PROOFS AND DEFINITIONS USING ELLIPSIS

Notes for a talk at the Stockholm PhD student seminar in theoretical philosophy

June 4, 2018

Anders Lundstedt
anders.lundstedt@philosophy.su.se

§0 Preliminaries

- $\mathbb{N}$ = the natural numbers = {0,1,2,...}.
- $\mathbb{N}^+$ = the positive natural numbers = {1,2,3,...}.
- "x", "y" and "z" will denote natural numbers and "i", "j", "k", "m", "n" will denote positive natural numbers, when the context does not dictate otherwise.
- [n,m] = {i in $\mathbb{N}$: $n \leq i \leq m$} = {n,n+1,...,m-1,m}.
- Binary operators associate to the left, unless otherwise noted.
- If $f : A \to B$ and $A' \subseteq A$ then $f{\downarrow}A'$ is the restriction of f to A', that is, $f{\downarrow}A' : A' \to B$ is given by

  $$f{\downarrow}A'(a) := f(a).$$

- For functions $f : A \to B'$ and $g : B \to C$ with $B' \subseteq B$ their composition $A \to C$ is denoted "gf":

  $$\begin{matrix} f & & g & & gf \\ A & \to & B' & \subseteq B \to & C = A \to C. \end{matrix}$$

  Composition associates to the right:

  $$hgf = h(gf).$$

**

§1 Introduction

To get things going, let us look at two definitions of exponentiation and for each definition a corresponding proof of the identity $x^n x^m = x^{n+m}$. The first definition uses ellipsis (three dots——"...") while the second definition is by recursion. For simplicity we define x^n only for x in $\mathbb{N}$ and n in $\mathbb{N}^+$, thus avoiding a separate case for x^0 in the first definition, which would introduce unnecessary complications.

**

Definition 1.1.

$$-^{-} : \mathbb{N}\times\mathbb{N}^+\to\mathbb{N},$$

$$x^n := x\cdot x\cdots x \quad (n \text{ factors}).$$

**

Definition 1.2.

$$-^{-} : \mathbb{N}\times\mathbb{N}^+\to\mathbb{N},$$

$$x^1 := x,$$

$$x^{n+1} := x^n\cdot x.$$

**

Examples.

— Computing 2^3 using Definition 1.1:

$$2^3 = 2\cdot 2\cdot 2 \quad \text{(by Definition 1.1)}.$$

— Computing 2^3 using Definition 1.2:

$$\begin{aligned} 2^3 &= 2^{2+1} \\ &= 2^2\cdot 2 \quad \text{(by Definition 1.2)} \\ &= 2^{1+1}\cdot 2 \\ &= 2^1\cdot 2\cdot 2 \quad \text{(by Definition 1.2)} \\ &= 2\cdot 2\cdot 2 \quad \text{(by Definition 1.2)}. \end{aligned}$$

**

Fact 1.3. Definition 1.1 and Definition 1.2 define the same function.

Proof. See Appendix A. □

**

Fact 1.4.

$$x^n \cdot x^m = x^{n+m}.$$

Proof 1.4.1. Using Definition 1.1:

$$x^n \cdot x^m = \underbrace{(x \cdot x \cdots x)}_{n \text{ factors}} \cdot \underbrace{(x \cdot x \cdots x)}_{m \text{ factors}} \quad \text{(by Definition 1.1)}$$

$$= x \cdot x \cdots x \quad (n+m \text{ factors})$$

$$= x^{n+m} \quad \text{(by Definition 1.1).}$$ □

Proof 1.4.2. Using Definition 1.2 and induction on m:

- Base case: We want to prove $x^n x^1 = x^{n+1}$. This is easy:

$$x^n \cdot x^1 = x^n \cdot x \quad \text{(by Definition 1.2)}$$

$$= x^{n+1} \quad \text{(by Definition 1.2).}$$

- Induction step: The induction hypothesis is

(IH) $x^n \cdot x^m = x^{n+m}$

and we want to prove

$$x^n \cdot x^{m+1} = x^{n+m+1}.$$

We have

$$x^n \cdot x^{m+1} = x^n \cdot x^m \cdot x \quad \text{(by Definition 1.2)}$$

$$= x^{n+m} \cdot x \quad \text{(by (IH))}$$

$$= x^{n+m+1} \quad \text{(by Definition 1.2).}$$ □

**

Here are some points regarding Definitions 1.1 and 1.2 and regarding Proofs 1.4.1 and 1.4.2:

- Definition 1.1, which is formulated using ellipsis, is easier to understand than Definition 1.2, which is formulated by recursion. One does not have to understand recursion to understand Definition 1.1. Indeed, Definition 1.1 (possibly amended with a separate treatment of the special case x^0) is the definition found in schoolbooks and school children are expected to understand it before they get to learn about recursion. Definition 1.1 is also the one currently found in the Wikipedia article on exponentiation.

