Semidirect Product of $\bigoplus$-algebra

Bharat Adsul
Indian Institute of Technology, Bombay

Saptarshi Sarkar
Indian Institute of Technology, Bombay

A. V. Sreejith
Indian Institute of Technology, Goa

Abstract

2012 ACM Subject Classification Dummy classification

Keywords and phrases Dummy keyword

Digital Object Identifier 10.4230/LIPIcs...

1 Algebra for countable words

A $\oplus$-*algebra* $(S, \cdot, \tau, \tau^*, \kappa)$ consists of a set S with $\cdot : S^2 \to S, \tau : S \to S, \tau^* : S \to S, \kappa : \mathcal{P}(S) \setminus \{\emptyset\} \to S$ such that (with infix notation for $\cdot$ and superscript notation for τ, τ^*, κ)

A-1 $(S, \cdot)$ is a semigroup.
A-2 $(a \cdot b)^\tau = a \cdot (b \cdot a)^\tau$ and $(a^n)^\tau = a^\tau$ for $a, b \in S$ and $n > 0$.
A-3 $(b \cdot a)^{\tau^*} = (a \cdot b)^{\tau^*} \cdot a$ and $(a^n)^{\tau^*} = a^{\tau^*}$ for $a, b \in S$ and $n > 0$.
A-4 For every non-empty subset P of S, every element c in P, every subset P' of P, and every non-empty subset P'' of $\{P^\kappa, a.P^\kappa, P^\kappa.b, a.P^\kappa.b \mid a, b \in P\}$, we have $P^\kappa = P^\kappa.P^\kappa = P^\kappa.c.P^\kappa = (P^\kappa)^\tau = (P^\kappa.c)^\tau = (P^\kappa)^{\tau^*} = (c.P^\kappa)^{\tau^*} = (P' \cup P'')^\kappa$.

For any $m \in S$, any $a \in \mathbb{N}$, we'll use m^a to denote the finite product $\cdot$ being applied to a-many m. If $a = 0$, it refers to the neutral element of S^1.

Consider a $\oplus$-algebra $(N, +, \hat{\tau}, \hat{\tau}^*, \hat{\kappa})$. Since in N, $+$ or finite product is not commutative in general, we will use notations like $\sum_{i=1}^{3} n_i$ to represent $n_1 + n_2 + n_3$ and $\sum_{i=3}^{1} n_i$ to represent $n_3 + n_2 + n_1$.

2 Semidirect Product Construction

In this section, we propose a generalization of semidirect product from semigroups to $\oplus$-semigroups. We first define this construction for $\oplus$-algebras.

We begin by introducing the setup of two commuting actions of a $\oplus$-algebra on another.

Consider two $\oplus$-algebra $(M, \cdot, \tau, \tau^*, \kappa)$ and $(N, +, \hat{\tau}, \hat{\tau}^*, \hat{\kappa})$. Note that $\cdot$ and $+$ need not be commutative. A function $\delta_l : M^1 \times N \to N$ is said to be a left action of M on N if it satisfies the following conditions. $\delta_l(m, n)$ is denoted by $m * n$ for convenience.

L-1 $1 * n = n$
L-2 $(m_1 \cdot m_2) * n = m_1 * (m_2 * n)$
L-3 $m * (n_1 + n_2) = m * n_1 + m * n_2$
L-4 $m * n^{\hat{\tau}} = (m * n)^{\hat{\tau}}$
L-5 $m * n^{\hat{\tau}^*} = (m * n)^{\hat{\tau}^*}$

Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

L-6 $m * \{n_1, \ldots, n_j\}^{\hat{\kappa}} = \{m * n_1, \ldots, m * n_j\}^{\hat{\kappa}}$

Similarly, a function $\delta_r : N \times M^1 \to N$ is said to be a right action of M on N if it satisfies the following conditions. $\delta_r(n, m)$ is denoted by $n * m$ for convenience.

R-1 $n * 1 = n$
R-2 $n * (m_1 \cdot m_2) = (n * m_1) * m_2$
R-3 $(n_1 + n_2) * m = n_1 * m + n_2 * m$
R-4 $n^{\hat{\tau}} * m = (n * m)^{\hat{\tau}}$
R-5 $n^{\hat{\tau}^*} * m = (n * m)^{\hat{\tau}^*}$
R-6 $\{n_1, \ldots, n_j\}^{\hat{\kappa}} * m = \{n_1 * m, \ldots, n_j * m\}^{\hat{\kappa}}$

δ_l and δ_r are compatible with each other if they satisfy the following condition.

LR $(m_1 * n) * m_2 = m_1 * (n * m_2)$.

We define the semidirect product of the two $\oplus$-algebras as $M \ltimes N = (M \times N, \tilde{\cdot}, \tilde{\tau}, \tilde{\tau}^*, \tilde{\kappa})$ where

1. $(m_1, n_1) \,\tilde{\cdot}\, (m_2, n_2) = (m_1 \cdot m_2, n_1 * m_2 + m_1 * n_2)$
2. $(m, n)^{\tilde{\tau}} = \left(m^{\tau}, \sum_{i=0}^{k-1} m^i * n * m^{\tau} + \left(\sum_{i=k}^{k+p-1} m^i * n * m^{\tau} \right)^{\hat{\tau}} \right)$ where k and p are respectively index[1] and period[2] of m
3. $(m, n)^{\tilde{\tau}^*} = \left(m^{\tau^*}, \left(\sum_{i=k+p-1}^{k} m^{\tau^*} * n * m^i \right)^{\hat{\tau}^*} + \sum_{i=k-1}^{0} m^{\tau^*} * n * m^i \right)$ where k and p are respectively index and period of m
4. $\{(m_1, n_1), \ldots, (m_p, n_p)\}^{\tilde{\kappa}} = (m, \{m * n_1 * m, \ldots, m * n_p * m\}^{\hat{\kappa}})$ where $m = \{m_1, \ldots, m_p\}^{\kappa}$

