Arithmetical Foundations A

Michael Pfender

September 3, 2018

Preprint Institut für Mathematik TU Berlin
submitted to **J Symb Logic**

Abstract

Free-variables categorical cartesian theories: Interpretation of free variables as identitic maps or projections. Iteration, full schema of primitive recursion, Hilbert's infinite hotel, Algebra and order on the Natural Numbers Object $\mathbb{N}$.

Contents

Introduction

We fix *constructive foundations* for arithmetic on a map theoretical, algorithmic level. In contrast to elementhood and quantification based traditional foundations such as Principia Mathematica **PM**, Zermelo-Fraenkel **set** theory **ZF**, or v. Neumann-Gödel-Bernays **set** theory **NGB**, our *fundamental primitive recursive theory* **PR** has as its *basic* "undefined" (not further defined) terms just terms for objects and maps. On that language level it is *variable free,* and it is free from formal quantification on *individuals* like numbers or number pairs.

Theory **PR** is strongly finitistic with only *bound* existential quantification, in the sense of Skolem 1919/1970, p. 153.[1]

PR is a formal, *combinatorial category* with cartesian i. e. universal product and a natural numbers object (NNO) $\mathbb{N}$, a *p. r. cartesian category,* cf. Romàn 1989.

The NNO $\mathbb{N}$ admits *iteration of endo maps* and the *full schema of primitive recursion.* Such NNO has been introduced in categorical terms by Freyd 1972, on the basis of the NNO of Lawvere 1964.

We remain on the purely syntactical level of this categorical theory and later extensions: no formal semantics necessary into an outside, non-combinatorial world, cf. Hilbert's formalistic program.

Fundamental (categorical) p. r. theory **PR** is developped from the endomap iteration scheme (§) of Eilenberg/Elgot 1970. We take as additional axiom Freyd's *uniqueness* of the initialised iterated endo map. This gives the full schema of

---

[1] "Was ich nun in dieser Abhandlung zu zeigen wünsche ist folgendes: *Faßt man die allgemeinen Sätze der Arithmetik als Funktionalbehauptungen auf, und basiert man sich auf der rekurrierenden Denkweise, so läßt sich diese Wissenschaft in folgerichtiger Weise ohne Anwendung der Russel-Whitehead'schen Begriffe "always" und "sometimes" begründen."*

primitive recursion including uniqueness of p. r. maps defined by that scheme.

Into our variable-free setting are introduced *free variables,* formally interpreted as names for identity and projection maps. As a consequence, we have in the present context 'free variable' as a *defined* notion. We have object and map constants such as terminal object, NNO, zero constant and successor map, and use free metavariables for objects and for maps.

Fundamental arithmetic is further developped along GOODSTEIN's 1971 *Free Variables Arithmetic* whose *uniqueness rules* are derived as theorems of categorical theory **PR** with its "eliminable" notion of *free variable.*

This gives the expected structure theorem for algebra and order on NNO $\mathbb{N}$. "On the way", via Goodstein's *truncated subtraction* and his commutativity of the maximum function, we obtain the *equality definability theorem:* If *predicative equality* of two p. r. maps "on all arguments" is derivably true, then *map* equality *between* these maps is derivable.

Within our cartesian categorical frame we derive further the structure of the Natural Numbers Object to be relied on in forthcoming parts II and III of present investigation.

1 Cartesian language

We develop from scratch the free-variables "but" categorial language of cartesian products, possibly nested, cartesian products of fundamental $\mathbb{1}$, object $\mathbb{1}$, *one-element set,* and *natural numbers object* "NNO" $\mathbb{N}$. NNO $\mathbb{N}$ comes with *zero* map $0 : \mathbb{1} \to \mathbb{N}$ and *successor* (endo) map $\mathrm{s} : \mathbb{N} \to \mathbb{N}$.

We ***define/interpret*** *free variables* as *identity maps* resp. left or right *projections* – possibly nested – out of cartesian products, onto their *factors.* Within the **axioms** for *cartesian theories* (bearing on objects and maps) we specify use and interpretation of these free variables which can be seen as *components* in terms of Linear Algebra.[2][3]

A special rôle is played by *terminal object* $\mathbb{1}$. It works as the *empty cartesian product* $\mathbb{N}^0$, comes with a (unique) "projection" map $\Pi : A \to \mathbb{1}$ for each object A, and is the *domain* object for *concrete "elements"* $\boldsymbol{a} : \mathbb{1} \to A$ of A, in particular for *(concrete) numbers* $\boldsymbol{n} : \mathbb{1} \to \mathbb{N}$. We turn to the formal development of the *cartesian theory* **CA** generated over the NNO $\mathbb{1} \xrightarrow{0} \mathbb{N} \xrightarrow{\mathrm{s}} \mathbb{N}$.

1.1 Fundamental object language symbols

The set of fundamental symbols of cartesian language **CA** is

$$\{\mathbb{1}, \mathbb{N}, \times, 0, \mathrm{s}, \mathrm{id}, \circ, \Pi, \ell, \mathrm{r}\}, \text{and equality sign '='}$$

$\mathbb{1}$ is the *one-element object,* $\mathbb{N}$ the *Natural Numbers Object, NNO,* of theories **CA** and **PR** to come, $\times$ the cartesian product of objects and of maps. 0 is the *zero constant* $0 : \mathbb{1} \to \mathbb{N}$, s is the "fundamental" *successor function* $\mathrm{s} : \mathbb{N} \to \mathbb{N}$ to formalise counting.

Identity is the family of *identity maps* to all objects, these *objects* obtained out of objects $\mathbb{1}$ and $\mathbb{N}$ by *cartesian product* $\times$,

[2]K. Polthier

[3]in subsection 3 we show on the example of a distributive law how to transform a free-variables equation into a variable-free map equation.

$\circ$ is map *composition,* occasionally replaced by concatenation, Π symbolises the family of *terminal maps* into object $\mathbb{1}$, ℓ and r are left resp. right *projections* out of cartesian product $A \times B$ onto *factors* A and B respectively.

Theory **PR** below – of *primitive recursion* – will come with an additional symbol § for endomap *iteration.*[4]

1.2 Cartesian category axioms

We give here the axioms of cartesian categorical theory **CA** in a fully formal way using Gentzen bars for expression of metamathematical **inferences.** The most characteristic such axioms are marked by a •

• **Ax** [$\mathbb{N}$]

(no antecedent for this inference)

$\{$**Obj** $\mathbb{1}$, $\mathbb{N}\}$

one-element object and *natural numbers object;*

map $0 : \mathbb{1} \to \mathbb{N}$ ***zero*** *constant*

map $\mathrm{s} : \mathbb{N} \to \mathbb{N}$ ***successor*** *function*

Ax [id]

Obj A

---

map $\mathrm{id}_A = \mathrm{id} : A \to A$

identity *map*

[4] Eilenberg/Elgot 1970

$$\textbf{Ax}\ [\,\textit{reflexivity}\,]\quad \frac{\textbf{map}\ f}{f = f}$$

$$\textbf{Ax}\ [\,\textit{symmetry}\,]\quad \frac{\textbf{map}\ f, g;\quad f = g}{g = f}$$

$$\textbf{Ax}\ [\,\textit{transitivity}\,]\quad \frac{\textbf{map}\ f, g, h;\quad f = g;\ g = h}{f = h}$$

• $\textbf{Ax}\ [\,\circ\,]\quad \dfrac{f : A \to B;\ \ g : B \to C}{\text{map } (g\,f) = (g \circ f) = g(f) : A \to C;}$

$(g \circ f) : A \to B \to C$

map ***composition***

(outmost brackets may be omitted)

$$\textbf{Ax}\ [\,\circ\,\text{sub}\,]\quad \frac{f, \tilde{f} : A \to B;\ \ g : B \to C;\ f = \tilde{f}}{g \circ f = g \circ \tilde{f}}$$ Leibniz' ***substitutivity***

Substitution of equals into same gives equals.

$$\textbf{Ax}\ [\,\text{sub}\circ\,]\quad \frac{f : A \to B;\ \ g, \tilde{g} : B \to C;\ g = \tilde{g}}{g \circ f = \tilde{g} \circ f\ \ \textbf{\textit{second}}\ \text{Leibniz' }\textbf{\textit{substitutivity}}}$$

Substitution of same into equals gives equals.

$$\textbf{Ax}\ [\,\circ\ \text{id}\,]\quad \frac{f : A \to B}{\begin{array}{l} f \circ \text{id} = f \circ \text{id}_A = f; \\ \text{id} \circ f = \text{id}_B \circ f = f \\ \textbf{\textit{neutrality}}\ \textit{of identities to composition} \end{array}}$$

It follows a first statement on the use of free variables.

$$\textbf{Lemma}\ [\,\circ\ \textbf{var}\,]\quad \frac{\begin{array}{l} f : A \to B; \\ \textbf{var}\ a \in A,\ a := \text{id}_A \end{array}}{\begin{array}{l} f(a) = f(\text{id}_A)\ \ =_{\text{by def}}\ \ f \circ \text{id}_A = f \\ \textbf{\textit{free variable as identity,}} \\ f(a) \in B\ \ \textit{“dependent variable”}\ \ \textbf{q. e. d.} \end{array}}$$

Next axiom is ***associativity*** *of composition.*

$$\bullet\ \textbf{Ax}\ [\,\text{ass}\ \circ\,]\quad \frac{\begin{array}{l} f : A \to B;\ \ g : B \to C;\ \ h : C \to D \\ \textbf{var}\ a \in A,\ a := \text{id}_A \end{array}}{\begin{array}{l} (h \circ g) \circ f = h \circ (g \circ f) : A \to D \\ = h \circ g \circ f = h\, g\, f = h(g(f(a)))) \end{array}}$$

Counting Remark: Up to insertion of (composition-neutral) identities, the maps of *category theory* generated over $\mathrm{s} : \mathbb{N} \to \mathbb{N}$ are just the iterated $\mathrm{s} \circ \ldots \circ \mathrm{s} : \mathbb{N} \xrightarrow{\mathrm{s}} \ldots \xrightarrow{\mathrm{s}} \mathbb{N}$ of the successor map, as well as the

numerals:

$$\frac{\text{(empty antecedent)}}{0 : \mathbb{1} \to \mathbb{N} \ \textit{\textbf{numeral}}}$$

$$\frac{\boldsymbol{n} : \mathbb{1} \to \mathbb{N} \ \text{numeral}}{(\mathrm{s} \circ \boldsymbol{n}) : \mathbb{1} \to \mathbb{N} \ \textit{\textbf{numeral}}}$$

example: $(\mathrm{s} \circ (\mathrm{s} \circ (\mathrm{s} \circ 0)))$

Cartesian structure

For each object is given a *terminal map* to object $\mathbb{1}$,

$$\textbf{Ax}\,[\,\Pi\,] \quad \frac{\textbf{Obj}\ A}{\textbf{map}\ \Pi = \Pi_A : A \to \mathbb{1}}$$

terminal *map*

• $$\textbf{Ax}\,[\,!\Pi\,] \quad \frac{f : A \to \mathbb{1}}{f = \Pi_A}$$

uniqueness

– equivalent to *naturality* of family Π given by (commutativity) of every DIAGRAM of form

$$\begin{array}{ccc} A & \xrightarrow{g} & B \\ \downarrow{\scriptstyle \Pi_A} & = & \downarrow{\scriptstyle \Pi_B} \\ \mathbb{1} & \xrightarrow{\text{id}} & \mathbb{1} \end{array}$$

Remark: This naturality axiom for family Π is not required for *half*-terminal *monoidal* categories, introduced in BUDACH & HOEHNCKE 1975. Theory $\widehat{\mathbf{S}}$ to come of *partially defined* (primitive) recursive maps is of that type.

Notation: Equality sign '=' inserted into (part of) a diagram means commutativity of (that part of) a diagram, equality of composition of arrows along both paths.

- **Ax** [**Obj** ×] $\dfrac{\mathbf{Obj}\ A, B}{\mathbf{Obj}\ (A \times B)}$

  (binary) ***cartesian product*** *of objects.*

  Iteration gives *nested* products.

  Outmost brackets may be omitted.

We introduce use of pairs of free variables as pairs of left and right *projections:*

Obj A, B

var $a \in A$, **var** $b \in B$

• **Ax** $[\,\ell, \mathrm{r}\,]$ ———————————————

map $\ell = \ell_{A,B} : A \times B \to A$

map $\mathrm{r} = \mathrm{r}_{A,B} : A \times B \to B$

left resp. right ***projection***

$a = \ell_{A,B},\ b = \mathrm{r}_{A,B}$

variables as projections.