- Proof 1.4.1, which uses the ellipsis-formulated Definition 1.1, is easier to understand than Proof 1.4.2, which is an induction proof using the recursion-formulated Definition 1.2. One does not have to understand the principle of mathematical induction to understand Proof 1.4.1. Indeed, Proof 1.4.1 is the proof found in schoolbooks and school children are expected to understand it before they get to learn about mathematical induction.

- Proof 1.4.2 presupposes that we know what we want to prove. This is not the case for Proof 1.4.1, which would work just as well to answer the question "What is another useful expression for $x^n \cdot x^m$?"

- The above points often generalize. It is very common that ellipsis formulations are simpler to understand and simpler to reason about and with.

**

Given the above it seems that we would prefer definitions and proofs formulated using ellipsis instead of recursion and induction. This is indeed the case in non-formalized mathematics, where ellipsis usage is widespread in both definitions and proofs. This is the case even in logic, consider e.g. common formulations such as

$$\varphi(x_1,\ldots,x_n),$$

$$\forall x_1 \cdots \forall x_n . \varphi(x_1,\ldots,x_n).$$

**

Compared to non-formalized mathematics, ellipsis is not at all as common in formalized mathematics. Definition by recursion and proof by induction are often used instead. For example, if one wants to use first-order arithmetic to reason about exponentiation, the straightforward way to go is to add a function symbol and the defining recursive equations. For another example, the standard library of the popular proof assistant Coq defines exponentiation recursively. The corresponding proof of $x^n \cdot x^m = x^{n+m}$ is a proof by induction that, at least on the surface, does not resemble Proof 1.4.1.

**

It might not be too surprising that ellipsis is less common in popular formalisms, such as first-order logic and type theory, since these have no obvious syntactic counterpart to the ellipsis. This is in sharp contrast with recursively defined functions——these can be almost literally translated to both first-order logic and to type theory (for example, in the first-order logic case just add needed function symbols to the language and their defining equations as axioms).

**

My starting point then is the question

> How should ellipsis be formalized?

There are good reasons for trying to answer this question:

- It is not obvious how ellipsis should be formalized.
- A formalization of ellipsis would make it easier to formalize non-formalized mathematics where ellipsis is used.
- A formalization of ellipsis would dispense with the possible worry that there is something fishy with ellipsis usage in mathematics. One might have the worry that some ellipsis usages are non-formalizable, or even that some ellipsis usages do not even produce valid definitions and proofs.
- A formalization of ellipis would allow us to study ellipsis mathematics metamathematically. In particular, we would be able to make precise comparisons of induction proofs and ellipsis proofs. I would expect this to lead to some novel and surprising insights.

**

I do not aim to give a definitive answer to how ellipsis should be formalized. I only want to show that at least some common usages of ellipsis are indeed formalizable. I will do this by providing formalization-friendly definitions and proofs that do capture the spirit of corresponding definitions and proofs that are formulated using ellipsis.

**

I do not claim any novelty in my formalization-friendly reformulations (nor do I claim that there is nothing novel). I will use a "fold" function and in computer science, the relation between "fold" functions and ellipsis definitions is already well known.

**

The structure of these notes are as follows.

- In §2 I will look at proofs of the result

  $$(x^n)^m = x^{nm}.$$

- In §3 I will consider the function $\sigma : \mathbb{N}^+ \to \mathbb{N}$ such that $\sigma(n)$ is the sum of the first n positive integers. I will look at definitions of σ and proofs of the result that

  $$2 \cdot \sigma(n) = n \cdot (n+1).$$

- In §4 I will provide another definition of σ and another proof of the above result. I think this definition and this proof should be seen as formalization-friendly reformulations of the corresponding ellipsis versions in §3.

- In §5 I dispense with some of the worries we might have that there is something fishy about ellipsis usage in mathematics. I do this by showing how the formalizing-friendly formulations in §4 are close in spirit to the ellipsis formulations in §3.

**

§2 More exponentiation

Fact 2.1.

$$(x^n)^m = x^{nm}.$$

Proof 2.1.1. Using Definition 1.1:

$$(x^n)^m = \underbrace{x^n \cdot x^n \cdot x^n}_{m \text{ factors}} \quad \text{(by Definition 1.1)}$$

$$= \underbrace{(x \cdot x \cdots x)}_{n \text{ factors}} \cdot \underbrace{(x \cdot x \cdots x)}_{n \text{ factors}} \cdots \underbrace{(x \cdot x \cdots x)}_{n \text{ factors}} \quad \text{(by Definition 1.1)}$$

$$= \underbrace{x \cdot x \cdots x}_{n \cdot m \text{ factors}}$$

$$= x^{nm} \quad \text{(by Definition 1.1).}$$ □

Proof 2.1.2. Using Definition 1.2 and induction on m:

- Base case: We want to prove $(x^n)^1 = x^{1n}$. This is immediate from Definition 1.2.
- Induction step: The induction hypothesis is

  (IH) $(x^n)^m = x^{nm}$

  and we want to prove

  $$(x^n)^{m+1} = x^{n(m+1)}.$$

  We have

  $$\begin{aligned} (x^n)^{m+1} &= (x^n)^m \cdot x^n && \text{(by Definition 1.2)} \\ &= x^{nm} \cdot x^n && \text{(by (IH))} \\ &= x^{nm+n} && \text{(by Fact 1.4)} \\ &= x^{n(m+1)}. \end{aligned}$$ □

**

§3 The sum of initial segments of the positive integers

Let $\sigma : \mathbb{N}^+ \to \mathbb{N}$ be the function such that $\sigma(n)$ is the sum of the first n positive integers. Here are a definition of σ formulated using ellipsis and a definition of σ formulated using recursion.