3 Verification that $M \ltimes N$ is a $\oplus$-algebra

3.1 Axiom A-1

$\forall a, b, c \in M \ltimes N, \quad (a \,\tilde{\cdot}\, b) \,\tilde{\cdot}\, c = a \,\tilde{\cdot}\, (b \,\tilde{\cdot}\, c)$

$$
\begin{aligned}
&((m_1, n_1) \,\tilde{\cdot}\, (m_2, n_2)) \,\tilde{\cdot}\, (m_3, n_3) \\
&= (m_1 m_2, n_1 * m_2 + m_1 * n_2) \,\tilde{\cdot}\, (m_3, n_3) \\
&= (m_1 m_2 m_3, n_1 * m_2 m_3 + m_1 * n_2 * m_3 + m_1 m_2 * n_3) \qquad [\text{by } \mathbf{R\text{-}3} \text{ and } \mathbf{R\text{-}2}]
\end{aligned}
$$

$$
\begin{aligned}
&(m_1, n_1) \,\tilde{\cdot}\, ((m_2, n_2) \,\tilde{\cdot}\, (m_3, n_3)) \\
&= (m_1, n_1) \,\tilde{\cdot}\, (m_2 m_3, n_2 * m_3 + m_2 * n_3) \\
&= (m_1 m_2 m_3, n_1 * m_2 m_3 + m_1 * n_2 * m_3 + m_1 m_2 * n_3) \qquad [\text{ by } \mathbf{L\text{-}3} \text{ and } \mathbf{L\text{-}2}]
\end{aligned}
$$

[1] index of m is the smallest positive integer k for which $m^k = m^{k+p}$ for some positive integer p
[2] period of m is the smallest positive integer p for which $m^k = m^{k+p}$ for index k of m

3.2 Axiom A-2

3.2.1 $(a.b)^{\tau} = a.(b.a)^{\tau}$

Consider $a = (m_1, n_1)$ and $b = (m_2, n_2)$. Let k(resp. k') and p(resp. p') be the index and period, respectively of m_1m_2(resp. m_2m_1). We show that k and k' cannot differ by more than 1 and p equals p'.

▶ **Lemma 1.** *$|k - k'| \leq 1$ and $p = p'$*

Proof. By the definition of index and period, we have $(m_1m_2)^k = (m_1m_2)^{k+p}$. Multiplying by m_2 on the left and by m_1 on the right, we get

$$\begin{aligned} &m_2(m_1m_2)^k m_1 = m_2(m_1m_2)^{k+p} m_1 \\ &\implies (m_2m_1)^{k+1} = (m_2m_1)^{k+p+1} \\ &\implies k' \leq k+1 \text{ and } p \bmod p' = 0 \end{aligned}$$

Similarly, $k \leq k'+1$ and $p' \bmod p = 0$ So, $|k - k'| \leq 1$ and $p = p'$. ◀

In 3.2.1, we'll write p to denote period of both m_1m_2 and m_2m_1.
By our semidirect product definition

$$\begin{aligned} &((m_1, n_1) \,\tilde{\cdot}\, (m_2, n_2))^{\tilde{\tau}} = (m_1m_2, n_1 * m_2 + m_1 * n_2)^{\tilde{\tau}} \\ &= \Bigg((m_1m_2)^{\tau}, \sum_{i=0}^{k-1} (m_1m_2)^i * (n_1 * m_2 + m_1 * n_2) * (m_1m_2)^{\tau} + \\ &\qquad \left(\sum_{i=k}^{k+p-1} (m_1m_2)^i * (n_1 * m_2 + m_1 * n_2) * (m_1m_2)^{\tau} \right)^{\hat{\tau}} \Bigg) \\ &= (x, y) \end{aligned}$$

$$\begin{aligned} &(m_1, n_1) \,\tilde{\cdot}\, \Big((m_2, n_2) \,\tilde{\cdot}\, (m_1, n_1) \Big)^{\tilde{\tau}} = (m_1, n_1) \,\tilde{\cdot}\, (m_2m_1, n_2 * m_1 + m_2 * n_1)^{\tilde{\tau}} \\ &= (m_1, n_1) \,\tilde{\cdot}\, \Bigg((m_2m_1)^{\tau}, \sum_{i=0}^{k'-1} (m_2m_1)^i * (n_2 * m_1 + m_2 * n_1) * (m_2m_1)^{\tau} + \\ &\qquad \left(\sum_{i=k'}^{k'+p-1} (m_2m_1)^i * (n_2 * m_1 + m_2 * n_1) * (m_2m_1)^{\tau} \right)^{\hat{\tau}} \Bigg) \\ &= \Bigg(m_1(m_2m_1)^{\tau}, n_1 * (m_2m_1)^{\tau} + \sum_{i=0}^{k'-1} m_1(m_2m_1)^i * (n_2 * m_1 + m_2 * n_1) * (m_2m_1)^{\tau} + \\ &\qquad \left(\sum_{i=k'}^{k'+p-1} m_1(m_2m_1)^i * (n_2 * m_1 + m_2 * n_1) * (m_2m_1)^{\tau} \right)^{\hat{\tau}} \Bigg) \\ &= (x', y') \end{aligned}$$

Since **A-2** holds in M, we have $x = x'$. So we now need to prove $y = y'$. For this we prove the following two lemmas.