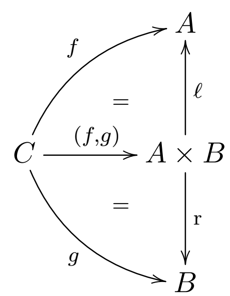
map $f : C \to A,\ g : C \to B$

• **Ax** $[\,\mathrm{indu}\,]$ ———————————————

map $(f, g) : C \to A \times B$

induced *map into product*

$\ell \circ (f, g) = f,\ \mathrm{r} \circ (f, g) = g$



Godement's DIAGRAM

uniqueness of horizontal arrow see below. This is the very beginning of map-theoretic, element-free category theory.

$$\textbf{Ax}\,[\,\mathrm{sub}(\ ,\ )\,]\quad \frac{f, \tilde{f} : C \to A;\ g, \tilde{g} : C \to B;\quad f = \tilde{f};\ g = \tilde{g}}{(f, g) = (\tilde{f}, \tilde{g})}$$

compatibility *of inducing* with '='

$$\textbf{Ax}\,[\,\mathrm{distr}\,]\quad \frac{h : D \to C,\ f : C \to A,\ g : C \to B}{(f, g) \circ h = (f \circ h, g \circ h) : D \to (A \times B)}$$

distributivity *of compositionn over forming the induced map into product.*

Use of **free variable** for induced map:

$$\textbf{Lemma}\quad \frac{\textbf{var}\ c \in C,\ c := \mathrm{id}_C}{\begin{array}{l}\ell \circ (f, g)(c) = \ell \circ (f(c), g(c)) = f(c),\\ \mathrm{r} \circ (f, g)(c) = \mathrm{r} \circ (f(c), g(c)) = g(c)\end{array}}$$

q. e. d.

$$\textbf{Ax}\,[\,\mathrm{retr.\ pairing}\,]\quad \frac{h : C \to (A \times B)}{(\ell_{A,B} \circ h, \mathrm{r}_{A,B} \circ h) = h}$$

pairing *is* ***retractive***

(*even* ***isomorphic***)

$$\textbf{Lemma}\ [\,!(\ ,\ )\,]\quad \frac{f : C \to A;\ g : C \to B;\quad h : C \to (A \times B);\quad \ell_{A,B} \circ h = f;\ \mathrm{r}_{A,B} \circ h = g}{h = (f, g)}$$

uniqueness *of induced map*

Proof:

$$\begin{aligned} h &= \mathrm{id}_{A\times B} \circ h \\ &= (\ell_{A,B} \circ \mathrm{id}_{A,B}, \mathrm{r}_{A,B} \circ \mathrm{id}_{A,B}) \circ h \quad \text{[retr. pairing]} \\ &= (\ell_{A,B}, \mathrm{r}_{A,B}) \circ h \\ &= (\ell_{A,B} \circ h, \mathrm{r}_{A,B} \circ h) \quad \text{[distr]} \\ &= (f, g) : C \to A \times B \quad \text{[sub(,)]} \end{aligned}$$

q. e. d.

$$\textbf{Lemma}\ [\,(\ell, \mathrm{r})\,]\quad \frac{\textbf{Obj}\ A, B}{(\ell_{A,B}, \mathrm{r}_{A,B}) = \mathrm{id}_{A\times B}}$$

Proof: uniqueness of induced into product $A \times B$ **q. e. d.**

$$\textbf{Def}\ [\,\times\ \text{maps}\,]\quad \frac{f : A \to A',\ g : B \to B'\quad \textbf{var}\ a := \ell_{A,B},\ b := \mathrm{r}_{A,B}}{(f \times g) = (f \circ \ell, g \circ \mathrm{r}) : (A \times B) \to (A' \times B')}$$

$$f \times g = (f \times g)(a, b) = (f(a), g(b))$$

cartesian map product

[**unary** $\times$]

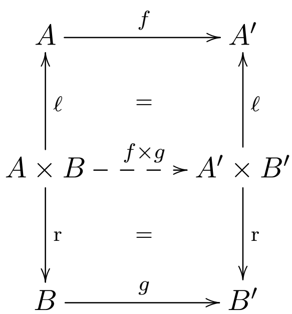
$$\frac{f : A \to A',\ g : B \to B',}{\begin{array}{l}(A \times g) \ =_{\text{def}}\ (\mathrm{id}_A \times g) : A \times B \to A \times B' \\ (f \times B) \ =_{\text{def}}\ (f \times \mathrm{id}_B) : A \times B \to A' \times B\end{array}}$$

Theorem [$\mathrm{nat}_{\ell,r}$]

$$\frac{\textbf{map}\ f : A \to A',\ g : B \to B'}{\ell \circ (f \times g) = f \circ \ell;\ \mathrm{r} \circ (f \times g) = g \circ \mathrm{r}}$$

naturality *of projection families* ℓ *and* r.

Proof: uniqueness of induced map into product $A' \times B'$, consider

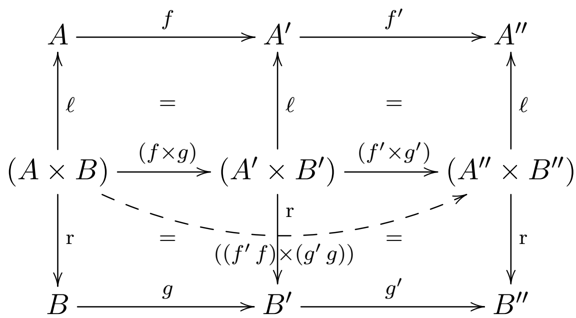


Cartesian map product DIAGRAM

$$
\textbf{Theorem } [\,\times\ \circ\,] \quad \frac{f : A \to A',\ f' : A' \to A''; \qquad g : B \to B',\ g' : B' \to B'';}{\begin{array}{l} \mathrm{id}_A \times \mathrm{id}_B = \mathrm{id}_{A\times B} : A \times B \to A \times B \\ (f' \circ f) \times (g' \circ g) = (f' \times g') \circ (f \times g) : \\ (A \times B) \to (A'' \times B'') \end{array}}
$$

bifunctoriality *of cartesian product*

Proof: uniqueness of induced map into product $A'' \times B''$ in

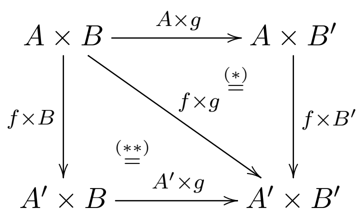


Cartesian bifunctoriality DIAGRAM

q. e. d.

$$
\textbf{Corollary } [\,\times\ \mathrm{id}\ \circ\,] \quad \frac{f : A \to A',\ g : B \to B'}{\begin{array}{l} f \times g = (f \times B') \circ (A \times g) \\ = (A' \times g) \circ (f \times B) \end{array}}
$$

map product ***decomposition***



map product decomposition DIAGRAM

Proof:

$$(f \times B') \circ (A \times g) = (f \times \mathrm{id}_{B'}) \circ (\mathrm{id}_A \times g)$$
$$= (f \circ \mathrm{id}_A) \times (\mathrm{id}_{B'} \circ g) \qquad \text{(by bifunctoriality)}$$
$$= f \times g \quad (*)$$

the latter by compatibility of (,) with equality, which entails compatibility of $\times$ with equality.

Analogously

$$(A' \times g) \circ (f \times B) = (\mathrm{id}_{A'} \times g) \circ (f \times \mathrm{id}_B)$$
$$= (\mathrm{id}_{A'} \circ f) \times (f \circ \mathrm{id}_B) \qquad \text{(by bifunctoriality)}$$
$$= f \times g \quad (**)$$

q. e. d.

Distributivity Corollary [<u>Distr</u> $\times$ $\circ$ (,)]

$$\frac{f : C \to A,\ g : C \to B,\ f' : A \to A',\ g' : B \to B'}{(f' \times g') \circ (f, g) = (f' \circ f, g' \circ g) : C \to A' \times B'}$$

Proof:

$$
\begin{aligned}
&(f' \times g') \circ (f, g) \\
&= (f' \circ \ell_{A',B'}, g' \circ \mathrm{r}_{A',B'}) \circ (f, g) \\
&= (f' \circ \ell_{A',B'} \circ (f, g), g' \circ \mathrm{r}_{A',B'} \circ (f, g)) \text{ by } \mathbf{Ax}\,[\,\mathrm{distr}\,] \\
&= (f' \circ (\ell_{A',B'} \circ (f, g)), g' \circ (\mathrm{r}_{A',B'} \circ (f, g))) \\
&= (f' \circ f, g' \circ g) \ \ \mathbf{q.\,e.\,d.}
\end{aligned}
$$

1.3 Interpretation of free variables

We start with a ("generic") example of *elimination* of free variables by their interpretation *into (possibly nested) projections* within a ring R.

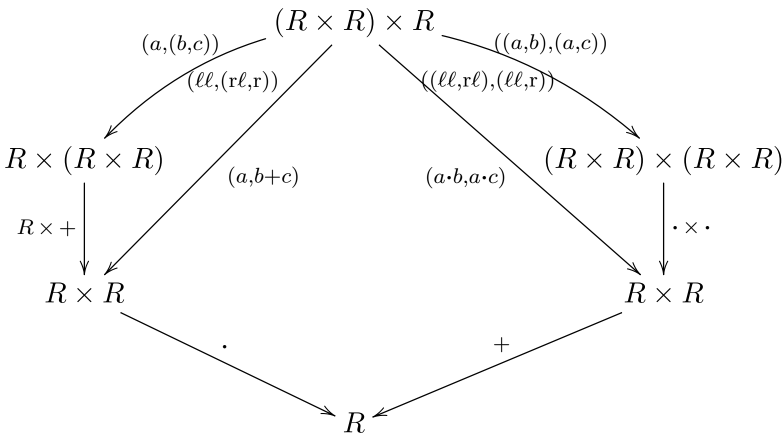
A distributive law $a \cdot (b + c) = a \cdot b + a \cdot c$ gets the map interpretation

$$
\begin{aligned}
&a \cdot (b + c) = (a \cdot b) + (a \cdot c) : \\
&R^3 \ =_{\text{by def}} \ R^2 \times R \ =_{\text{by def}} \ (R \times R) \times R \to R \\
&\qquad \text{with } \textit{systematic} \text{ interpretation of variables:} \\
&a := \ell\ \ell,\ b := \mathrm{r}\ \ell,\ c := \mathrm{r} : R^3 = (R \times R) \times R \to R
\end{aligned}
$$

and infix writing of operations $x\, op\, y : R \times R \to R$ prefix interpreted as $op \circ (x, y)$, here

$$
\cdot \circ (a, + \circ (b, c)) = + \circ (\cdot \circ (a, b), \cdot \circ (a, c)) : R^3 \to R
$$

In form of a commuting diagram:



An *iterated map*[5] $f^{\S} : A \times \mathbb{N}$ may be written in free-variables notation as

$$f^{\S} = f^{\S}(a, n) = f^{n}(a) : A \times \mathbb{N} \to A$$

with $a := \ell : A \times \mathbb{N} \to A$, and $n := \mathrm{r} : A \times \mathbb{N} \to \mathbb{N}$

Systematic map interpretation of free-variables equations:

1. Extract the common codomain (domain of values), say B, of both sides of the equation (this codomain may be implicit);
2. "Expand" operator priority into additional bracket pairs;
3. Transform infix into prefix notation on both sides of the equation;

[5] see below

4. Order the (finitely many) variables appearing in the equation, for example lexically;
5. If these variables $a_1, a_2, \ldots, a_{\underline{m}}$ range over the objects $A_1, A_2, \ldots, A_{\underline{m}}$, then fix as common *domain object* (source of commuting diagram), the object

   $A = A_1 \times A_2 \times \ldots \times A_{\boldsymbol{m}} =_{\text{def}} (\ldots((A_1 \times A_2) \times \ldots) \times A_{\boldsymbol{m}});$
6. Interpret the variables as *identities* or (possibly nested) *projections,* will say: replace, within the equation, all the occurences of a *variable* by the corresponding – in general *binary nested* – projection;
7. Replace each symbol "0" by "$0\ \Pi_D$" where "D" is the (common) domain of (both sides) of the equation;
8. Insert composition symbol $\circ$ between terms which are not bound together by an *induced map operator* as in (f_1, f_2);
9. By the above, we have the following two-maps-cartesian-Product **rule,** forth and back: For $a := \ell_{A,B} : (A \times B) \to A$, $b := \mathrm{r}_{A,B} : (A \times B) \to B$ and $f : A \to A'$ as well as $g : B \to B'$, the following identity holds:

$$\begin{aligned}
&(f \times g)(a, b) = (f \times g) \circ (\ell_{A,B}, \mathrm{r}_{A,B}) \\
&= (f \times g) \circ \mathrm{id}_{(A \times B)} = (f \times g) \\
&= (f \circ \ell_{A,B}, g \circ \mathrm{r}_{A,B}) \\
&= (f \circ a, g \circ b) = (f(a), g(b)) : A \times B \to A' \times B'
\end{aligned}$$

10. For free variables $a \in A$, $n \in \mathbb{N}$ interpret the term $f^n(a)$ as the map $f^{\S}(a, n) : A \times \mathbb{N} \to A$, *iterated* of endomap $f : A \to A$, see next section.