**

Definition 3.1.

$$\sigma : \mathbb{N}^+ \to \mathbb{N}$$

$$\sigma(n) := 1+2+\cdots+n.$$

**

Definition 3.2.

$$\sigma : \mathbb{N}^+ \to \mathbb{N}$$

$$\sigma(1) := 1,$$

$$\sigma(n+1) := \sigma(n)+n+1.$$

**

Examples.

- Computing $\sigma(3)$ using Definition 3.1:

$$\begin{aligned}\sigma(3) &= 1+2+3 \quad \text{(by Definition 3.1)}\\ &= 6.\end{aligned}$$

- Computing $\sigma(3)$ using Definition 3.2:

$$\begin{aligned}\sigma(3) &= \sigma(2+1)\\ &= \sigma(2)+2+1 \quad \text{(by Definition 3.2)}\\ &= \sigma(1+1)+3\\ &= \sigma(1)+1+1+3 \quad \text{(by Definition 3.2)}\\ &= \sigma(1)+2+3\\ &= 1+2+3 \quad \text{(by Definition 3.2)}\\ &= 6.\end{aligned}$$

**

Fact 3.3. Definitions 3.1 and 3.2 define the same function.

Proof. See Appendix A. □

**

Fact 3.4.

$$2\cdot\sigma(n) = n\cdot(n+1).$$

Proof 3.4.1. Using Definition 3.1 we have

$$\begin{aligned}
&(1)\quad \sigma(n) = 1 + 2 + \cdots + (n-1) + n && \text{(by Definition 3.1),}\\
&(2)\quad \sigma(n) = n + (n-1) + \cdots + 2 + 1 && \text{(by reversing the order in (1)),}\\
&(3)\quad 2\cdot\sigma(n) = (1+n) + (2+(n-1)) + \cdots + ((n-1)+2) + (n+1) && \text{(by summing same-column terms from (1) and (2))}\\
&\qquad\qquad = (n+1)+(n+1)+\cdots+(n+1) \quad (n \text{ terms})\\
&\qquad\qquad = n\cdot(n+1). && \square
\end{aligned}$$

Proof 3.4.2. Using Definition 3.2 and induction on n:

- Base case: We want to prove $2\cdot\sigma(1) = 1\cdot(1+1)$. This is easy:

$$\begin{aligned}
2\cdot\sigma(1) &= 2\cdot 1 && \text{(by Definition 3.2)}\\
&= 1\cdot(1+1).
\end{aligned}$$

- Induction step: The induction hypothesis is

$$\text{(IH)}\quad 2\cdot\sigma(n) = n\cdot(n+1)$$

and we want to prove

$$2\cdot\sigma(n+1) = (n+1)\cdot(n+2).$$

We have

$$\begin{aligned} 2\cdot\sigma(n+1) &= 2\cdot(\sigma(n)+n+1) && \text{(by Definition 3.2)} \\ &= 2\cdot\sigma(n)+2\cdot(n+1) \\ &= n\cdot(n+1)+2\cdot(n+1) && \text{(by (IH))} \\ &= (n+1)\cdot(n+2). \end{aligned}$$

□

**

§4 Using tuples to capture ellipsis reasoning

In the following I will limit myself to tuples of natural numbers, but the definitions and facts not mentioning tuples and functions specific to the natural numbers should immediately generalize.

**

Using ellipsis notation we can write

"$\langle x_1,...,x_n\rangle$"

to denote a tuple of length n whose element at position i is x_i. Several definitions without ellipsis are possible. I will use the following.

**

Definition 4.1. The set $\mathbb{N}^n$ of *tuples (of natural numbers) of length n* is the set of functions [1,n]→ℕ.

**

Notation. "t_i" and "t[i]" will mean "t(i)" when t is a tuple.

**

Definition 4.1 relates to the ellipsis notation of tuples by

for all tuples t of length n: $t = \langle t_1,...,t_n\rangle$.

Since the point of this section is to avoid ellipsis I will not rely on ellipsis notation in definitions and proofs. (I will still use ellipsis notation for some purely illustrative purposes.)

**

Examples.