▶ **Lemma 2.** *$n_1 * (m_2m_1)^\tau + \sum_{i=0}^{j} m_1(m_2m_1)^i * (n_2 * m_1 + m_2 * n_1) * (m_2m_1)^\tau$ is equal to $\sum_{i=0}^{j}(m_1m_2)^i * (n_1 * m_2 + m_1 * n_2) * (m_1m_2)^\tau + (m_1m_2)^{j+1} * (n_1 * m_2) * (m_1m_2)^\tau$*

Proof. When $j = 0$, we have

$$\begin{aligned}
&n_1 * (m_2m_1)^\tau + m_1 * (n_2 * m_1 + m_2 * n_1) * (m_2m_1)^\tau \\
&= n_1 * m_2(m_1m_2)^\tau + m_1 * n_2 * m_1(m_2m_1)^\tau + (m_1m_2) * n_1 * m_2(m_1m_2)^\tau \\
&= (n_1 * m_2 + m_1 * n_2) * (m_1m_2)^\tau + (m_1m_2) * (n_1 * m_2) * (m_1m_2)^\tau
\end{aligned}$$

Assuming the lemma to be true for j by induction hypothesis, we prove it for $j + 1$.

$$\begin{aligned}
&n_1 * (m_2m_1)^\tau + \sum_{i=0}^{j+1} m_1(m_2m_1)^i * (n_2 * m_1 + m_2 * n_1) * (m_2m_1)^\tau \\
&= n_1 * (m_2m_1)^\tau + \sum_{i=0}^{j} m_1(m_2m_1)^i * (n_2 * m_1 + m_2 * n_1) * (m_2m_1)^\tau \\
&\qquad + m_1(m_2m_1)^{j+1} * (n_2 * m_1 + m_2 * n_1) * (m_2m_1)^\tau
\end{aligned}$$

[by induction hypothesis]

$$\begin{aligned}
&= \sum_{i=0}^{j}(m_1m_2)^i * (n_1 * m_2 + m_1 * n_2) * (m_1m_2)^\tau + (m_1m_2)^{j+1} * (n_1 * m_2) * (m_1m_2)^\tau \\
&\qquad + m_1(m_2m_1)^{j+1} * (n_2 * m_1 + m_2 * n_1) * (m_2m_1)^\tau \\
&= \sum_{i=0}^{j}(m_1m_2)^i * (n_1 * m_2 + m_1 * n_2) * (m_1m_2)^\tau + (m_1m_2)^{j+1} * (n_1 * m_2) * (m_1m_2)^\tau \\
&\qquad + (m_1m_2)^{j+1} m_1 * n_2 * m_1(m_2m_1)^\tau + (m_1m_2)^{j+1} m_1m_2 * (n_1 * m_2) * (m_1m_2)^\tau \\
&= \sum_{i=0}^{j+1}(m_1m_2)^i * (n_1 * m_2 + m_1 * n_2) * (m_1m_2)^\tau + (m_1m_2)^{j+2} * (n_1 * m_2) * (m_1m_2)^\tau
\end{aligned}$$

This proves the lemma by induction. ◀

▶ **Lemma 3.** *For any $j \in [k', k'+p-1]$, $\sum_{i=j}^{k'+p-1} m_1(m_2m_1)^i * (n_2 * m_1 + m_2 * n_1) * (m_2m_1)^\tau$ is equal to*
$(m_1m_2)^j * (m_1 * n_2) * (m_1m_2)^\tau + \sum_{i=j+1}^{k'+p-1}(m_1m_2)^i * (n_1 * m_2 + m_1 * n_2) * (m_1m_2)^\tau$
$+(m_1m_2)^{k'+p} * (n_1 * m_2) * (m_1m_2)^\tau$

Proof. Induction on the range of the summation. When j is $k' + p - 1$, we have

$$\begin{aligned}
&m_1(m_2m_1)^{k'+p-1} * (n_2 * m_1 + m_2 * n_1) * (m_2m_1)^\tau \\
&= (m_1m_2)^{k'+p-1} m_1 * (n_2 * m_1 + m_2 * n_1) * (m_2m_1)^\tau \\
&= (m_1m_2)^{k'+p-1} * (m_1 * n_2) * m_1(m_2m_1)^\tau + (m_1m_2)^{k'+p-1} m_1m_2 * n_1 * m_2(m_1m_2)^\tau \\
&= (m_1m_2)^{k'+p-1} * (m_1 * n_2) * (m_1m_2)^\tau + (m_1m_2)^{k'+p} * (n_1 * m_2) * (m_1m_2)^\tau
\end{aligned}$$

Assuming true for $j+1$, we prove for j.