These 10 interpretation steps transform a cartesian [a cartesian p. r.] free-variables equation into a variable-free, categorical equation of theory **CA** [and of **PR** to come]:

Elimination of (free) variables by their interpretation as *projections,* and vice versa: *Introduction of free variables* as *names* for identities resp. projections. We allow for mixed notation too. All this, for the time being, just in the context of cartesian theories.

All of our theories are free from classical, (axiomatic) formal unbound quantification.[6] Free-variables equations are understood intuitively as *universally quantified.* But a free variable $a \in A$ occurring only in the premise of an *implication* takes (in suitable context), the meaning

for any given $a \in A$: premise $(\ldots a) \implies$ conclusion, i. e.

if exists $a \in A$ s. t. premise $(\ldots a)$, *then* conclusion;

provided that (free) variable $a \in A$ does not occur in conclusion.

2 Primitive Recursion

We introduce Gödel's primitive recursion – called by him just *recursion*[7] –, beginning with the iteration schema in Eilenberg/Elgot 1970. We show the *full schema of primitive recursion* and uniqueness of the NNO $\mathbb{N}$ within the categorical

[6] critizised by Skolem 1919

[7] later Ackermann found a *recursive* function which is *n*ot primitive recursive, cf. **Appendix A.** The same holds for *evaluation* of primitive recursive map codes below.

theory **PR** of primitive recursion to be described in this section.

2.1 Iteration axioms added

- **Ax** [§]
$$\frac{f : A \to A \text{ (endomap)},\ \mathbf{var}\ a \in A,\ \mathbf{var}\ n \in \mathbb{N}}{}$$

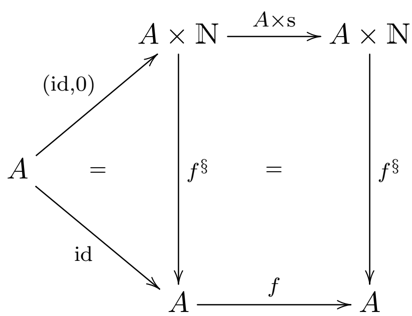
$f^{\S} = f^{\S}(a, n) : A \times \mathbb{N} \to A$ (*iterated*);

$f^{\S}(a, 0) := f^{\S}(\mathrm{id}_A, 0_A) = f^{\S}(\mathrm{id}_A, 0\,\Pi_A) = a = \mathrm{id}_A :$
$A \to A \times \mathbb{N}$ (*anchoring*);

$f^{\S} \circ (A \times \mathrm{s}) = f^{\S}(a, \mathrm{s}\,n) = f \circ f^{\S} = f(f^{\S}(a, n)) :$
$A \times \mathbb{N} \to A \to A$ (*iteration step*);

$f^n(a) := f^{\S}(a, n)$

apply *iteratively endomap f to initial argument a, iterate n times.*



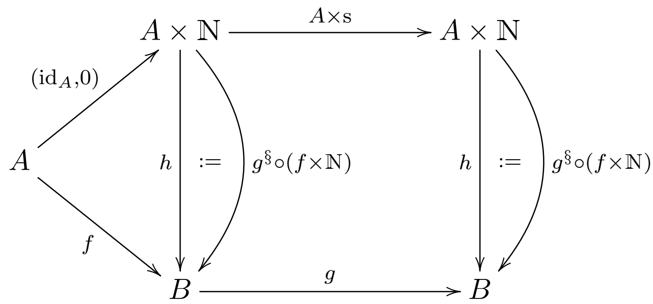
(§)

Iteration DIAGRAM

$f : A \to B;\ \ g : B \to B;$

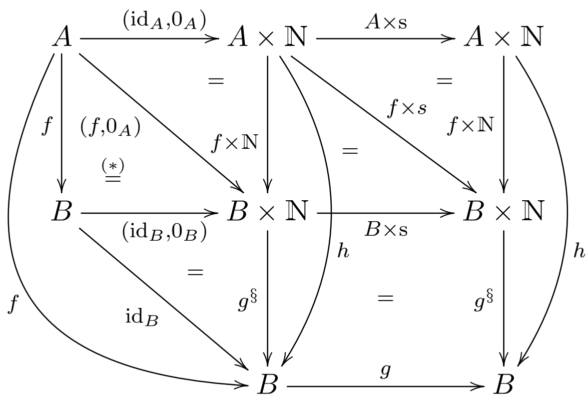
$h := g^{\S}\,(f \times \mathrm{id}_{\mathbb{N}}) : A \times \mathbb{N} \to B \times \mathbb{N} \to B$

Lemma [FR]



commutes

Proof: Consider DIAGRAM



In particular equation $(*)$ holds by uniqueness of terminal map $A \to \mathbb{1} : 0_B\, f = 0\,\Pi_B\, f = 0\,\Pi_A = 0_A$ and "then" by distributivity of $\circ$ over $(\ ,\ )$ **q. e. d.**

$f : A \to B;\ g : B \to B;\ h : A \times \mathbb{N} \to B;$

var $a \in A$, **var** $n \in \mathbb{N}$;

$h(a, 0) = f(a);$

$h(a, \mathrm{s}\, n) = g\, h(a, n)$

• **Ax** [FR!] ———————————————

$h = g^{\S}\,(f \times \mathrm{id}_{\mathbb{N}})$ i. e.

$h(a, n) = g^n(f(a)) : A \times \mathbb{N} \to B :$

Freyd's ***uniqueness*** *of the iterated endomap g*

initialised *by map f*

[“$g^{\S}\,(f \times \mathrm{id}_{\mathbb{N}})$ does the job”, see [FR] above.]

$f : A \to A;\ h : A \times \mathbb{N} \to A$

var $a \in A$, **var** $n \in \mathbb{N}$;

$h(a, 0) = a = \mathrm{id}_A(a);$

$h(a, \mathrm{s}\, n) = f\, h(a, n)$

Corollary [§!] ———————————————

$h = f^{\S}$

uniqueness *of “simply” iterated* $f^{\S}$

$f, \tilde{f} : A \to A;\ f = \tilde{f}$

Lemma [§ =] ———————————————

$f^{\S} = \tilde{f}^{\S} : A \times \mathbb{N} \to A$

compatibility *of iteration* § *with equality*

Proof:

$$\underline{\mathrm{Ax}}\,[\S],[\mathrm{sub}\circ]\quad \frac{\tilde f = f}{\begin{array}{l}\tilde f^{\S}(a,0) = \mathrm{id}_A \\ \tilde f^{\S}(a,s\,n) = \tilde f \circ \tilde f^{\S}(a,n) = f \circ \tilde f^{\S}(a,n)\end{array}}$$

and – the latter postcedent –

$$[\,\S!\,]\quad \frac{\begin{array}{l}\tilde f^{\S}(a,0) = \mathrm{id}_A \\ \tilde f^{\S}(a,s\,n) = f \circ \tilde f^{\S}(a,n)\end{array}}{\tilde f^{\S} = f^{\S}}$$

q. e. d.

2.2 Full schema of primitive recursion

Already for definition and characterisation of *multiplication* and moreover for proof of the laws of Arithmetic, the following ***full schema*** (pr) of primitive recursion is needed:

$$\textbf{Theorem (pr)} \quad \frac{\begin{array}{l} g = g(a) : A \to B \\ h = h((a,n),b) : (A \times \mathbb{N}) \times B \to B \end{array}}{\begin{array}{l} f = f(a,n) : A \times \mathbb{N} \to B \textbf{ s.t.} \\ \text{(anchor)} \quad f(a,0) = g(a), \text{ and} \\ \text{(step)} \quad f(a, \mathrm{s}\, n) = h((a,n), f(a,n)). \\ f =: \mathrm{pr}[g,h] \\ + \\ \text{(pr!) } \textit{uniqueness of } f \text{ to satisfy} \\ \text{these (anchor) and (step) equations.} \end{array}}$$

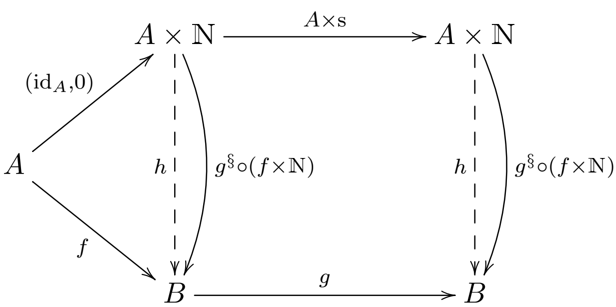
Interpretation: *General primitive recursive map $f = f(a,b)$ **initialised** by a map $g = g(a)$ and iteratively extended using a **step** map $h = h((a,n),b)$ which depends on previous value b but (possibly) also from initial argument $a \in A$ as well as from running recursion parameter $n \in \mathbb{N}$.*

Schema (pr) without use of free variables:[8]

[8] see Freyd 1972 and (then) Pfender, Kröplin, and Pape 1994

$$
\text{(pr)}\quad \frac{\begin{array}{l} g : A \to B \\ h : (A \times \mathbb{N}) \times B \to B \end{array}}{\begin{array}{l} \mathrm{pr}[g,h] := f : A \times \mathbb{N} \to B \\ f(\mathrm{id}_A, 0) = g : A \to B \\ f\,(\mathrm{id}_A \times \mathrm{s}) = h\,(\mathrm{id}_{A\times\mathbb{N}}, f) : \\ \quad (A \times \mathbb{N}) \to (A \times \mathbb{N}) \times B \to B \\ (\mathrm{pr!}) : f \ \textit{unique.} \end{array}}
$$

Schema (pr) is a consequence of iteration schema **Ax** [§] and *uniqueness of the initialised iterated* h, this taken as **axiom** (FR!), commuting diagram[9]



Remarks:

- Full schema (pr) of primitive recursion is an **axiom** in the classical theory of primitive recursion, subsystem of any classical (gödelian) arithmetical theory **T**.

[9] Freyd 1972

- Free-Variables Arithmetics of the natural numbers $\mathbb{N}$, the integers $\mathbb{Z}$, and the rationals $\mathbb{Q}$ can be based on the axioms of the cartesian theory **PR** of primitive recursion as defined in the above.

- Goodstein's[10] uniqueness axioms U_1 to U_4 – basic for his *Free-Variables Arithmetics* – are theorems of **PR**.

- In "Begründung der elementären Arithmetik durch die rekurrierende Denkweise ohne die Anwendung scheinbarer Veränderlichen mit unendlichem Ausdehnungsbereich", SKOLEM 1919 exhibits the strongly finitistic logical kernel of Principia Mathematica **PM,** and forshadows in particular GOODSTEIN 1971.

2.3 Proof of full schema

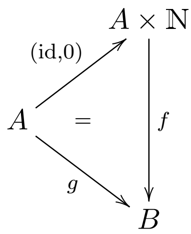
Proof of schema (pr) out of [§] and (FR!) : [11]

Construction of the map $f = \mathrm{pr}\,[\,g, h\,] : A \times \mathbb{N} \to B$ out of data $g : A \to B$ (*initialisation*) and $h : (A \times \mathbb{N}) \times B \to B$ (*iteration step*):

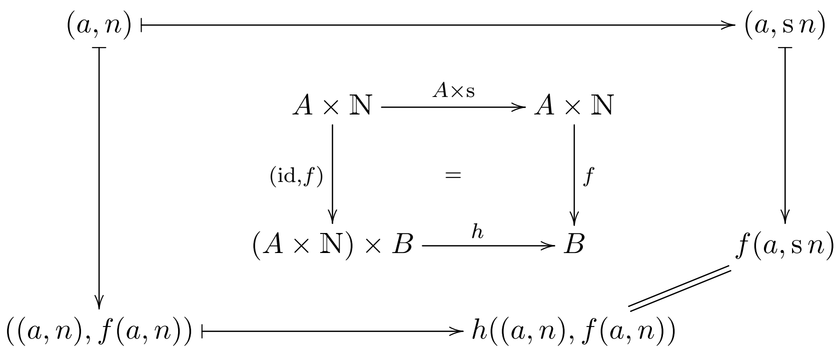
Wanted $f : A \times \mathbb{N} \to B$ is to satisfy (init) und (step) given as the two commuting DIAGRAMS

[10] GOODSTEIN 1971

[11] this proof and everything before has been verified by A. Cloete and G. Myrach within the proof verification system *HOL light*



(init)

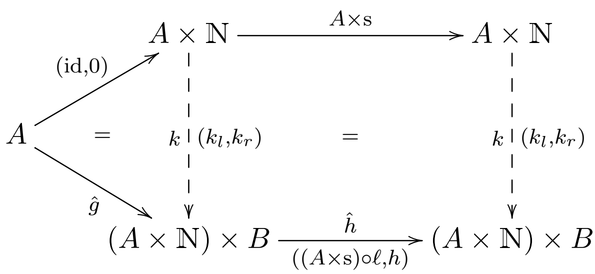


(step)

With $\hat{g} := ((\mathrm{id}_A, 0), g)$ and $\hat{h} := ((A \times \mathrm{s}) \circ \ell, h)$ we get by (FR!) a uniquely determined map

$$k = (k_l, k_r) : A \times \mathbb{N} \to (A \times \mathbb{N}) \times B$$

satisfying

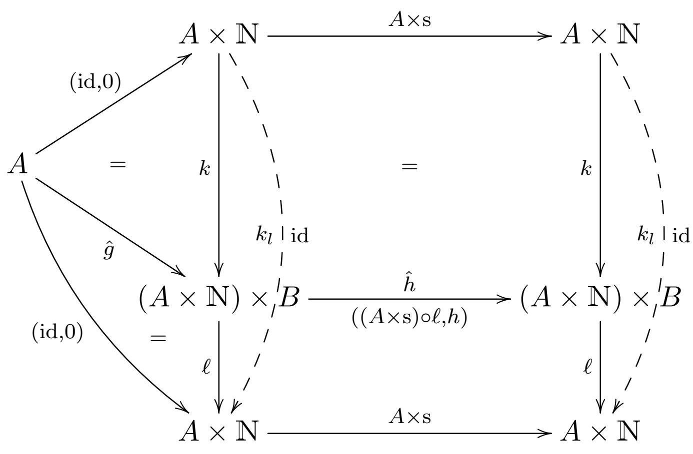


i. e.

$$k \circ (\mathrm{id}_A, 0) = \hat{g} \quad \text{and}$$
$$k \circ (A \times \mathrm{s}) = \hat{h} \circ k$$

[It will turn out that $k = (\mathrm{id}_{A \times \mathbb{N}}, f)$ for wanted map $f : A \times \mathbb{N} \to B$.]