- The identity function on [1,n] is in $\mathbb{N}^n$. (Ellipsis notation: $\langle 1,...,n\rangle$.)
- The [1,3]→ℕ function i↦4-i is in $\mathbb{N}^3$. (Alternative notation: $\langle 3,2,1\rangle$.)
- For any x in ℕ, the constant [1,n] function -↦x is in $\mathbb{N}^n$. (Ellipsis notation: $\langle x,...,x\rangle$.)
- For any t in $\mathbb{N}^{n+1}$ and any m in [1,n], t↓[1,m] is in $\mathbb{N}_m$. (Ellipsis notation: $\langle t_1,...,t_m\rangle$.)
- For any f : $\mathbb{N}^+$→ℕ, f↓[1,n] is in $\mathbb{N}^n$. (Ellipsis notation: $\langle f(1),...,f(n)\rangle$.)

- For any $f : [1,n]\to[1,n]$ and any t in $\mathbb{N}^n$, tf is in $\mathbb{N}^n$. (Ellipsis notation: $\langle t[f(1)],...,t[f(n)]\rangle$.)

**

Definition 4.2.

- ι_n is the identity function on $[1,n]$.

- The $\mathbb{N}^n\times\mathbb{N}\to\mathbb{N}^{n+1}$ function $t,x\mapsto t::x$ is defined by

$$t::x(i) := t(i) \text{ if } i \leq n,$$

$$t::x(n+1) := x.$$

**

Remark. In ellipsis notation, Definition 4.2 would become

- $\iota_n = \langle 1,...,n\rangle$,

- $\langle x_1,...,x_n\rangle::x_{n+1} = \langle x_1,...,x_n,x_{n+1}\rangle$.

**

Notation.

- "$\langle x\rangle$", for x in $\mathbb{N}$, abbreviates the tuple $-\mapsto x$ in $\mathbb{N}^1$.

- "$f(u,v)$", for $f : \mathbb{N}\times\mathbb{N}\to\mathbb{N}$ and u and v in $\mathbb{N}^n$, abbreviates the tuple $i\mapsto f(u(i),v(i))$ in $\mathbb{N}^n$.

**

Remark. In ellipsis notation, the last notation above becomes

$$f(\langle u_1,...,u_n\rangle,\langle v_1,...,v_n\rangle) = \langle f(u_1,v_1),...,f(u_n,v_n)\rangle.$$

**

Fact 4.3. For all t in $\mathbb{N}^{n+1}$:

$$t = t{\downarrow}[1,n]::t_{n+1}.$$

Proof. See Appendix A. □

**

By Fact 4.3, every tuple u in $\mathbb{N}^{n+1}$ is of the form $v::x$. This allows us to define functions on $\mathbb{N}^n$ by recursion on n, as the following definition illustrates.

**

Definition 4.4. The functions $lf_n : (\mathbb{N}\times\mathbb{N}\to\mathbb{N})\times\mathbb{N}^n\to\mathbb{N}$ are defined by

$$lf_1(*,\langle x\rangle) := x,$$

$$lf_{n+1}(*,t::x) := lf_n(*,t)*x.$$

**

Remark. With ellipsis notation and using parentheses to emphasize the associativity, Definition 4.4 becomes

$$lf_n(*,\langle x_1,x_2,x_3,\ldots,x_n\rangle) := ((x_1*x_2)*x_3)*\cdots*x_n.$$

**

Remark. "lf" is short for "left fold", which is the common computer science name for this function. The operation $*$ associates to the left in the ellipsis version of the left fold definition. There is also the "right fold", in the ellipsis definition of which the operation $*$ associates to the right.

**

Example. Computing $lf_3(+,\iota_3)$:

$$\begin{aligned}
lf_3(+,\iota_3) &= lf_3(+,\iota_3{\downarrow}[1,2]::\iota_3[3]) && \text{(by Fact 4.3)}\\
&= lf_3(+,\iota_2::3)\\
&= lf_2(+,\iota_2)+3 && \text{(by Definition 4.4)}\\
&= lf_2(+,\iota_2{\downarrow}[1,1]::\iota_2[2])+3 && \text{(by Fact 4.3)}\\
&= lf_2(+,\iota_1::2)+3\\
&= lf_1(+,\iota_1)+2+3 && \text{(by Definition 4.4)}\\
&= lf_1(+,\langle 1\rangle)+2+3\\
&= 1+2+3 && \text{(by Definition 4.4)}\\
&= 6.
\end{aligned}$$

**

Fact 4.5. For all associative and commutative $*$:

$$lf_n(*,u)*lf_n(*,v) = lf_n(*,u*v).$$

Proof. See Appendix A. □

**

Remark. In ellipsis notation, the equation in Fact 4.5 becomes

$$(u_1*\cdots*u_n)*(v_1*\cdots*v_n) = (u_1*v_1)*\cdots*(u_n*v_n).$$

**

Fact 4.6. For all commutative and associative $*$ and all bijections $b : [1,n]\to[1,n]$:

$$lf_n(*,tb) = lf_n(*,t).$$

Proof. See Appendix A. □

**

Remark. In ellipsis notation, the equation in Fact 4.6 becomes

$$t_1*\cdots*t_n = tb(1)*\cdots*tb(n).$$

**

Definition 4.7.

$$\sigma(n) := lf_n(+,\iota_n).$$

**

Remark. In ellipsis notation, Definition 4.7 becomes

$$\sigma(n) := \iota_n[1]+\cdots+\iota_n[n],$$

which unfolds to

$$\sigma(n) = 1+\cdots+n.$$

**

Fact 4.8. Definition 4.7 defines the same function as Definitions 3.1 and 3.2.