$$\sum_{i=j}^{k'+p-1} m_1(m_2m_1)^i * (n_2 * m_1 + m_2 * n_1) * (m_2m_1)^\tau$$

$$= m_1(m_2m_1)^j * (n_2 * m_1 + m_2 * n_1) * (m_2m_1)^\tau + \sum_{i=j+1}^{k'+p-1} m_1(m_2m_1)^i * (n_2 * m_1 + m_2 * n_1) * (m_2m_1)^\tau$$

$$= (m_1m_2)^j m_1 * n_2 * m_1(m_2m_1)^\tau + (m_1m_2)^j m_1m_2 * n_1 * m_2(m_1m_2)^\tau + \sum_{i=j+1}^{k'+p-1} m_1(m_2m_1)^i * (n_2 * m_1 + m_2 * n_1) * (m_2m_1)^\tau$$

$$= (m_1m_2)^j * (m_1 * n_2) * (m_1m_2)^\tau + (m_1m_2)^{j+1} * (n_1 * m_2) * (m_1m_2)^\tau + \sum_{i=j+1}^{k'+p-1} m_1(m_2m_1)^i * (n_2 * m_1 + m_2 * n_1) * (m_2m_1)^\tau$$

$$= (m_1m_2)^j * (m_1 * n_2) * (m_1m_2)^\tau + (m_1m_2)^{j+1} * (n_1 * m_2) * (m_1m_2)^\tau$$
$$+ (m_1m_2)^{j+1} * (m_1 * n_2) * (m_1m_2)^\tau + \sum_{i=j+2}^{k'+p-1} (m_1m_2)^i * (n_1 * m_2 + m_1 * n_2) * (m_1m_2)^\tau$$
$$+ (m_1m_2)^{k'+p} * (n_1 * m_2) * (m_1m_2)^\tau$$

$$= (m_1m_2)^j * (m_1 * n_2) * (m_1m_2)^\tau + \sum_{i=j+1}^{k'+p-1} (m_1m_2)^i * (n_1 * m_2 + m_1 * n_2) * (m_1m_2)^\tau + (m_1m_2)^{k'+p} * (n_1 * m_2) * (m_1m_2)^\tau$$

This completes the proof of the lemma. ◀

Continuing with the verification of the axiom **A-2** , we now have

$$
\begin{aligned}
&y' \\
&= n_1 * (m_2m_1)^\tau + \sum_{i=0}^{k'-1} m_1(m_2m_1)^i * (n_2 * m_1 + m_2 * n_1) * (m_2m_1)^\tau \\
&\qquad + \left(\sum_{i=k'}^{k'+p-1} m_1(m_2m_1)^i * (n_2 * m_1 + m_2 * n_1) * (m_2m_1)^\tau \right)^{\hat{\tau}}
\end{aligned}
$$

[by lemma 2]

$$
\begin{aligned}
&= \sum_{i=0}^{k'-1} (m_1m_2)^i * (n_1 * m_2 + m_1 * n_2) * (m_1m_2)^\tau + (m_1m_2)^{k'} * (n_1 * m_2) * (m_1m_2)^\tau \\
&\qquad + \left(\sum_{i=k'}^{k'+p-1} m_1(m_2m_1)^i * (n_2 * m_1 + m_2 * n_1) * (m_2m_1)^\tau \right)^{\hat{\tau}}
\end{aligned}
$$

[by lemma 3]

$$
\begin{aligned}
&= \sum_{i=0}^{k'-1} (m_1m_2)^i * (n_1 * m_2 + m_1 * n_2) * (m_1m_2)^\tau + (m_1m_2)^{k'} * (n_1 * m_2) * (m_1m_2)^\tau \\
&\qquad + \Big((m_1m_2)^{k'} * (m_1 * n_2) * (m_1m_2)^\tau \\
&\qquad + \sum_{i=k'+1}^{k'+p-1} (m_1m_2)^i * (n_1 * m_2 + m_1 * n_2) * (m_1m_2)^\tau \\
&\qquad + (m_1m_2)^{k'+p} * (n_1 * m_2) * (m_1m_2)^\tau \Big)^{\hat{\tau}}
\end{aligned}
$$

Now by lemma 1, we have to consider three cases.

<u>**Case 1:** $k = k'$</u>

If $k = k'$, then since $(m_1m_2)^k = (m_1m_2)^{k+p}$ and since axiom **A-2** holds in N, we have

$$
\begin{aligned}
&y' \\
&= \sum_{i=0}^{k-1} (m_1m_2)^i * (n_1 * m_2 + m_1 * n_2) * (m_1m_2)^\tau \\
&\qquad + \Big((m_1m_2)^k * (n_1 * m_2) * (m_1m_2)^\tau + (m_1m_2)^k * (m_1 * n_2) * (m_1m_2)^\tau \\
&\qquad + \sum_{i=k+1}^{k+p-1} (m_1m_2)^i * (n_1 * m_2 + m_1 * n_2) * (m_1m_2)^\tau \Big)^{\hat{\tau}} \\
&= \sum_{i=0}^{k-1} (m_1m_2)^i * (n_1 * m_2 + m_1 * n_2) * (m_1m_2)^\tau \\
&\qquad + \left(\sum_{i=k}^{k+p-1} (m_1m_2)^i * (n_1 * m_2 + m_1 * n_2) * (m_1m_2)^\tau \right)^{\hat{\tau}} \\
&= y
\end{aligned}
$$