For our unique k consider first its left component $k_l = \ell \circ k : A \times \mathbb{N} \to A \times \mathbb{N}$ unique – by (FR!) – in

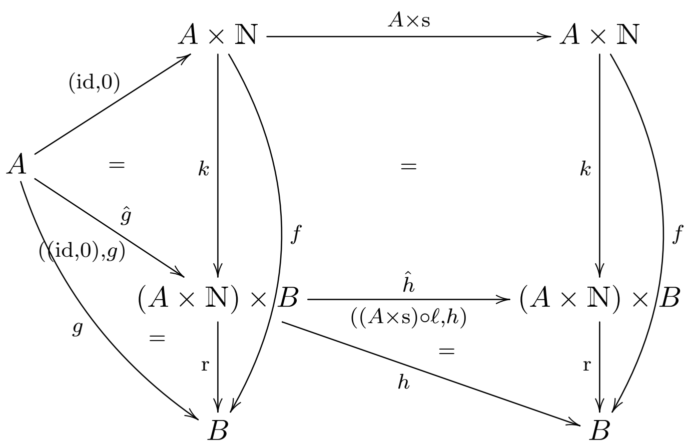


We have

$$\ell \circ k \circ (\mathrm{id}_A, 0) = \ell \circ \hat{g} = (\mathrm{id}_A, 0) \quad \text{and}$$
$$\ell \circ k \circ (A \times \mathrm{s}) = \ell \circ \hat{h} \circ k = (A \times \mathrm{s}) \circ \ell \circ k$$

Since these two equations hold likewise for $\mathrm{id}_{A\times\mathbb{N}}$ instead of $\ell \circ k$, equation $\ell \circ k = \mathrm{id}_{A\times\mathbb{N}}$ follows by uniqueness (FR!) of such a map.

Taking now $f := \mathrm{r} \circ k : A \times \mathbb{N} \to B$ we have the following diagram for this (unique) right component of $k : A \times \mathbb{N} \to (A \times \mathbb{N}) \times B$:



Obtain

$$k = (\ell \circ k, \mathrm{r} \circ k) = (\mathrm{id}_{A\times\mathbb{N}}, f)$$
$$f \circ (\mathrm{id}_A, 0) = \mathrm{r} \circ k \circ (\mathrm{id}_A, 0) = \mathrm{r} \circ \hat{g} = g \quad \text{and}$$
$$f \circ (A \times \mathrm{s}) = \mathrm{r} \circ k \circ (A \times \mathrm{s}) = \mathrm{r} \circ \hat{h} \circ k$$
$$= h \circ k = h \circ (\mathrm{id}_{A\times\mathbb{N}}, f)$$

So this map $f : A \times \mathbb{N} \to B$ is *available* to fullfill the requirements of $\mathrm{pr}\,[\,g, h\,] : A \times \mathbb{N} \to B$.

Uniqueness proof for such map f: Let f' be a map assumed likewise to satisfy equations (init) and (step).

Then take $k' := (\mathrm{id}_{A\times\mathbb{N}}, f') : A \times \mathbb{N} \to (A \times \mathbb{N}) \to B$ and calculate:

$$\begin{aligned}
k' \circ (\mathrm{id}_A, 0) &= (\mathrm{id}_{A\times\mathbb{N}}, f') \circ (\mathrm{id}_A, 0) \\
&= ((\mathrm{id}_A, 0), f' \circ (\mathrm{id}_A, 0)) \\
&= ((\mathrm{id}_A, 0), g) = \hat{g} \quad \text{as well as} \\
k' \circ (A \times \mathrm{s}) &= (\mathrm{id}_{A\times\mathbb{N}}, f') \circ (A \times \mathrm{s}) \\
&= ((A \times \mathrm{s}), f' \circ (A \times \mathrm{s})) \\
&= ((A \times \mathrm{s}), h) = \hat{h} \circ k'
\end{aligned}$$

Since by (FR!) k above is the *unique* map to satisfy the equations above, we have necessarily $k' = k$ and hence $f' = \mathrm{r} \circ k' = \mathrm{r} \circ k = f : A \times \mathbb{N} \to B$ **q. e. d.**

2.4 Program version of full schema

$$g = g(a) : A \to B \quad \text{(init)}$$

$$h = h((a,n),b) : (A \times \mathbb{N}) \times B \to B \quad \text{(step)}$$

(pr prog)

---

function $f = \mathrm{pr}[g,h]$

$= \mathrm{pr}[g,h](a,n) : A \times \mathbb{N} \to B ::$

var $b \in B$

$b := g(a);$

for $j := 0$ to $n-1$ do

$\{ b := h((a,j),b)$

od

result $\quad f(a,n) := b$

Dangerous bound: Recursion parameter $j \in [0, n-1]$ in a for loop given by *full schema* may be *used* within this loop, but not *modified* in the loop body, as for example by a statement of form $j := j+2$. Same for the *passive* parameter $a \in A$.

Examples of use of the *full schema,* in particular of dependence of recursion step from *passive parameter* $a \in A$ and/or from *recursion parameter* $n \in \mathbb{N}$ will be given at several occasions in the below. Mentioned is here the recursive definition of the *faculty* function

$\mathrm{fac} = \mathrm{fac}(n) = n! : \mathbb{N} \to \mathbb{N}.$

2.5 Uniqueness of the NNO

Category theorists like constructions which are *uniquely* given by their defining properties, unique up to *natural isomorphisms,* or – functorial constructions – up to natural equivalence. For the (binary) cartesian product with its projection families as *natural map* families, this is true by considerations earlier above, same for terminal object $\mathbb{1}$ and the family $\Pi : A \to \mathbb{1}$ of terminal maps (projections).

Now what about the Natural Numbers Object

$$\mathbb{1} \xrightarrow{0} \mathbb{N} \xrightarrow{s} \mathbb{N}\,?$$

This DIAGRAM has the property wanted, property which should be called *categoricity:* by its LAWVERE *existence* and *uniqueness* properties below, it is just the *initial diagram* $\mathbb{1} \xrightarrow{0} \mathbb{N} \xrightarrow{s} \mathbb{N}$ of form

$\mathbb{1} \xrightarrow{a_0} A \xrightarrow{f} A$.

So *purely map theoretically* the notion of an NNO *is categoric:* Within a cartesian map theory NNO $\mathbb{1} \xrightarrow{0} \mathbb{N} \xrightarrow{s} \mathbb{N}$ is unique up to *natural isomorphism.*

Specialised, sequences definition of NNO: LAWVERE defines the NNO $\mathbb{N}$ as follows:

$a_0 : \mathbb{1} \to A$ a *point*

$f : A \to A$ an endo map *to be iterated*

(NNO$_{\mathrm{FWL}}$) ———————————————

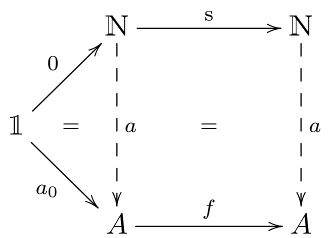
$a : \mathbb{N} \to A$ *resulting sequence*

$a \circ 0 = a_0 : \mathbb{1} \to A$ *start of sequence*

$a \circ \mathrm{s} = f \circ a : \mathbb{N} \to A$ *progress of sequence*

$+$ *uniqueness* of such sequence $a : \mathbb{N} \to A$

in DIAGRAM form:



LAWVERE NNO DIAGRAM

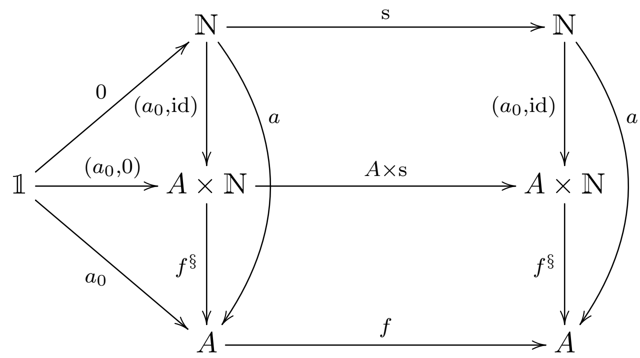
We show that this early NNO scheme is obtained from FREYD's scheme.

NNO Lemma: For $a_0 : \mathbb{1} \to A$ and $f : A \to A$ (antecedent in LAWVERE's NNO scheme) the map

$$a \; =_{\mathrm{def}} \; f^{\S} \circ (a_0, \mathrm{id}_{\mathbb{N}}) : \mathbb{N} \to A \times \mathbb{N} \xrightarrow{f^{\S}} A$$

uniquely makes the above diagram commute.

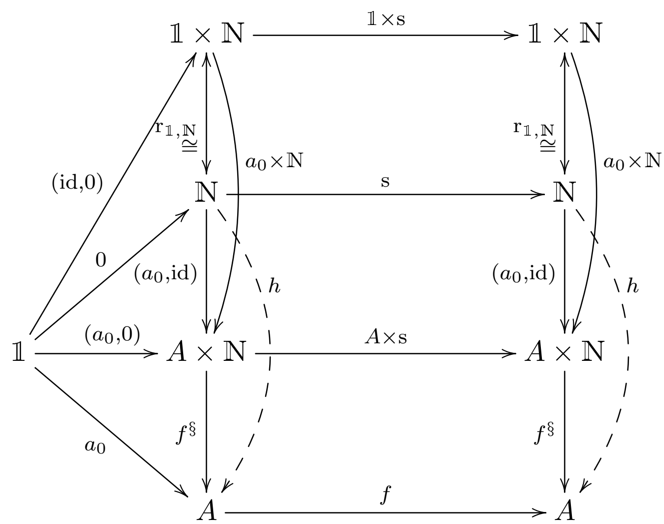
Proof: Consider the following DIAGRAM:



This diagram commutes with $a := f^{\S} \circ (a_0, \mathrm{id}_{\mathbb{N}})$, unique a as is seen by extending the diagram with **isomorphism**

$$\mathrm{r}_{\mathbb{1},\mathbb{N}} : \mathbb{1} \times \mathbb{N} \to \mathbb{N},\ \text{inverse } (\Pi_{\mathbb{N}}, \mathrm{id}_{\mathbb{N}})$$

into commuting DIAGRAM



FREYD to LAWVERE NNO specialisation DIAGRAM

$h = h(n) : \mathbb{N} \to A$ is to be another *sequence* assumed to fullfill the postcedent above in place of $a : \mathbb{N} \to A$. By uniqueness of the initialised iterated $f^{\S} \circ (a_0 \times \mathrm{id}_{\mathbb{N}})$ it must equal

$$a = f^{\S} \circ (a_0, \mathrm{id}_{\mathbb{N}}) : \mathbb{N} \to A \ \ \textbf{q. e. d.}$$

Remark: Conversely LAWVERE's NNO is said to have the properties of an NNO in FREYD's version quoted above. But for his proof of this assertion FREYD relies on internal hom structure – *axiomatic* exponentiation B^A – coming with *axiomatic* internal evaluation $\epsilon_{A,B} : B^A \times A \to B$ which is available in his context of an Elementary (higher order) Topos, not available in present context.

