \\
&-\xi - 2 < n \iff \xi > -(n + 2)
\end{align*}
\]

(40)

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:

\[
\begin{align*}
\frac{n-5-2\xi}{2} \geq 0 & \iff -n - 5 - 2\xi \geq 0 \iff \xi \leq \frac{n-5}{2} \\
n - 2 - \xi \geq 0 & \iff \xi \leq n - 2.
\end{align*}
\]

(40)

where the condition $\xi \leq \frac{n-5}{2}$ is chosen to define the upper level of $\xi$ 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:

\[
\begin{align*}
\frac{n-5-2\xi}{2} < n & \iff -n - 5 - 2\xi < 0 \iff \xi > \frac{-(n+5)}{2} \\
n - 2 - \xi < n & \iff \xi > 2 \iff \xi \geq -1
\end{align*}
\]

(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 $|\tilde{m}_5^{-1}|_{m_5} = |(\rho)(2^{\frac{3n-5-2\xi}{2}})|_{m_5}$ for $\frac{n-5}{2} \leq \xi \leq \frac{n-1}{2}$, and being $\phi$ an odd
number, $\phi = 1$ or $\phi = 3$. By substituting $m_5, \tilde{m}_5$ and $|\tilde{m}_5^{-1}|_{m_5}$ in (3):

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

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

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

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

$$= \left((2^{n+\beta})(2^{2n} - 1)(2^{n} + 2^{n+1} + 1)(\rho)(2^{n+5-2\xi})\right) 2^{n+2} 2^{n+1} + 1,$$

where the cases of $\phi$ derives into the same expression:

$$\phi = \begin{cases} 1, & \rho = +1, \\ 3, & \rho = -1. \end{cases}$$

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

which can be rewritten as:

$$\left|2^{4n}\right|_{2^n+2} 2^{n+1} + 1 = 1,$$

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 $(-2^n + 2^{n+1} - 1, 2^n - 2^{n+1} + 1)$ 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 $\{2^{n+\beta}, 2^n - 1, 2^n + 1, 2^n - 2^{n+1} + 1, 2^n + 2^{n+1} + 1, 2^n\pm1 + 1\}$

In this section the lemmas 3 to 8 related to the multiplicative inverses of the moduli set $\{2^{n+\beta}, 2^n - 1, 2^n + 1, 2^n - 2^{n+1} + 1, 2^n + 2^{n+1} + 1, 2^n\pm1 + 1\}$ 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:

$$\left|2^{5n} - 2^n\right|_{2^n+1} = \frac{904}{15} \times 2^{n-5} + \frac{56}{15},$$

we have to show that:

$$\left|\frac{904}{15} \times 2^{n-5} + \frac{56}{15}\right|_{2^n+1} = 1.$$  

With:

$$\left|\frac{904}{15} \times 2^{n-5} + \frac{56}{15}\right|_{2^n+1} = \left|\frac{904}{15} \times 2^{n-5} + \frac{56}{15}\right|_{2^n+1} = \frac{1808}{24} - 112 = \left|\frac{113}{112}\right|_{2^n+1} = 1.$$  

To finish the proof we have to show that:

$$\frac{904}{15} \times 2^{n-5} + \frac{56}{15} = -2^{n-2} + 2^{4i+10} + 2^6 + 2^3.$$
For the proof of (50) we use the sum of \( n \) terms of a geometric series with common ratio \( r \):

\[
\sum_{i=0}^{n} r^i = \frac{r^n - r^{n+1}}{1 - r}.
\]  

(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):

\[
-2^{n-2} + \sum_{i=0}^{n-9} 2^{4i+10} + 2^6 + 2^3 = -2^{n-2} + 2^{10} \times \frac{1 - 2^{-5}}{1 - 2} + 72 = -2^3 \times 2^{-n-5} - \frac{1024}{15} + \frac{1024 \times 2^{n-5}}{15} + \frac{1080}{15} = \frac{-120 \times 2^{n-5}}{15} + \frac{1024 \times 2^{n-5}}{15} + \frac{56}{15} = \frac{904}{15} \times 2^{n-5} + \frac{56}{15}.
\]

(52)

Thus, lemma 3 is proved.

\[ \square \]

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

\[
|(2^{5n} - 2^n)^{-1}|_{2^n+1} + 1 = \frac{-256}{15} \times 2^{-7} + \frac{31}{15},
\]

(53)

we have to show that:

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

(54)