<u>**Case 2:** $k' = k+1$</u>

If $k' = k+1$, we have

$$y' = \sum_{i=0}^{k}(m_1m_2)^i*(n_1*m_2+m_1*n_2)*(m_1m_2)^\tau + (m_1m_2)^{k+1}*(n_1*m_2)*(m_1m_2)^\tau$$

$$\Big((m_1m_2)^{k+1}*(m_1*n_2)*(m_1m_2)^\tau + \sum_{i=k+2}^{k+p}(m_1m_2)^i*(n_1*m_2+m_1*n_2)*(m_1m_2)^\tau + (m_1m_2)^{k+1+p}*(n_1*m_2)*(m_1m_2)^\tau\Big)^{\hat\tau}$$

$$= \sum_{i=0}^{k-1}(m_1m_2)^i*(n_1*m_2+m_1*n_2)*(m_1m_2)^\tau + (m_1m_2)^k*(n_1*m_2+m_1*n_2)*(m_1m_2)^\tau + (m_1m_2)^{k+1}*(n_1*m_2)*(m_1m_2)^\tau$$

$$\Big((m_1m_2)^{k+1}*(m_1*n_2)*(m_1m_2)^\tau + \sum_{i=k+2}^{k+p-1}(m_1m_2)^i*(n_1*m_2+m_1*n_2)*(m_1m_2)^\tau + (m_1m_2)^{k+p}*(n_1*m_2+m_1*n_2)*(m_1m_2)^\tau + (m_1m_2)^{k+1+p}*(n_1*m_2)*(m_1m_2)^\tau\Big)^{\hat\tau}$$

Since $(m_1m_2)^k = (m_1m_2)^{k+p}$ and $(m_1m_2)^{k+1} = (m_1m_2)^{k+1+p}$ and since axiom **A-2** holds in N, we have

$$y' = \sum_{i=0}^{k-1}(m_1m_2)^i*(n_1*m_2+m_1*n_2)*(m_1m_2)^\tau$$

$$+\Big((m_1m_2)^k*(n_1*m_2+m_1*n_2)*(m_1m_2)^\tau + (m_1m_2)^{k+1}*(n_1*m_2)*(m_1m_2)^\tau + (m_1m_2)^{k+1}*(m_1*n_2)*(m_1m_2)^\tau + \sum_{i=k+2}^{k+p-1}(m_1m_2)^i*(n_1*m_2+m_1*n_2)*(m_1m_2)^\tau\Big)^{\hat\tau}$$

$$= \sum_{i=0}^{k-1}(m_1m_2)^i*(n_1*m_2+m_1*n_2)*(m_1m_2)^\tau + \Big(\sum_{i=k}^{k+p-1}(m_1m_2)^i*(n_1*m_2+m_1*n_2)*(m_1m_2)^\tau\Big)^{\hat\tau}$$

$$= y$$

Case 3: $k = k' + 1$

If $k = k' + 1$, then

$$
\begin{aligned}
&y\\
&= \sum_{i=0}^{k'} (m_1m_2)^i * (n_1 * m_2 + m_1 * n_2) * (m_1m_2)^{\tau}\\
&\qquad + \left(\sum_{i=k'+1}^{k'+p} (m_1m_2)^i * (n_1 * m_2 + m_1 * n_2) * (m_1m_2)^{\tau} \right)^{\hat{\tau}}\\
&= \sum_{i=0}^{k'} (m_1m_2)^i * (n_1 * m_2 + m_1 * n_2) * (m_1m_2)^{\tau}\\
&\qquad + \Big((m_1m_2)^{k'+1} * (n_1 * m_2) * (m_1m_2)^{\tau}\\
&\qquad + (m_1m_2)^{k'+1} * (m_1 * n_2) * (m_1m_2)^{\tau}\\
&\qquad + \sum_{i=k'+2}^{k'+p-1} (m_1m_2)^i * (n_1 * m_2 + m_1 * n_2) * (m_1m_2)^{\tau}\\
&\qquad + (m_1m_2)^{k'+p} * (n_1 * m_2) * (m_1m_2)^{\tau}\\
&\qquad + (m_1m_2)^{k'+p} * (m_1 * n_2) * (m_1m_2)^{\tau} \Big)^{\hat{\tau}}
\end{aligned}
$$

[by lemma 3]

$$
\begin{aligned}
&= \sum_{i=0}^{k'} (m_1m_2)^i * (n_1 * m_2 + m_1 * n_2) * (m_1m_2)^{\tau}\\
&\qquad + \Big((m_1m_2)^{k'+1} * (n_1 * m_2) * (m_1m_2)^{\tau}\\
&\qquad + \sum_{i=k'+1}^{k'+p-1} m_1(m_2m_1)^i * (n_2 * m_1 + m_2 * n_1) * (m_2m_1)^{\tau}\\
&\qquad + m_1(m_2m_1)^{k'+p} * (n_2 * m_1) * (m_2m_1)^{\tau} \Big)^{\hat{\tau}}
\end{aligned}
$$

Since $k = k' + 1$, we have $(m_1m_2)^{k'+1} = (m_1m_2)^{k'+p+1}$. Now because axiom **A-2** holds in N, we can next write y as

$$\begin{aligned}
& y \\
&= \Bigg(\sum_{i=0}^{k'} (m_1m_2)^i * (n_1 * m_2 + m_1 * n_2) * (m_1m_2)^\tau \\
&\qquad + (m_1m_2)^{k'+1} * (n_1 * m_2) * (m_1m_2)^\tau \Bigg) \\
&\qquad + \Bigg(\sum_{i=k'+1}^{k'+p-1} m_1(m_2m_1)^i * (n_2 * m_1 + m_2 * n_1) * (m_2m_1)^\tau \\
&\qquad + m_1(m_2m_1)^{k'+p} * (n_2 * m_1) * (m_2m_1)^\tau \\
&\qquad + (m_1m_2)^{k'+p+1} * (n_1 * m_2) * (m_1m_2)^\tau \Bigg)^{\hat{\tau}}
\end{aligned}$$