In RCF 3 in the References it is shown that the initial *cartesian closed* theory with NNO admits *code self-evaluation* and hence is inconsistent. This is one motivation for not considering here higher order recursion theory. The other motivation is simplicity: the Gödelian case is built on first-order in Smorynski 1977, no power sets needed.

2.6 Hilbert's infinite hotel

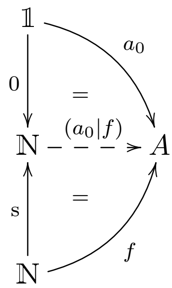
$\mathbb{N} \cong \mathbb{1} + \mathbb{N}$

$\mathbb{N}$ *is isomorphic to the coproduct of* $\mathbb{1}$ *and* $\mathbb{N}$

paradoxon on infinity

"But" maps $a_0 : \mathbb{1} \to A,\ f : \mathbb{N} \to A$ induce a unique map $(a_0|f) : \mathbb{N} \to A$ "out of the sum/coproduct"

$\mathbb{1} \xrightarrow{0} \mathbb{N} \xleftarrow{\mathrm{s}} \mathbb{N}$ such that

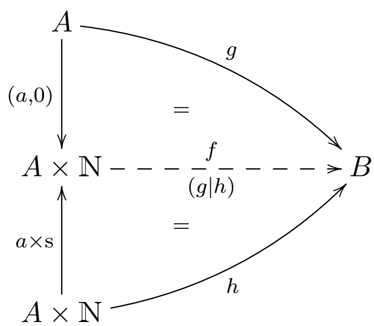


[Coproducts are *universal,* hence unique up to isomorphism.]

We **prove** a more general, *parametrised* version of **coproduct property** of $\mathbb{1} \xrightarrow{0} \mathbb{N} \xleftarrow{\mathrm{s}} \mathbb{N}$ namely: For A an arbitrary ("parameter") object A

$$A \times \mathbb{N} \cong A \times (\mathbb{1} + \mathbb{N}) \cong A + (A \times \mathbb{N})$$
$$[\cong (A \times \mathbb{1}) + (A \times \mathbb{N})\,]$$

Proof: We obtain, via full schema (pr) the following **coproduct** diagram where $a := \mathrm{id}_A : A \to A$, and "inducing" maps $g : A \to B,\ h : A \times \mathbb{N} \to B$ are given. They induce a unique map $f = (g|h) : A \times \mathbb{N}$ out of the *coproduct* $A \times \mathbb{N}$, what we have to show:



Map

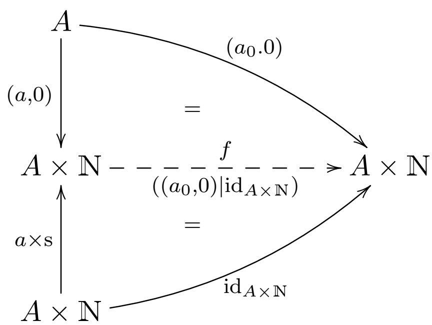
$$f = (g|h) \;=_{\text{def}}\; \mathrm{pr}[g, h \circ \ell] : A \times \mathbb{N} \to B$$

is the *unique* commutative fill-in into this *coproduct diagram,* since by full scheme (pr) of primitive recursion

$$f(a,0) = g(a) : A \to B$$
$$f(a, \mathrm{s}\, n) = h(a,n) = (h \circ \ell)((a,n), f(a,n)) : (A \times \mathbb{N}) \to B$$

Infinite-hotel interpretation:

Replace within the latter coproduct diagram object B by $A \times \mathbb{N}$, component map g by $(a_0, 0) : A \to A \times \mathbb{N}$ and $h = \mathrm{id}_{A \times \mathbb{N}}$, and get special "hotel" coproduct diagram



Hotel $\mathbb{N}$ has an infinite number $n \in \mathbb{N}$ of rooms. Each room n is occupied by a guest $(a, n) \in A \times \mathbb{N}$.

A new guest $a_0 \in A$ arrives at that fully occupied hotel. Since the hotel is infinite, the manager has (at least) 2 possibilies to host all present guests *and* the new one:

- the *actual*-infiniteness possibility: per simultaneous message he asks all present guests to change to respective next room:

$(a, n) \mapsto (a, n+1)$, and hosts simultaneously the new guest a_0 in room 0, $a_0 \mapsto (a_0, 0) \in A \times \mathbb{N}$.

- the *potential*-infiniteness possibility: The hotel has *potential* for an infinity of rooms (new rooms can be aquired in time or even constructed). All rooms the manager has at his disposal at present are occupied. A new guest arrives. The manager travels along all of these rooms and aquires at his disposal a next room. Then he travels backwards and asks subsequently the finitely many present guests to move "upwards", first the guest with highest room number, and eventually allocates room 0 to the arriving guest.

- the latter possibility is realised mathematically by interpretation of $A \times \mathbb{N}$ as the – (one-sided) potentially infinite – tape of a TURING machine, and the hotel manager as the (processing) head of a (very simple) such machine. A is the *tape alphabet* of the TURING machine. In computer science this simple TURING machine is – works as – a (potentially infinite) STACK.

3 Algebra and order on the NNO

In "Development of Mathematical Logic" (Logos Press 1971) R. L. Goodstein gives four basic uniqueness-rules for free-variable Arithmetics. We show here these rules for theory **PR** and that these four rules are sufficient for proving the commutative and associative laws for multiplication and the distributive law, for addition as well as for truncated subtraction $a \setminus n$.

For our *evaluation and consistency* considerations below we need from present section equality *predicate* $[a \doteq b] : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ and that this predicate **defines** map equality, see *equality definability scheme.* This scheme is a consequence of (Goodstein's) max commutativity which is difficult to show and which you may take on faith.

3.1 Free-variable NNO Algebra

Basic **GA**[12] operations are *addition* '$+$', *predecessor* 'pre', *truncated subtraction* '$\smallsetminus$' [in GOODSTEIN predecessor written $\mathrm{pre}\, n := n \dot{-} 1$], as well as *multiplication* '$\cdot$'.

We[13] include into Goodstein's uniqueness rules a "passive parameter" a. These extended rules are derivable by use of Freyd's uniqueness theorem (pr!), part of *full scheme* (pr) of primitive recursion which he deduces from his uniqueness (FR!) of the *initialised iterated.*

3.1.1 Goodstein's rules parametrised

Let $f, g : A \times \mathbb{N} \to \mathbb{N}$ be maps, $\mathrm{s} : \mathbb{N} \to \mathbb{N}$ the successor map $n \mapsto n+1$ and $\mathrm{pre} : \mathbb{N} \to \mathbb{N}$ the predecessor map, here usually written as $n \mapsto n \smallsetminus 1$.

Then Goodstein's rules read:

[12]Goodstein Arithmetic

[13]Sandra Andrasek and the author

$$\mathrm{U}_1 \quad \frac{f(a, sn) = f(a, n) : A \times \mathbb{N} \to B}{f(a, n) = f(a, 0) : A \times \mathbb{N} \to B}$$

no change by application of successor

infers equality *with value at zero* for f

$$\mathrm{U}_2 \quad \frac{f(a, \mathrm{s}\, n) = \mathrm{s}\, f(a, n) : A \times \mathbb{N} \to \mathbb{N}}{f(a, n) = f(a, 0) + n : A \times \mathbb{N} \to \mathbb{N}}$$

accumulation of successors into $+n$

$$\mathrm{U}_3 \quad \frac{f(a, sn) = \mathrm{pre}\ f(a, n) : A \times \mathbb{N} \to \mathbb{N}}{f(a, n) = f(a, 0) \smallsetminus n : A \times \mathbb{N} \to \mathbb{N}}$$

accumulation of predecessors into $\smallsetminus n$

$$\mathrm{U}_4 \quad \frac{\begin{array}{l} f(a, 0) = g(a, 0) : A \to \mathbb{N} \\ f(a, sn) = g(a, sn) : A \times \mathbb{N} \to \mathbb{N} \end{array}}{f(a, n) = g(a, n) : A \times \mathbb{N} \to \mathbb{N}}$$

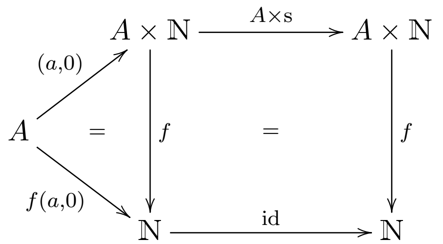
uniqueness of map definition by case-distinction

Rule U_4 is nothing else than *uniqueness* of the *induced map out of the sum* $A \times \mathbb{N} \cong (A \times \mathbb{1}) + (A \times \mathbb{N})$, this sum canonically realised via *injections* $\iota = (\mathrm{id}_A, 0) : A \to A \times \mathbb{N}$ as well as – right injection – $\kappa = \mathrm{id}_A \times \mathrm{s} : A \times \mathbb{N} \to A \times \mathbb{N}$.

Proof of these four rules is straight forward for theory **PR**

using Freyd's uniqueness (FR!) and uniqueness clause (pr!) of the *full scheme of primitive recursion* respectively, as follows:

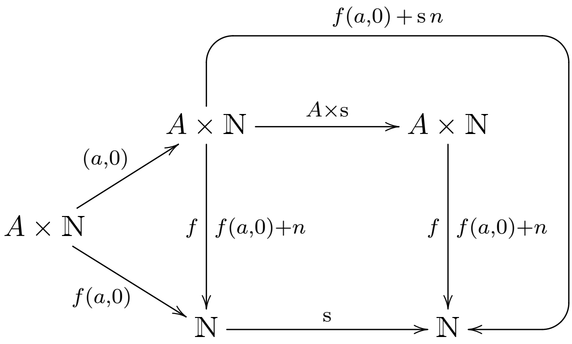
For scheme U_1 consider, with free variable $a := \ell : A \times \mathbb{N} \to A$,



(FR!)

$$f(a,n) = f = \mathrm{id}_{\mathbb{N}}^{\S} \circ (f(a,0) \times \mathbb{N})$$
$$= \ell_{\mathbb{N},\mathbb{N}} \circ (f(a,0) \times \mathbb{N}) : A \times \mathbb{N} \to \mathbb{N} \times \mathbb{N} \to \mathbb{N}$$
$$= f(a,0) \circ \ell_{A,\mathbb{N}} : A \times \mathbb{N} \to A \to \mathbb{N}$$
$$= f(a,0) : A \times \mathbb{N} \xrightarrow{A \times \Pi_{\mathbb{N}}} A \times \mathbb{1} \xrightarrow{A \times 0} A \times \mathbb{N} \xrightarrow{f} \mathbb{N}$$

Proof of U_2 of *"summing up successors":*



pentagon commutative for both $f,\ f(a,0) + n$

(FR!) ———

$$f(a,n) = f(a,0) + n$$

Proof of U_3 is exactly analogous to the above: Replace in statement of U_2 and its proof *stepwise augmentation* $f(a, sn) = \mathrm{s}\, f(a, n)$ by *stepwise descent*

$$f(a, \mathrm{s}\, n) = f(a, n) \smallsetminus 1 \ =_{\text{by def}} \ \mathrm{pre}\ f(a, n)$$

On right hand side replace *successor* $\mathrm{s} : \mathbb{N} \to \mathbb{N}$ by *predecessor* $\mathrm{pre} : \mathbb{N} \to \mathbb{N}$ which in turn is defined by the full scheme (pr) of primitive recursion. In *postcedent* replace *iterated successor* $a + n : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ by *iterated predecessor* $a \smallsetminus n : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$.

[In GOODSTEIN's *original,* $\mathrm{pre}(n) = n \smallsetminus 1 : \mathbb{N} \to \mathbb{N}$ is a *basic,* "undefined" map constant]

We give a **direct proof** of U_4 :

We tailor first this scheme for convenient use of "full" uniqueness scheme (pr!) as follows:

$$U_4 \quad \frac{\begin{array}{l} f = f(a, n),\ f' = f'(a, n) : A \times \mathbb{N} \to B \\ f(a, 0) = f'(a, 0) : A \to B \\ f(a, \mathrm{s}\, n) = f'(a, \mathrm{s}\, n) : A \times \mathbb{N} \to A \times \mathbb{N} \to B \end{array}}{f = f' : A \times \mathbb{N} \to B.}$$

Choose the *anchor map*

$$g = g(a) := f(a, 0) = f'(a, 0) : \\ A \to A \times \mathbb{N} \to B$$

and the *step map*

$$h = h((a, n), b) := f(a, \mathrm{s}\, n) = f'(a, \mathrm{s}\, n) : \\ (A \times \mathbb{N}) \times B \xrightarrow{\ell} A \times \mathbb{N} \to B$$

We obtain via the *full* scheme (pr!) of primitive recursion:

$$\text{(pr!)}\quad \frac{\begin{array}{l} f(a,0) = g(a) = f'(a,0) \quad \text{(anchor hypothesis)} \\ f(a,\mathrm{s}\,n) = h((a,n), f(a,n)) = f'(a,\mathrm{s}\,n) \ \text{(step hypothesis)} \end{array}}{f = \mathrm{pr}[\,g,h] = f' : A \times \mathbb{N} \to B \quad \textbf{q. e. d.}}$$

Combination of *reflexivity, symmetry,* and *transitivity* of *equality* $f = g : A \to B$ between maps with the defining *equations* for the fundamental *operations* and with *rules* U_1 to U_4 above, **defines** categorical Goodstein's **free-variables Arithmetic** which we name **Goodstein Arithmetic GA**.