Proof. See Appendix A. □

**

Fact 4.9.

$$lf_n(+,-\mapsto x) = n\cdot x.$$

Proof. The proof depends on how we define multiplication. One way is to simply define multiplication on $\mathbb{N}^+\times\mathbb{N}$ by the above equation. □

**

Fact 4.10.

$$2\cdot\sigma(n) = n\cdot(n+1).$$

Proof. Let rev_n be the "reverse order" bijection $[1,n]\to[1,n]$, that is, rev_n is defined by

$$rev_n(i) := n+1-i,$$

by which rev_n is a bijection. For all i in [1,n] we have

$$\begin{aligned}(\iota_n+\iota_n rev_n)(i) &= \iota_n(i)+\iota_n rev_n(i)\\ &= \iota_n(i)+\iota_n(n+1-i)\\ &= i+n+1-i\\ &= n+1.\end{aligned}$$

Thus

$$(*)\quad \iota_n+\iota_n rev_n = -\mapsto n+1.$$

Then

$$\begin{aligned}2\cdot\sigma(n) &= 2\cdot lf_n(+,\iota_n) && \text{(by Definition 4.7)}\\ &= lf_n(+,\iota_n)+lf_n(+,\iota_n)\\ &= lf_n(+,\iota_n)+lf_n(+,\iota_n rev_n) && \text{(by Fact 4.6)}\\ &= lf_n(+,\iota_n+\iota_n rev_n) && \text{(by Fact 4.5)}\\ &= lf_n(+,-\mapsto n+1) && \text{(by (*))}\\ &= n\cdot(n+1) && \text{(by Fact 4.9).}\end{aligned}$$ □

**

§5 Conclusion

Let us compare the proof of Fact 4.10 with Proof 3.4.1. First, let us just simply slightly reorganize Proof 3.4.1 (the reader may want to verify that the structure of the proof remains the same):

$$
\begin{aligned}
2\cdot\sigma(n) &= \sigma(n) + \sigma(n)\\
&= \begin{array}{rcccccc} 1 & + & 2 & + \cdots + & (n-1) & + & n \\ + 1 & + & 2 & + \cdots + & (n-1) & + & n \end{array} && \text{(by Definition 3.1)}\\
&= \begin{array}{rcccccc} 1 & + & 2 & + \cdots + & (n-1) & + & n \\ + n & + & (n-1) & + \cdots + & 2 & + & 1 \end{array} && \text{(by reversing the lower sum)}\\
&= (1+n) + (2+(n-1)) + \cdots + ((n-1)+2) + (n+1) && \text{(by summing terms in same column)}\\
&= (n+1)+(n+1)+\cdots+(n+1) && (n \text{ terms})\\
&= n\cdot(n+1).
\end{aligned}
$$

**

Now let us look at how closely Proof 3.4.1 is mirrored in the proof of Fact 4.10:

— The equation

$$
\begin{array}{rcccccc} 1 & + & 2 & + \cdots + & (n-1) & + & n \\ + 1 & + & 2 & + \cdots + & (n-1) & + & n \end{array}
$$

$$
= \begin{array}{rcccccc} 1 & + & 2 & + \cdots + & (n-1) & + & n \\ + n & + & (n-1) & + \cdots + & 2 & + & 1 \end{array} \quad \text{(by reversing the lower sum)}
$$

corresponds to

$$
\mathrm{lf}_n(+,\iota_n)+\mathrm{lf}_n(+,\iota_n) = \mathrm{lf}_n(+,\iota_n)+\mathrm{lf}_n(+,\iota_n\mathrm{rev}_n) \quad \text{(by Fact 4.6).}
$$

— The equation

$$
\begin{array}{rcccccc} 1 & + & 2 & + \cdots + & (n-1) & + & n \\ + n & + & (n-1) & + \cdots + & 2 & + & 1 \end{array}
$$

$$
= (1+n) + (2+(n-1)) + \cdots + ((n-1)+2) + (n+1) \quad \text{(by summing same-column terms)}
$$

corresponds to

$$
\mathrm{lf}_n(+,\iota_n)+\mathrm{lf}_n(+,\iota_n\mathrm{rev}_n) = \mathrm{lf}_n(+,\iota_n+\iota_n\mathrm{rev}_n) \quad \text{(by Fact 4.5).}
$$

— The equation

$$(1+n) + (2+(n-1)) + \cdots + ((n-1)+2) + (n+1)$$

$$= (n+1)+(n+1)+\cdots+(n+1) \quad (n \text{ terms})$$

corresponds to

$$\mathrm{lf}_n(+, \iota_n + \iota_n \mathrm{rev}_n) = \mathrm{lf}_n(+, \mathrm{const}_{n+1}) \quad (\text{by } (*)).$$

— The equation

$$\underbrace{(n+1)+\cdots+(n+1)}_{n \text{ terms}} = n \cdot (n+1)$$

corresponds to

$$\mathrm{lf}_n(+, \mathrm{const}_{n+1}) = n \cdot (n+1) \quad (\text{by Fact 4.9}).$$

**

Given the above, I think it should be clear that §4 provides a formalization-friendly version of the ellipsis formulations in §3. In particular, we have a proof that do not use any ellipsis but still closely mirrors the ellipsis proof in §3.