[by lemma 2]

$$\begin{aligned}
&= n_1 * (m_2m_1)^\tau + \sum_{i=0}^{k'} m_1(m_2m_1)^i * (n_2 * m_1 + m_2 * n_1) * (m_2m_1)^\tau \\
&\quad + \Bigg(\sum_{i=k'+1}^{k'+p-1} m_1(m_2m_1)^i * (n_2 * m_1 + m_2 * n_1) * (m_2m_1)^\tau \\
&\quad + m_1(m_2m_1)^{k'+p} * (n_2 * m_1) * (m_2m_1)^\tau \\
&\quad + m_1(m_2m_1)^{k'+p} * (m_2 * n_1) * (m_2m_1)^\tau \Bigg)^{\hat{\tau}} \\
&= n_1 * (m_2m_1)^\tau + \sum_{i=0}^{k'-1} m_1(m_2m_1)^i * (n_2 * m_1 + m_2 * n_1) * (m_2m_1)^\tau \\
&\quad + m_1(m_2m_1)^{k'} * (n_2 * m_1 + m_2 * n_1) * (m_2m_1)^\tau \\
&\quad + \Bigg(\sum_{i=k'+1}^{k'+p-1} m_1(m_2m_1)^i * (n_2 * m_1 + m_2 * n_1) * (m_2m_1)^\tau \\
&\quad + m_1(m_2m_1)^{k'+p} * (n_2 * m_1 + m_2 * n_1) * (m_2m_1)^\tau \Bigg)^{\hat{\tau}}
\end{aligned}$$

[by axiom **A-2** in N]

$$\begin{aligned}
&= n_1 * (m_2m_1)^\tau + \sum_{i=0}^{k'-1} m_1(m_2m_1)^i * (n_2 * m_1 + m_2 * n_1) * (m_2m_1)^\tau \\
&\quad + \Bigg(m_1(m_2m_1)^{k'} * (n_2 * m_1 + m_2 * n_1) * (m_2m_1)^\tau \\
&\quad + \sum_{i=k'+1}^{k'+p-1} m_1(m_2m_1)^i * (n_2 * m_1 + m_2 * n_1) * (m_2m_1)^\tau \Bigg)^{\hat{\tau}} \\
&= n_1 * (m_2m_1)^\tau + \sum_{i=0}^{k'-1} m_1(m_2m_1)^i * (n_2 * m_1 + m_2 * n_1) * (m_2m_1)^\tau \\
&\quad + \Bigg(\sum_{i=k'}^{k'+p-1} m_1(m_2m_1)^i * (n_2 * m_1 + m_2 * n_1) * (m_2m_1)^\tau \Bigg)^{\hat{\tau}} \\
&= y'
\end{aligned}$$

3.2.2 $(m^a)^\tau = m^\tau$

Consider a random element $(m, n) \in M \ltimes N$ and some random positive integer $a \in \mathbb{N} \setminus \{0\}$. We have to show that $((m, n)^a)^{\tilde{\tau}} = (m, n)^{\tilde{\tau}}$.

Let index and period of m be k and p respectively, and that of m^a be k' and p'.

▶ **Lemma 4.** *$k \le ak'$ and $ap' \bmod p = 0$.*

Proof. By definition of index and period, we have $(m^a)^{k'} = (m^a)^{k'+p'}$ that is, $m^{ak'} = m^{ak'+ap'}$. So $k \le ak'$ and p divides ap'. ◀

We can show (by induction) that $(m, n)^a = (m^a, \sum_{j=0}^{a-1} m^j * n * m^{a-1-j})$.

So we have

$$
\begin{aligned}
((m,n)^a)^{\tilde{\tau}} = \Bigg((m^a)^\tau, & \sum_{i=0}^{k'-1} \Big((m^a)^i * \Big[\sum_{j=0}^{a-1} m^j * n * m^{a-1-j}\Big] * (m^a)^\tau \Big) \\
& + \Big(\sum_{i=k'}^{k'+p'-1} \big((m^a)^i * \Big[\sum_{j=0}^{a-1} m^j * n * m^{a-1-j}\Big] * (m^a)^\tau \big) \Big)^{\hat{\tau}} \Bigg) \\
& \text{[by axiom } \mathbf{A\text{-}2} \text{ in } M] \\
& = \Bigg(m^\tau, \sum_{i=0}^{k'-1} \sum_{j=0}^{a-1} m^{ia+j} * n * m^\tau \\
& \qquad + \Bigg(\sum_{i=k'}^{k'+p'-1} \sum_{j=0}^{a-1} m^{ia+j} * n * m^\tau \Bigg)^{\hat{\tau}} \Bigg) \\
& = \Bigg(m^\tau, \sum_{i=0}^{ak'-1} m^i * n * m^\tau + \Bigg(\sum_{i=ak'}^{ak'+ap'-1} m^i * n * m^\tau \Bigg)^{\hat{\tau}} \Bigg)
\end{aligned}
$$