With:

\[
|2^{5n} - 2^n|_{2^n+1} + 1 = \frac{1}{32} \times \left( 2^{(2-1)} \right) + \frac{1}{2} |2^n + 1|_{2^n+1} = \frac{15}{32}.
\]

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

\[
\frac{15}{32} \times (\frac{-256}{15} \times 2^n + \frac{31}{15})|_{2^n+1} + 1 = 1.
\]

(55)

To finish the proof we have to show that:

\[
|(2^{5n} - 2^n)^{-1}|_{2^n+1} = -\sum_{i=0}^{n-11} 2^{4i+8} - 2^3 - 2^2 - 2^1 - 2^0.
\]

(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):

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

(57)

Thus, lemma 4 is proved.

\[ \square \]

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

\[
|(2^{6n} - 2^{2n})^{-1}|_{2^{n-1}+1} = \frac{-452}{15} \times 2^{n-5} - \frac{28}{15},
\]

(58)

we have to show that:

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

(59)

With:

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

10
(59) can be written as:

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

To finish the proof we have to show that:

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

By using (51):

\[
2^{n-3} - \sum_{i=0}^{n-9} 2^{4i+9} - 2^5 - 2^2 = 2^{n-3} - 2^9 \times \frac{1 - 2^{-n-5}}{1 - 2^4} - 36 = 2^2 \times 2^{n-5} + \frac{512}{15} \times 2^{n-5} - \frac{512}{15} \times \frac{2^{n-5}}{15} - \frac{540}{15} =
\]

\[
= 60 \times 2^{n-5} - \frac{512}{15} \times 2^{n-5} - \frac{28}{15} = - \frac{452}{15} \times 2^{n-5} - \frac{28}{15}. \tag{62}
\]

Thus, lemma 5 is proved.

\[\square\]

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

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

we have to show that:

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

With:

\[
\left| 2^{6n} - 2^{2n} \right|_{2^{n+1}+1} =
\]

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

(64) can be written as:

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

To finish the proof we have to show that:

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

By using (51):

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

Thus, lemma 6 is proved.

\[\square\]

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:

\[
\left| (2^{7n} - 2^{3n}) \times \left( \frac{226}{15} \times 2^{n-5} + \frac{14}{15} \right) \right|_{2^{n-1}+1} = 1. \tag{69}
\]
Thus, lemma 8 is proved.

(70) can be written as:

\[ |(−120) × \left(\frac{226}{15} \times 2^{n−5} + \frac{14}{15}\right)|_{2^{n−1+1}} = 1. \]

To finish the proof we have to show that:

\[ \frac{226}{15} \times 2^{n−5} + \frac{14}{15} = -2^{n−4} + \sum_{i=0}^{n−9} 2^{4i+8} + 2^4 + 2^1. \]

By using (51):

\[ -2^{n−4} + \sum_{i=0}^{n−9} 2^{4i+8} + 2^4 + 2^1 = -2^{n−4} + 2^8 \times \frac{1−2^{n−5}}{1−2^4} + 18 = -2^4 \times 2^{n−5} - \frac{256}{15} + \frac{256 \times 2^{n−5}}{15} + \frac{270}{15} = \]

\[ = -\frac{30 \times 2^{n−5}}{15} + \frac{256 \times 2^{n−5}}{15} + \frac{14}{15} = \frac{226}{15} \times 2^{n−5} + \frac{14}{15}. \]

Thus, lemma 7 is proved.

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

\[ |(2^{7n} − 2^{3n})^{-1}|_{2^{n+1}+1} = -\frac{1024}{15} \times 2^{n−7} + \frac{124}{15}, \]

we have to show that:

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

With:

\[ |2^{7n} − 2^{3n}|_{2^{n+1}+1} = \frac{1}{128} \times \left(\frac{2^{n+1}}{7} - \frac{1}{8} \times 2^{n+1}\right)|_{2^{n+1}+1} = \frac{15}{128}, \]

(74) can be written as:

\[ \left|\frac{15}{128} \times \left(-\frac{1024}{15} \times 2^{n+1} \times 2^{−8} + \frac{124}{15}\right)\right|_{2^{n+1}+1} = 1. \]

To finish the proof we have to show that:

\[ |(2^{7n} − 2^{3n})^{-1}|_{2^{n+1}+1} = -\sum_{i=0}^{n−11} 2^{4i+10} − 2^5 − 2^4 − 2^3 − 2^2. \]

By using (51):

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

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