3.1.2 Arithmetical equations

We **quote** here – with *passive parameters* made visible – GOODSTEIN's arithmetical equations together with his **proofs.**

The first equation is (Goodstein's statement numbers)

Lemma:

$$(a \setminus n) \setminus 1 =^{\mathbf{GA}} (a \setminus 1) \setminus n : \mathbb{N} \times \mathbb{N} \to \mathbb{N} \qquad (1.)$$

$a \in \mathbb{N}$ free, "passive" $a := \ell : A \times \mathbb{N} \to A$

$n \in \mathbb{N}$ free, *recursive,* $n := \mathrm{r} : A \times \mathbb{N} \to \mathbb{N}$

Proof:

$$\mathrm{U}_3\quad \frac{(a \setminus \mathrm{s}\,n) \setminus 1 \ =_{\text{by def}} \ ((a \setminus n) \setminus 1) \setminus 1}{\begin{array}{l} (a \setminus n) \setminus 1 = ((a \setminus 0) \setminus 1) \setminus n \\ \qquad =_{\text{by def}} \ (a \setminus 1) \setminus n : \mathbb{N} \times \mathbb{N} \to \mathbb{N} \quad \textbf{q. e. d.} \end{array}}$$

Next equation is

stepwise simplification rule for truncated subtraction:

$$\mathrm{s}\, a \setminus \mathrm{s}\, b = a \setminus b : \mathbb{N} \times \mathbb{N} \to \mathbb{N} \qquad (1.1)$$

Proof:

$$\mathrm{U}_3 \quad \frac{\mathrm{s}\, a \setminus \mathrm{s}\, \mathrm{s}\, b \;=_{\text{by def}}\; (\mathrm{s}\, a \setminus \mathrm{s}\, b) \setminus 1}{\mathrm{s}\, a \setminus \mathrm{s}\, b = (\mathrm{s}\, a \setminus \mathrm{s}\, 0) \setminus b}$$

$$=_{\text{by def}}\; a \setminus b : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$$

the latter by definition of the *predecessor* "$\setminus 1$" **q. e. d.**

Lemma: $a \setminus a = 0 : \mathbb{N} \to \mathbb{N}$ (1.2)

Proof:

$$\mathrm{U}_1 \quad \frac{\mathrm{s}\, a \setminus \mathrm{s}\, a = a \setminus a \quad \text{(by stepwise simplification 1.1 above)}}{a \setminus a = 0 \setminus 0 \;=_{\text{by def}}\; 0}$$

q. e. d.

Lemma: $0 \setminus a = 0 : \mathbb{N} \to \mathbb{N}$ (1.3)

Proof:

$$0 \setminus \mathrm{s}\, a \;=_{\text{by def}}\; (0 \setminus a) \setminus 1$$

$$= (0 \setminus 1) \setminus a \quad \text{(by (1.) above)}$$

$$\mathrm{U}_1 \quad \frac{= 0 \setminus a : \mathbb{N} \to \mathbb{N}}{0 \setminus a = 0 \setminus 0 = 0 : \mathbb{N} \to \mathbb{N}}$$

q. e. d.

Proposition:

$$a \smallsetminus (b + c) = (a \smallsetminus b) \smallsetminus c : (\mathbb{N} \times \mathbb{N}) \times \mathbb{N} \to \mathbb{N} \quad (1.31)$$

Proof:

$$a \smallsetminus (b + \mathrm{s}\, c) \;=_{\text{by def}}\; a \smallsetminus \mathrm{s}\,(b + c) \quad \text{(definition of +)}$$

$$=_{\text{by def}}\; (a \smallsetminus (b + c)) \smallsetminus 1 \quad \text{(definition of } \smallsetminus \text{)}$$

$$\mathrm{U}_3 \; \overline{\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad}$$

$$a \smallsetminus (b + c) = (a \smallsetminus (b + 0)) \smallsetminus c \;=_{\text{by def}}\; (a \smallsetminus b) \smallsetminus c$$

q. e. d.

Full Simplification:

$$(a + n) \smallsetminus (b + n) = a \smallsetminus b : \mathbb{N}^2 \times \mathbb{N} \to \mathbb{N} \qquad (1.4)$$

Proof:

$$(a + \mathrm{s}\, n) \smallsetminus (b + \mathrm{s}\, n)$$

$$=_{\text{by def}}\; \mathrm{s}\,(a + n) \smallsetminus \mathrm{s}\,(b + n) = (a + n) \smallsetminus (b + n)$$

by *substitution* – realised essentially as composition – of $(a + n)$ into a and $(a + n)$ into b within *stepwise simplification equation* 1.1 above

$$\mathrm{U}_1 \; \overline{\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad}$$

$$(a + n) \smallsetminus (b + n) = (a + 0) \smallsetminus (b + 0) \;=_{\text{by def}}\; a \smallsetminus b.$$

Lemma: $0 + n = n \; [\, =_{\text{by def}} \; n + 0 \,] \; : \mathbb{N} \to \mathbb{N} \quad (2)$

Proof:

$$\mathrm{U}_2 \quad \frac{\mathrm{id}_{\mathbb{N}}\, \mathrm{s}\, a = \mathrm{s}\, a}{\mathrm{id}_{\mathbb{N}}(a) = \mathrm{id}_{\mathbb{N}}(0) + a}$$

and hence

$$a = \mathrm{id}_{\mathbb{N}}(a) = \mathrm{id}_{\mathbb{N}}(0) + a = 0 + a : \mathbb{N} \to \mathbb{N} \quad \textbf{q. e. d.}$$

Lemma: $a + \mathrm{s}\, b = \mathrm{s}\, a + b : \mathbb{N} \times \mathbb{N} \to B$ (2.1)

Proof by U_2 as follows, with free variable $b := \mathrm{r} : \mathbb{N}^2 \to \mathbb{N}$ as *recursion variable:*

For $f = f(a, b) \ =_{\mathrm{def}} \ a + \mathrm{s}\, b : \mathbb{N} \times \mathbb{N} \to N$:

$$U_2 \quad \frac{f(a, \mathrm{s}\, b) \ =_{\mathrm{by\,def}} \ a + \mathrm{s}\,\mathrm{s}\, b = \mathrm{s}(a + \mathrm{s}\, b) = \mathrm{s}\, f(a, b) : \mathbb{N}^2 \to \mathbb{N}}{f(a, b) = a + \mathrm{s}\, b = f(a, 0) + b}$$

$$=_{\mathrm{by\,def}} \ (a + \mathrm{s}\, 0) + b \ =_{\mathrm{by\,def}} \ \mathrm{s}\, a + b \quad \textbf{q. e. d.}$$

Theorem:

$$a + b = b + a : \mathbb{N} \times \mathbb{N} \to \mathbb{N} \qquad (2.2)$$
$$a := \ell : \mathbb{N}^2 \to \mathbb{N}$$
$$b := \mathrm{r} : \mathbb{N}^2 \to \mathbb{N}$$

Proof:

$$\frac{\begin{array}{l} a+0 \;=_{\text{by def}}\; a = 0 + a \text{ by (2) above} \\ a + \mathrm{s}\, b = \mathrm{s}\, a + b \text{ by (2.1) above (and symmetry of equality)} \end{array}}{\begin{array}{l} a+b \;=_{\text{by def}}\; f(a,b) = g(a,b) \\ =_{\text{by def}}\; \mathrm{s}\, a + b : \mathbb{N}^2 \to \mathbb{N} \end{array}} \; U_4$$

q. e. d.

This gives also sort of *permutability* for truncated subtraction:

$$(a \smallsetminus b) \smallsetminus c = (a \smallsetminus c) \smallsetminus b : (\mathbb{N} \times \mathbb{N}) \times \mathbb{N} \to \mathbb{N}$$

Proof:

$(a \smallsetminus b) \smallsetminus c = a \smallsetminus (b + c)$ by (1.31) above

$= a \smallsetminus (c + b)$ by commutativity of addition

$= (a \smallsetminus c) \smallsetminus b$ again by (1.31) **q. e. d.**

From *full simplification* (1.4) and *left neutrality* of zero (2) above with respect to addition we get immediately *"one-term" simplification*

Lemma:

$$(a + n) \smallsetminus n = (a + n) \smallsetminus (0 + n) = a : \mathbb{N} \times \mathbb{N} \to \mathbb{N} \quad (2.3)$$

Associativity of Addition

$$(a + b) + c = a + (b + c) : (\mathbb{N} \times \mathbb{N}) \times \mathbb{N} \to \mathbb{N}$$

Proof: for $f((a,b),c) \;=_{\text{def}}\; a + (b + c) : \mathbb{N}^2 \times \mathbb{N} :$

$$f((a,b),\mathrm{s}\,c) = a + (b + \mathrm{s}\,c) = a + \mathrm{s}(b+c)$$

$$= \mathrm{s}(a + (b+c)) = \mathrm{s}\,f((a,b),c)$$

$$U_2 \quad \overline{}$$

$$a + (b+c) = f((a,b),c) = f((a,b),0) + c$$

$$=_{\text{by def}} \ (a + (b+0)) + c = (a+b) + c$$

q. e. d.

Recall p. r. **Definition** of *Multiplication:*

$$a \cdot 0 = 0 : \mathbb{N} \to \mathbb{N}$$
$$a \cdot (n+1) = (a \cdot n) + a$$

For this operation we have not only *annihilation by zero from the right* but also

Left zero-Annihilation $0 \cdot n = 0 : \mathbb{N} \to \mathbb{N}$.

Proof:

$$U_1 \quad \frac{0 \cdot \mathrm{s}\,n = (0 \cdot n) + 0 = 0 \cdot n}{0 \cdot n = 0 \cdot 0 = 0}$$

q. e. d.

For proving the other equational laws making the natural numbers object $\mathbb{N}$ into a *unitary commutative semiring* with in addition truncated subtraction introduced above Goodstein's derived scheme V_4 below is helpfull.

For proof of that scheme we rely on

Commutativity of maximum operation:[14]

$$\max(a,b) \ =_{\text{def}} \ a + (b \searrow a)$$
$$= b + (a \searrow b) \ =_{\text{by def}} \ \max(b,a) : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$$

Proof[15]: As a first step we show

Diagonal Reduction Lemma for maximum:

$$\max(a,b) = \max(a \searrow 1, b \searrow 1) + \text{sgn}(a+b)$$

Proof of Lemma: first we show **equation**

$$\max(a, \text{s}\, b) = \max(a \searrow 1, \text{s}\, b \searrow 1) + \text{sgn}(a + \text{s}\, b) \qquad (1)$$

[where $\text{sgn}(0) = 0, \ \text{sgn}(\text{s}\, n) = 1$] as follows:

$$\max(0 \searrow 1, \text{s}\, b) = \text{s}\, b$$
$$= \max(0 \searrow 1, s\, b \searrow 1) + \text{sgn}(0 + s\, b) \qquad (2)$$

and

$$\max(\text{s}\, a, \text{s}\, b) = \text{s}\, a + (\text{s}\, b \searrow \text{s}\, a)$$
$$= \text{s}\, a + (b \searrow a) = \text{s}(a + (b \searrow a))$$
$$= \text{s} \max(a,b) = \max(a,b) + 1$$
$$= \max(\text{s}\, a \searrow 1, \text{s}\, b \searrow 1) + \text{sgn}(\text{s}\, a + \text{s}\, b) \qquad (3)$$

From (2) and (3) **follows equation** (1) by uniqueness rule U_4.