Since p divides ap', let $ap' = xp$, Rewriting above equation, we get

$$
\begin{aligned}
((m,n)^a)^{\tilde{\tau}} &= \Bigg(m^\tau, \sum_{i=0}^{ak'-1} m^i * n * m^\tau + \Bigg(\sum_{i=ak'}^{ak'+xp-1} m^i * n * m^\tau \Bigg)^{\hat{\tau}} \Bigg) \\
&= \Bigg(m^\tau, \sum_{i=0}^{ak'-1} m^i * n * m^\tau + \Bigg(\Bigg(\sum_{i=ak'}^{ak'+p-1} m^i * n * m^\tau \Bigg)^x \Bigg)^{\hat{\tau}} \Bigg) \\
& \text{[by axiom } \mathbf{A\text{-}2} \text{ in } N] \\
&= \Bigg(m^\tau, \sum_{i=0}^{ak'-1} m^i * n * m^\tau + \Bigg(\sum_{i=ak'}^{ak'+p-1} m^i * n * m^\tau \Bigg)^{\hat{\tau}} \Bigg)
\end{aligned}
$$

If $ak' - 1 \ge k$, then $m^{ak'-1} = m^{ak'+p-1}$, and since axiom **A-2** holds in N, we can rewrite above equation as

$$((m,n)^a)^{\tilde{\tau}} = \left(m^\tau, \sum_{i=0}^{ak'-2} m^i * n * m^\tau + \left(\sum_{i=ak'-1}^{ak'+p-2} m^i * n * m^\tau \right)^{\hat{\tau}} \right)$$

We can keep doing this until we reach the following equation

$$\begin{aligned}((m,n)^a)^{\tilde{\tau}} &= \left(m^\tau, \sum_{i=0}^{k-1} m^i * n * m^\tau + \left(\sum_{i=k}^{k+p-1} m^i * n * m^\tau \right)^{\hat{\tau}} \right) \\ &= (m,n)^{\tilde{\tau}}\end{aligned}$$

This completes the verification of axiom **A-2**.

3.3 Axiom 3

Similar to verification of axiom **A-2**.

3.4 Axiom 4

Let $P = \{(m_1,n_1),(m_2,n_2),\ldots,(m_i,n_i)\}$ be some non-empty subset of $M \ltimes N$.

To prove, $\forall c \in P,\ \forall Q \subseteq P,\ \forall R \subseteq \{P^{\tilde{\kappa}}, a \mathbin{\tilde{\cdot}} P^{\tilde{\kappa}}, P^{\tilde{\kappa}} \mathbin{\tilde{\cdot}} b, a \mathbin{\tilde{\cdot}} P^{\tilde{\kappa}} \mathbin{\tilde{\cdot}} b \mid a,b \in P\},\ R \neq \phi$,

$P^{\tilde{\kappa}} = P^{\tilde{\kappa}} \mathbin{\tilde{\cdot}} P^{\tilde{\kappa}} = P^{\tilde{\kappa}} \mathbin{\tilde{\cdot}} c \mathbin{\tilde{\cdot}} P^{\tilde{\kappa}} = (P^{\tilde{\kappa}})^{\tilde{\tau}} = (P^{\tilde{\kappa}} \mathbin{\tilde{\cdot}} c)^{\tau} = (P^{\tilde{\kappa}})^{\tau^*} = (c \mathbin{\tilde{\cdot}} P^{\tilde{\kappa}})^{\tau^*} = (Q \cup R)^{\tilde{\kappa}}$

$P^{\tilde{\kappa}} = (m,n)$ where $m = \{m_1, m_2, \ldots, m_i\}^{\kappa}$ and $n = \{m*n_1*m, m*n_2*m, \ldots, m*n_i*m\}^{\hat{\kappa}}$

Note

$$\begin{aligned} n*m &= \{m*n_1*m, m*n_2*m,\ldots,m*n_i*m\}^{\hat{\kappa}} * m \\ &= \{m*n_1*m^2, m*n_2*m^2,\ldots,m*n_i*m^2\}^{\hat{\kappa}} && \text{[by action axiom } \textbf{R-6}] \\ &= \{m*n_1*m, m*n_2*m,\ldots,m*n_i*m\}^{\hat{\kappa}} && \text{[since axiom } \textbf{A-4} \text{ holds in } M] \\ &= n \end{aligned}$$

Similarly, we can show that $m*n = n$, $n*m^\tau = n$, $m^{\tau^*}*n = n$, $n*m_jm = n$ and $mm_j*n = n$ for any $j \in \{1,\ldots,i\}$

$$\begin{aligned} &(m,n) \mathbin{\tilde{\cdot}} (m,n) \\ &= (m^2, n*m + m*n) \\ &= (m, n+n) && \text{[since axiom } \textbf{A-4} \text{ holds in } M \text{ and } m*n = n*m = n] \\ &= (m,n) && \text{[since axiom } \textbf{A-4} \text{ holds in } N] \end{aligned}$$

$$\begin{aligned} &(m,n) \mathbin{\tilde{\cdot}} (m_j,n_j) \mathbin{\tilde{\cdot}} (m,n) \\ &= (mm_jm, n*m_jm + m*n_j*m + mm_j*n) \\ &= (m, n + m*n_j*m + n) && \text{[since axiom } \textbf{A-4} \text{ holds in } M \text{ and } mm_j*n = n*m_jm = n] \\ &= (m,n) && \text{[since axiom } \textbf{A-4} \text{ holds in } N] \end{aligned}$$

$$\begin{aligned}
&(m,n)^{\tilde{\tau}}\\
&=\left(m^{\tau},\sum_{i=0}^{k-1} m^i * n * m^{\tau} + \left(\sum_{i=k}^{k+p-1} m^i * n * m^{\tau}\right)^{\hat{\tau}}\right)\\
&=\left(m, n * m + \sum_{i=1}^{k-1} m * n * m + \left(\sum_{i=k}^{k+p-1} m * n * m\right)^{\hat{\tau}}\right) && \text{[since axiom } \mathbf{A\text{-}4} \text{ holds in } M]\\
&=\left(m, n + \sum_{i=1}^{k-1} n + \left(\sum_{i=k}^{k+p-1} n\right)^{\hat{\tau}}\right) && [\text{since } m*n = n*m = n]\\
&=(m, n^{\hat{\tau}})\\
&=(m,n) && \text{[since axiom } \mathbf{A\text{-}4} \text{ holds in } N]
\end{aligned}$$