**

I claim that, using similar techniques, Definition 1.1 and Proofs 1.4.1 and 2.1.1 can be reformulated in a formalization-friendly way. This is something I leave for future work.

**

To show that the formulation in §4 really is formalization-friendly, one could construct an actual formalization of it. I think proof assistants based on dependent type theory, for example Coq or Agda, would be a suitable choice for this. For now, I leave this for future work.

**

Appendix A: Some proofs

Fact 1.3. Definition 1.1 and Definition 1.2 define the same function.

Proof. Let us denote exp according to Definition 1.1 by $\exp_1$ and let us denote exp according to Definition 1.2 by $\exp_2$. We need to prove

$$\text{for all } x \text{ in } \mathbb{N} \text{ and all } n \text{ in } \mathbb{N}^+\text{: } \exp_1(x,n) = \exp_2(x,n).$$

We prove this by induction on n.

- Base case: We want to prove $\exp_1(x,1) = \exp_2(x,1)$. This follows directly from the definitions:

$$\exp_1(x,1) = x \qquad \text{(by Definition 1.1)}$$

$$= \exp_2(x,1) \qquad \text{(by Definition 1.2).}$$

- Induction step: The induction hypothesis is

$$\text{(IH) } \exp_1(x,n) = \exp_2(x,n)$$

and we want to prove

$$\exp_1(x,n+1) = \exp_2(x,n+1).$$

We have

$$\exp_1(x,n+1) = \underbrace{x \cdot x \cdots x}_{n+1 \text{ factors}} \qquad \text{(by Definition 1.1)}$$

$$= \underbrace{(x \cdot x \cdots x) \cdot x}_{n \text{ factors}}$$

$$= \exp_1(x,n) \cdot x \qquad \text{(by Definition 1.1)}$$

$$= \exp_2(x,n) \cdot x \qquad \text{(by (IH))}$$

$$= \exp_2(x,n+1) \qquad \text{(by Definition 1.2).}$$

**

Fact 3.3. Definitions 3.1 and 3.2 define the same function.

Proof. Let us denote σ according to Definition 3.1 by σ_1 and let us denote σ according to Definition 3.2 by σ_2. We need to prove

$$\text{for all } n \text{ in } \mathbb{N}^+\text{: } \sigma_1(n) = \sigma_2(n).$$

We prove this by induction on n.

- Base case: We want to prove $\sigma_1(1) = \sigma_2(1)$. This follows directly from the definitions:

$$\sigma_1(1) = 1 \quad \text{(by Definition 3.1)}$$

$$= \sigma_2(1) \quad \text{(by Definition 3.2).}$$

- Induction step: The induction hypothesis is

(IH) $\sigma_1(n) = \sigma_2(n)$

and we want to prove

$$\sigma_1(n+1) = \sigma_2(n+1).$$

We have

$$\sigma_1(n+1) = 1+2+\cdots+n+n+1 \quad \text{(by Definition 2.1)}$$

$$= \sigma_1(n)+n+1 \quad \text{(by Definition 2.1)}$$

$$= \sigma_2(n)+n+1 \quad \text{(by (IH))}$$

$$= \sigma_2(n+1) \quad \text{(by Definition 2.2).}$$ □

**

Fact 4.3. For all t in $\mathbb{N}^{n+1}$:

$$t = t{\downarrow}[1,n]::t_{n+1}.$$

Proof.

$$t = i \mapsto t(i)$$

$$= i \mapsto (t{\downarrow}[1,n](i) \text{ if } i \leq n \text{ otherwise } t_{n+1})$$

$$= t{\downarrow}[1,n]::t_{n+1} \quad \text{(by Definition 4.2).}$$ □

**

Fact 4.5. For all associative and commutative $*$:

$$lf_n(*,u)*lf_n(*,v) = lf_n(*,u*v).$$

Proof. Induction on n.

