APPENDIX TO INTUITIVE AND FORMAL MODELS OF WHOLE NUMBER MULTIPLICATION: RELATIONS AND EMERGING STRUCTURES

ANDREA MAFFIA, MARIA ALESSANDRA MARIOTTI

Notation and definitions

Assuming Zermelo-Fraenkel set theory, we define whole numbers as follows:

- $0 = \emptyset$ (empty set)
- $n^+ = n \cup \{n\}$

Here n^+ denotes the successor of the whole number n. A generic set A is considered as having n elements when there is a bijection between A and n; we write $|A| = n$. We use the symbol $A \backslash B$ to designate the complementary set of B in A, where $B \subseteq A$.

Addition is defined recursively:

- $n + 0 = n$
- $n + m^+ = (n + m)^+$.
- $n - m = p$ when $m + p = n$.

Multiplication and division are defined in the FRSM as follows.

- $0 \cdot n = 0$
- $m^+ \cdot n = m \cdot n + n$
- $n{:}m$ is q with a remainder $0 \leq r < m$ when $n \cdot q + r = m$

Multiplication and division are also defined in FARM:

- $n * m = |n \times m|$
- $n \div m$ is q with a remainder $0 \leq r < m$ when $n * q + r = m$

Where the symbol "×" is used for Cartesian product. We use the symbol "·" to denote multiplication in FRSM and the symbol "∗" to represent multiplication in FARM. ":" indicates division in FRSM and "÷" stands for division in FARM.

Claim 1

For any whole numbers n and m, we have $n \cdot m = m \cdot n$.

Proof of Claim 1

Proof	**Comments**
We use $m = 0$ as the base case.	Here we use induction on m.
We must prove that $n \cdot 0 = 0 \cdot n$.	This corresponds to putting 0 instead of m.
The base case $0 \cdot 0 = 0 \cdot 0$ is true.	We use induction on n and we adopt $n = 0$ as the base case.
Inductive hypothesis: $n \cdot 0 = 0 \cdot n$.	We assume it as true for n, and we prove it for n^+.
$n^+ \cdot 0 = n \cdot 0 + 0$	Because of the definition of multiplication.
$n \cdot 0 + 0 = 0 \cdot n + 0$	Because of the inductive hypothesis.
$0 \cdot n + 0 = 0 + 0$	Because any number multiplied by 0 is 0.
$0 + 0 = 0$	Because of the definition of addition.
$0 = 0 \cdot n^+$	Because any number multiplied by 0 is 0.
So, we have proved commutativity in the case $m = 0$.	Because of transitivity of the equality.
We assume that $n \cdot m = m \cdot n$ and we obtain	This is an inductive hypothesis. We then have to prove it in the case of m^+.
$m^+ \cdot n = m \cdot n + n$	Because of the definition of multiplication.
$m \cdot n + n = n \cdot m + n$	Because of the inductive hypothesis.
The proof would be finished if $n \cdot m + n = n \cdot m^+$.	To prove that, we resort again to mathematical induction on n.
It is easy to see it in the base case $n = 0$.	Because in that case both sides of the equivalence are 0.
Then we assume $n \cdot m^+ = n \cdot m + n$ and so	This is the inductive hypothesis.
$n^+ \cdot m^+ = n \cdot m^+ + m^+$	Because of the definition of multiplication.
$n \cdot m^+ + m^+ = n \cdot m + n + m^+$	Because of the inductive hypothesis.
$n \cdot m + n + m^+ = n \cdot m + (n + m)^+$	Because of associativity of sum.
$n \cdot m + (n + m)^+ = n \cdot m + (m + n)^+$	Because of commutativity of sum.
$n \cdot m + (m + n)^+ = n \cdot m + m + n^+$	Because of the definition of sum.
$n \cdot m + m + n^+ = n^+ \cdot m + n^+$	Because of the definition of multiplication.
□	So the proof is complete because of the transitivity of equivalence.

Claim 2

For any whole numbers n, m and p, we have $n \cdot m + n \cdot p = n \cdot (m + p)$.