Let index and period of mm_j be k' and p' respectively. Note that $(mm_j)^2 = mm_jmm_j = mm_j$.

$$\begin{aligned}
&((m,n) \tilde{\cdot} (m_j,n_j))^{\tilde{\tau}}\\
&=(mm_j, n*m_j + m*n_j)^{\tilde{\tau}}\\
&=\left((mm_j)^{\tau}, \sum_{i=0}^{k'-1}(mm_j)^i * n * (mm_j)^{\tau} + \left(\sum_{i=k'}^{k'+p'-1}(mm_j)^i * n * (mm_j)^{\tau}\right)^{\hat{\tau}}\right)\\
&=\left(m^{\tau}, \sum_{i=0}^{k'-1} mm_j * n * mm_j + \left(\sum_{i=k'}^{k'+p'-1} mm_j * n * mm_j\right)^{\hat{\tau}}\right)\\
&=\left(m^{\tau}, \sum_{i=0}^{k'-1} n + \left(\sum_{i=k'}^{k'+p'-1} n\right)^{\hat{\tau}}\right)\\
&=(m, n^{\hat{\tau}})\\
&=(m,n)
\end{aligned}$$

Similarly, we can show $(m,n) = ((m,n)^{\tilde{\kappa}})^{\tau^*} = ((m_j,n_j) \tilde{\cdot} (m,n)^{\tilde{\kappa}})^{\tau^*}$.

So we are left to show $(m,n) = (Q \cup R)^{\tilde{\kappa}}$.

$Q \subseteq P$. Let

$$Q = \{(m_{x1}, n_{x1}), (m_{x2}, n_{x2}), \ldots (m_{xi}, n_{xi})\}$$

where $\{x1, x2, \ldots xi\} \subseteq \{1, 2, \ldots, i\}$.

Also let $\{m_1, m_2, \ldots, m_i\} = P_1$ and $\{m*n_1*m, m*n_2*m, \ldots, m*n_i*m\} = P_2$. So,

$$m = P_1^{\kappa}, \quad n = P_2^{\hat{\kappa}}$$

We have

$$\begin{aligned}
R \subseteq \{&(m,n), (m_j,n_j) \tilde{\cdot} (m,n), (m,n) \tilde{\cdot} (m_{j'}, n_{j'}),\\
&(m_j,n_j) \tilde{\cdot} (m,n) \tilde{\cdot} (m_{j'}, n_{j'}) \mid j, j' \in \{1,2,\ldots,i\}\}\\
= \{&(m,n), (m_jm, n_j*m + m_j*n), (mm_{j'}, n*m_{j'} + m*n_{j'}),\\
&(m_jmm_{j'}, n_j*mm_{j'} + m_j*n*m_{j'} + m_jm*n_{j'}) \mid j, j' \in \{1,2,\ldots,i\}\}
\end{aligned}$$

R is non-empty. Consider $(Q \cup R)^{\tilde{\kappa}} = (x^{\kappa}, y^{\hat{\kappa}})$. Then

$$x \subseteq P_1 \cup \{m, m_j m, m m_{j'}, m_j m m_{j'} \mid j, j' \in \{1, 2, \ldots, i\}\}$$
$$\Rightarrow x = Q_1 \cup R_1$$

where $Q_1 \subseteq P_1$ and $R_1 \subseteq \{P_1^{\kappa}, m_j P_1^{\kappa}, P_1^{\kappa} m_{j'}, m_j P_1^{\kappa} m_{j'}\}$ and R_1 is non-empty. Since axiom **A-4** holds in M,

$$x^{\kappa} = P_1^{\kappa} = m$$

Similarly,

$$\begin{aligned} y \subseteq P_2 \cup \{& m * n * m, m * n_j * m + m m_j * n * m, m * n * m_{j'} m + m * n_{j'} * m, \\ & m * n_j * m + m m_j * n * m_{j'} m + m * n_{j'} * m \mid j, j' \in \{1, 2, \ldots, i\}\} \\ = P_2 \cup \{& n, m * n_j * m + n, n + m * n_{j'} * m, \\ & m * n_j * m + n + m * n_{j'} * m \mid j, j' \in \{1, 2, \ldots, i\}\} \\ \Rightarrow y = Q_2 \cup R_2 & \end{aligned}$$

where $Q_2 \subseteq P_2$ and $R_2 \subseteq \{P_2^{\hat{\kappa}}, m * n_j * m + P_2^{\hat{\kappa}}, P_2^{\hat{\kappa}} + m * n_{j'} * m, m * n_j * m + P_2^{\hat{\kappa}} + m * n_{j'} * m \mid j, j' \in \{1, 2, \ldots, i\}\}$. R_2 is non-empty.

Since axiom **A-4** holds in N, we get $y^{\hat{\kappa}} = P_2^{\hat{\kappa}} = n$

This concludes verification of axiom **A-4**.