— Base case: We want to prove

$$\text{for all } u \text{ and } v \text{ in } \mathbb{N}^1\text{: } lf_1(*,u)*lf_1(*,v) = lf_1(*,u*v).$$

We have

$$\begin{aligned} lf_1(*,u)*lf_1(*,v) &= lf_1(*,\langle u_1\rangle)*lf_1(*,\langle v_1\rangle) \\ &= u_1*v_1 && \text{(by Definition 4.4)} \\ &= lf_1(*,\langle u_1*v_1\rangle) && \text{(by Definition 4.4)} \\ &= lf_1(*,u*v). \end{aligned}$$

— Induction step: The induction hypothesis is

(IH) $\text{for all } u \text{ and } v \text{ in } \mathbb{N}^n\text{: } lf_n(*,u)*lf_n(*,v) = lf_n(*,u*v)$

and we want to prove

$$\text{for all } u \text{ and } v \text{ in } \mathbb{N}^{n+1}\text{: } lf_{n+1}(*,u)*lf_{n+1}(*,v) = lf_{n+1}(*,u*v).$$

We have

$$\begin{aligned} lf_{n+1}(*,u)*lf_{n+1}(*,v) &= (lf_n(*,u{\downarrow}[1,n])*u_{n+1})*(lf_n(*,v{\downarrow}[1,n])*v_{n+1}) \\ &\quad \text{(by Fact 4.3 and Definition 4.4)} \\ &= (lf_n(*,u{\downarrow}[1,n])*lf_n(*,v{\downarrow}[1,n]))*(u_{n+1}*v_{n+1}) \\ &\quad \text{(by associativity and commutativity)} \\ &= (lf_n(*,u{\downarrow}[1,n]*v{\downarrow}[1,n])*(u_{n+1}*v_{n+1}) \\ &\quad \text{(by (IH))} \\ &= (lf_n(*,(u*v){\downarrow}[1,n])*(u*v)_{n+1} \\ &= lf_{n+1}(*,u*v) \\ &\quad \text{(by Fact 4.3 and Definition 4.4).} \end{aligned}$$

□

**

Fact 4.6. For all commutative and associative $*$ and all bijections $b : [1,n]\to[1,n]$:

$$lf_n(*,tb) = lf_n(*,t).$$

Proof. Induction on n using n = 1 and n = 2 as base cases.

- Base case n = 1: Trivial since the bijection $i\mapsto i$ is the unique function $[1,1]\to[1,1]$.

- Base case n = 2: We want to prove

  for all bijections $b : [1,2]\to[1,2]$ and all t in $\mathbb{N}^2$:
  $lf_2(*,tb) = lf_2(*,t)$.

  There are two different bijections $b : [1,2]\to[1,2]$.

  - Case $b = i\mapsto i$: Trivial.

  - Case $b = i\mapsto 3-i$: We have

    $lf_2(*,tb)$

    $= lf_2(*,(tb)\downarrow[1,1])*tb(2)$ (by Fact 4.3 and Definition 4.4)

    $= lf_2(*,\langle t_2\rangle)*t_1$

    $= t_2*t_1$ (by Definition 4.4)

    $= t_1*t_2$ (by commutativity)

    $= lf_2(*,\langle t_1\rangle)*t_2$ (by Definition 4.4)

    $= lf_2(*,t\downarrow[1:1])*t_2$

    $= lf_2(*,t)$ (by Fact 4.3 and Definition 4.4).

- Induction step n = m+2: The induction hypothesis is

  (IH) for all bijections $b : [1,m+1]\to[1,m+1]$ and all t in $\mathbb{N}^{m+1}$:
  $lf_{m+1}(*,tb) = lf_{m+1}(*,t)$.

  We want to prove

  for all bijections $b : [1,m+2]\to[1,m+2]$ and all t in $\mathbb{N}^{m+2}$:
  $lf_{m+2}(*,tb) = lf_{m+2}(*,t)$.

  - Case $b(m+2) = m+2$: Then $b\downarrow[1,m+1]$ is a bijection $[1,m+1]\to[1,m+1]$ and

    (*) $(tb)\downarrow[1,m+1] = t\downarrow[1,m+1]b\downarrow[1,m+1]$.

Thus

$lf_{m+2}(*,tb)$

$= lf_{m+1}(*,(tb)\downarrow[1,m+1])*tb(m+2)$ (by Fact 4.3 and Definition 4.4)

$= lf_{m+1}(*,t\downarrow[1,m+1]b\downarrow[1,m+1])*tb(m+2)$ (by (*))

$= lf_{m+1}(*,t\downarrow[1,m+1])*tb(m+2)$ (by (IH))

$= lf_{m+1}(*,t\downarrow[1,m+1])*t_{m+2}$

$= lf_{m+2}(*,t)$ (by Fact 4.3 and Definition 4.4).