Furthermore

$$\max(a, 0) = a = (a \searrow 1) + \text{sgn}(a)$$
$$= \max(a \searrow 1, 0 \searrow 1) + \text{sgn}(a + 0) \qquad (4)$$

---

[14] in GOODSTEIN 1964 this is taken as an axiom

[15] Goodstein 1971 adapted by G. Myrach

Together with (1) above this gives again by U_4 the **Diagonal Reduction Lemma.**

From this we get immediately by substitution

Opposite Diagonal Reduction Lemma for maximum:

$$\max(b, a) = \max(b \smallsetminus 1, a \smallsetminus 1) + \mathrm{sgn}(b + a)$$
$$= \max(b \smallsetminus 1, a \smallsetminus 1) + \mathrm{sgn}(a + b) \quad \textbf{q. e. d.}$$

Let *increment* map

$$\phi = \phi(n, (a, b)) : \mathbb{N} \times (\mathbb{N} \times \mathbb{N}) \to \mathbb{N} \text{ be defined by}$$
$$\phi(0, (a, b)) = 0 : \mathbb{N} \times \mathbb{N} \to \mathbb{N} \text{ and}$$
$$\phi(\mathrm{s}\, n, (a, b)) = \phi(n, (a, b)) + \mathrm{sgn}((a \smallsetminus n) + (b \smallsetminus n)) :$$
$$\mathbb{N} \times (\mathbb{N} \times \mathbb{N}) \to \mathbb{N}$$

We show for this ϕ

$$\max(a \smallsetminus n, b \smallsetminus n) + \phi(n, (a, b))$$
$$= \max(a \smallsetminus \mathrm{s}\, n, b \smallsetminus \mathrm{s}\, n) + \phi(\mathrm{s}\, n, (a, b)) \qquad (5)$$

as well as

$$\max(b \smallsetminus n, a \smallsetminus n) + \phi(n, (a, b))$$
$$= \max(b \smallsetminus \mathrm{s}\, n, a \smallsetminus \mathrm{s}\, n) + \phi(\mathrm{s}\, n, (a, b)) \qquad (6)$$

(same increment)

First we show equation (5): Substitution of $(a \smallsetminus n)$ for a and $(b \smallsetminus n)$ for b within **Reduction Lemma** above gives

$$\max(a \smallsetminus n, b \smallsetminus n)$$
$$= \max((a \smallsetminus n) \smallsetminus 1, (b \smallsetminus n) \smallsetminus 1) + \mathrm{sgn}((a \smallsetminus n) + (b \smallsetminus n))$$

Adding $\phi(n,(a,b))$ to both sides of this equation gives

$$\begin{aligned}
&\max(a \diagdown n, b \diagdown n) + \phi(n,(a+b)) \\
&= \max((a \diagdown n) \diagdown 1, (b \diagdown n) \diagdown 1) \\
&\quad + \operatorname{sgn}((a \diagdown n) + (b \diagdown n)) + \phi(n,(a+b)) \\
&=_{\text{by def}} \max(a \diagdown \mathrm{s}\, n, b \diagdown \mathrm{s}\, n) + \phi(\mathrm{s}\, n,(a,b)) \\
&\text{i. e. equation (5)}
\end{aligned}$$

We show equation (6): By substitution of $(b \diagdown n)$ for b and $(a \diagdown n)$ for a in **Opposite Reduction Lemma** and addition of $\phi(n,(a,b))$ on both sides we get

$$\begin{aligned}
&\max(b \diagdown n, a \diagdown n) + \phi(n,(a,b)) \\
&= \max((b \diagdown n) \diagdown 1, (a \diagdown n) \diagdown 1) \\
&\quad + \operatorname{sgn}((b \diagdown n) + (a \diagdown n)) + \phi(n,(a,b)) \\
&= \max((b \diagdown n) \diagdown 1, (a \diagdown n) \diagdown 1) \\
&\quad + \operatorname{sgn}((a \diagdown n) + (b \diagdown n)) + \phi(n,(a,b)) \\
&=_{\text{by def}} \max((b \diagdown n) \diagdown 1, (a \diagdown n) \diagdown 1) + \phi(\mathrm{s}\, n,(a,b)) \\
&= \max(b \diagdown \mathrm{s}\, n, a \diagdown \mathrm{s}\, n) + \phi(\mathrm{s}\, n,(a,b)) \\
&\text{i. e. equation (6)}
\end{aligned}$$

From the two Lemmata we get by uniqueness U_1

$$\begin{aligned}
&\max(a \diagdown n, b \diagdown n) + \phi(n,(a,b)) \\
&= \max(a \diagdown 0, b \diagdown 0) + \phi(0,(a,b)) = \max(a,b) + 0 = \max(a,b) \\
&\quad \text{as well as} \\
&\max(b \diagdown n, a \diagdown n) + \phi(n,(a,b)) \\
&= \max(b \diagdown 0, a \diagdown 0) + \phi(0,(a,b)) = \max(b,a) + 0 = \max(b,a)
\end{aligned}$$

and hence

$$\max(a, b) = \max(a \smallsetminus n, b \smallsetminus n) + \phi(n, (a, b)) \text{ as well as}$$
$$\max(b, a) = \max(b \smallsetminus n, a \smallsetminus n) + \phi(n, (a, b))$$

and so, by substitution of b into n :

$$\max(a, b) = \max(a \smallsetminus b, b \smallsetminus b) + \phi(b, a, b)$$
$$= (a \smallsetminus b) + \phi(b, (a, b))$$
$$= \max(b \smallsetminus b, a \smallsetminus b) + \phi(b, (a, b))$$
$$= \max(b, a) : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$$

q. e. d. max commutativity.

This given we **show** for **GA** (and hence for **PR**) scheme

$$\mathrm{V}_4 \quad \frac{\begin{array}{l} f,\ g,\ h : A \times \mathbb{N} \to \mathbb{N} \\ f(a, 0) = g(a, 0) : A \to \mathbb{N} \\ f(a, sn) = f(a, n) + h(a, n) : A \times \mathbb{N} \to \mathbb{N} \\ g(a, sn) = g(a, n) + h(a, n) : A \times \mathbb{N} \to \mathbb{N} \end{array}}{f(a, n) = g(a, n).}$$

Rule V_4 can be derived by applying rule U_1 to the distance map

$$d(a, n) = |f(a, n), g(a, n)| = |f(a, n) - g(a, n)|$$
$$=_{\text{by def}} \ (f(a, n) \smallsetminus g(a, n)) + (g(a, n) \smallsetminus f(a, n)) :$$
$$A \times \mathbb{N} \to \mathbb{N}^2 \xrightarrow{+} \mathbb{N}$$

$$
\begin{aligned}
d(a,0) &= (f(a,0) \dot{-} g(a,0)) + (g(a,0) \dot{-} f(a,0)) = 0 \\
d(a,sn) &= (f(a,sn) \dot{-} g(a,sn)) + (g(a,sn) \dot{-} f(a,sn)) \\
&= (f(a,n) + h(a,n)) \dot{-} (g(a,n) + h(a,n)) \\
&\quad + (g(a,n) + h(a,n)) \dot{-} (f(a,n) + h(a,n)) \\
&= (f(a,n) \dot{-} g(a,n)) + (g(a,n) \dot{-} f(a,n)) \\
&= d(a,n) : A \times \mathbb{N} \to \mathbb{N}
\end{aligned}
$$

whence by U_1:

$$
\begin{aligned}
&d(a,n) = d(a,0) = 0 \text{ i. e.} \\
&(f(a,n) \dot{-} g(a,n)) + (g(a,n) \dot{-} f(a,n)) = 0 \text{ whence} \\
&f(a,n) \dot{-} g(a,n) = 0 = g(a,n) \dot{-} f(a,n) : A \times \mathbb{N} \to \mathbb{N}
\end{aligned}
$$

and hence

$$
\begin{aligned}
f(a,n) &= f(a,n) + (g(a,n) \dot{-} f(a,n)) \\
&= \max(f(a,n), g(a,n)) \\
&= \max(g(a,n), f(a,n)) \\
&= g(a,n) + (f(a,n) \dot{-} g(a,n)) \\
&= g(a,n) \quad \textbf{q. e. d.}
\end{aligned}
$$

3.2 Equality definability

Individual equality is **defined** as equality *predicate*

$$[m \doteq n] : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$$

via weak order as follows:

$[m \leq n] \ =_{\mathrm{def}} \ \neg\,[m \smallsetminus n] : \mathbb{N}^2 \to \mathbb{N} \to \mathbb{N}$ where

protoboolean operation negation given as

$\neg\, n \ =_{\mathrm{def}} \ 1 \smallsetminus n$ directly p. r. defined by

$\neg\, 0 \ =_{\mathrm{def}} \ 1 = \mathrm{s}\,0 : \mathbb{1} \to \mathbb{N}$

$\neg\, \mathrm{s}\, n \ =_{\mathrm{def}} \ 0 : \mathbb{1} \to \mathbb{N}$

This order on $\mathbb{N}$ is *reflexive* and *transitive.*

Individual equality – first on $\mathbb{N}$ – then is easily **defined** by

$$[m \doteq n] \ =_{\mathrm{def}} \ [m \leq n \ \wedge \ n \leq m]$$
$$=_{\mathrm{by\,def}} \ [m \leq n] \cdot [n \leq m] : \mathbb{N}^2 \to \mathbb{N}$$

[It is a *protopredicate.*]

We now have at our disposition all ingredients for

Equality definability theorem

$$f = f(a) : A \to B, \ g = g(a) : A \to B \text{ in } \mathbf{PR}$$

$$\text{(EqDef)} \quad \frac{\mathbf{PR} \vdash \mathrm{true}_A \ =_{\mathrm{by\,def}} \ 1 \circ \Pi_A = [f(a) \doteq_B g(a)] : \ A \xrightarrow{\Delta} A \times A \xrightarrow{f \times g} B \times B \xrightarrow{\doteq_B} \mathbb{N}}{\mathbf{PR} \vdash f = g : A \to B \ \text{ i.e. } \ f =^{\mathbf{PR}} g : A \to B}$$

A map equation which holds true predicatively for "all" arguments individually gives rise to an argument-free *categorical equation* ***between*** *the maps concerned.*

Proof: We begin with the special case $B = \mathbb{N}$: Let $f,\ g : A \to \mathbb{N}$ **PR** maps satisfying the *antecedent* of (EqDef). Then

$$\begin{aligned}\mathbf{PR} \vdash f(a) &= f(a) + 0 = f(a) + (g(a) \setminus f(a)) \text{ by antecedent} \\ &= \max(f(a), g(a)) \text{ by definition of } \max(m, n) \\ &= \max(g(a), f(a)) \text{ by } \max \text{ commutativity} \\ &= g(a) + (f(a) \setminus g(a)) \\ &= g(a) + 0 = g(a) : A \to B\end{aligned}$$

The general case for codomain object B follows since *individual equality* on (binary) cartesian products is canonically defined *componentwise* and B is a cartesian product of $\mathbb{N}$'s **q. e. d.**

Equality convention

Motivated by **equality definability** just proved, we write from now on $f(a) = g(a)$ or $[f(a) = g(a)]$ or $[f = g]$ instead of $f(a) \doteq g(a)$.

These *fundamentals* given we continue with properties of the algebraic structure on $\mathbb{N}$.

3.3 Further Algebra on the NNO

Theorem: In free–variables arithmetics the *commutative law* for *multiplication:* $n \cdot m = m \cdot n$ holds.

Proof: We need the following

Lemma:

(i) $0 \cdot n = 0$

(ii) $sa \cdot n = a \cdot n + n$

Proof:

(i) $0 \cdot 0 = 0$ and
$0 \cdot sn = 0 \cdot (n+1) = 0 \cdot n + 0 = 0 \cdot n = 0 \cdot 0 = 0.$

(ii) We show $f(a,n) := sa \cdot n = g(a,n) := a \cdot n + n$ using V_4:
$f(a,0) = g(a,0)$ because for $n = 0$ we get $(sa) \cdot 0 = 0$ as well as $a \cdot 0 + 0 = a \cdot 0 = 0$.

$$\begin{aligned}
f(a,sn) &= (sa) \cdot (sn) = (a+1) \cdot (n+1) \\
&= (a+1) \cdot n + (a+1) = (sa) \cdot n + sa \\
&= f(a,n) + h(a,n) \qquad \text{with} \qquad h(a,n) := sa \\
g(a,sn) &= a \cdot (sn) + sn = a \cdot (n+1) + (n+1) \\
&= a \cdot n + a + n + 1 = a \cdot n + n + a + 1 \\
&= a \cdot n + n + sa \\
&= g(a,n) + h(a,n).
\end{aligned}$$

So V_4 gives $f(a,n) = g(a,n)$ i.e. $sa \cdot n = a \cdot n + n$.

q. e. d.

We continue with the proof of $a \cdot n = n \cdot a$:

From $a \cdot 0 = 0 = 0 \cdot a$ and $a \cdot sn = a \cdot n + n = sn \cdot a$ by the Lemma, we conclude $a \cdot n = n \cdot a$ by V_4.

q. e. d.

Theorem: In free–variable arithmetics multiplication distributes over addition: $a \cdot (m+n) = a \cdot m + a \cdot n$.

Proof: Case $n = 0$ is trivial by definition of $+$ and $\cdot$.