Proof of Claim 2

Proof	**Comments**
It is easily verified when $n = 0$ because $0 \cdot m + 0 \cdot p = 0 + 0 = 0$ and also $0 \cdot (m + p) = 0$.	We use this as the base case of our induction on n.
We assume that $n \cdot m + n \cdot p = n \cdot (m + p)$	This is the inductive hypothesis.
We obtain that $n^+ \cdot m + n^+ \cdot p = n \cdot m + m + n \cdot p + p$	Because of the definition of multiplication.
that is $n \cdot m + n \cdot p + m + p$	Because of the commutativity of sum.
This is equal to $n \cdot (m + p) + (m + p)$.	Because of the inductive hypothesis.
$n \cdot (m + p) + (m + p) = n^+ \cdot (m + p)$.	Because of the definition of multiplication.
□	

Claim 3

For any whole numbers a and b with $b \leq a$ ($b \subseteq a$), we have $|a \setminus b| = a - b$.

Proof of Claim 3

Proof	**Comments**
Let be $|a \setminus b| = d$ Then, there is a bijection z between $a \setminus b$ and d. We define the function $$h(x) = \begin{cases} z(x) & if\ x \in a \setminus b \\ x + d & if\ x \in b \end{cases}$$	We call d the whole number corresponding to the cardinality of the set $|a \setminus b|$.
We can prove that h is a bijection between a and $d + b$.	
Indeed, $z(x)$ is a bijection and so the elements of $a \setminus b$ are as many as the elements of d.	The function z is a bijection between two subsets of a and $d + b$ (that are the domain and codomain of the function h). Indeed, z has $a \setminus b$ (that is included in a) as domain and d (that is included in $d + b$) as codomain.
Furthermore, through the translation $x + d$ the first b elements of a go in the last b elements of $d + b$.	This is shown in Figure A1.
Therefore $a = d + b$.	This because of the definition of subtraction.
So $a - b = d = |a \setminus b|$.	
□	

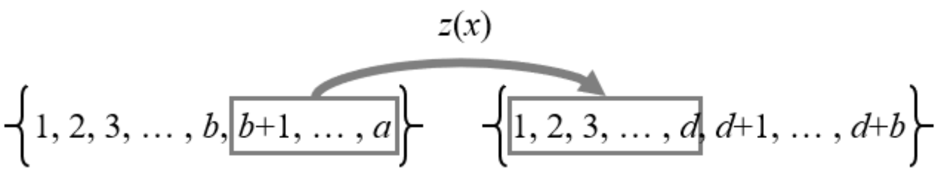

Figure A1. $z(x)$ is a bijection between $a \setminus b$, that is included in a, and $d \subseteq d + b$.

Claim 4

For any whole numbers n and m, $m^+ * n = m * n + n$

Proof of Claim 4

Proof	**Comments**
We define $k: m^+ \times n \setminus m \times n \to n$ as $$k\big((m, y)\big) = y$$ This function is a bijection and so $m^+ \times n \setminus m \times n$ is isomorphic to n.	This function takes just the second element of any couple in its domain. The letter m appears as first element because the elements $m^+ \times n \setminus m \times n$ are all couples of this kind.
$\lvert m^+ \times n \setminus m \times n \rvert = \lvert m^+ \times n \rvert - \lvert m \times n \rvert$	Because of Claim 3.
so, by transitivity, $n = \lvert m^+ \times n \rvert - \lvert m \times n \rvert$.	This is equivalent to the thesis because of the definition of subtraction.
□	

Claim 5

For any whole numbers n and m, $m \cdot n = m * n$.

Proof of Claim 5

Proof	**Comments**
If $m = 0$, both $n \cdot m$ and $n * m$ are zero.	This is the base case.
Let us assume that $n \cdot m = n * m$, so	This is the inductive hypothesis.
$n \cdot m^+ = n \cdot m + n$	Because of the definition of multiplication within FRSM.
$n \cdot m + n = n * m + n$	Because of the inductive hypothesis.
and so	
$n \cdot m^+ = n * m^+$.	Because of Claim 4.
□	The thesis follows by mathematical induction.