– Case b(m+2) ≠ m+2: Let i be the unique number in [1,m+1] such that b(i) = m+2. Using ellipsis, for illustrative purposes, we then have

$lf_{m+2}(*,tb)$

$= lf_{m+2}(*,\langle tb(1),...,tb(i),...,tb(m+1),tb(m+2)\rangle)$

$= lf_{m+1}(*,\langle tb(1),...,tb(i),...,tb(m+1)\rangle)*tb(m+2)$

$= lf_{m+1}(*,\langle tb(1),...,tb(m+1),...,tb(i)\rangle)*tb(m+2)$
(by (IH))

$= lf_{m}(*,\langle tb(1),...,tb(m+1),...,tb(m)\rangle)*tb(i)*tb(m+2)$

$= lf_{m}(*,\langle tb(1),...,tb(m+1),...,tb(m)\rangle)*tb(m+2)*tb(i)$
(by associativity and commutativity)

$= lf_{m+1}(*,\langle tb(1),...,tb(m+1),...,tb(m),tb(m+2)\rangle)*tb(i)$

$= lf_{m+1}(*,\langle t_1,...,t_{m+1}\rangle)*tb(i)$
(by (IH))

$= lf_{m+1}(*,\langle t_1,...,t_{m+1}\rangle)*t_{m+2}$

$= lf_{m+2}(*,\langle t_1,...,t_{m+2}\rangle)$

$= lf_{m+2}(*,t)$.

We formulate the above without ellipsis as follows. Define
$b' : [1,m+1] \to [1,m+1]$ by

$$b'(j) := j \text{ if } j \neq i \text{ and } j \neq m+1,$$

$$b'(i) := m+1,$$

$$b'(m+1) := i.$$

Define $b'' : [1,m+1] \to [1,m+1]$ by

$$b''(j) := bb'(j) \text{ if } j \neq m+1,$$

$$b''(m+1) := b(m+2).$$

Then b' and b'' are bijections $[1,m+1] \to [1,m+1]$. We have

$$\begin{aligned}
&lf_{m+2}(*,tb) \\
&= lf_{m+1}(*,(tb)\downarrow[1,m+1])*tb(m+2) \\
&\quad \text{(by Fact 4.3 and Definition 4.4)} \\
&= lf_{m+1}(*,(tb)\downarrow[1,m+1]b')*tb(m+2) \\
&\quad \text{(by (IH))} \\
&= lf_{m+1}(*,tbb')*tb(m+2) \\
&= lf_{m}(*,(tbb')\downarrow[1,m])*tbb'(m+1)*tb(m+2) \\
&\quad \text{(by Fact 4.3 and Definition 4.4)} \\
&= lf_{m}(*,(tbb')\downarrow[1,m])*tb(m+2)*tbb'(m+1) \\
&\quad \text{(by associativity and commutativity)} \\
&= lf_{m}(*,(tb'')\downarrow[1,m])*tb''(m+1)*tbb'(m+1) \\
&\quad \text{(by definition of b'')} \\
&= lf_{m+1}(*,(tb'')\downarrow[1,m+1])*tbb'(m+1) \\
&\quad \text{(by Fact 4.3 and Definition 4.4)} \\
&= lf_{m+1}(*,t\downarrow[1,m+1]b'')*tbb'(m+1) \\
&= lf_{m+1}(*,t\downarrow[1,m+1])*tbb'(m+1) \\
&\quad \text{(by (IH))} \\
&= lf_{m+1}(*,t\downarrow[1,m+1])*tb(i) \\
&= lf_{m+1}(*,t\downarrow[1,m+1])*t_{m+2} \\
&= lf_{m+2}(*,t) \\
&\quad \text{(by Fact 4.3 and Definition 4.4).}
\end{aligned}$$

□

**

Fact 4.8. Definition 4.7 defines the same function as Definitions 3.1 and 3.2.

Proof. We have already shown that Definitions 3.1 and 3.2 define the same function so it suffices to show that Definitions 3.2 and 4.7 define the same function. Let us denote σ according to Definition 3.2 by σ_2 and let us denote σ according to Definition 4.7 by σ_3. We want to prove

$$\text{for all } n \text{ in } \mathbb{N}^+\text{: } \sigma_2(n) = \sigma_3(n).$$

We prove this by induction on n.

- Base case: We want to prove $\sigma_2(1) = \sigma_3(1)$. This follows directly from definitions:

$$\begin{aligned}
\sigma_2(1) &= 1 && \text{(by Definition 3.2)}\\
&= lf_1(+, \langle 1\rangle) && \text{(by Definition 4.4)}\\
&= lf_1(+, \iota_1) && \text{(by Definition 4.2)}\\
&= \sigma_3(1) && \text{(by Definition 4.7).}
\end{aligned}$$

- Induction step: The induction hypothesis is

  (IH) $\sigma_2(n) = \sigma_3(n)$

  and we want to prove

$$\sigma_2(n+1) = \sigma_3(n+1).$$

  We have

$$\begin{aligned}
\sigma_2(n+1) &= \sigma_2(n)+n+1 && \text{(by Definition 3.2)}\\
&= \sigma_3(n)+n+1 && \text{(by (IH))}\\
&= lf_n(+, \iota_n)+n+1 && \text{(by Definition 4.7)}\\
&= lf_{n+1}(+, \iota_n::(n+1)) && \text{(by Definition 4.4)}\\
&= lf_{n+1}(+, \iota_{n+1}) && \text{(by Definition 4.2)}\\
&= \sigma_3(n+1) && \text{(by Definition 4.7).}
\end{aligned}$$

□

**