From the hypothesis $a \cdot (m+n) = a \cdot m + a \cdot n$ we infer the next step $a \cdot (m + sn) = a \cdot m + a \cdot sn$ by rule V_4 above – with passive parameter (a, m) – as follows:

$$\text{with} \quad f((a,m),n) := a \cdot (m+n)$$
$$g((a,m),n) := a \cdot m + a \cdot n \qquad \text{and}$$
$$h((a,m),n) := a$$

we have

$$\begin{aligned}
f((a,m),sn) &= a \cdot (m+sn) = a \cdot (m + (n+1)) \\
&= a \cdot ((m+n)+1) = a \cdot (m+n) + a \\
&= f((a,m),n) + h((a,m),n) \\
g((a,m),sn) &= a \cdot m + a \cdot sn = a \cdot m + a \cdot (n+1) \\
&= a \cdot m + a \cdot n + a \\
&= g((a,m),n) + h((a,m),n).
\end{aligned}$$

From this V_4 gives

$f((a,m),n) = g((a,m),n)$ i. e.

$a \cdot (m+n) = a \cdot m + a \cdot n$

q. e. d.

Theorem: In free–variable arithmetics the associative law holds:

$$a \cdot (m \cdot n) = (a \cdot m) \cdot n$$

Proof: We prove the law applying rule V_4 with "active" parameter n and passive parameter (a, m) to

$$f((a,m),n) := a \cdot (m \cdot n)$$
$$g((a,m),n) := (a \cdot m) \cdot n \quad \text{and}$$
$$h((a,m),n) := a \cdot m$$

For $n = 0$ we have: $a \cdot (m \cdot n) = a \cdot 0 = 0$ and on the other hand: $(a \cdot m) \cdot 0 = 0$.

For V_4–step we have:

$$\begin{aligned} f((a,m),sn) &= a \cdot (m \cdot sn) = a \cdot (m \cdot (n+1)) \\ &= a \cdot (m \cdot n + m) = a \cdot (m \cdot n) + a \cdot m \\ &= f((a,m),n) + h((a,m),n) \\ g((a,m),sn) &= (a \cdot m) \cdot (n+1) = (a \cdot m) \cdot n + a \cdot m \\ &= g((a,m),n) + h((a,m),n). \end{aligned}$$

By V_4 we get

$$f((a,m),n) = g((a,m),n) \text{ i. e.}$$
$$a \cdot (m \cdot n) = (a \cdot m) \cdot n$$

q. e. d.

Minus distributivity theorem: In free–variable arithmetics *multiplication distributes* over *truncated subtraction:*

$$a \cdot (m \setminus n) = a \cdot m \setminus a \cdot n$$

Proof by V_4 as follows.

$$f((a,m),n) := a \cdot (m \setminus n)$$
$$g((a,m),n) := a \cdot m \setminus a \cdot n$$

Anchoring

$$f((a,m),0) := a \cdot (m \smallsetminus 0) = a \cdot m$$
$$= a \cdot m \smallsetminus a \cdot 0 = g((a,m),0)$$

V_4 *progress* $h((a,m),n) := 0$

$$\mathrm{V}_4 \quad \frac{\begin{array}{l} f((a,m),0) = g((a,m),0) : A \times \mathbb{N} \to \mathbb{N} \\ f((a,m),sn) = f((a,m),n) + 0 : (A \times \mathbb{N}) \times \mathbb{N} \to \mathbb{N} \\ g((a,m),sn) = g((a,m),n) + 0 : (A \times \mathbb{N}) \times \mathbb{N} \to \mathbb{N} \end{array}}{f((a,m),n) = g((a,m),n) : (A \times \mathbb{N}) \times \mathbb{N} \to \mathbb{N}}$$

i. e. $a \cdot (m \smallsetminus n) = a \cdot m \smallsetminus a \cdot n$

$A \times (\mathbb{N} \times \mathbb{N}) \to \mathbb{N}$ **q. e. d.**

Proposition: Addition and multiplication in free-variable arithmetics are weakly monotonous i. e.

$$\begin{aligned} m \le n &\implies m \smallsetminus n = 0 \\ &\implies (a+m) \smallsetminus (a+n) = 0 \text{ by absorption law for } \smallsetminus \\ &\implies a+m \ \le \ a+n \\ m \le n &\implies m \smallsetminus n = 0 \\ &\implies (a \cdot m) \smallsetminus (a \cdot n) = a \cdot (m \smallsetminus n) = 0 \\ &\implies a \cdot m \ \le \ a \cdot n \end{aligned}$$

where *protoboolean* ***implication*** is defined as the p. r. predicate

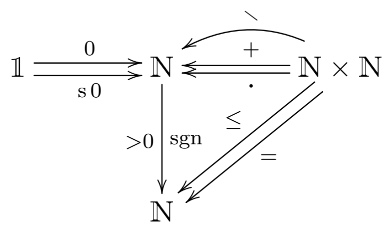
$$[a \implies b] \ =_{\mathrm{def}} \ [a \le b] : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$$

cf. section on *arithmetical logic* below **q. e. d.**

Putting things together, we obtain

3.4 Structure theorem for the NNO

- $\mathbb{N}$ admits the structure



  of a *unitary commutative semiring with zero,* combined with

- a foundational important additional algebraic structure namely *truncated subtraction* $m \smallsetminus n : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ with its *simplification properties,* and such that multiplication *distributes* over this kind of subtraction;

- linear *order* $[m \leq n] : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ as a reflexive and transitive *predicate* – this order is p. r. *decidable;*

- $\max(a, b) \ =_{\text{def}} \ a + (b \smallsetminus a) = b + (a \smallsetminus b) = \max(b, a) : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ is in fact the *maximum* with respect to the order

  $[a \leq b] : \mathbb{N} \times \mathbb{N} \to \mathbb{N}.$

  Furthermore we have

- fundamental equality *predicate*

$$[m = n] \ =_{\text{by def}} \ [m \leq n] \wedge [m \geq n] : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$$

  which is an *equivalence predicate,* and which makes up a *trichotomy* with strict order

$$[m < n] \ =_{\text{def}} \ \operatorname{sgn}(n \smallsetminus m)$$
$$= [m \leq n] \wedge \neg[m = n] : \mathbb{N}^2 \to \mathbb{N}$$

Proof of the latter assertion as **exercise.**

- **Algebra Combined with Order:** As expected, addition is strongly monotonic in both arguments, multiplication is strongly monotonic for both arguments strictly greater than zero, and truncated subtraction is weakly monotonic in its first argument and weakly antitonic in its second.

  Proofs as **exercises.**

3.5 Exponentiation and faculty

- **exponentiation**

  NNO exponentiation $\exp(a, n) = a^n : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ is **defined** (iteratively) p. r. as follows:

$$a^0 = \exp(a, 0) = 1 : A = \mathbb{N} \xrightarrow{\Pi} \mathbb{1} \xrightarrow{0} \mathbb{N} = B$$

$$a^{\mathrm{s}\,n} = a^n \cdot a = \exp(a, n) \cdot a :$$

$$(A \times \mathbb{N}) \times B = (\mathbb{N} \times \mathbb{N}) \times \mathbb{N} \xrightarrow{\exp \times \ell\,\ell} \mathbb{N} \times \mathbb{N} \xrightarrow{\cdot} \mathbb{N} = B$$

- **super exponentiation**

  super exponentiation $\mathrm{sexp}(a, n) = a^{\uparrow n} : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ is **defined** iteratively p. r. as follows:

$$a^{\uparrow 0} = \mathrm{sexp}(a, 0) = a^0 = 1 : A = \mathbb{N} \xrightarrow{\Pi} \mathbb{1} \xrightarrow{0} \mathbb{N} = B$$

$$a^{\uparrow \mathrm{s}\,n} = a^{a \uparrow n} = a^{(a \uparrow n)} = \exp(a, \mathrm{sexp(a, n)}) :$$

$$(A \times \mathbb{N}) \times B$$

$$= (\mathbb{N} \times \mathbb{N}) \times \mathbb{N} \xrightarrow{\ell} \mathbb{N} \times \mathbb{N} \xrightarrow{(\ell, \mathrm{sexp})} \mathbb{N} \times \mathbb{N} \xrightarrow{\exp} \mathbb{N} = B$$

- **faculty** $\mathrm{fac} = \mathrm{fac}(n) : \mathbb{N} \to \mathbb{N}$ is **defined** by full schema as follows:

$$0! = \mathrm{fac}(0) = 1 : A = N \xrightarrow{\Pi} \mathbb{1} \xrightarrow{1} \mathbb{N} = B$$

$$(n+1)! = \mathrm{fac}(\mathrm{s}\, n) = n! \cdot (n+1) = h((a,n), \mathrm{fac}(a,n)) :$$

$$(A \times \mathbb{N}) \times B \to B \text{ with}$$

$$h = h((a,n), b) = (n+1) \cdot b :$$

$$(\mathbb{N} \times \mathbb{N}) \times \mathbb{N} \xrightarrow{(\mathrm{s\,r}) \times \mathbb{N}} \mathbb{N} \times \mathbb{N} \xrightarrow{\cdot} \mathbb{N}$$

We have here an example where step function of full schema depends not only from previous value b but also from *recursion parameter* n [16]

- **Binomial coefficients**

$$\text{(choose)} \quad \frac{\begin{array}{l} g(n) = 1\, \Pi_{\mathbb{N}}(n) : \mathbb{N} \to \mathbb{1} \to \mathbb{Q} \\ h = h((n,k), b) = b \cdot \frac{n-k}{1+k} : (\mathbb{N} \times \mathbb{N}) \times \mathbb{Q} \to \mathbb{Q} \quad \text{(step)} \end{array}}{\begin{array}{l} \texttt{function } \binom{n}{k} = \mathrm{pr}[g,h](n,k) : (\mathbb{N} \times \mathbb{N}) \to \mathbb{Q}, \\ \binom{n}{0} = 1 : \mathbb{N} \to \mathbb{Q} \quad \text{(init)} \\ \binom{n}{k+1} = \binom{n}{k} \cdot \frac{n-k}{1+k} : \mathbb{N} \times \mathbb{N} \to \mathbb{Q} \end{array}}$$

This is an example again where the recursion step depends not only on the actual value of the recursive function to be constructed, but also from the actual value of the *recursion parameter,* here $k \in \mathbb{N}$.

[16] an example asked for by K. Polthier

Exercise

- **show** $\binom{m}{n} \in \mathbb{N}$
- **show** $\binom{m}{n} = \frac{n!}{k!(n-k!)}$
- **show** the **bimomial theorem**

  $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k : (\mathbb{N} \times \mathbb{N}) \times \mathbb{N} \to \mathbb{N}$

Outlook

In part B to come we treat embedding extension of theory **PR** by *predicate abstraction* and partial maps, as well as by truth object $\mathbf{2} = \{\text{false}, \text{true}\}$. Within that theory we discuss different types of general recursion, cf. Church's thesis.

References

[1] S. Eilenberg, C. C. Elgot 1970: *Recursiveness.* Academic Press.

[2] P. J. Freyd 1972: Aspects of Topoi. *Bull. Australian Math. Soc.* **7,** 1-76.

[3] K. Gödel 1931: Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I. *Monatsh. der Mathematik und Physik* **38,** 173-198.

[4] R. Goldblatt 1979: *Topoi. The Categorical Analysis of Logic.* Studies in Logic and the Foundations of Mathematics. North-Holland.

[5] R. L. Goodstein 1971: *Development of Mathematical Logic,* ch. 7: Free-Variable Arithmetics. Logos Press.

[6] D. Hilbert 1970: Mathematische Probleme. Vortrag Paris 1900. *Gesammelte Abhandlungen.* Springer.

[7] A. Kock, G. E. Reyes 1977: Doctrines in Categorical Logic. Part A.8 in Barwise ed. 1977. *Handbook of Mathematical Logic.* North Holland.

[8] F. W. Lawvere 1964: An Elementary Theory of the category of Sets. *Proc. Nat. Acad. Sc. USA* **51,** 1506-1510.

[9] M. Pfender, M. Kröplin, D. Pape 1994: Primitive Recursion, Equality, and a Universal Set. *Math. Struct. in Comp. Sc.* **4,** 295-313.

[10] M. Pfender, R. Reiter, M. Sartorius 1982: Constructive Arithmetics. *Lecture Notes in Math.* **962,** 228-236.

[11] R. Reiter 1980: Mengentheoretische Konstruktionen in arithmetischen Universen. Diploma Thesis. Techn. Univ. Berlin.

[12] R. Reiter 1982: Ein algebraisch-konstruktiver Abbildungskalkül zur Fundierung der elementaren Arithmetik. Dissertation, rejected by Math. dpt. of TU Berlin.

[13] L. Romàn 1989: Cartesian categories with natural numbers object. *J. Pure and Appl. Alg.* **58,** 267-278.

[14] Th. Skolem 1919: Begründung der elementären Arithmetik durch die rekurrierende Denkweise ohne die Anwendung scheinbarer Veränderlichen mit unendlichem Ausdehnungsbereich, Skolem 1970, pp. 153-188.

[15] Th. Skolem 1970: *Selected Works in Logic.* Universitetsforlaget Oslo - Bergen - Tromsö.

[16] C. Smorynski 1977: The Incompleteness Theorems. Part D.1 in Barwise ed. 1977. *Handbook of Mathematical Logic*. North Holland.